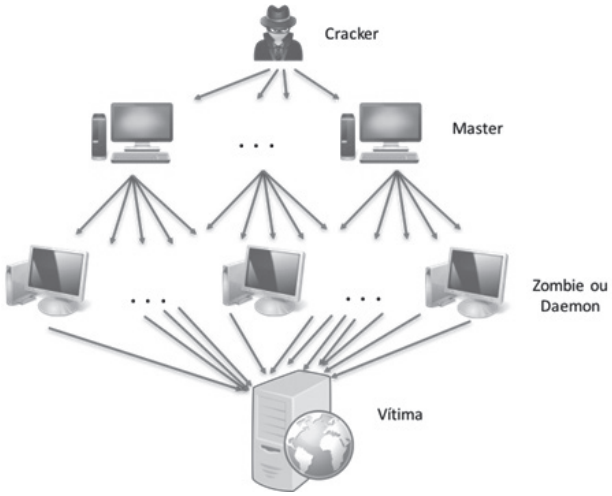
DDoS – Ataques distribuídos e coordenados

O *cracker* define alguns sistemas *master*, que se comunicam com os *daemons* ou *zombies* que realizam os ataques à vítima.

Figura 2.4 | Ataque DDoS



Fonte: elaborada pelo autor.

Os ataques DDoS são importantes em segurança da informação e de redes porque mostram grande avanço e "profissionalização" desses ataques, pois há o agrupamento e o uso de diferentes técnicas para a contaminação dos *masters* e dos *zombies*, que inclusive são controlados por canais seguros (NAKAMURA; GEUS, 2007). Há uso de *scanning* de portas e de vulnerabilidades para a busca de *hosts* vulneráveis que são explorados para fazer parte da rede de ataque, também conhecida como *botnets*.

Exemplificando

As primeiras ferramentas de DDoS surgiram em 1999, o *Tribe Flood Network* (TFN) e o *trin00* e implementavam *IP Spoofing*, *SYN Flooding*, *Smurf* e *ICMP Flooding*. A evolução do DDoS incluiu o uso de vírus e *worms* para a disseminação dos ataques e montagem das *botnets*, além da inclusão de *backdoors* para a propagação de novos tipos de ataques (NAKAMURA; GEUS, 2007).

Malware

O conceito de *malware* é interessante por englobar os famosos vírus, *worms,* cavalos de Troia, *ransomware*, *spyware*, *backdoor*, entre outros. O termo *malware*

vem do inglês malicious software, ou software malicioso, que causa, intencionalmente, danos à vítima.

Reflita

Em segurança da informação, devemos nos preocupar com *malwares*. Porém, não podemos deixar de lado os códigos que não são propositadamente maliciosos, mas podem comprometer a confidencialidade, a integridade e a disponibilidade da informação, fruto de bugs na implementação ou de erros na configuração, por exemplo, que abrem brechas para serem explorados em ataques.

Os *malwares* mais conhecidos são os vírus e os *worms* (ou vermes). Apesar de serem similares, há diferenças conceituais importantes entre eles. Os vírus precisam ser executados pelo usuário para contaminarem a vítima. Já os *worms* se autopropagam com a exploração de vulnerabilidades existentes no ambiente, de modo que não necessitam de ações de usuários.

Os cavalos de Troia ou *trojans* seguem a ideia da Guerra de Troia, quando os gregos conseguiram entrar em Troia dentro de um cavalo, que teria sido um "presente de grego", o que levou a cidade fortificada à ruína. Os cavalos de Troia, em segurança da informação, executam tarefas legítimas ao mesmo tempo em que atividades ilícitas são realizadas no equipamento da vítima, por exemplo, roubo de informações armazenadas ou envio de tudo o que o usuário digita.

O *ransomware* tem feito muitas vítimas ultimamente, consiste no sequestro de informações que são recuperadas apenas mediante pagamento de um resgate. Métodos criptográficos são utilizados nesse ataque, no qual o *cracker* envia a chave para a recuperação das informações após o pagamento do valor estipulado.

Já o *backdoor* é uma condição que possibilita o acesso remoto ou a execução de comandos com a existência de uma "porta não autorizada" em softwares e hardwares.

Pesquise mais

Conheça mais detalhes sobre códigos maliciosos como vírus, *worms, bot*/*botnets*, *spyware*, *backdoor*, cavalos de Troia e *rootkit* na *Cartilha de Segurança para Internet*, do Cert.br. Há um resumo comparativo e métodos de prevenção, vale a pena acessar.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet**. 2012. Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 8 maio 2016.

Phishing

Esse é um ataque que busca capturar informações pessoais enquanto o fraudador se faz passar por uma pessoa ou empresa confiável, com o uso de uma comunicação eletrônica oficial.

Pesquise mais

Veja as principais características do *phishing na Cartilha de Segurança para Internet do CERT*:

CERT.BR. **Cartilha de segurança para internet**. 2012. Disponível em: <http://cartilha.cert.br/golpes/>. Acesso em: 24 maio 2016.

Sem medo de errar

Vamos retornar agora ao mapa de ameaças à Food-XYZ. As vulnerabilidades existem em ativos e podem ser exploradas por agentes de ameaça. Já as ameaças existem independentemente dos ativos. Assim, é importante lembrar que uma ameaça se torna um incidente de segurança quando um agente de ameaça explora uma vulnerabilidade de um ativo. O contexto é a maior comunicação entre diferentes localidades, o possível uso de serviços na nuvem e a possibilidade de implantação de novos serviços.

As ameaças existem e representam os potenciais de ataques. Uma forma de conseguir visualizar essas ameaças é observando os ativos. Assim, primeiramente é preciso identificar os elementos a serem protegidos.

- Pessoas:
  - usuários;
  - administradores de sistemas;
  - suporte técnico.
- Ativos físicos:
  - servidores (hardware);
  - data center;
  - equipamentos de comunicação (roteadores, *switches*, pontos de rede, cabeamento).

- Ativos tecnológicos:

  - serviços (software): servidor de arquivos, e-mail, RH, financeiro, ferramentas colaborativas;

  - protocolos (software): TCP/IP, SNMP, SIP, H.323, SMTP, HTTPS, NTFS;

  - aplicações (software): comunicação colaborativa (como o *Skype*), servidor de arquivos pelo Windows e acessos aos demais serviços via web;

  - aplicativos móveis (software): todos os serviços acessados via dispositivos móveis.

- Informação:

  - comunicação (rede) entre matriz e filial;

  - informações de ferramentas colaborativas;

  - informações de sistemas de RH e financeiro (como o SAP);

  - credenciais de acesso;

  - arquivos armazenados no servidor (como o Windows).

O segundo passo é definir algumas categorias de ameaças. Para isso, é possível utilizar alguns catálogos de ameaças, como o STRIDE, da Microsoft. Uma categorização bastante comum é a baseada em comprometimento das propriedades básicas de segurança da informação. Nesse caso, as seguintes categorias de ameaças podem ser utilizadas:

- Perda de confidencialidade.
- Perda de integridade.
- Perda de disponibilidade.

O terceiro passo pode complementar as informações, indicando como cada ameaça pode se tornar um incidente de segurança:

- Perda de confidencialidade: *keylogger*, que captura tudo o que o usuário digita.
- Perda de integridade: *malware* que realiza manipulação *on-the-fly*, com a alteração dos dados digitados antes do envio ao servidor.
- Perda de disponibilidade: DoS na rede.

O quarto passo deve ser feito por você, complementando a lista de ataques ou técnicas que levam a ameaça a se tornar um incidente de segurança.

No quinto passo, você deve ligar todos os elementos para ter uma visão de segurança cada vez mais apurada. Vincule os ativos às ameaças. Estas já estão relacionadas aos ataques e às técnicas que levam ao incidente.

Atenção

As ameaças à rede podem virar incidentes de segurança quando um agente de ameaça explora uma vulnerabilidade de um ativo, comprometendo uma das propriedades básicas de segurança da informação: confidencialidade, integridade e disponibilidade.

Avançando na prática

Ameaça à Rede em Data Centers

Descrição da situação-problema

Os data centers (centros de dados que hospedam os servidores físicos e rodam os serviços) podem ser vistos sob dois pontos de vista: um data center operado pela própria empresa, localmente, e um data center operado por um prestador de serviços, também conhecido como nuvem computacional. Você é o responsável pela segurança de redes de uma empresa, um provedor de serviços de data center, ou seja, um provedor de nuvem. Nesse cenário, os clientes de sua empresa utilizam os recursos do data center com muitos acessos e possuem muitos dados armazenados. Apresente uma visão de segurança com foco em ameaças à rede de sua empresa, o provedor de serviços de data center.

Lembre-se

As ameaças possuem categorias diferentes, tais como as baseadas em comprometimento das propriedades básicas de segurança da informação: confidencialidade, integridade e disponibilidade. Uma ameaça se torna um incidente de segurança quando um agente de ameaça explora as vulnerabilidades de um ativo.

Resolução da situação-problema

Considerando que um agente de ameaça pode explorar vulnerabilidades de um ativo para realizar ataques e causar um incidente de segurança, é preciso identificar quais são os ativos a serem protegidos. A partir dos ativos, devemos pensar nos agentes de ameaça, nos ataques que podem acontecer e também nas ameaças.

Os principais ativos de um data center são a rede e os hardwares, bem como os administradores de sistemas e técnicos que trabalham para manter a empresa funcionando. Uma outra visão possível dos ativos diz respeito aos serviços oferecidos aos clientes. Por exemplo, a disponibilização de um sistema de relacionamento com clientes baseado em dados de vendas. Esse serviço pode ser utilizado pelos clientes do data center, e você, como responsável pela segurança de redes, deve se preocupar em proteger o serviço, os acessos e os dados de seus clientes.

Assim, considere as seguintes ameaças à rede, em uma lista não exaustiva:

- Perda de confidencialidade das credenciais de acesso dos clientes ao sistema, que leva à necessidade de uso de canal seguro na autenticação.
- Perda de confidencialidade ou integridade dos dados do banco de dados, que leva à necessidade de segurança na aplicação e no banco de dados.
- Perda de disponibilidade do sistema, da rede ou do banco de dados, que leva à necessidade de uso de técnicas como alta disponibilidade e o uso de mecanismos de segurança contra ataques de negação de serviço.

Faça você mesmo

Você viu, nesta seção, uma série de ameaças e ataques que podem comprometer qualquer empresa. Reforce o conhecimento listando as ameaças e os ataques, exemplificando cada uma delas.

Faça valer a pena

1. O DoS, ou *Denial of Service*, afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

2. O DDoS, ou *Distributed Denial of Service*, afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

3. Um *cracker* é uma ameaça que afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

Seção 2.3

Ferramentas de segurança I

Diálogo aberto

Olá!

Após avançarmos na visão sobre as vulnerabilidades e as ameaças de redes na Food-XYZ, chegou a hora de preparar a proteção da empresa. Você está liderando a integração tecnológica da Food-XYZ, uma empresa do ramo alimentício que está se expandindo internacionalmente. Essa expansão passa pela criação de equipes locais de P&D e de marketing, além das tradicionais áreas de vendas e produção.

Na empresa Food-XYZ, você realizou a integração tecnológica entre a matriz brasileira e a filial canadense. Em seguida, fez a integração entre o Brasil e a filial da China, além de finalizar a análise sobre o uso de serviços na nuvem e a implantação de novos serviços. Com essa rede, as equipes de cada localidade poderão interagir de forma contínua e com alto grau de produtividade, por meio do uso de ferramentas modernas de comunicação e trabalho colaborativo. O data center da empresa é local e está no Brasil. Nele estão servidores em *cluster* para os serviços de comunicação colaborativa, e-mail, RH, financeiro, projetos colaborativos e servidor de arquivos. O acesso a esses serviços também pode ser feito com o uso de dispositivos móveis, por meio de aplicativos específicos. Cada localidade (Brasil, Canadá e China) possui acesso à internet, que é utilizado para o estabelecimento de Rede Privada Virtual (VPN, *Virtual Private Network*), usada para as comunicações entre elas.

Você já possui uma visão sobre as vulnerabilidades e as ameaças de redes, e agora é o momento de detalhar a proteção da Food-XYZ. Os mecanismos de defesa, contramedidas ou controles de segurança realizam a proteção de uma empresa. Já conhecemos vários mecanismos de defesa, que podem ser tecnológicos, físicos, processuais ou regulatórios. Para a Food-XYZ, você irá focar a proteção à rede, considerando ataques tradicionais conhecidos, como o *Denial of Service* (DoS), o *Distributed Denial of Service* (DDoS), as invasões a servidores da empresa e os *malwares*, que podem comprometer a confidencialidade, a integridade e a disponibilidade da informação.

Os mecanismos de proteção possuem as finalidades de prevenção, detecção e resposta. Considere essas finalidades para definir as proteções à rede. Explique como cada controle de segurança atua na proteção da Food-XYZ.

Bom estudo e bom trabalho!

Não pode faltar

Proteção à rede

A proteção de uma empresa é feita com o uso de mecanismos de segurança tecnológicos, físicos, processuais e regulatórios. É com a sua implementação que as finalidades de prevenção, detecção e resposta a incidentes são cumpridas. A rede de uma empresa é um dos escopos que devem ser protegidos, representando informações em meio digital que existem principalmente em transmissão. O desafio de proteção à rede é ainda maior porque é pela rede que informações digitais armazenadas em servidores podem ser acessadas. Assim, uma organização básica para a proteção à rede envolve:

- Proteção de informações que trafegam pela rede: necessidade de garantir confidencialidade, integridade e disponibilidade das informações, que envolvem dois principais controles: criptografia para confidencialidade e integridade; e tecnologias que garantam a disponibilidade da rede, como configurações ou tecnologias específicas que limitem o número de determinados tipos de conexões e evitem ataques de negação de serviço (DoS) contra equipamentos de rede.

- Proteção contra acesso a informações armazenadas em servidores: necessidade de garantir a confidencialidade, a integridade e a disponibilidade das informações em servidores, limitando o acesso a essas informações por meio de alguns controles principais: autenticação (nos níveis de rede e de usuário), controle de acesso de rede, como o *firewall*, sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS).

- Proteção contra o acesso de usuários contaminados com *malware* ou contra a contaminação dos servidores com *malwares*: usuários legítimos que tenham suas credenciais roubadas podem dar o acesso indevido a uma rede, ou os usuários podem acessar informações de uma forma legítima, mas, caso estejam contaminados com *malwares*, acabam comprometendo a confidencialidade, integridade ou disponibilidade da informação. *Malwares* podem também afetar diretamente as propriedades básicas de segurança das informações nos servidores. Alguns dos principais controles de segurança: antivírus, antimalware, DLP, IDS, IPS.

Tecnologias de autenticação, isto é, para validar a identidade dos usuários, serão discutidas na próxima seção, enquanto as demais serão discutidas a partir de agora. Já a criptografia será tema de uma unidade de ensino.

Firewall

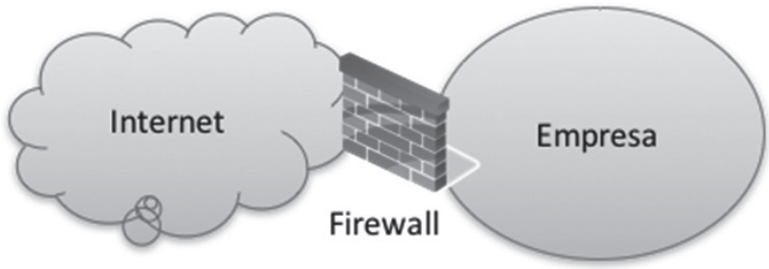
O *firewall* é um dos mais conhecidos controles de segurança da informação, surgindo juntamente com a própria internet. Os primeiros *firewalls* foram implementados em roteadores, no final da década de 1980, por serem os pontos de ligação natural entre duas redes. As regras de filtragem dos roteadores, conhecidas também como "listas de controle de acesso" (*Access Control List*, ACL), tinham como base decisões do tipo "permitir" ou "descartar" os pacotes, que eram tomadas de acordo com a origem, o destino e o tipo das conexões (NAKAMURA; GEUS, 2007).

Segundo Nakamura e Geus (2007), o *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, pelo qual deve passar todo o tráfego, permitindo que o controle, a autenticação e os registros de tráfego sejam realizados. Assim, esse ponto único constitui um mecanismo utilizado geralmente para proteger uma rede confiável de uma rede pública não confiável. O *firewall* pode ser utilizado também para separar diferentes sub-redes, grupos de trabalho ou LANs dentro de uma organização. A proteção de perímetro é então realizada pelos *firewalls*, que fazem o controle das conexões para os diferentes segmentos de rede. Os conceitos de segmentação de rede e de proteção de perímetros estão relacionados diretamente com os *firewalls* (Figura 2.5).

Assimile

Você pode considerar que o *firewall* é um ponto de controle entre duas redes, com uma delas sendo não confiável (internet) e uma confiável (da empresa). Passam desse ponto de controle somente conexões legítimas para serviços legítimos. Pense, portanto, nos serviços legítimos que uma empresa deve disponibilizar, como um serviço web, por exemplo. Pense também em quem pode fazer o acesso. Nesse caso, é normal que toda a internet possa acessar esse serviço. Desse modo, se todos podem acessar o serviço web, o controle que deve ser feito pelo *firewall* é: qualquer um da internet pode acessar a porta do serviço web.

Figura 2.5 | *Firewall* separando duas redes – internet e empresa



Fonte: elaborada pelo autor.

Basicamente, o *firewall* controla as conexões de quem pode acessar qual serviço da rede que está sendo protegida. As regras do *firewall* que definem esse controle utilizam tradicionalmente dois pares de informações: endereço IP e porta TCP/UDP de origem do acesso, e endereço IP e porta TCP/UDP de destino. Este tipo de *firewall* é o filtro de pacotes.

No exemplo a seguir (Quadro 2.1), de Nakamura e Geus (2007), o *firewall* (filtro de pacotes) possui regras que permitem aos usuários internos acessar páginas web que funcionem na porta TCP 80.

Quadro 2.1 | Regras de um filtro de pacotes que permitem aos usuários internos acessarem a web

Regra	End. de Origem: Porta de Origem	End. de Destino: Porta de Destino	Ação
1	IP da rede interna: porta alta	Qualquer endereço: 80 (HTTP)	Permitir
2	Qualquer endereço: 80 (HTTP)	IP da rede interna: porta alta	Permitir
3	Qualquer endereço: qualquer porta	Qualquer endereço: qualquer porta	Negar

Fonte: Nakamura e Geus (2007, p. 216).

É importante notar que há duas informações relevantes no Quadro 2.1, composto por três regras: a primeira informação é que a regra 1 é a requisição, enquanto a regra 2 é a resposta, o que demonstra que o sentido das conexões é importante para a definição das regras, devendo considerar também a resposta, e não somente a requisição; e a segunda informação é que a regra 3 mostra um conceito importante a ser utilizado na configuração de *firewalls* – uma regra de negação de todas as demais conexões.

Reflita

O uso de um conjunto de regras para uma única necessidade resulta em complexidade na configuração de *firewalls*. No exemplo da necessidade de usuários internos acessarem sítios web, devem ser criadas três regras

no filtro de pacotes. A última regra, de negar todas as demais conexões, mostra um conceito importante: todas as conexões são proibidas por padrão, exceto aquelas que são explicitamente permitidas – no exemplo, somente usuários internos podem acessar serviços web. A empresa, nesse caso, não disponibiliza nenhum serviço.

Outro ponto importante sobre *firewalls* é que eles trabalham de uma forma sequencial com suas regras, ou seja, o *firewall* vai analisando todas as regras existentes consecutivamente, até que uma delas seja verdadeira e a conexão possa seguir em frente ou ser negada. No caso da regra ser do tipo "permitir", a conexão segue adiante. Se for do tipo "negar", a conexão é encerrada. Isso faz com que uma regra que leve em consideração as *flags* do estabelecimento de conexões TCP/IP (SYN, ACK, SYN-ACK) se torne mais completa, como é o caso destas apresentadas no Quadro 2.2, também de Nakamura e Geus (2007).

Quadro 2.2 | Regras de um filtro de pacotes usando *flags* TCP/IP

Regra	End. de Origem: Porta de Origem: Flag	End. de Destino: Porta de Destino	Ação
1	IP da rede interna: porta alta: SYN	Qualquer endereço: 80 (HTTP)	Permitir
2	Qualquer endereço: 80 (HTTP)	IP da rede interna: porta alta	Permitir
3	Qualquer endereço: Qualquer porta	Qualquer endereço: Qualquer porta	Negar

Fonte: Nakamura e Geus (2007, p. 217).

No exemplo do Quadro 2.2, a ação de "permitir" só é executada caso a conexão esteja sendo iniciada (*flag* SYN), o que restringe alguns ataques vindos da internet que fazem o *IP Spoofing* de um endereço da rede interna.

Uma evolução dos *firewalls* de filtro de pacotes são aqueles do tipo filtro de pacotes dinâmicos, também conhecidos como baseados em estados (*stateful packet filter*). Esse tipo de *firewall* utiliza uma tabela de estados das conexões, tornando as regras mais simples, pois não é mais necessário considerar as *flags* das conexões, e nem diferenciar requisições de respostas. A tabela de estados das conexões é sempre acrescida de uma conexão válida por uma regra do *firewall*. Essa tabela é consultada em cada resposta, o que faz com que todos os pacotes daquela sessão sejam aceitos.

Com esse tipo de firewall, o conjunto de regras pode considerar apenas os inícios das conexões que usam o flag SYN. Dessa forma, o conjunto de regras fica mais enxuto e, consequentemente, mais fácil de administrar, minimizando as possibilidades de erros na sua criação. No exemplo do Quadro 2.3, a Regra 1 é usada para verificar se uma conexão pode ser iniciada, e a resposta à requisição é permitida com a verificação

dos pacotes de acordo com a tabela de estados do *firewall*. Caso um *cracker* tente acessar a porta alta aberta por uma *backdoor*, por exemplo, ele não terá sucesso, pois a regra que permite essa conexão não existe (NAKAMURA; GEUS, 2007).

Quadro 2.3 | Regras de um filtro de pacotes baseados em estados

Regra	End. de Origem: Porta de Origem	End. de Destino: Porta de Destino	Ação
1	IP da rede interna: porta alta	Qualquer endereço: 80 (HTTP)	Permitir
2	Qualquer endereço: qualquer porta	Qualquer endereço: qualquer porta	Negar

Fonte: Nakamura e Geus (2007, p. 218).

Pesquise mais

Conheça detalhes das tecnologias de *firewalls*, sua forma de funcionamento e suas arquiteturas de rede no capítulo 7 do livro *Segurança de Redes em Ambientes Cooperativos*, de Nakamura e Geus (2007).

NAKAMURA, Emilio T.; GEUS, Paulo L. de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

Os *firewalls* podem atuar ainda no nível de aplicação, o que permite que dados de protocolos como o HTTP, utilizado na web, possam ser analisados. A partir dessa análise, é possível realizar algumas tarefas, como a filtragem de conteúdo, por exemplo. Outra funcionalidade de um firewall que atua no nível de aplicação é o *proxy*. Iremos discutir essas funcionalidades na próxima seção.

IDS

Os Sistemas de Detecção de Intrusão (*Intrusion Detection Systems*, IDS) possuem um papel importante para a segurança da informação e de redes porque permitem a detecção de ataques em andamento, principalmente contra serviços legítimos, que passam pelas regras do *firewall*. Essa importância está relacionada ao monitoramento e à detecção, já que o IDS não pode prevenir um ataque em andamento.

Algumas das principais funcionalidades do IDS são (NAKAMURA; GEUS, 2007):

- Monitoramento e análise das atividades dos usuários e dos sistemas.
- Avaliação da integridade de arquivos importantes do sistema e de dados.
- Análise estatística do padrão de atividade.

- Análise baseada em assinaturas de ataques conhecidos.
- Análise de atividades anormais.
- Análise de protocolos.
- Detecção de erros de configuração do sistema.
- Identificação do destino do ataque.
- Registro para investigações.

Um dos principais tipos de IDS é o baseado em *host* (*Host-Based* IDS, HIDS), que realiza a detecção de:

- Acessos a arquivos.
- Alteração de arquivos.
- Modificação de privilégio de usuários.
- Acesso a processos do sistema.
- Execução de programas.
- Uso de CPU.
- Conexões.

Pesquise mais

Uma ferramenta que monitora a integridade de arquivos do sistema é o *Open Source Tripwire*. Ela realiza o monitoramento e pode enviar alertas caso os arquivos protegidos sejam modificados.

Open Source Tripwire. Disponível em: <https://sourceforge.net/projects/tripwire/>. Acesso em: 21 maio 2016.

Outro tipo de IDS é o tradicional baseado em rede (*Network IDS*, NIDS), que atua analisando cabeçalhos e conteúdos dos pacotes em trânsito, com comparações baseadas em assinaturas. Os pontos fracos do NIDS estão relacionados com a dificuldade de detecção de ataques que usam técnicas para driblar os mecanismos implementados e também com a dificuldade de ação em caso de detecção de atividades suspeitas, pois há muitos alarmes falsos.

IPS

Sistemas de Prevenção de Intrusão (*Intrusion Prevention System*, IPS) possuem grande similaridade com o IDS, porém funcionam de uma forma mais ativa após a detecção de atividades suspeitas, tomando ações diretas, como o término daquela conexão. A diferença fundamental é que o IPS atua de uma forma *in-line*, ou seja, todo o tráfego passa pelo IPS, diferentemente do IDS, que opera passivamente. Com esse posicionamento na rede, o IPS atua de modo similar ao *firewall* no que tange à análise de todos os pacotes que entram na rede protegida.

Pesquise mais

Dentre as ações que um IPS pode tomar, estão: enviar um alarme ao administrador (como poderia ser em um IDS); derrubar pacotes maliciosos; bloquear o tráfego a partir do endereço de origem; redefinir a conexão. Verifique mais características de um IPS em:

Palo Alto Networks. **O que é um sistema de prevenção de intrusão?** Disponível em: <https://www.paloaltonetworks.com.br/resources/learning-center/what-is-an-intrusion-prevention-system-ips.html>. Acesso em: 21 maio 2016.

Antivírus e antimalware

Como visto na seção anterior, os *malwares* incluem códigos maliciosos, como vírus, *worms*, cavalos de Troia, *spyware*, *bots*, *keyloggers* e *rootkits*. As primeiras ferramentas de segurança eram voltadas para os vírus, códigos maliciosos que dominavam o cenário de segurança no início. Essas ferramentas, os antivírus, fizeram fama desde essa época e continuam evoluindo. Atualmente, muitos antivírus atuam também sobre outros tipos de *malwares*, apesar de conservarem o nome de "antivírus".

Assim, os antimalwares podem indicar que se tratam de controles que vão além dos do antivírus, porém eles são similares. As ferramentas que se declaram antimalwares geralmente são mais novas, já nasceram quando o termo *malware* estava mais disseminado, o que era diferente na época dos "vírus".

Há ainda ferramentas antimalwares mais avançadas, normalmente direcionadas a *malwares* específicos, como é o caso dos que atacam transações financeiras. Geralmente disponibilizadas pelas próprias instituições financeiras, essas ferramentas buscam dificultar o funcionamento dos *malwares* que trazem prejuízos aos bancos.

Exemplificando

Um tipo de *malware* protegido pelos antimalwares é o *ransomware*, que realiza um sequestro de informações da vítima, com o envio da chave criptográfica de liberação das informações somente após o pagamento de um resgate. Um dos *ransonwares* é o Locky, que é discutido em:

Trend Micro. **Novo crypto-ransomware Locky usa macros maliciosas do Word**. Disponível em: <http://blog.trendmicro.com.br/novo-crypto-ransomware-locky-usa-macros-maliciosas-do-word/#.Vz9AQXarRD8>. Acesso em: 20 maio 2016.

Sem medo de errar

Vamos retornar agora à Food-XYZ. Você deve definir controles de segurança, mecanismos de defesa ou contramedidas para a série de vulnerabilidades e ameaças encontradas.

O foco é a proteção à rede, considerando ataques tradicionais que você já conhece, como o *Denial of Service* (DoS), o *Distributed Denial of Service* (DDoS) e as invasões a servidores da empresa. Já os *malwares* também devem ser considerados, pois atuam em ataques relacionados à:

- Perda de confidencialidade: *keylogger*, que captura tudo o que o usuário digita. Ex.: *Revealer Keylogger*.
- Perda de integridade: *malware* que realiza manipulação *on-the-fly*, com a alteração dos dados digitados antes do envio ao servidor. Ex.: *Eupuds*.
- Perda de disponibilidade: DoS na rede. Ex.: *Smurf*.

Os mecanismos de proteção possuem as finalidades de prevenção, detecção e resposta. As seguintes ferramentas podem ser consideradas:

- *Firewall*: prevenção contra ataques, filtrando as conexões de rede de modo a permitir somente os acessos a serviços legítimos.
- IDS: detecção de ataques, analisando assinaturas ou comportamentos de ataques e enviando alertas.
- IPS: prevenção de ataques, atuando diretamente nas conexões e tomando ações em caso de detecção de ataques em andamento.
- Antivírus e antimalware: prevenção de ataques, fazendo com que *malwares* não funcionem ou não contaminem os ativos protegidos pela ferramenta.

Atenção

As ferramentas de segurança visam à prevenção, detecção e resposta a ataques, protegendo os ativos contra ataques que comprometam uma das propriedades básicas de segurança da informação: confidencialidade, integridade e disponibilidade.

Segmentação de Rede

Descrição da situação-problema

Uma boa segurança começa com uma segmentação de rede adequada, que limita os acessos e, portanto, as superfícies de ataques. Considere uma empresa que possui uma intranet para controle de RH, uma extranet para conexão direta com fornecedores e parceiros comerciais, além de um website para pedidos on-line de clientes. Como seria a segmentação de redes dessa empresa e quais ferramentas de segurança você utilizaria nesse caso?

Lembre-se

Ferramentas de segurança possuem objetivos específicos, não são capazes de resolver todos os problemas de segurança existentes, sendo necessário, portanto, utilizá-las em conjunto.

Resolução da situação-problema

A segmentação de rede pode considerar, em princípio, três redes:

- Intranet.
- Extranet.
- Internet.

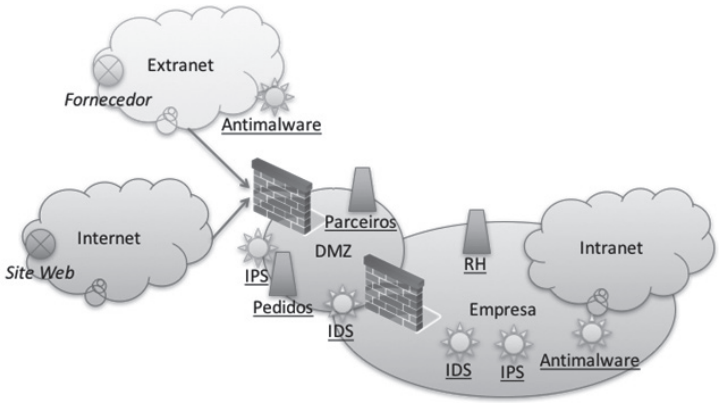
Cada rede possui acesso a serviços específicos:

- Intranet acessa sistema de RH.
- Extranet acessa sistema de fornecedores.
- Internet acessa sistema de pedidos on-line.

A Figura 2.6 mostra a segmentação de redes com o uso de uma zona desmilitarizada (*Demilitarized Zone*, DMZ) e as ferramentas de segurança utilizadas. Com a DMZ, caso um serviço como o de parceiros seja atacado, a rede interna continua intacta. O

posicionamento dos servidores é importante, como é o caso do servidor de RH, que está na rede interna, sem que seja possível alcançá-lo da extranet ou da internet. Há a possibilidade de criação de uma segunda DMZ que separa os servidores de pedidos e o de parceiros, o que assegura maior nível de proteção.

Figura 2.6 | Segmentação de redes e ferramentas de segurança



Fonte: elaborada pelo autor.

Faça você mesmo

Utilize o exemplo da segmentação de rede e crie as regras de *firewalls*, que são dois no caso discutido.

Faça valer a pena

1. As ferramentas de segurança possuem um papel importante. Qual é esse papel?

a) Nenhum.

b) CID.

c) Prevenção, detecção e resposta.

d) *Firewall*.

e) Riscos.

2. Qual das seguintes alternativas corresponde a ferramentas de segurança?

a) Firewall e IDS.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) Ameaças.

3. Qual das ferramentas de segurança possui como função a detecção?

a) Nenhuma.

b) *Firewall*.

c) IDS.

d) Criptografia.

e) IPS.

Seção 2.4

Ferramentas de segurança II

Diálogo aberto

Olá!

Você tem visto nos noticiários que vários sites estão sofrendo ataques que expõem as senhas de acesso de seus usuários? Esse é um problema cada vez mais comum, por isso iremos estudar nesta aula os principais mecanismos de autenticação. Agora é um bom momento para tratarmos dessa e de outras questões de segurança.

Você está liderando a integração tecnológica da Food-XYZ, uma empresa do ramo alimentício que está se expandindo internacionalmente. Essa expansão passa pela criação de equipes locais de P&D e de marketing, além das tradicionais áreas de vendas e produção. Você já realizou a integração tecnológica entre a matriz brasileira e a filial canadense em um primeiro momento. Logo após, você fez a integração entre a matriz e a filial chinesa, além de finalizar a análise sobre o uso de serviços na nuvem e a implantação de novos serviços.

Com essa rede, as equipes de cada localidade poderão interagir de uma forma contínua e com alto grau de produtividade, por meio do uso de ferramentas modernas de comunicação e trabalho colaborativo. O data center da empresa é local e está no Brasil. Nele estão servidores em *cluster* para os serviços de comunicação colaborativa, e-mail, RH, financeiro, projetos colaborativos e servidor de arquivos. O acesso a esses serviços também pode ser feito com o uso de dispositivos móveis por meio de aplicativos específicos. Cada localidade (Brasil, Canadá e China) possui acesso à internet, que é utilizado para o estabelecimento de Rede Privada Virtual (VPN, *Virtual Private Network*), usada para as comunicações entre elas.

Você já possui uma visão sobre as vulnerabilidades e as ameaças de redes, e começou a detalhar a proteção da Food-XYZ definindo mecanismos de defesa, contramedidas ou controles de segurança, que podem ser tecnológicos, físicos, processuais ou regulatórios. Também trabalhou com tecnologias de segurança como *firewall*, IDS, IPS, antivírus e antimalware. Seu objetivo é consolidar a defesa da Food-

XYZ, adotando outras tecnologias complementares. Para isso, foque a autenticação de usuários e a proteção de conteúdos da empresa. No caso da autenticação, um roubo de credenciais de um funcionário da Food-XYZ pode dar acesso indevido aos *crackers*, que passam a acessar serviços e informações como se fossem usuários legítimos. Já a proteção do conteúdo pode ser vista sob dois prismas: o conteúdo acessado pelos funcionários, que pode resultar em perda de produtividade e contaminações por *malware*; ou as informações críticas da empresa serem enviadas indevidamente para terceiros, seja por *malwares* ou por funcionários mal-intencionados.

Lembre-se de que os mecanismos de proteção possuem finalidades de prevenção, detecção e resposta. Considere essas finalidades para definir as proteções à rede. Explique como cada controle de segurança atua na proteção da Food-XYZ.

Bom estudo e bom trabalho!

Não pode faltar

Efetividade dos controles de segurança

Nós já vimos que um controle de segurança não é capaz de resolver todos os problemas de segurança isoladamente. Um *firewall* deixa portas abertas para serviços legítimos. Um IDS pode detectar ataques em andamento nessas portas abertas pelo *firewall*, porém uma ação ainda é esperada. O IPS dá uma resposta, agindo preventivamente contra os ataques em andamento, porém técnicas de evasão podem ser utilizadas. Já os antimalwares atuam no *endpoint*, ou no equipamento do usuário, mas mesmo assim ataques que partem de usuários contaminados causam grandes prejuízos às empresas.

Exemplificando

Um dos *malwares* que mais tem causado prejuízos aos bancos é o *malware* de boleto. Nessa fraude, os números do boleto são adulterados de diferentes formas, fazendo com que os recursos financeiros caiam em contas de fraudadores (ou de seus laranjas) (ALECRIM, 2014).

ALECRIM, Emerson. **RSA**: *malware* que altera boletos bancários pode ter causado prejuízo de R$ 8,5 bilhões. 2014. Disponível em: <https://tecnoblog.net/159220/rsa-fraudes-boletos-bolware/>. Acesso em: 20 maio 2016.

Além dos ataques que partem de usuários contaminados com *malware*, há problemas ainda mais complexos de serem resolvidos, como aqueles em que *crackers* roubam credenciais de usuários, passando a ter acesso a sistemas e informações críticas de uma forma direta, como se fossem os usuários legítimos. Nesse caso, os ataques não visam à exploração de vulnerabilidades de sistemas, mas sim o roubo de identidades desses usuários, normalmente com a descoberta da senha, que é o método de autenticação mais comum.

Outras ameaças devem ser ainda consideradas, como o vazamento de informações confidenciais através de métodos de comunicação seguros, por exemplo, o envio de documentos de projetos para concorrentes a partir de um funcionário, por e-mail. Nesse caso, a comunicação acontece de dentro da empresa para fora, de modo legítimo e, portanto, mecanismos de segurança como *firewall*, IDS, IPS ou antimalware não são efetivos, já que eles visam proteger a empresa contra ataques vindos do exterior.

Reflita

O mercado financeiro possui uma característica interessante: mesmo investindo uma grande quantidade de recursos, os prejuízos ainda são bastante altos. Por que você acha que as fraudes acontecem, mesmo com os bancos adotando uma série de controles de segurança, como a instalação de softwares nos equipamentos dos clientes?

Problemas com senhas

Um dos ataques que tem acontecido cada vez mais em todo o mundo é o que rouba credenciais dos usuários, permitindo que o *cracker* acesse os serviços como se fosse o usuário legítimo.

Exemplificando

O roubo de 1,2 bilhões de senhas de 420 mil websites mostra a dimensão do problema com as senhas (BRITO, 2014).

BRITO, Edvaldo. 'Maior roubo de dados da história' captura 1,2 bilhão senhas, diz jornal. **TechTudo**, 2014. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/08/maior-roubo-de-dados-da-historia-captura-12-bilhao-senhas-diz-jornal.html>. Acesso em: 5 jun. 2016.

Você já teve uma senha roubada? Repete a mesma senha em websites diferentes? Consegue memorizar senhas únicas para cada serviço que acessa?

Senhas podem ser roubadas, descobertas ou quebradas. O roubo de senhas pode acontecer de variadas formas, por exemplo, com o envio de *phishing*, em um ataque no qual o usuário é enganado e passa, voluntariamente, seus dados de acesso a um serviço. Uma das técnicas de *phishing* é o envio de e-mail direcionando a um sítio falso, muito parecido com o verdadeiro, em que o usuário entra com suas credenciais de acesso, que são roubadas.

O envio do usuário a uma página falsa também pode ser feito com o ataque de *DNS Poisoning* ou envenenamento do DNS, em que o endereço correto é digitado em seu navegador, porém o acesso se realiza em um servidor falso.

Pesquise mais

Saiba mais sobre ataques de *phishing* em:

ALECRIM, Emerson. **O que é phishing scam e como evitá-lo?** 2013. Disponível em: <http://www.infowester.com/phishing_scam.php>. Acesso em: 23 maio 2016.

Saiba mais sobre o ataque ao DNS em:

KASPERSKY Lab. **O que é envenenamento de cache de servidor de nomes de domínio (DNS)?** [s.d.]. Disponível em: <http://brazil.kaspersky.com/internet-security-center/definitions/dns>. Acesso em: 23 maio 2016.

Outra forma de roubo de senhas é através da exploração de vulnerabilidades nos serviços (web ou banco de dados), que levam o *cracker* a roubar toda a base de senhas. Vários ataques desse tipo são vistos ultimamente.

Pesquise mais

Um dos ataques que resultou em roubo de senhas foi contra o *Minecraft*.

ROCHA, Leonardo. **Hackers vazam 7 milhões de senhas da comunidade *Lifeboat* de *Minecraft***. 2016. Disponível em: <http://www.tecmundo.com.br/seguranca-de-dados/104182-hackers-vazam-7-milhoes-senhas-comunidade-lifeboat-minecraft.htm>. Acesso em: 23 maio 2016.

Fatores de autenticação

A autenticação corresponde à validação de uma identidade. A pergunta que devemos fazer é: "como eu sei que o usuário é quem ele diz ser?". A autenticação

é uma das áreas da segurança da informação, absolutamente fundamental em um mundo on-line, em que não temos contato direto com a pessoa que está fazendo o acesso. A validação do usuário é realizada com base nos fatores de autenticação, que são três:

1. Algo que o usuário sabe: senhas ou dados pessoais (KBA, *Knowledge Based Authentication*).
2. Algo que o usuário possui: cartões, chaveiros ou *tokens*.
3. Algo que o usuário é: biometria, como impressão digital, face, voz, íris, comportamental.

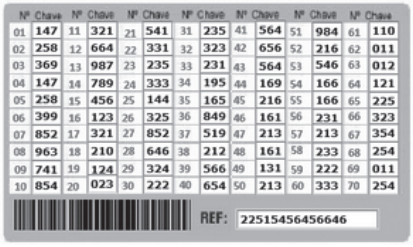
Assimile

Autenticação de dois fatores ou duplo fator de autenticação é um método bastante utilizado nos mais variados serviços on-line. Um dos principais é o uso do conjunto formado por senha e *token*. A senha corresponde à autenticação baseada em algo que o usuário sabe, e o *token* representa algo que o usuário possui. O outro fator de autenticação que pode ser utilizado é baseado em algo que o usuário é, como a biometria (exemplo: impressão digital). Com a autenticação de dois fatores, o fraudador deve roubar a senha e o *token*, por exemplo. Ou a senha e a biometria, em um outro exemplo.

Tokens

Os *tokens* representam normalmente um segundo fator de autenticação, sendo utilizados em conjunto com as senhas. Há várias formas de uso do *token*, tais como cartões com números definidos em posições, chaveiros físicos que apresentam números ou aplicativos celulares. Esses *tokens* podem ser vistos, respectivamente, nas Figuras 2.7, 2.8 e 2.9.

Figura 2.7 | Cartão de segurança com códigos de segurança de bancos



Fonte: elaborada pelo autor.

Figura 2.8 | *Token* OTP

Fonte: <http://www.infosecurity-magazine.com/opinions/token-debate-worthless-worthless/>. Acesso em: 5 jun. 2016.

Figura 2.9 | *Soft token*

Fonte: <https://www.securenvoy.com/two-factor-authentication/soft-tokens-explained.shtm>. Acesso em: 5 jun. 2016.

Há ainda uma outra forma do *token* ser utilizado em um acesso ou transação, por meio do uso de dispositivo móvel. O provedor de serviços gera um *token* (código), que é enviado ao dispositivo móvel cadastrado do usuário, via mensagem de texto. Nesse caso, o segundo fator de autenticação é o próprio dispositivo móvel, em posse do usuário. Este digita o código recebido para acessar o serviço ou efetivar uma transação. Atualmente há variações, como o uso de código QR (*Quick Response*, aquelas barras bidimensionais que podem ser facilmente lidas com a câmera do dispositivo móvel), em que códigos são gerados para um acesso específico e um aplicativo é utilizado para a validação.

Uma característica importante dos *tokens* é que os números são utilizados uma única vez, sendo atualizados a cada acesso ou transação, isso faz com que os *tokens* sejam conhecidos também como OTP (*One-Time Password*), ou senha de uso único. Esse mecanismo representa o fator de autenticação baseado em algo que o usuário possui. Dessa forma, o fraudador deve roubar o cartão, chaveiro ou dispositivo do usuário para obter os números correspondentes àquele acesso ou transação.

O OTP pode ser baseado em tempo ou em listas. No caso do OTP baseado em tempo, o *token* do usuário deve estar sincronizado com o horário do servidor, que,

com uma semente única, gera os números correspondentes, devendo ser iguais. Já no caso do OTP baseado em listas, uma sequência de senhas é gerada e compartilhada entre o servidor e o usuário. A cada uso a senha é descartada, e no próximo acesso ou transação, uma nova senha deverá ser utilizada.

Reflita

Pense nas fraudes bancárias. Elas evoluem o tempo todo. Um dos ataques consegue, inclusive, driblar a autenticação de dois fatores. Veja mais em:

LEMKE, Camilla. **KL-*Remote***: *toolkit* para fraudes bancárias contorna autenticação de dois fatores e identificação de dispositivos. Disponível em <https://under-linux.org/content.php?r=9227>. 2016. Acesso em: 23 maio 2016.

Biometria

A biometria representa a autenticação baseada em alguma coisa que o usuário é: pode ser baseada em alguma característica física única (impressão digital, face, voz, íris, veias) ou em alguma característica comportamental (modo de andar, modo de digitar, modo de usar o dispositivo móvel).

Há avanços substanciais nas tecnologias biométricas e as aplicações têm aumentado a cada dia. Podemos ver a biometria sendo utilizada pelos bancos brasileiros nos caixas eletrônicos (impressão digital e veias da palma da mão) e há grande uso de biometria de impressão digital e de face em várias aplicações em dispositivos móveis.

No futuro, acessaremos serviços e realizaremos transações de uma forma cada vez mais transparente, pois os sistemas saberão que quem está lá é o usuário legítimo, sem que seja necessário perguntar algo (como uma senha) ou solicitar a apresentação de algo em sua posse (como um *token*).

Para usar a biometria, os sistemas criam modelos matemáticos dos usuários, também conhecidos como *templates* biométricos ou referências biométricas. A cada acesso ou transação, análises probabilísticas dos usuários são realizadas de acordo com as referências biométricas existentes para a decisão sobre a legitimidade da identidade. Assim, a biometria traz consigo alguns indicadores diferentes, relacionados à sua forma de funcionamento, que é distinta das senhas. Há, por exemplo, a incidência de taxas de erros, representados pela falsa aceitação ou falso positivo (quando um usuário não legítimo é tratado como legítimo) e a falsa rejeição ou falso negativo (quando um usuário legítimo não consegue o acesso).

Um ponto fundamental, no entanto, está relacionado à sua característica probabilística (e não binária, como a senha). No caso da senha, a verificação é binária,

ou seja, a senha está correta ou incorreta. Já no caso da biometria, essa verificação é baseada em cálculos matemáticos, e a resposta de cada cálculo sempre varia. Dessa forma, uma senha pode ser protegida com um *hash*, por exemplo, o que não é possível com uma referência biométrica. Além disso, no caso da senha, se ela for roubada, "basta" trocá-la. No caso da biometria, isso é impossível, pois não dá para trocar uma característica física ou comportamental do usuário.

Filtros de conteúdo e DLP *(Data Loss Prevention)*

Além dos controles de segurança para autenticação e daqueles vistos na aula anterior, há outros que merecem destaque.

Os filtros de conteúdo, também conhecidos como *proxies*, funcionam para controlar o acesso de usuários a websites duvidosos, que podem levar à contaminação por *malwares*. Além disso, eles possuem um papel importante na produtividade, uma vez que o acesso a sites impróprios ou não relacionados aos negócios da empresa pode ser bloqueado baseado em endereços ou palavras-chave.

Um controle importante é o DLP (*Data Loss Prevention*), que tem como objetivo proteger o ambiente contra vazamentos de informação. O DLP pode atuar na rede, monitorando todo o tráfego para que sejam conhecidos as origens, os destinos e os tipos de informações que estão sendo enviadas pela rede empresarial; monitorando arquivos armazenados nos servidores da empresa; e, ainda, monitorando arquivos em estações de trabalho.

Pesquise mais

O DLP é importante para controlar o vazamento de informações. Veja mais sobre essa tecnologia em:

PANDINI, William. **DLP**: o que é e como funciona? 2015. Disponível em: <http://blog.ostec.com.br/seguranca-perimetro/dlp-o-que-e-e-como-funciona>. Acesso em: 20 maio 2016.

Sem medo de errar

Voltando ao caso da Food-XYZ, você deve definir controles de segurança, mecanismos de defesa ou contramedidas para a série de vulnerabilidades e ameaças encontradas. O foco é a proteção dos acessos dos usuários e também de conteúdos da Food-XYZ.

Vamos dividir a atividade em duas partes: a primeira foca a autenticação dos usuários; a segunda, a proteção de conteúdos.

Em um primeiro momento, é preciso conhecer os problemas que serão resolvidos com os controles de segurança a serem definidos. Complemente as ameaças relacionadas aos métodos tradicionais de autenticação e ao conteúdo da Food-XYZ.

Alguns exemplos: senhas podem ser roubadas, adivinhadas ou quebradas com força bruta. Já o conteúdo pode ser roubado. Em todos os casos, a propriedade básica de segurança da informação afetada é a confidencialidade.

No segundo momento, pense nos controles de segurança a serem utilizados. Os mecanismos de proteção possuem as finalidades de prevenção, detecção e resposta. As seguintes ferramentas podem ser consideradas:

- *Token*: prevenção contra ataques às senhas, atuando como segundo fator de autenticação.
- Biometria: prevenção contra ataques às senhas, atuando como segundo fator de autenticação ou mesmo substituindo as senhas.
- Filtro de conteúdo: prevenção de ataques, atuando na filtragem do que os usuários acessam, evitando a contaminação por visitas a sites maliciosos.
- DLP: prevenção de ataques, fazendo com que *malwares* e funcionários mal-intencionados enviem para fora da empresa informações sigilosas.

Atenção

As ferramentas de segurança relacionadas à autenticação são utilizadas pelos usuários, visando validar a identidade para a concessão dos acessos. Os três fatores de autenticação são: (1) aquilo que o usuário sabe; (2) aquilo que o usuário possui; (3) aquilo que o usuário é.

Avançando na prática

Concedendo Acesso a Usuários

Descrição da situação-problema

Seu amigo Carlitos trabalha na Drink-HIJ, em uma função similar à sua na Food-XYZ. Ele, porém, está realizando as integrações tecnológicas dentro do Brasil, nas

seguintes localidades: Recife, Florianópolis e Manaus. Carlitos está em Florianópolis e pediu a sua ajuda para definir as melhores tecnologias a fim de permitir que diferentes usuários acessem os serviços da Drink-HIJ. Ele detalhou um pouco quem são esses usuários:

- Usuários internos de Florianópolis, Recife e Manaus acessam os servidores que estão na matriz (Florianópolis) e hospedam os seguintes serviços: sistema de vendas, sistema financeiro, sistema de benefícios e servidor de arquivos.

Usuários internos de Florianópolis, Recife e Manaus usam a internet para acessar serviços de comunicação e e-mail.

- Clientes acessam o sistema de vendas via internet, no qual podem pagar e fazer pedidos.
- Clientes acessam o sistema de vendas via aplicativo móvel, no qual podem pagar e fazer pedidos.
- Prestadores de serviços de TI acessam os servidores de Florianópolis via internet, usando VPN.

O que você sugere para seu amigo Carlitos?

Lembre-se

Ferramentas de segurança possuem objetivos específicos, e também custos associados. Uma análise de riscos ajuda na priorização de investimentos, a partir do entendimento de todos os aspectos de segurança envolvidos. Para seu amigo, considere que não é necessária a "segurança máxima", como seria no caso de uma empresa que é alvo constante de *crackers* do mundo inteiro.

Resolução da situação-problema

Para conceder os acessos aos usuários da Drink-HIJ, considere os seguintes controles de segurança utilizados visando à autenticação: senhas, *tokens*, biometria de impressão digital e biometria de face.

- Usuários internos de Florianópolis, Recife e Manaus que acessam os servidores da matriz (Florianópolis): usuários locais podem utilizar senhas tradicionais, enquanto usuários de outras localidades também devem utilizar as senhas, mas vinculadas a um *token* via SMS, já que se encontram em locais remotos e representam, portanto, um ponto adicional de ataques.

- Usuários internos de Florianópolis, Recife e Manaus que acessam serviços de comunicação e e-mail: métodos tradicionais dos prestadores dos serviços.
- Clientes: senhas tradicionais e biometria facial para os dispositivos móveis.
- Prestadores de serviços de TI: autenticação de dois fatores, similar aos usuários internos de outras localidades.

Faça você mesmo

Considere os controles de segurança que você definiu nessa atividade para mapear os riscos existentes para cada um dos usuários.

Faça valer a pena

1. Um dos principais problemas com senhas é que elas podem ser roubadas. Qual alternativa a seguir representa um ataque de roubo de senhas?

a) Nenhuma.

b) *Firewall*.

c) *Phishing*.

d) *Scan*.

e) *Cracker*.

2. Qual alternativa representa o fator de autenticação correspondente às senhas?

a) Confidencialidade.

b) Integridade.

c) O que o usuário sabe.

d) O que o usuário é.

e) Ameaças.

3. Qual fator de autenticação é representado pelos *tokens*?

a) Confidencialidade.

b) Integridade.

c) O que o usuário sabe.

d) O que o usuário possui.

e) Ameaças.

Referências

CARDOSO, Luis Filipe. **Protocolo de funcionamento do *WhatsApp***. 2015. Disponível em: <http://luisfcardoso.blogspot.com.br/2015/08/protocolo-de-funcionamento-do-whatsapp.html>. Acesso em: 19 abr. 2016.

COSTA, Anderson Danilo Guedes; LAPA, Igor Raphael dos Passos. VoIP: Análise de protocolos com o *Wireshark*. **Engenharia da Computação em Revista**, v.4, n. 1, 2010.

ITFORUM. ***Skype* adota protocolo SIP para atender empresas**, 2009. Disponível em: <http://itforum365.com.br/noticias/detalhe/33936/skype-adota-protocolo-sip-para-atender-empresas>. Acesso em: 19 abr. 2016.

LIMA, Vanderson Ramos Diniz de; LIJÓ, Maria Camila; SOUSA, Marcelo Portela. Segurança em redes sem fio: princípios, ataques e defesas. **Revista de Tecnologia da Informação e Comunicação**, Campina Grande, v. 4, n. 2, out. 2014. Disponível em: <http://www.rtic.com.br/artigos/v04n02/v04n02a01.pdf>. Acesso em: 27 abr. 2016.

MICROSOFT Corporation. **Ameaças e contramedidas de segurança na web**. 2004. Disponível em: <https://technet.microsoft.com/pt-br/library/dd569900.aspx>. Acesso em: 6 maio 2016.

NAKAMURA, Emilio T.; GEUS, Paulo L. de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

O ANALISTA. **Cisco revisa código após backdoor em firewall da Juniper**. 2015. Disponível em: <http://www.oanalista.com.br/2015/12/22/cisco-revisa-codigo-apos-backdoor-em-firewall-da-juniper/>. Acesso em: 1 maio 2016.

ORACLE. **Overview of Secure Network Communications for SAP**. Disponível em: <https://docs.oracle.com/cd/E21454_01/html/821-2598/cnfg_sap-snc_t.html>. Acesso em: 19 abr. 2016.

ROHR, Altieres. Jeep foi hackeado graças à 'porta de rede aberta' sem senha. **G1**. **Segurança Digital**. 2015. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/jeep-foi-hackeado-gracas-porta-de-rede-aberta-sem-senha.html>. Acesso em: 1 maio 2016.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5. ed. São Paulo: Pearson Education, 2011.

XAVIER, Felipe. **Kevin Mitnick, a lenda hacker!** 2010. Disponível em: <https://fexavier.wordpress.com/2010/01/18/kevin-mitnick-a-lenda-hacker/>. Acesso em: 26 abr. 2016.

Criptografia

Convite ao estudo

Olá!

Você já está habituado a explorar as propriedades básicas da segurança da informação (confidencialidade, integridade e disponibilidade) e já está apto a aplicar os fundamentos básicos, como os elementos a serem protegidos, os mecanismos de defesa e os elementos do risco. Além disso, você também já pode aplicar a segurança de redes para proteger um ambiente, a partir do entendimento de vulnerabilidades e ameaças existentes, utilizando as principais ferramentas de defesa, como autenticação, *firewall*, IDS, IPS ou antimalware.

Chegamos agora às aulas de um dos assuntos mais fascinantes da segurança da informação e de redes – a criptografia. Hoje em dia, a criptografia faz parte da vida de todos, de uma forma ou de outra. Quem acessa a internet o faz usando o SSL (*Secure Sockets Layer*), que adota a criptografia para criar um canal seguro entre o navegador e o website. Quem se comunica pela internet usando o *Skype* utiliza a criptografia. E aplicativos de mensagens como o *WhatsApp* também adotam a criptografia.

Em termos de propriedades básicas de segurança da informação, a criptografia atua para proteger a confidencialidade e a integridade da informação, que estão em transmissão ou armazenadas.

Em um caso clássico de extrema importância para a segurança da informação, em 2016, nos Estados Unidos, o FBI iniciou um processo contra a Apple para que a empresa ajudasse na quebra do sigilo de um *iPhone* de um terrorista que supostamente continha informações protegidas com criptografia.

Iremos discutir os principais aspectos da criptografia, começando com os conceitos e apresentando as bases para o entendimento e aplicação desse importante mecanismo de segurança.

Os principais objetivos de aprendizagem desta unidade são:

- Consolidar o conceito de criptografia, registrando a sua evolução ao longo da história.
- Consolidar os conceitos dos principais tipos de criptografia, com a adoção de exemplos para a criptografia de chave privada, de chave pública e a esteganografia.
- Consolidar os conceitos de assinatura digital e *key escrow*, e também conhecer os algoritmos criptográficos *Diffie-Hellman* e RSA.
- Definir, registrar e descrever algumas aplicações de criptografia: cartões de banco, VPN, SSL, HTTPS.

Durante as aulas desta unidade, você irá trabalhar com uma situação que remete ao dia a dia de muitas empresas: você trabalha em uma empresa que desenvolve projetos de design de novos produtos para diferentes indústrias, a cr14t1v3. Um dos últimos projetos foi a criação de um modelo de supercarro esportivo para uma montadora húngara. Outro projeto foi a criação do design de uma batedeira de luxo para um fabricante uruguaio. A empresa não possui muitos funcionários, mas possui uma equipe de estrelas formada por cerca de 15 artistas. Toda a equipe da cr14t1v3 utiliza um conjunto de computadores modernos, que estão interligados na rede interna para o trabalho colaborativo. Há uma equipe de tecnologia que mantém um data center local, que suporta os sistemas de gestão e também o servidor de arquivos, que é crítico para o negócio da empresa.

Você já deve ter percebido que a cr14t1v3 trabalha com informações críticas, que são os designs criados para seus clientes. A necessidade de criptografia é ainda mais evidente no caso da empresa, e você irá trabalhar nesse caso para consolidar todos os conceitos desta unidade.

Boas aulas!

Seção 3.1

Evolução em segurança da informação: criptografia

Diálogo aberto

Olá!

Seja bem-vindo à aula inicial sobre um assunto tão importante, que é muitas vezes confundido diretamente com a própria área de segurança da informação e de redes. De uma certa forma, isso não deixa de ter um fundo de verdade, pois a criptografia é utilizada cada vez mais por nós, em vários contextos diferentes.

Pense em você quando paga uma conta no banco, troca mensagens com seus amigos, ou armazena documentos pessoais na nuvem. A criptografia está lá, sendo utilizada de uma forma transparente, protegendo as suas informações. Você, como usuário, já vê benefícios no seu uso. O seu desafio nesta unidade de ensino é entender os principais conceitos de criptografia para poder aplicá-los profissionalmente, de acordo com as necessidades, que são muitas.

Neste início, vamos pensar na cr14t1v3, uma empresa de design de novos produtos para diferentes indústrias. Com toda a equipe utilizando um conjunto de computadores modernos, que estão interligados na rede interna para o trabalho colaborativo, há uma série de riscos envolvidos. Além da rede, há o data center local, que suporta os sistemas de gestão e também o servidor de arquivos.

A sua tarefa inicial será de mostrar para o conselho administrativo da cr14t1v3 que há um conjunto de riscos que levam à necessidade de um controle de segurança específico – a criptografia. Faça um mapeamento de riscos com foco na proteção das informações, considerando a confidencialidade e a integridade como as propriedades básicas de segurança da informação a serem garantidas.

Boa aula!

Não pode faltar

Introdução

Uma das definições de criptografia diz que ela é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: ***kryptos***, que significa oculto, e ***graphien***, que significa escrever. O objetivo da criptografia não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado. De um modo geral, se a mensagem cair nas mãos de um intruso, este, ao lê-la, não a compreenderá. Apenas o remetente e o destinatário, em princípio, com um acordo pré-estabelecido (as chaves), é que têm acesso ao significado da mensagem. O termo criptografia é usado muitas vezes como sinônimo de criptologia, abrangendo, desta forma, a criptanálise, que tem por função descobrir os segredos ou quebrar a confidencialidade entre emissor e receptor (FIARRESGA, 2010).

Até o século XX, a criptografia era considerada uma arte, de modo que a construção de bons códigos, ou a quebra dos códigos, era baseada em criatividade e qualidades pessoais. Isso mudou no século 20, com o aparecimento de rigorosos estudos que fizeram a criptografia virar ciência. Antes, a criptografia tinha como objetivo a comunicação secreta, e atualmente foram acrescentados objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, dinheiro digital.

Uma definição mais moderna é que a criptografia é o estudo científico de técnicas para a segurança de informações, transações e computação distribuída (KATZ; LINDELL, 2007).

O público da criptografia também mudou, passando de militares e organizações de inteligência para todos, desde o acesso a websites até a proteção de informações em notebooks.

Conceitos

Imagine que Alice quer enviar uma mensagem para Beto por um canal, que normalmente é inseguro. Nesse canal um atacante pode escutar a mensagem, afetando a privacidade ou a confidencialidade da comunicação entre Alice e Beto.

Com o uso da criptografia, Alice pode enviar uma mensagem cifrada para Beto. Alice utiliza um algoritmo criptográfico que utiliza uma chave secreta para cifrar a mensagem original. O resultado é um texto incompreensível para o atacante. Beto recebe a mensagem cifrada e utiliza a mesma chave secreta (compartilhada com Alice) para decifrar a mensagem e chegar ao conteúdo original.

Esse é o funcionamento básico da criptografia simétrica ou de chave privada, em

que a chave secreta é a mesma para a cifragem e decifragem e que, portanto, deve ser compartilhada.

Os processos de cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são ininteligíveis.

Exemplificando

Um exemplo de criptografia, bastante simples, é o ROT-13, que é uma cifra de substituição que troca cada letra da mensagem por uma que está 13 posições à frente no alfabeto. Uma mensagem de Alice para Beto com o conteúdo "Oi" viraria, com o uso do ROT-13, "Bv", já que "O" é substituída por "B", que está 13 posições à frente, e "i" é substituída por "v".

As técnicas ou tipos de criptografia serão discutidas na próxima aula, e incluem a criptografia de chave privada ou simétrica, a criptografia de chave pública ou assimétrica, além de algoritmos de *hash*, utilizados para a integridade. Além dos algoritmos criptográficos, há técnicas similares à criptografia, como a esteganografia, que também será discutida na próxima aula.

Os objetivos básicos da criptografia são (KATZ; LINDELL, 2007), (MENEZES; OORSCHOT; VANSTONE 2001), (FIARRESGA, 2010):

- Sigilo: proteção dos dados contra divulgação não autorizada.
- Autenticação: garantia que a entidade se comunicando é aquela que ela afirma ser.
- Integridade: garantia de que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.
- Não repúdio: garantia que não se pode negar a autoria de uma mensagem.
- Anonimato: garantia de não rastreabilidade de origem de uma mensagem.

Assimile

A criptografia é muito mais do que sigilo e garantia de confidencialidade. Pense em variadas aplicações: autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicos, dinheiro digital.

Segurança dos sistemas criptográficos

A segurança da criptografia não pode ser medida somente pelo tamanho da chave utilizada, sendo necessário conhecer o algoritmo e a matemática envolvida no processo de codificação de dados. Desse modo, um algoritmo que utiliza chaves de 256 bits não significa que é mais seguro do que outros algoritmos, como o DES de 128 bits, caso existam falhas no algoritmo ou em sua implementação (NAKAMURA; GEUS, 2007).

Há a possibilidade de atacar uma informação protegida com criptografia pelo algoritmo ou pela descoberta da chave secreta.

Exemplificando

O algoritmo RC4 já foi pivô de problemas no WEP (*Wired Equivant Privacy*), protocolo de segurança utilizado em redes Wi-Fi em 2001. Já em 2013, o TLS/SSL teve uma grave falha de segurança divulgada relacionada ao mesmo algoritmo RC4 (SOPHOS, 2013).

Exemplificando

O DES (*Data Encryption Standard*) teve sua efetividade invalidada em 1997, quando uma mensagem cifrada com o algoritmo foi quebrado pela primeira vez. Os custos dos equipamentos que realizavam o ataque de força bruta foram diminuindo, ao mesmo tempo em que o tempo para a quebra também foi sendo drasticamente reduzida. Em 1998, um equipamento com custo de US$ 250 mil quebrou uma chave de 56 bits em aproximadamente dois dias (NOMIYA, 2010).

A segurança de sistemas criptográficos depende de uma série de fatores, tais como (NAKAMURA; GEUS, 2007):

- Geração de chaves: sem uma geração aleatória de chaves, o algoritmo utilizado pode revelar padrões que diminuem o espaço de escolha das chaves, o que facilita a sua descoberta.
- Mecanismo de troca de chaves: as chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras e, para tanto, protocolos como o *Diffie-Hellman* são utilizados. Esse protocolo será discutido nas próximas aulas.

- Taxa de troca das chaves: quanto maior a frequência de troca automática das chaves, maior será a segurança, pois isso diminui a janela de oportunidade de ataques, pois, caso uma chave seja quebrada, em pouco tempo ela já não é mais útil para a comunicação.
- Tamanho da chave: são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.

Reflita

Pense em um algoritmo criptográfico e a chave que protege determinada informação. É mais fácil quebrar o código (algoritmo) ou encontrar a chave?

Um dos métodos para se quebrar a chave criptográfica é o ataque de força bruta, em que diferentes combinações são testadas.

A segurança está no tamanho das chaves, e não no algoritmo criptográfico. Os algoritmos criptográficos mais utilizados são públicos, tendo sido avaliados por toda a comunidade científica.

História

A história da criptografia é composta por grandes eventos, como os citados a seguir (MEDEIROS, 2015), (KATZ; LINDELL, 2007), (FIARRESGA, 2010).

O primeiro uso documentado da criptografia foi em torno de 1900 a.C., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição. Já entre 600 a.C. e 500 a.C., os hebreus utilizavam a cifra de substituição simples, que era fácil de ser revertida com o uso de cifragem dupla para obter o texto original. A Cifra de César é um dos exemplos mais clássicos de criptografia, em que as substituições eram feitas com as letras do alfabeto avançando três casas.

Com a Cifra de Vigenère a evolução consistiu no uso de diferentes valores de deslocamento para as substituições.

A criptoanálise, que buscava padrões que identificavam mensagens ocultas, cresceu na Idade Média. Já a máquina criada pelo alemão Kasiski, o Enigma, foi utilizada para a segurança das comunicações na Segunda Guerra Mundial. O Enigma era uma máquina física, assim como o Colossus, que conseguiu decifrar mensagens do Enigma após uma engenharia reversa a partir de uma máquina furtada.

A Teoria Matemática da Comunicação, de Claude Shannon, criada em 1948,

possibilitou um grande avanço em criptografia e criptoanálise, que floresceu ainda mais durante a Guerra Fria entre os Estados Unidos e a União Soviética.

Outro avanço importante foi a criação de criptografia de chave pública, em 1976, por Diffie e Hellman, que levou ao desenvolvimento do algoritmo RSA.

Antes, da proteção de comunicação em guerras; hoje a criptografia faz parte do cotidiano de todos, muitas vezes de uma forma transparente, como é o caso do acesso web, de transações bancárias e de acesso às redes.

Uso atual de criptografia

A Apple, por exemplo, utiliza práticas de segurança-padrão do setor e emprega rígidas políticas para proteção dos dados (APPLE, 2016). A segurança dos dados e a privacidade das informações pessoais do *iCloud* (serviço de nuvem da Apple), que é acessado a partir de diferentes dispositivos, trata de diferentes tipos de dados, tanto em trânsito quanto armazenados no servidor. Dados do usuário, por exemplo, são protegidos com a criptografia AES de, no mínimo, 128 bits. Já a criptografia AES de 256 bits é utilizada para armazenar e transmitir senhas e informações de cartões de crédito. Além disso, a Apple também usa criptografia assimétrica de curva elíptica e empacotamento de chave.

Pesquise mais

Veja os mecanismos de segurança utilizados pela Apple no seu serviço *iCloud* em (APPLE, 2016).

APPLE. 2016. **Visão geral da segurança e privacidade do iCloud**. Disponível em: <https://support.apple.com/pt-br/HT202303>. 18/04/16. Acesso em: 15 jun. 2016.

Já o serviço de mensagens *WhatsApp* começou em abril de 2016 a utilizar criptografia em todas as suas comunicações, incluindo mensagens de voz e outros arquivos, entre seus usuários. Com o que chamam de "criptografia de ponta a ponta", as mensagens são embaralhadas ao deixar o telefone da pessoa que as envia e só conseguem ser decodificadas no telefone de quem as recebe. Segundo um comunicado da empresa, "Quando você manda uma mensagem, a única pessoa que pode lê-la é a pessoa ou grupo para quem você a enviou. Ninguém pode olhar dentro da mensagem. Nem cibercriminosos. Nem *hackers*. Nem regimes opressores. Nem mesmo nós" (COSTA, 2016, p. 1).

Pesquise mais

O *WhatsApp* é um fenômeno de uso, e um ótimo exemplo do nosso dia a dia. Veja como a criptografia é utilizada no *WhatsApp* em Costa (2016). Detalhes mais técnicos podem ser entendidos em Matsuki (2016) e WhatsApp (2016).

COSTA, Camilla. BBC Brasil. **Quatro coisas que mudam com a criptografia no *WhatsApp* – e por que ela gera polêmica.** Disponível em: <http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc>. Acesso em: 15 jun.2016.

MATSUKI, Edgard. Portal EBC. **Entenda o que é a criptografia de ponta-a-ponta, utilizada pelo *WhatsApp***. Brasília, 2016. Disponível em: <http://www.ebc.com.br/tecnologia/2016/04/entenda-o-que-e-criptografia-de-ponta-ponta-utilizada-pelo-whatsapp>. Acesso em: 15 jun.2016.

WHATSAPP. **Perguntas frequentes**, 2016. Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 15 jun.2016.

Sem medo de errar

No estudo de caso da cr14t1v3, nesta aula, você deve mapear os riscos com foco na proteção das informações, considerando a confidencialidade e a integridade como as propriedades básicas de segurança da informação a serem garantidas.

Você deve pensar no fluxo da informação e analisar as duas dimensões que precisam de proteção: a informação que transita na rede e a informação que é armazenada.

Sendo uma empresa de design, há o uso de computadores modernos, que estão interligados na rede interna para o trabalho colaborativo. Além da rede, há o data center local, que suporta os sistemas de gestão e também o servidor de arquivos.

De acordo com o fluxo de informações, e pensando em alavancar o uso da criptografia, considere:

- Projetos de design que estão sendo desenvolvidos nos computadores.
- Rede da empresa, que é utilizada para o trabalho colaborativo.
- Servidor de arquivos, que armazena os projetos.
- Sistemas de gestão, que armazenam informações operacionais.

Relacione agora quais são as propriedades básicas de segurança da informação que devem ser garantidas para cada fluxo definido acima, pensando em criptografia:

- Projetos de design: precisam de confidencialidade e integridade.
- Rede: precisa de confidencialidade e integridade.
- Servidor de arquivos: precisa de confidencialidade e integridade.
- Sistemas de gestão: precisa de confidencialidade e integridade.

Há muito em comum entre a proteção que a cr14t1v3 deve adotar, e as ameaças, de uma forma geral, são:

- *Crackers* invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações.
- Concorrentes invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações.
- Funcionários vazando informações sobre projetos da empresa.
- *Crackers* invadindo os sistemas de gestão para roubar, copiar ou alterar informações operacionais.

Atenção

Além de ser utilizada para sigilo e integridade das informações, a criptografia pode ainda ser utilizada para outras funções: assinatura digital, autenticidade, não repúdio, anonimato.

Avançando na prática

Usando criptografia para proteger dados de seu notebook

Descrição da situação-problema

Um dos grandes problemas das empresas em um mundo móvel e conectado é a proteção de dados que estão em trânsito, mas não na rede, e sim nos dispositivos que

saem dos perímetros da empresa. Um exemplo é o uso de notebooks, que contêm informações empresariais altamente críticas e que precisam ser protegidas. Imagine se um funcionário perde o notebook em uma viagem para visitar um cliente ou se ele tem o equipamento roubado no aeroporto. Como ficam as informações da empresa, e quais são as consequências? O que você faria para proteger essas informações que estão em notebooks? Considere que você trabalha com projetos estratégicos multimilionários para governos estrangeiros e realiza negociações relativas ao escopo desses projetos e aos valores envolvidos.

Lembre-se

Os impactos resultantes de um incidente de segurança envolvendo notebooks são extremamente altos. Com muitas informações críticas e estratégicas, os resultados podem ser catastróficos. Não há como afirmar com certeza se há uma relação direta com a situação da Petrobras hoje, mas ela já foi vítima de um roubo deste tipo (REUTERS, 2008).

Resolução da situação-problema

As informações dos notebooks são extremamente críticas e envolvem governos e cifras bilionárias, que em caso de vazamento, podem resultar em processos judiciais, plágio de projetos e perdas de contratos para concorrentes.

O uso da criptografia possibilita que, em caso de perda ou roubo do equipamento, todas as informações continuem protegidas por uma chave criptográfica. A segurança depende do nível dessa chave, que pode sofrer ataques de força bruta. Nesse ponto, o tamanho da chave importa, pois dificulta a sua descoberta.

Já a criptografia pode ser aplicada em diferentes níveis. Um dos níveis é o uso individual em cada arquivo, que é uma tarefa mais trabalhosa para o dono do notebook, se comparado com o outro nível, que é a aplicação da criptografia em todo um sistema de arquivos. Neste caso, todos os arquivos gravados nesse sistema de arquivos que utiliza a criptografia são protegidos de uma forma transparente após a sua montagem pelo usuário.

Faça você mesmo

Faça uma pesquisa sobre ferramentas de criptografia para notebooks que você pode aplicar em seu dia a dia.

Faça valer a pena

1. Alice quer enviar uma mensagem para Beto, que está em outra localidade. O que pode acontecer com a mensagem no caminho entre Alice e Beto?

a) A mensagem pode ser somente trocada por um fraudador.

b) A mensagem pode ser somente capturada por um fraudador.

c) A mensagem pode ser somente negada por um fraudador.

d) A mensagem pode ser somente capturada ou trocada por um fraudador.

e) A mensagem pode ser trocada, capturada ou negada por um fraudador.

2. Alice quer enviar uma mensagem para Beto, que está em uma outra localidade. No caso de roubo da mensagem por um fraudador no meio do caminho, qual propriedade básica da segurança da informação está sendo comprometida?

a) A mensagem não está sendo comprometida.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) Confidencialidade e integridade.

3. Alice quer enviar uma mensagem para Beto, que está em uma outra localidade. No caso da captura da mensagem por um fraudador no meio do caminho, qual propriedade básica da segurança da informação está sendo comprometida?

a) A mensagem não está sendo comprometida.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) Confidencialidade e integridade.

Seção 3.2

Técnica de criptografia

Diálogo aberto

Olá!

Na aula anterior começamos a discutir os principais conceitos relacionados à criptografia, principalmente quanto à sua necessidade para a confidencialidade e integridade, sendo utilizada ainda para autenticação de mensagens, não repúdio e anonimato. Além disso, vimos que a segurança de sistemas criptográficos depende do algoritmo e do tamanho das chaves, incluindo fatores como mecanismo de geração e troca de chaves.

E nesta aula vamos avançar no entendimento da criptografia, tendo contato direto com as principais técnicas que utilizamos no nosso dia a dia. Você já percebeu que, quando acessamos um banco pela internet, um dos pontos que temos que verificar é o cadeado próximo ao endereço Web? É a criptografia em ação, com o SSL (*Secure Sockets Layer*) em ação.

Vamos entender, nesta aula, como funciona a criptografia de chave privada ou simétrica, e também a criptografia de chave pública ou assimétrica. Essas são as duas principais técnicas utilizadas por aplicações, protocolos e sistemas diversos, como o IPSec (*Internet Protocol Security*), o SSL ou o iOS, sistema operacional da Apple. Esses exemplos serão discutidos em detalhes nas próximas seções.

Além desses dois tipos de criptografia (de chave privada e de chave pública), há ainda os algoritmos de *hash* criptográfico, que são utilizados para garantia de integridade das informações. O *hash* e outras funções importantes, como a assinatura digital e o certificado digital, serão discutidas na próxima seção. Nesta seção, assim, você terá contato com as principais técnicas básicas de criptografia, complementada pela esteganografia, que busca ocultar uma mensagem dentro de outra, que a torna diferente da criptografia.

Para exercitarmos os conceitos desta seção, vamos voltar à cr14t1v3, uma empresa de design de novos produtos para diferentes indústrias. Lembre-se de que a empresa

possui um data center local, que suporta os sistemas de gestão e também o servidor de arquivos acessados por toda a equipe da cr14t1v3, que utiliza bastante a rede interna interligada para o trabalho colaborativo. Sua missão agora é mostrar para o conselho administrativo da cr14t1v3 que há uma série de algoritmos criptográficos que podem ser utilizados pela empresa, e você irá apresentar os objetivos de cada um deles, destacando suas vantagens e desvantagens.

Boa aula!

Não pode faltar

Um pouco mais sobre criptografia

A criptografia é o estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação como confidencialidade, integridade, autenticação de entidade e autenticação de origem de dados (MENEZES; OORSCHOT; VANSTONE 2001).

Como vimos na aula passada, a criptografia é baseada em um conjunto de técnicas que incluem a cifragem, funções de *hash* e assinaturas digitais. A escolha da melhor técnica depende de critérios como (MENEZES; OORSCHOT; VANSTONE 2001):

- Nível de segurança requerido.
- Funcionalidade ou objetivo de segurança.
- Métodos de operação dos algoritmos, que podem ser diferentes para cada funcionalidade.
- Desempenho.
- Facilidade de implementação.

É analisando esses critérios acima que a técnica de criptografia deve ser definida para cada objetivo e informação a ser protegida.

Há uma grande quantidade de técnicas em criptografia; nesta e nas próximas aulas iremos focar:

- Criptografia de chave privada ou simétrica.
- Criptografia de chave pública ou assimétrica.
- Funções de *hash* criptográfico.
- Assinatura digital.

Além dessas técnicas, iremos discutir nestas aulas a esteganografia e também protocolos como o *Diffie-Hellman*, voltado para a troca de chaves, além de funções de criptografia como o *key escrow* (custódia de chaves, em que chaves múltiplas dão acesso a uma informação).

Pesquise mais

Os conceitos básicos e as principais técnicas de criptografia, incluindo os algoritmos mais utilizados, são descritos resumidamente em Nascimento (2011).

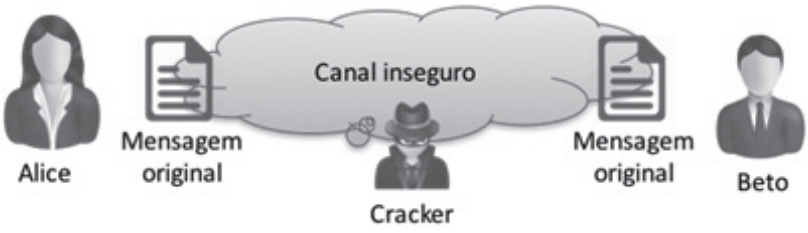
NASCIMENTO, Anderson Clayton do. **Criptografia e infraestrutura de chaves públicas**. Brasília: Universidade de Brasília, 2011. Disponível em: <http://home.ufam.edu.br/regina_silva/CEGSIC/Textos%20Base/Criptografia_e_ICP.pdf>. Acesso em: 26 jun. 2016.

Criptografia de chave privada

A função essencial da criptografia é a garantia de confidencialidade ou de sigilo da informação, em que há a proteção dos dados contra divulgação não autorizada.

Imagine que Alice quer enviar uma mensagem para Beto por um canal, que normalmente é inseguro. Nesse canal, um atacante pode escutar a mensagem, afetando a privacidade ou a confidencialidade da comunicação entre Alice e Beto.

Figura 3.1 | Alice envia mensagem para Beto por um canal inseguro

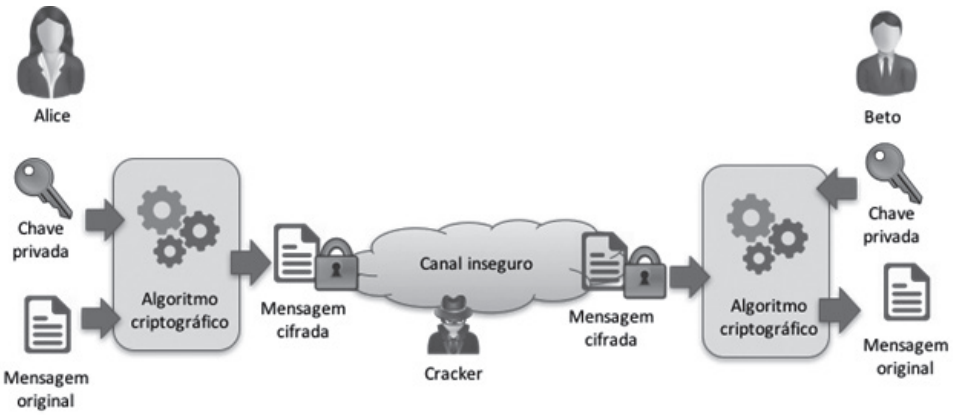


Fonte: elaborada pelo autor

Com o uso da criptografia, Alice pode enviar uma mensagem cifrada para Beto. Alice utiliza um algoritmo criptográfico e uma chave secreta privada para cifrar a mensagem original. O resultado é um texto incompreensível para o atacante. Beto recebe a mensagem cifrada e utiliza a mesma chave secreta (compartilhada com Alice) para decifrar a mensagem e chegar ao conteúdo original. Os processos de

cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são inteligíveis, e vice-versa.

Figura 3.2 | Alice e Beto utilizam criptografia para troca de mensagem



Fonte: elaborada pelo autor

Esse é o funcionamento básico da criptografia simétrica ou de chave privada, em que a chave secreta é a mesma (simétrica) para a cifragem e a decifragem, e que, portanto, deve ser compartilhada. Este é um dos grandes desafios deste tipo de criptografia: como fazer a troca segura de chaves. No exemplo de Alice e Beto, ambos têm que combinar a chave privada para que eles possam cifrar e decifrar a mensagem. No caso de uso do mesmo canal inseguro para a troca da chave privada, a mensagem poderá ser comprometida, pois o atacante poderá ficar "escutando" o canal para a obtenção da chave privada, uma vez que é utilizada para cifrar e decifrar a mensagem.

Reflita

Como você faria para trocar uma chave privada com o seu interlocutor? Usaria o mesmo canal inseguro? Usaria um canal alternativo?

Agora imagine que você faz parte de um grupo de 50 pessoas. Como você faria para trocar uma chave privada com todos do grupo? E como você faria para trocar mensagens individuais com as 50 pessoas do grupo? Teria que utilizar 50 chaves privadas diferentes? Usaria a mesma chave para várias mensagens ou usaria uma chave privada diferente para cada mensagem?

Assim, a troca de chaves, é um dos grandes desafios da criptografia simétrica. Mais do que a troca de chaves, o gerenciamento delas, que envolve tempo de validade, armazenamento, geração, uso e substituição, é fundamental. Iremos discutir na próxima aula o gerenciamento de chaves criptográficas, que exige o entendimento de outro tipo de criptografia, a assimétrica ou de chaves públicas. Esse outro tipo de criptografia é tradicionalmente utilizado para a criação de um canal seguro, que por sua vez pode ser utilizado para a troca de chaves privadas. Iremos discutir protocolos de troca de chaves criptográficas na próxima aula.

Assimile

A criptografia de chave privada ou simétrica é rápida de ser executada em termos de processamento computacional, porém incorpora o desafio da troca de chaves. A criptografia de chave pública ou assimétrica é computacionalmente mais pesada, porém é adequada para ser utilizada na troca de chaves.

Antes de avançarmos para a criptografia de chave pública, é importante conhecermos os principais algoritmos simétricos. Eles são baseados em dois tipos:

- Cifras de fluxo: a cifragem é feita normalmente a cada dígito (byte).
- Cifras de blocos: agrupa um conjunto de bits da mensagem em blocos, e a cifragem é feita sobre cada um desses blocos.

Exemplificando

O AES (*Advanced Encryption Standard*), também conhecido por Rijndael, é considerado o padrão de criptografia, substituindo o DES (*Data Encryption Standard*). O AES é uma cifra de blocos de 128 bits.

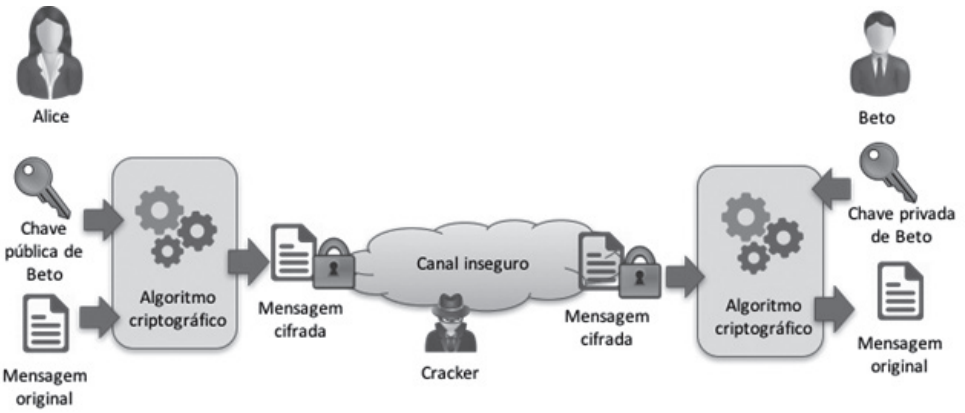
Criptografia de chave pública

A criptografia de chave pública ou assimétrica utiliza um par de chaves para a troca de mensagens. Uma chave do par é utilizada para cifrar a mensagem, que só pode ser decifrada pelo par correspondente. Dessa forma, diferentemente da criptografia de chave privada, em que a chave é compartilhada, na criptografia de chave pública não é necessária a troca de chaves privadas.

O par de chaves da criptografia de chave pública é composto por uma chave pública e uma chave privada. A chave pública pode ser divulgada publicamente, e é

utilizada para cifrar uma mensagem. Uma vez cifrada, essa mensagem só poderá ser decifrada pelo detentor da chave privada, que nunca é compartilhada. No exemplo da Figura 3.3, Alice cifra a mensagem enviada para Beto com a chave pública dele. A decifragem só pode ser feita com a chave privada correspondente, que está em poder de Beto.

Figura 3.3 | Alice e Beto utilizam criptografia de chave pública para troca de mensagem



Fonte: elaborada pelo autor.

Desta forma, caso a mensagem seja capturada em um canal inseguro, o atacante não poderá recuperar a mensagem original sem a chave privada correspondente, que está com o seu dono. Essa chave privada, em tese, nunca foi transmitida, o que reduz as chances de seu comprometimento.

O que está por trás do par de chaves utilizado na criptografia assimétrica é a função matemática conhecida como *trapdoor* ou "alçapão", em que é fácil realizar o cálculo em uma direção, porém dificílimo na direção oposta sem o uso de uma informação especial.

Exemplificando

O número 6895601 é o produto de dois números primos. A fatoração é difícil sem que um dos números primos seja revelado. O algoritmo criptográfico RSA utiliza a fatoração de números primos bastante grandes para proteger as informações, e é um dos algoritmos mais conhecidos de chave pública. A chave pública do RSA é gerada com base nesses dois grandes números primos e publicada. A mensagem é decifrada com a chave privada correspondente, que possui a informação especial que ajuda na fatoração dos dois números primos.

Os algoritmos criptográficos de curvas elípticas também são de chaves públicas, e exploram os problemas matemáticos da álgebra de curvas elípticas sobre campos finitos, como os logaritmos discretos. Os algoritmos de curvas elípticas são matematicamente mais complexos, porém utilizam chaves de tamanho menores e são mais rápidos de serem executados para o mesmo nível de segurança dos algoritmos de chave pública baseados em fatoração.

Esteganografia

A esteganografia tem origem nos termos gregos "*steganos*", que significa "coberta, escondia ou protegida", e "*graphein*", que significa "escrita", e é o uso de técnicas para ocultar a existência de uma mensagem dentro de outra. O termo foi utilizado primeiramente em 1499 por Johannes Trithemius, na obra *Steganographia*, que foi publicada apenas em 1606, e era considerada um livro de mágicas.

A diferença entre a criptografia e esteganografia é que a primeira oculta o significado da mensagem, enquanto a segunda oculta a existência da mensagem.

Alguns exemplos de uso da esteganografia são:

- Uso de tintas invisíveis.
- Mensagens escondidas no corpo do mensageiro, como na cabeça raspada, que era depois escondida após o crescimento dos cabelos.
- Código Morse costurado na roupa do mensageiro.
- Mensagens escritas nos envelopes nas áreas dos selos.
- Inserção de mensagens nos bits menos significativos de áudios ou imagens.
- Inserção de mensagens em seções de arquivos.
- Uso de caracteres *Unicode* que se parecem com conjunto de caracteres ASCII padrão.

Pesquise mais

Uma ferramenta de esteganografia que esconde mensagens em imagens GIF com a manipulação do mapa de cores, o que torna a imagem visivelmente inalterada, é o *Gifshuffle*, disponível em Kwan (2010).

KWAN, Matthew. (2010) **The Gifshuffle home page**. Disponível em: <http://www.darkside.com.au/gifshuffle/>. Acesso em: 27 jun. 2016.

Sem medo de errar

Na cr14t1v3, uma empresa de design de novos produtos para diferentes indústrias, há um data center local, o qual suporta os sistemas de gestão e também o servidor de arquivos. Estes que são acessados por toda a equipe da cr14t1v3, que utiliza bastante a rede interna interligada para o trabalho colaborativo. Sua missão agora é mostrar para o conselho administrativo da cr14t1v3 que há uma série de algoritmos criptográficos que podem ser utilizados pela empresa, e você apresentará os objetivos de cada um deles, destacando suas vantagens e desvantagens.

Relembrando a última aula, de acordo com o fluxo de informações, e pensando em alavancar o uso da criptografia, considere:

- Projetos de design que estão sendo desenvolvidos nos computadores.
- Rede da empresa, que é utilizada para o trabalho colaborativo.
- Servidor de arquivos, que armazena os projetos.
- Sistemas de gestão, que armazenam informações operacionais.

Relembrando também as ameaças contra a cr14t1v3, há:

- *Crackers* invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações.
- Concorrentes invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações.
- Funcionários vazando informações sobre projetos da empresa.
- *Crackers* invadindo os sistemas de gestão para roubar, copiar ou alterar informações operacionais.

Os algoritmos criptográficos utilizados na cr14t1v3 podem ser de dois tipos:

1. Algoritmos de chave privada ou simétrica: as chaves são compartilhadas, o que dificulta a troca de chaves e possui baixa escalabilidade, já que para trocar mensagens distintas com 50 pessoas são necessárias 50 chaves privadas diferentes. São algoritmos que possuem bom desempenho computacional.
2. Algoritmos de chave pública ou assimétrica: as mensagens são cifradas com uma chave pública e decifradas com a chave privada correspondente. Não há os desafios de troca de chaves, porém o desempenho é pior, se comparado

com o algoritmo de chave privada.

3. Algoritmos de *hash*: as mensagens são calculadas unidirecionalmente, gerando um conjunto menor de informações (*hash*). Para verificação, o mesmo cálculo unidirecional é feito, e os *hashs* são comparados. Serão vistos na próxima aula.

4. Algoritmos de assinatura digital: as mensagens podem ter a origem verificada. Serão vistos na próxima aula.

Assim, o uso dos dois tipos de algoritmos criptográficos pode ocorrer da seguinte forma:

- *Crackers* invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações: algoritmos de chave privada para proteger as informações armazenadas. Uso de chave privada compartilhada. Para proteger a integridade, uso do *hash*.

- Concorrentes invadindo a rede, os computadores ou o servidor de arquivos para roubar projetos da empresa, podendo ainda alterar ou copiar essas informações: algoritmos de chave privada para proteger as informações armazenadas. Uso de chave privada compartilhada. Para proteger a integridade, uso do *hash*.

- Funcionários vazando informações sobre projetos da empresa: algoritmos de chave privada para proteger as informações armazenadas. Uso de chave privada compartilhada para proteção de confidencialidade. Uso de assinaturas digitais para verificar a origem da informação.

- *Crackers* invadindo os sistemas de gestão para roubar, copiar ou alterar informações operacionais. Algoritmos de chave privada para proteger as informações armazenadas. Uso de chave privada compartilhada para proteção de confidencialidade. Para proteger a integridade, uso do *hash*.

Atenção

Além de ser utilizado para sigilo e integridade das informações, a criptografia pode ainda ser utilizada para outras funções: assinatura digital, autenticidade, não repúdio, anonimato.

Avançando na prática

A criptografia pode fazer você perder seus dados

Descrição da situação-problema

Em um mundo digital como o atual, a vida das pessoas pode estar em um notebook. São fotos, áudios, vídeos, documentos e senhas que estão armazenadas no dispositivo pessoal.

Imagine o grande prejuízo no caso de perda do dispositivo. Imagine agora uma situação que tem atormentado muitas pessoas ao redor do mundo: o sequestro das informações do equipamento. Conhecido como *ransonware*, um *malware* utiliza a criptografia para tornar toda a informação da vítima indisponível. Com o *ransonware*, a vítima deve pagar para ter de volta sua vida digital. O *cracker* exige um pagamento, normalmente em *bitcoins* (moeda baseada em criptografia), para enviar a chave privada que decifra as informações.

Você sabe qual tipo de criptografia é utilizado pelos *ransonwares*? O que é possível fazer para ter de volta as informações que estão agora cifradas no dispositivo? Faça uma discussão "criptográfica" sobre os *ransomwares*.

Lembre-se

Um tipo de *malware* é o *ransomware*, que realiza um sequestro de informações da vítima, com a liberação da chave criptográfica de liberação das informações somente após o pagamento de um resgate. Um dos ransonwares é o *Locky*, que é discutido em Trend (2016).

TREND. **Novo *crypto-ransomware Locky* usa macros maliciosas do Word**. 2016. Disponível em: <http://blog.trendmicro.com.br/novo-cryptoransomware-locky-usa-macros-maliciosas-do-word/#.Vz9AQXarRD8>. Acesso em: 20 maio 2016.

Resolução da situação-problema

Os *ransonwares* utilizam dois tipos de criptografia – de chaves privadas e de chaves públicas. Um funcionamento típico é que uma chave simétrica (como do AES) é gerada no equipamento da vítima, que é utilizada para cifrar os dados. Essa chave pode ser protegida com a chave pública do *cracker*, o único que pode decifrar a chave AES com o uso da chave privada correspondente. Uma vez de posse da chave utilizada para a cifragem, o *cracker* revela a chave simétrica assim que o pagamento do resgate é realizado.

Não é viável tentar quebrar a chave privada utilizada para cifrar as informações da vítima, porém pode haver situações em que seja possível recuperá-las não explorando a criptografia, mas algumas características do sistema operacional, como os arquivos temporários.

Outra forma de recuperar as informações é restaurando os backups, se eles existirem. Nesse caso, é importante verificar a periodicidade das cópias de segurança, de modo que serão perdidas as informações geradas desde o último backup realizado.

Faça você mesmo

Faça uma pesquisa sobre os principais *ransomwares* que fazem vítimas por todo o mundo, analisando as informações sob o ponto de vista da criptografia.

Faça valer a pena

1. Alice quer enviar uma mensagem para Beto, que está em uma outra localidade. Sendo a mensagem de Alice bastante crítica, pode ela enviar a mensagem em claro? Por quê?

a) Sim, porque a mensagem é crítica.

b) Sim, porque a mensagem está em claro.

c) Sim, porque a mensagem usa criptografia.

d) Não, porque a mensagem pode ser interceptada.

e) Não, porque a mensagem irá para outra localidade.

2. Alice quer enviar uma mensagem para Beto, que está em uma outra localidade. Sendo a mensagem de Alice bastante crítica, ela resolve utilizar criptografia. Qual tipo de criptografia ela deve utilizar?

a) Nenhuma.

b) Criptografia de chave privada.

c) *Hash*.

d) Autenticação.

e) Esteganografia.

3. Alice quer enviar uma mensagem para Beto, que está em uma outra localidade. Sendo a mensagem de Alice bastante crítica, ela resolve utilizar criptografia. Qual tipo de criptografia ela deve utilizar?

a) Nenhuma.

b) Criptografia de chave pública.

c) *Hash*.

d) Autenticação.

e) Esteganografia.

Seção 3.3

Soluções de chave pública

Diálogo aberto

Olá!

Voltamos agora para avançarmos no entendimento da criptografia. Você já viu que há várias aplicações para a criptografia, e ela está no nosso dia a dia, seja na segurança de dados ou das comunicações. Você já viu também que há diferentes técnicas criptográficas, como a criptografia de chave privada e a criptografia de chave pública. Além disso, viu ainda que a esteganografia oculta a existência da própria mensagem.

Chegou agora a hora de explorarmos a criptografia de chave pública, que surgiu na década de 70 para solucionar um problema clássico da criptografia: a troca de chaves por um canal inseguro. É interessante que você conheça os principais algoritmos de chave pública, como o RSA e o Diffie-Hellman, que são utilizados em praticamente qualquer aplicação da internet, desde a segurança de arquivos até o acesso a websites.

Para exercitarmos os conceitos desta seção, vamos novamente à empresa cr14t1v3, que cria design de novos produtos para diferentes indústrias. Não se esqueça de que a empresa possui um data center local, que suporta os sistemas de gestão e também o servidor de arquivos, e estes são acessados por toda a equipe da cr14t1v3. Todos utilizam bastante a rede interna interligada para o trabalho colaborativo. Sua missão nesta aula é mostrar para o conselho administrativo da cr14t1v3 que a criptografia de chave pública é essencial para a empresa e, para tanto, você irá fazer as ligações necessárias entre as necessidades da cr14t1v3 e os algoritmos criptográficos estudados nesta aula.

Boa aula!

Não pode faltar

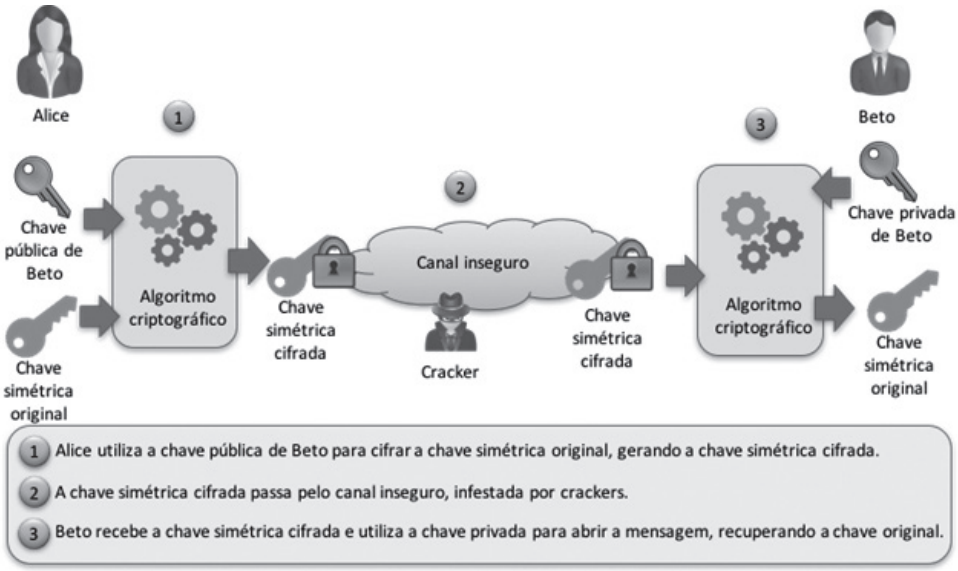
Criptografia de chave pública

Um dos desafios do uso da criptografia é o processo de troca de chaves. Na criptografia de chave privada ou simétrica, em que as chaves para cifragem e decifragem são as mesmas, a troca de chaves por um canal inseguro está sujeita ao ataque *man-in-the-middle*, no qual a chave pode ser capturada, o que faz com que a mensagem possa ser naturalmente aberta pelo inimigo (GOYA, 2006), (NAKAMURA; GEUS, 2007).

Já a criptografia de chave pública ou assimétrica utiliza um par de chaves (pública e privada), que são utilizadas em conjunto para a cifragem (com a chave pública) e decifragem (com a chave privada). Como a chave é pública, não há o problema de a chave ser capturada por *man-in-the-middle* como ocorre com a criptografia simétrica. O lado negativo, porém, está no poder de processamento necessário para a cifragem e decifragem, que é maior na criptografia assimétrica.

Dessa forma, é muito custoso o uso da criptografia de chave pública para proteger mensagens inteiras, e isso faz com que ela seja mais utilizada para a proteção da chave privada da criptografia simétrica que é, de fato, utilizada para proteger as mensagens. A Figura 3.4 mostra a criptografia de chave pública sendo utilizada para a troca de chave privada compartilhada entre Alice e Beto.

Figura 3.4 | Criptografia de chave pública sendo utilizada para a troca de chave privada compartilhada



Fonte: elaborada pelo autor.

Esse mecanismo de uso em conjunto da criptografia de chave pública com a criptografia de chave privada é bastante comum em várias aplicações, como é o caso do SSL (*Secure Sockets Layer*, para transmissões seguras), por exemplo, que iremos discutir com mais detalhes na próxima aula.

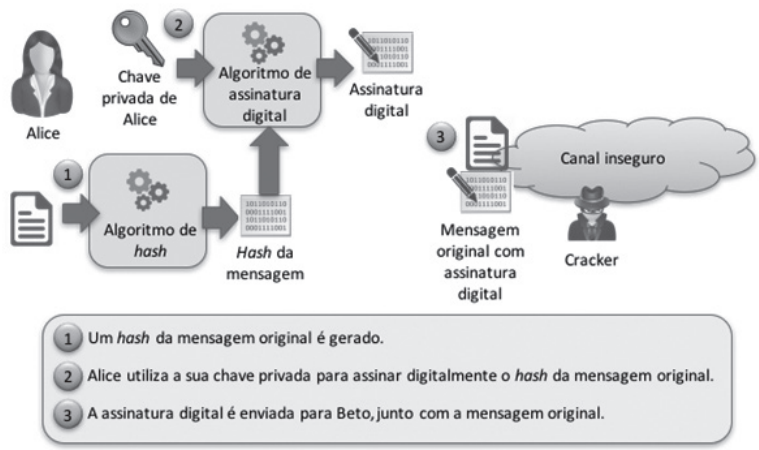
O início da criptografia de chave pública foi na década de 70, quando o pesquisador norte-americano Ralph Merkle divulgou um trabalho sobre distribuição de chaves públicas, o que fez com que Whitfield Diffie e Martin Hellman criassem, em 1976, um sistema de troca de chaves, o Diffie-Hellman.

Porém, antes do Diffie-Hellman, ainda na década de 70, os criptógrafos britânicos James H. Ellis, Clifford Cocks e Malcolm J. Williamson conceberam os principais mecanismos da criptografia de chave pública, que se tornaram públicas após a reclassificação como não confidencial pelo governo britânico em 1997 (SIMON, 2010).

Assinatura digital

Na criptografia de chave pública, a cifragem é realizada com o uso da chave pública do destinatário, enquanto a decifragem é realizada com o uso da chave privada correspondente. Para cada operação de cifragem-decifragem, há o uso de um par de chaves (pública e privada). O processo inverso, em que uma mensagem é "cifrada" com a chave privada, é o mecanismo utilizado para validar a origem de uma mensagem. O destinatário recebe a mensagem "cifrada" ou "assinada" pelo detentor da chave privada e utiliza a chave pública correspondente para realizar a validação da assinatura. Caso a validação não seja possível, a mensagem não foi originada no detentor real da chave privada. As Figuras 3.5 e 3.6 mostram esse processo, respectivamente, da assinatura digital e da verificação da assinatura.

Figura 3.5 | Alice assina digitalmente uma mensagem

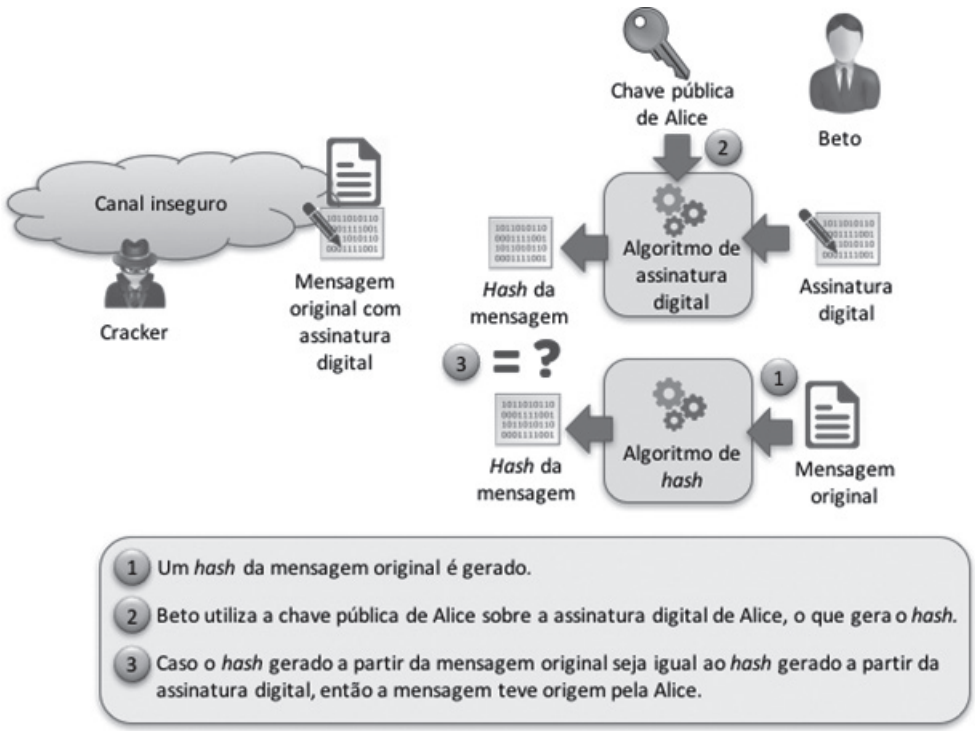


Fonte: elaborada pelo autor.

Na Figura 3.5, Alice utiliza sua chave privada para assinar a mensagem. A assinatura é realizada sobre um *hash* da mensagem, que é o resultado de um cálculo matemático em uma via (não é possível a reversão, ou seja, não é possível chegar à mensagem original a partir de um *hash*). O que é enviado ao destinatário é a mensagem original, juntamente com a assinatura digital, um algoritmo que é aplicado sobre o *hash* da mensagem original.

Na Figura 3.6, Beto realiza o processo de verificação da assinatura digital, a partir da mensagem original e da assinatura digital recebidas. Beto utiliza a chave pública de Alice sobre a assinatura digital para chegar ao *hash*, realizando a "decifragem" correspondente ao uso da chave privada por Alice. Ao mesmo tempo, Beto gera um *hash* da mensagem recebida. Caso os dois *hashes* obtidos sejam iguais, então a mensagem realmente veio de Alice.

Figura 3.6 | Beto verifica a assinatura digital de Alice



Fonte: elaborada pelo autor.

Assim, há duas funções principais para a criptografia de chave pública:

- Garantia de confidencialidade, com cifragem de mensagem utilizando a chave pública do destinatário. Somente o destinatário pode decifrar a mensagem, com a sua chave privada correspondente.

- Garantia de integridade e autenticidade com a assinatura digital, que utiliza a chave privada para cifrar uma mensagem (*hash*); esta só pode ser decifrada com a chave pública do originador da mensagem. Caso o *hash* decifrado seja o mesmo, a mensagem está íntegra, e essa verificação só poderá ser feita com a decifragem usando a chave pública do remetente.

Reflita

Você acha que a técnica de assinaturas digitais pode ser burlada?

Um cenário que pode ocorrer no uso de assinatura digital é que um impostor pode se passar por uma outra pessoa, divulgando uma chave pública fraudulenta em seu lugar. A vítima usaria a chave pública do impostor, acreditando ser da pessoa legítima. Com a divulgação fraudulenta, a vítima pode cifrar a mensagem com a chave pública falsa do impostor, de modo que o fraudador pode capturar essa mensagem e decifrar a original com o uso da chave privada fraudulenta correspondente. Nesse caso, o real destinatário pode nem mesmo receber a mensagem que seria destinada a ele.

Pesquise mais

Para resolver o cenário de chaves públicas fraudulentas, os certificados digitais estabelecem uma relação de confiança a partir das autoridades certificadoras, que são as responsáveis pela divulgação das chaves públicas de todos os usuários. Veja mais sobre o assunto em Ofício (2016).

OFÍCIO ELETRÔNICO. **O que é certificado digital?** 2016. Disponível em: <https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf>. Acesso em: 14 jul. 2016.

Diffie-Hellman

O Diffie-Hellman, criado em 1976 por Whitfield Diffie e Martin Hellman, foi o primeiro método criptográfico para troca de chaves; este permite que duas entidades que não possuem conhecimento prévio uma da outra possam compartilhar uma chave secreta mesmo com o uso de um canal inseguro.

Matematicamente, o Diffie-Hellman utiliza o cálculo de logaritmos discretos em um campo infinito para gerar e estabelecer uma chave secreta compartilhada, a partir de uma informação prévia comum que não é crítica, no caso de ser comprometida.

Os passos gerais são:

- Um número (n1) é compartilhado por Alice e Beto, o qual pode ser capturado por um terceiro.
- Alice e Beto escolhem, cada um, um número que não é compartilhado com ninguém. Alice escolhe n2 e Beto escolhe n3.
- Alice e Beto realizam, cada um, um cálculo entre n1, que é compartilhado entre eles, n2 e n3, respectivamente. São gerados assim n4 e n5.
- Alice e Beto trocam entre si os números n4 e n5, que são números gerados a partir dos cálculos entre n1, que é compartilhado entre ambos, e n2 e n3, que são números privados de Alice e Beto, respectivamente. Os números n4 e n5 são irreversíveis para n2 e n3, que são os números privados e secretos.
- Alice e Beto fazem um cálculo, respectivamente, entre n2 e n5, e entre n3 e n4, o que gera uma chave n6, que é comum aos dois.
- O número n6 é a chave comum, secreta e compartilhada, que é utilizada na comunicação segura.

Assimile

Com o Diffie-Hellman, uma chave secreta compartilhada é gerada pelas entidades, sem que sejam transmitidas em um canal de comunicação.

Pesquise mais

Veja como o Diffie-Hellman funciona em detalhes, incluindo todos os cálculos matemáticos realizados em Marques (2013).

MARQUES, Thiago Valentim. **Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula**. Dissertação de Mestrado. João Pessoa: UFPB, 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/281/2011_00133_THIAGO_VALENTIM_MARQUES.pdf?sequence=1>. Acesso em: 14 jul. 2016.

RSA

Os pesquisadores do MIT, Ron Rivest, Adi Shamir e Leonard Adleman, publicaram o algoritmo RSA em 1978, com o uso de exponenciação modular do produto de dois números primos muito grandes para cifragem e decifragem, além da assinatura digital.

O algoritmo RSA é composto por 3 partes:

1. Geração de chaves pública e privada.
2. Cifragem.
3. Decifragem.

De uma forma bastante geral, a geração das chaves pública e privada é feita a partir de dois números primos, que passam por uma série de cálculos até que se chegue às chaves pública e privada.

A quebra da chave privada, que é utilizada na decifragem, é considerada improvável, já que não há algoritmos eficientes para realizar a operação matemática envolvida, uma fatoração de inteiros em fatores primos, principalmente quando o número de algarismos é 100 ou maior. O tempo de cifragem de uma mensagem é desprezível, porém o tempo de decifragem pode tornar o processo inviável (SILVA, 2006).

Pesquise mais

Detalhes do algoritmo RSA, com todas as suas operações matemáticas que são realizadas para a geração das chaves, cifragem e decifragem, podem ser vistas em Silva (2006)

SILVA, Elen Viviani Pereira da. **Introdução à Criptografia RSA**. Monografia. Ilha Solteira: UNESP, 2006. Disponível em <http://www.impa.br/opencms/pt/eventos/downloads/jornadas_2006/trabalhos/jornadas_elen_pereira.pdf>. 2006. Acesso em: 14 jul. 2016.

Key escrow

A custódia de chaves, caução de chaves, ou *key escrow* faz com que cópias de chaves criptográficas existam para o acesso a informações cifradas no caso de ordens judiciais, por exemplo. A justiça, nesse caso, seria um custodiante e teria uma cópia das chaves para acessar as informações em caso de necessidade.

Exemplificando

No caso de necessidade de acesso a dados de um sistema ou dispositivo capturado de um terrorista após um ataque, como seria possível o acesso? Isso ocorreu de fato no ataque terrorista de 2015 em San Bernardino, Estados Unidos. O FBI procurou analisar os dados do dispositivo móvel que era do terrorista. Porém, sem o *key escrow*, outros caminhos tiveram que ser seguidos. Com criptografia de senha única, como é o caso dos dispositivos da Apple, era necessário criar uma nova versão do sistema operacional iOS para que a senha pudesse ser descoberta por força bruta (VENTURA, 2016). A Apple se negou a criar uma versão do sistema operacional que permitia esse tipo de ataque e o FBI alega que conseguiu descobrir a senha do dispositivo (que dava acesso à chave privada) por meio de técnicas ainda não confirmadas que possibilitaram o ataque de força bruta (PRADO, 2016).

VENTURA, Felipe. **Por que a Apple está lutando contra o FBI para não criar brechas de criptografia**. 2016. Disponívelem: <http://gizmodo.uol.com.br/apple-contra-fbi-criptografia/>. Acessoem: 10 jul. 2016.

PRADO, Jean. **FBI conseguiu acessar os dados de um *iPhone* sem ajuda da Apple. Estamos perdidos?** 2016. <https://tecnoblog.net/193403/fbiiphone-criptografia-quebrada/>. Acesso em: 10 jul. 2016.

Reflita

Há outra função similar, que é a de recuperação de chaves. Imagine que o presidente de sua empresa sofra um incidente que torne impossível o acesso às informações da empresa. Nesse caso, um mecanismo de backup e recuperação de chaves pode ser utilizado pela empresa, que seria ativado em caso de necessidades.

Com o uso do *key escrow*, o sistema criptográfico cria múltiplas chaves que dão acesso às informações. No caso citado anteriormente, o FBI, por exemplo, poderia ter uma das chaves múltiplas, que daria o acesso às informações, quando necessário (SCHAUL, 2015). De posse da chave, o FBI seria um custodiante da chave.

Há ainda outra técnica de chave compartilhada que faria com que duas entidades tivessem, cada uma, parte de uma chave para o acesso às informações. Nesse caso, a Apple poderia ter uma parte da chave, e o FBI outra parte. A informação seria acessada no momento em que as duas partes das chaves fossem utilizadas em conjunto (SCHAUL, 2015).

Sem medo de errar

Na cr14t1v3, que cria design de novos produtos para diferentes indústrias, há um data center local, o qual suporta os sistemas de gestão e também o servidor de arquivos, que são acessados por toda a equipe da cr14t1v3. Todos utilizam bastante a rede interna interligada para o trabalho colaborativo. Como utilizar a criptografia de chave pública na cr14t1v3?

A criptografia assimétrica ou de chave pública pode ser utilizada pela cr14t1v3 para duas funções principais:

- Assinatura digital, de modo a controlar a origem dos projetos criados, bem como para garantir a integridade. Para tanto, cada especialista da cr14t1v3 pode utilizar sua chave privada para assinar digitalmente seus projetos desenvolvidos.
- Troca de mensagens entre os funcionários de forma segura, com o uso de criptografia de chave pública, em que são utilizadas as chaves públicas de cada destinatário, que conseguem ler as mensagens com o uso das chaves privadas correspondentes.

Atenção

Uma das grandes vantagens da criptografia de chave pública é o compartilhamento de chaves, que é facilitado quando há a troca de informações entre várias pessoas. Para tanto, basta utilizar a chave pública correspondente do destinatário.

Avançando na prática

Certificados digitais

Descrição da situação-problema

Uma das aplicações de criptografia de chave pública são os certificados digitais. Os certificados digitais são representações de chaves públicas que contam com as confiáveis autoridades certificadoras (*Certificate Authority*, CA) para divulgação das chaves públicas, o que evita o uso de chaves públicas fraudulentas. Para verificar se determinado certificado digital é válido, o destinatário verifica a assinatura digital do certificado digital, realizado pela autoridade certificadora.

Explique com os conceitos vistos na aula o processo de assinatura digital do

certificado digital, feito pela autoridade certificadora, e também o da verificação da validade do certificado digital, que foi assinado pela autoridade certificadora. Pense em Maria enviando uma mensagem para João.

Lembre-se

A criptografia de chave pública utiliza um par de chaves, a pública e a privada, que executam operações inversas para chegarem às mensagens: Uso da chave pública para cifragem e conferência de assinatura e uso da chave privada para decifragem, e vice-versa.

Resolução da situação-problema

A autoridade certificadora assina o certificado digital de João, que é o destinatário. Maria então obtém o certificado digital de João e deve realizar a verificação junto à autoridade certificadora.

A autoridade certificadora assina digitalmente o certificado digital de João. Essa assinatura digital é feita com a autoridade certificadora utilizando sua chave privada para assiná-lo.

Maria, de posse do certificado digital de João, verifica a sua validade junto à autoridade certificadora. Para tanto, utiliza a chave pública da autoridade certificadora para verificar se a assinatura digital do certificado digital de João é válida.

Caso esteja tudo certo, Maria utiliza o certificado digital de João para cifrar a mensagem, que chega a João. Este então abre a mensagem utilizando a chave privada correspondente, que somente ele possui.

Faça você mesmo

Expanda o exercício explorando a aplicação do *hash*, nos moldes do que foi discutido durante a aula.

Faça valer a pena

1. Qual tipo de criptografia utiliza uma chave secreta compartilhada, também conhecida como chave privada?

a) Esteganografia.

b) *Firewall*.

c) Criptografia de chave pública.

d) Criptografia de chave privada.

e) Criptografia de chave compartilhada.

2. Qual tipo de criptografia utiliza um par de chaves para as operações de cifragem e decifragem?

a) Esteganografia.

b) Firewall.

c) Criptografia de chave pública.

d) Criptografia de chave privada.

e) Criptografia de chave compartilhada.

3. A criptografia de chave pública é bastante utilizada em nosso dia a dia, principalmente para resolver um dos principais problemas existentes na internet. Qual seria este problema?

a) Não há problemas na internet.

b) Ataques de DoS.

c) Troca de chaves.

d) Ataques a servidores.

e) Autenticação.

Seção 3.4

Aplicações de criptografia

Diálogo aberto

Olá!

Já vimos os principais conceitos de criptografia, analisamos as diferenças entre as criptografias de chave privada e de chave pública, discutimos assinaturas digitais e agora vamos para as situações em que a tecnologia é utilizada.

Iremos ver que, de fato, a criptografia está em nosso dia a dia. Nesta aula iremos trazer a criptografia para mais perto, e você irá se surpreender com o fato de nem precisarmos saber o quanto utilizamos os algoritmos de criptografia já discutidos. Para não acreditarmos cegamente que a criptografia salva tudo, veremos também alguns casos importantes de incidentes de segurança envolvendo a criptografia.

Você irá encontrar a criptografia no seu computador, no seu dispositivo móvel, na comunicação pessoal com seus amigos, no acesso remoto para sua empresa, nas transações financeiras e nas compras que você faz pela internet. Vamos aproveitar e discutir esses pontos durante esta aula.

Para consolidar mais uma vez os temas discutidos, pense na empresa que desenvolve projetos de design de novos produtos para diferentes indústrias, a cr14t1v3. No trabalho colaborativo entre a equipe de estrelas composta por cerca de 15 artistas, há o uso de sistemas de gestão, ferramentas colaborativas e um servidor de arquivos. Sua tarefa nesta aula é de determinar quais aplicações de criptografia podem ser utilizadas pela cr14t1v3. Lembre-se de que entre os projetos desenvolvidos pela empresa estão a criação de um modelo de supercarro esportivo para uma montadora húngara e a criação do design de uma batedeira de luxo para um fabricante uruguaio.

Boa aula!

Não pode faltar

Aplicações de criptografia

Os diferentes tipos de criptografia, em especial as de chave privada e de chave pública, possibilitam o estabelecimento de um mundo mais seguro com as suas diferentes implementações em variadas aplicações.

Exemplificando

A força da criptografia é tão grande que ela é considerada um dos tipos de algoritmo que dominam o nosso mundo (ROCHA, 2014).

De acordo com o que foi visto nas aulas anteriores, a criptografia pode ser utilizada em uma série de aplicações, tais como:

- Proteção da comunicação: autenticação de entidades, integridade e confidencialidade em mensagens pessoais como os do aplicativo *WhatsApp*, em comunicação de voz como o do *Skype*, em e-mails com o uso de sistemas como o PGP ou em acesso remoto por VPN.
- Proteção de dados armazenados: confidencialidade de dados em dispositivos móveis, em notebooks e desktops diretamente pelo sistema operacional, por sistema específico ou na nuvem.
- Proteção de transações: autenticação de entidades, integridade e confidencialidade no uso de cartões, em transações bancárias, em compras on-line.

Reflita

Além dessas aplicações, a criptografia também possui um uso que vai para o lado negro, o terrorismo. A criptografia é uma das armas utilizadas pelo Estado Islâmico (GÓMEZ, 2015).

Criptografia para proteção de comunicações

O mundo é regido pela comunicação, que precisa ser protegida, em todos os seus níveis. Cada método de comunicação pode aplicar a criptografia para proteger a origem, a integridade e a confidencialidade.

As mensagens instantâneas, como o aplicativo para dispositivos móveis *WhatsApp* e o *Messenger* do *Facebook*, são um tipo de comunicação que aplica a criptografia. Outras comunicações que também aplicam a criptografia são a voz (como o *Skype*) e os *e-mails*. Para as empresas, as redes privadas virtuais (VPN, *Virtual Private Network*) são fundamentais para a comunicação segura.

No caso do *WhatsApp*, a criptografia utilizada é ponta a ponta, ou seja, entre os dispositivos que estão trocando as mensagens. Com esse tipo de criptografia, somente quem está conversando possui a chave para ler a mensagem (WHATSPAPP, 2016). Tudo é feito de uma forma transparente para o usuário, não sendo possível desabilitá-la.

Pesquise mais

Veja mais sobre a criptografia aplicada pelo aplicativo *WhatsApp* em (WHATSAPP, 2016).

WHATSAPP. **Perguntas frequentes**. Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 18 jul. 2016.

Outro aplicativo para troca de mensagens, o *Messenger* do *Facebook*, passou a adotar em julho de 2016 a criptografia ponta a ponta, já utilizada pelo *WhatsApp*, que também é de propriedade do *Facebook*. A implementação, porém, é diferente. Enquanto no *WhatsApp* toda a comunicação é cifrada com a criação de uma camada adicional de criptografia, no *Messenger* do *Facebook* a cifragem é feita especificamente em uma conversação, que depende da sessão e do dispositivo que está sendo utilizado para a comunicação (G1, 2016).

Pesquise mais

Veja mais sobre a criptografia aplicada pelo *Messenger* do *Facebook* em (G1, 2016).

G1. ***Facebook* libera criptografia de ponta a ponta em chats do '*Messenger*'**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/facebook-libera-criptografia-de-ponta-ponta-em-chats-do-messenger.html>. jul. Acesso em: 18 jul. 2016.

O *Skype* também aplica a criptografia para as comunicações de voz e também para a troca de mensagens, com uso tanto da criptografia de chaves privadas (algoritmo AES de 256 bits) quanto da criptografia de chaves públicas (algoritmo RSA de 1536 ou 2048 bits) (SKYPE, 2016).

Assimile

Com a criptografia ponta a ponta, toda a comunicação fica protegida em sua transmissão, não sendo possível o "grampo", pois as chaves só são conhecidas pelas duas pontas (origem e destino). Uma forma de quebrar o sigilo dessa comunicação protegida pela criptografia ponta a ponta é atacando um dos dispositivos da ponta.

Já no caso de e-mails, os baseados na nuvem, como o *Gmail* ou o *Yahoo!*, a criptografia é aplicada na camada de transporte, normalmente com o uso do protocolo TLS (*Transport Layer Security*), que é utilizado para proteger o tráfego HTTP (*HyperText Transfer Protocol*), pelo HTTPS (*HyperText Transfer Protocol Secure*). Os protocolos TLS, HTTPS e o SSL (*Secure Sockets Layer*) serão discutidos mais adiante nesta aula.

Outra aplicação importante de criptografia para as comunicações é a rede privada virtual ou VPN (*Virtual Private Network*). A VPN possibilita, com a aplicação da criptografia, que entidades em uma rede pública ou compartilhada acessem uma rede privada como se estivessem nela. O acesso pode ser individual, como no caso de um acesso remoto, ou pode ser de uma rede para outra (*gateway-to-gateway VPN*) (NAKAMURA & GEUS, 2007). A criptografia possibilita o tunelamento das comunicações, por exemplo o uso de protocolos como IPSec ou TLS.

Pesquise mais

Uma VPN, porém, não é baseada exclusivamente em criptografia, como é o caso do MPLS (*Multi-Protocol Label Switching*) ou do L2TP (*Layer 2 Tunnelling Protocol*), que são utilizados em provedores de rede que protegem o tráfego em uma outra camada. Conheça mais sobre VPN no Capítulo 10 de Nakamura e Geus (2007).

NAKAMURA, Emilio T., GEUS, Paulo L de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec. 2007.

Criptografia para proteção de dados armazenados

Já vimos como a criptografia pode ser utilizada para informações que estão em transmissão e a necessidade de proteger os dados que são armazenados em dispositivos móveis, em desktops e notebooks, em servidores ou na nuvem.

Como na proteção das comunicações, a proteção de dados armazenados pode ser feita em diferentes níveis. Há desde mecanismos no próprio sistema operacional até sistemas próprios que aplicam a criptografia.

Em sistemas *Windows*, por exemplo, é possível aplicar a criptografia em arquivos específicos ou em todo o sistema de arquivos com o BitLocker.

Pesquise mais

Veja como a Apple implementa a criptografia em seus dispositivos móveis em Apple (2011).

Apple. **Visão geral sobre a segurança**. Disponível em: <http://www.apple.com/br/ipad/business/docs/iOS_Security.pdf>. Acesso em: 24 jul. 2016.

Além da proteção que pode ser utilizada diretamente do sistema operacional (é transparente e habilitado por padrão para o caso do iOS, sistema operacional para dispositivos móveis da Apple (APPLE, 2011)), há softwares que podem ser utilizados especificamente para a criptografia de dados.

Exemplificando

O software *VeraCrypt* é uma das alternativas para criptografia de disco. Ele foi baseado no *TrueCrypt*, outro *software* bastante utilizado, mas que foi descontinuado. O *VeraCrypt* pode ser encontrado em CodePlex (2016).

CODEPLEX. Disponível em: <https://veracrypt.codeplex.com>. Acesso em: 24 jul. 2016.

Criptografia para proteção de transações

Outra aplicação importante da criptografia é para a proteção de transações, que estão presentes em várias situações do nosso cotidiano on-line. Quando realizamos uma compra pela internet, por exemplo, temos que ter a tranquilidade de saber que o número do cartão de crédito está sendo transferido de uma forma segura até a loja. Além disso, uma vez que a transferência dos dados de cartão foi feita de uma forma segura, esses dados devem estar protegidos no servidor da loja virtual.

Reflita

Se a criptografia é utilizada em compras on-line, porque há ataques e fraudes que levam consumidores e lojas a prejuízos?

O caso de uso da criptografia em compras on-line ilustra bem o fato de que a criptografia é um dos controles de segurança da informação e de redes que podem e devem ser utilizados, não devendo ser o único.

Pesquise mais

É interessante conhecer os requisitos de segurança para a proteção de dados de cartões. Os requisitos 3 e 4 do padrão PCI DSS (*Payment Card Industry Data Security Standard*) (PCI, 2013), por exemplo, especificam o uso da criptografia.

PCI Security Standards Council. **Padrão de Segurança de Dados**. 2013. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/PCI_DSS_v3.pdf>. Acesso em: 24 jul.2016.

Os protocolos de segurança para transações mais utilizados, também pelos bancos, para o transporte seguro dos dados são SSL (*Secure Sockets Layer*), TLS (*Transport Layer Security*) e HTTPS (*HyperText Transfer Protocol Secure*). Esse conjunto de protocolos é utilizado para transações web com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a confidencialidade, eles podem visar também à integridade dos dados e à autenticidade das partes.

Para o entendimento básico das diferenças entre SSL, TLS e HTTPS, o SSL evoluiu para o TLS, de modo que o SSL 3.1 é o TLS 1.0. Já o HTTPS é o HTTP dentro do SSL/TLS. O túnel bidirecional do HTTP é criado entre duas entidades e, quando esse túnel é seguro por uma conexão SSL/TLS, então o conjunto é conhecido como HTTPS. No HTTPS, a conexão SSL/TLS é estabelecida antes, e os dados HTTP são trocados sobre essa conexão SSL/TLS.

Pesquise mais

O site SSL Pulse (SSL, 2016) está em inglês, mas provê alguns indicadores interessantes sobre o acesso seguro a websites. Em julho de 2016, 59,5% dos sites testados apresentavam segurança inadequada. 10,1% utilizavam cifras inadequadas (menores do que 128 bits), enquanto o uso da criptografia de chaves públicas estava adequado (chaves iguais ou maiores do que 2048 bits). 30,5% dos sites ainda utilizavam o SSL v2.0 e v3.0, reconhecidamente vulneráveis.

SSL Pulse. **Survey of the SSL Implementation of the Most Popular Web Sites**. 2016. Disponível em: <https://www.trustworthyinternet.org/ssl-pulse/>. Acesso em: 14 jul. 2016.

Incidentes de segurança envolvendo criptografia

Nos últimos anos o protocolo SSL foi alvo de diferentes ataques, o que culminou na recomendação pela não utilização do SSL e na expansão do uso da nova versão do TLS. Esses protocolos usam um conjunto de algoritmos criptográficos, e a forma como alguns deles eram utilizados continham vulnerabilidades que comprometiam a segurança do canal seguro (FERREIRA, 2014).

Uma grave vulnerabilidade baseada no algoritmo criptográfico RC4 implementado no protocolo WEP (*Wired Equivalent Privacy*) utilizado em redes Wi-Fi foi publicada (LINHARES; GONÇALVES, 2005).

Já em 2016, foi descoberto um problema com os processadores *Qualcomm Snapdragon*, utilizado em dispositivos *Android*. No sistema FDE (*Full Disk Encryption*) do Android, uma chave mestra de 128 bits e um salt de 128 bits são criados aleatoriamente. A chave mestra, também conhecida como DEK (*Device Encryption Key*), é protegida com criptografia baseada em credenciais do usuário, que pode ser um PIN, uma senha ou um padrão, armazenadas no dispositivo. O *Android* utiliza o *KeyMaster* para ligar o DEK com o hardware da *Qualcomm*, em uma área considerada segura, o TEE (*Trusted Execution Environment*), que armazena e executa as funções criptográficas. O responsável pela implementação do *KeyMaster* é o fabricante de hardware, no caso a *Qualcomm*, em que o TEE é chamado de QSEE (*Qualcomm Secure Execution Environment*). O QSEE permite que alguns aplicativos, chamados de "*Trustlets*", rodem no ambiente seguro, como é o caso do *KeyMaster*. O problema é que é possível explorar uma vulnerabilidade do *Android* para trocar aplicativos do QSEE, o que pode levar à escalada de privilégios, ao sequestro de todo o espaço, o que pode resultar no acesso às chaves criptográficas, que por sua vez são protegidas nas credenciais do usuário. De posse dessas chaves, é possível realizar ataques de força bruta, já que os mecanismos de segurança do sistema operacional passam a ser driblados (como a remoção dos dados após um determinado número de tentativas erradas de entrada de credenciais do usuário) (OSBORNE, 2016).

Novas frentes em criptografia

O foco das aulas foi em criptografia de chave privada e criptografia de chave pública. O mundo da criptografia, porém, vai além, com conceitos que abordam de uma forma diferente a proteção dos dados.

A criptografia baseada em identidade (IBE, *Identity-Based Encryption*), por exemplo, é uma dessas abordagens. Em 1984, Adi Shamir propôs um sistema de autenticação de chaves no qual uma chave pública pode ser derivada a partir de informações da identidade do usuário. Em 2001, Dan Boneh e Matt Franklin implementaram um IBE baseado em curvas elípticas e em construção matemática conhecida como Weil

Pairing. No mesmo ano, Clifford Cocks descreveu outra solução IBE baseada em resíduos quadráticos em grupos compostos (SILVEIRA, 2013).

O IBE foi originalmente construído para simplificar o gerenciamento de certificados em sistemas de e-mail, de forma que não fosse mais necessário que o destinatário publicasse sua chave pública. No IBE há uma entidade externa, o gerador de chave privada (PKG, *Private Key Generator*), que gera a chave privada para a leitura das mensagens recebidas. Há a vantagem da chave pública ser o próprio endereço de e-mail, nesse caso. Porém, como a chave privada é gerada no PKG, há o *key escrow*.

Pesquise mais

A criptografia baseada em identidade é discutida em detalhes em Silveira (2013).

SILVEIRA, João Pedro Cipriano. **Aplicações de Criptografia Baseada em Identidade com Cartões de Identificação Eletrônica**. Disponível em: <https://ubibliorum.ubi.pt/bitstream/10400.6/1931/1/Disserta%C3%A7%C3%A3o.pdf>. Acesso em: 14 jul. 2016.

Além do IBE, a criptografia leve utiliza algoritmos de criptografia adaptados para funcionarem em ambientes restritos, com pouca memória, processamento e armazenamento, como os elementos da internet das coisas (MACEDO, 2016).

Já a criptografia homomórfica possibilita que os dados cifrados sejam processados diretamente, sem a necessidade de decifragem anterior ao seu uso (PAIVA, 2015).

E a criptografia quântica é baseada na mecânica quântica, possuindo assim propriedades diferentes da criptografia tradicional (de chave pública e de chave privada) que a tornam mais segura (UNO; FALEIROS, 2016).

Sem medo de errar

A cr14t1v3 possui um alto grau de dependência de criptografia para proteger o seu negócio.

O trabalho colaborativo requer comunicação segura com o uso de aplicações que utilizam a criptografia ponta a ponta. Uma alternativa, ou melhor, um mecanismo adicional é o uso de HTTPS com TLS em aplicações Web utilizados para comunicação e colaboração entre os funcionários.

Além disso, como um nível de proteção complementar, o tunelamento VPN deve ser disponibilizado quando o acesso remoto é permitido.

As informações dos sistemas de gestão também devem ser protegidas com criptografia em dois pontos fundamentais: na comunicação entre o usuário e o servidor e nos dados armazenados no servidor.

Já o servidor de arquivos da cr14t1v3 deve aplicar a criptografia para impedir o vazamento das informações de projetos.

Os dados que residem nos dispositivos móveis, notebooks e desktops dos funcionários da cr14t1v3 também devem ser protegidos. Caso os sistemas operacionais desses dispositivos não façam a proteção de uma forma transparente, é recomendável a escolha de uma aplicação específica de cifragem, como o *VeraCrypt*.

Atenção

A aplicação de criptografia deve levar em consideração a forma como as chaves criptográficas são geradas, armazenadas e utilizadas. Em alguns dispositivos móveis, por exemplo, o usuário não precisa memoriar uma chave adicional, já que toda a cadeia de chaves criptográficas é gerada e utilizada a partir do método de destravamento do próprio dispositivo.

Avançando na prática

Criptografia para acesso remoto

Descrição da situação-problema

O acesso remoto aumenta a produtividade das empresas e reduz custos operacionais. Porém, caso não seja disponibilizado de uma forma segura, o efeito será inverso, a produtividade irá para o espaço com os retrabalhos. Podem surgir com os ataques cibernéticos, e os custos operacionais também podem disparar com a necessidade de restabelecer o negócio após um incidente de segurança.

Com foco em criptografia, elabore uma estratégia de segurança para disponibilizar um acesso remoto o mais seguro possível, pensando que a empresa trabalha com informações críticas do mercado financeiro.

Lembre-se

A criptografia pode ser utilizada para proteger as informações que estão armazenadas ou em transmissão.

Resolução da situação-problema

Com foco em criptografia e pensando nas informações mais críticas possíveis, o acesso remoto pode seguir a seguinte estratégia:

- Uso de certificados digitais para todos os usuários.
- Autenticação de dois fatores.
- Estabelecimento de canal seguro entre o dispositivo do usuário e o servidor VPN com garantia de integridade, autenticação e confidencialidade.
- Uso de aplicações específicas com camada adicional de segurança com TLS.
- Protocolo adicional nas aplicações com o estabelecimento de chave de sessão única para cada acesso.
- Servidor com cifragem dos dados acessados pela VPN;
- Dispositivos dos funcionários remotos com criptografia de armazenamento.

Faça você mesmo

Imagine que você trabalha em uma empresa que fechou uma parceria para desenvolver um projeto estratégico para um determinado cliente militar. Como você faria para proteger os diferentes tipos de informações geradas durante o projeto, seja na sua empresa ou na empresa parceira, que devem ser compartilhadas o tempo todo?

Faça valer a pena

1. A criptografia pode ser aplicada para várias situações. Assinale a alternativa que ilustra uma dessas situações.

a) Proteção contra ataques de negação de serviços.

b) Proteção contra acessos físicos.

c) Proteção contra ataques de força bruta.

d) Proteção contra alteração de dados.

e) Proteção contra ataque de rede.

2. Uma das aplicações mais utilizadas da criptografia é para proteger as comunicações. Assinale a alternativa que apresenta um protocolo de segurança utilizado para essa aplicação da criptografia.

a) FTP.

b) *Web*.

c) *Firewall*.

d) SSL.

e) Chave privada.

3. Uma das aplicações mais utilizadas da criptografia é para proteger os dados armazenados. Assinale a alternativa que representa essa aplicação da criptografia.

a) Cifragem de disco.

b) *Web*.

c) *Firewall*.

d) SSL.

e) Chave privada.

Referências

APPLE. **Visão geral da segurança e privacidade do iCloud**. 2016. Disponível em: <https://support.apple.com/pt-br/HT202303>. Acesso em: 15 jun. 2016.

COSTA, Camilla. **Quatro coisas que mudam com a criptografia no *WhatsApp* – e por que ela gera polêmica**. 2016. Disponível em <http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc>. Acesso em: 15 jun. 2016.

FERREIRA, Marcos. **Tipos de ataques aos protocolos SSL/TLS**. 2014. Disponível em: <https://www.trustsign.com.br/blog/tipos-de-ataques-aos-protocolos-ssltls/index.html>. Acesso em: 24 jul. 2016.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e matemática**. 2010. Disponível em: <http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf>. Acesso em: 16 jun. 2016.

GÓMEZ, Luis. Criptografia é a nova arma do **El País** 2015. Disponível em: <http://brasil.elpais.com/brasil/2015/12/22/internacional/1450801344_367770.html>. Acesso em: 10 jul. 2016.

GOYA, Denise Hideko. **Proposta de Esquemas de Criptografia e de Assinatura sob Modelo de Criptografia de Chave Pública sem Certificado**. 2006. Disponível em: <http://www.ime.usp.br/~dhgoya/dis_denise.pdf>. Acesso em: 10 jun. 2016.

KATZ, Jonathan; LINDELL, Yehuda Lindell. **Introduction to Modern Cryptography**. 1 edition. [S.l.]: Chapman and Hall/CRC, August 2007.

KESSLER, Gary C. **An Overview of Cryptography**. 2016. Disponível em: <http://www.garykessler.net/library/crypto.html>. Acesso em: 14 jul. 2016.

KWAN, Matthew. **The Gifshuffle home page**. Disponível em: <http://www.darkside.com.au/gifshuffle/>. Acesso em: 27 jun. 2016.

LINHARES, André Guedes, GONÇALVES, Paulo André da. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf>. Acesso em: 24 jul. 2016.

MACEDO, Henrique. **Algoritmos de criptografia leve**. Disponível em: <http://calhau.dca.fee.unicamp.br/wiki/images/8/84/Algoritmos_de_Criptografia_Leve_v1.pdf>. Acesso em: 24 jul. 2016.

MATSUKI, Edgard. **Entenda o que é a criptografia de ponta a ponta, utilizada pelo *WhatsApp***. 2016. Disponível em <http://www.ebc.com.br/tecnologia/2016/04/entenda-o-que-e-criptografia-de-ponta-ponta-utilizada-pelo-whatsapp>. Acesso em: 15 jun. 2016.

MARQUES, Thiago Valentim. **Criptografia**: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/281/2011_00133_THIAGO_VALENTIM_MARQUES.pdf?sequence=1>. Acesso em: 14 jul. 2016.

MEDEIROS, Flávio. **Uma breve história sobre criptografia**. 2015. Disponível em: <https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/>. Acesso em: 26 jun. 2016.

MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. **Handbook of applied criptography**. 2001. Disponível em: <http://cacr.uwaterloo.ca/hac/>. Acesso em: 26 jun. 2016.

NAKAMURA, Emilio T.; GEUS, Paulo L de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

NASCIMENTO, Anderson Clayton do. **Criptografia e infraestrutura de chaves públicas**. 2011. Disponível em: <http://home.ufam.edu.br/regina_silva/CEGSIC/Textos%20Base/Criptografia_e_ICP.pdf>. Acesso em: 26 jun. 2016.

NOMIYA, Diogo Ventura. **DES e AES**. <http://www.gta.ufrj.br/grad/10_1/aes/index_files/Page604.htm>. Acesso em: 16 jun. 2016.

OSBORNE, Charlie. How to crack Android encryption on millions of smartphones. **ZDNet .**2016. <http://www.zdnet.com/article/how-to-crack-android-encryption-onmillions-of-smartphones/>. Acesso em: 11 jul. 2016.

PAIVA, Gustavo Cezar de Medeiros. **Criptografia homomórfica e suas aplicações**. 2015. Disponível em: <https://www.ibm.com/developerworks/community/blogs/tlcbr/entry/mp233?lang=em>. Acesso em: 24 jul. 2016.

REUTERS. **Saiba mais-Petrobras e PF decidem calar sobre roubo de notebooks**. 2008. Disponível em: <http://g1.globo.com/Noticias/Politica/0,,MUL301259-5601,00-SAIBA+MAISPETROBRAS+E+PF+DECIDEM+CALAR+SOBRE+ROUBO+DE+NOTEBOOKS.html>. Acesso em: 16 jun. 2016.

ROCHA, Leonardo. **Força invisível**: os 7 tipos de algoritmos que dominam o nosso mundo. 2014. Disponível em: <http://www.tecmundo.com.br/tecnologia/56148-forcainvisivel-7-tipos-algoritmos-dominam-nosso-mundo.htm>. Acesso em: 14 jul. 2016.

SCHAUL, Kevin. The Washington Post. **Encryption techniques and access they give**. 2015. Disponível em: <https://www.washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/>. Acesso em: 10 jul. 2016.

SIMON, Singh. **O livro dos códigos**. São Paulo: Record, 2010.

SILVA, Elen Viviani Pereira da. **Introdução à Criptografia RSA**. 2006. Disponível em: <http://www.impa.br/opencms/pt/eventos/downloads/jornadas_2006/trabalhos/jornadas_elen_pereira.pdf>. Acesso em: 14 jul. 2016.

SKYPE. **O *skype* usa criptografia**? 2016. Disponível em: <https://support.skype.com/pt/faq/FA31/o-skype-usa-criptografia>. Acesso em: 24 jul. 2016.

SILVEIRA, João Pedro Cipriano. Engenharia. **Aplicações de criptografia baseada em identidade com cartões de identificação eletrônica**. 2013.Disponível em: <https://ubibliorum.ubi.pt/bitstream/10400.6/1931/1/Disserta%C3%A7%C3%A3o.pdf>. Acesso em: 14 jul. 2016.

TREND MICRO. **Novo crypto-ransomware Locky usa macros maliciosas do Word**. 2016. Disponível em: <http://blog.trendmicro.com.br/novo-crypto-ransomware-locky-usa-macros-maliciosas-do-word/#.Vz9AQXarRD8>. Acesso em: 20 maio 2016.

TRINTA, Fernando Antonio Mota; MACÊDO, Rodrigo Cavalcanti de. **Um estudo sobre criptografia e assinatura digital**. 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 26 jun. 2016.

UNO, Daniel Nobuo; FALEIROS, Antônio Cândido. **Princípios de Criptografia Quântica**. 2016. Disponível em: <http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>. Acesso em: 24 jul. 2016.

WHATSAPP. **Perguntas frequentes**. 2016. Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 15 jun. 2016.

Processos e políticas de segurança

Convite ao estudo

Olá! Estamos chegando ao fechamento do ciclo em segurança da informação e de redes, no qual você obtém uma visão geral dos assuntos mais importantes da área.

Nestas próximas aulas, iremos nos concentrar em aspectos não tecnológicos da segurança da informação e de redes, que são parte fundamental para que as proteções funcionem de fato nas empresas. Lembre-se de que o papel da segurança da informação é garantir confidencialidade, integridade e disponibilidade das informações, que podem existir em forma física (papéis, por exemplo), em forma digital (em servidores ou em redes, por exemplo) e na cabeça das pessoas. Para essa proteção ampla requerida, é preciso considerar e utilizar os processos e as políticas de segurança. Iremos ver que há normas que auxiliam nessa tarefa, como as da família ABNT ISO/IEC 27.000. Para finalizar, iremos discutir as tendências da área de segurança da informação e de redes, quando ficará evidente que ainda há muito a fazer nessa área.

Os principais objetivos de aprendizagem desta unidade são:

- Definir, registrar e descrever aspectos não tecnológicos de segurança da informação, com destaque para: desastres, falhas, terrorismo e engenharia social.
- Consolidar os conceitos de políticas de segurança da informação, discutindo processos e cultura de segurança.

- Definir, registrar e descrever as principais normas de segurança da informação, incluindo as famílias NBR ISO/IEC 27.000 e 22.301.
- Registrar e descrever algumas tendências em segurança da informação, incluindo tecnologias emergentes, ameaças emergentes e futuras.

Durante as aulas desta unidade, exercite os conteúdos de acordo com o seguinte contexto: você está montando uma empresa de consultoria de segurança da informação e de redes, a Conseg-123. A empresa já começou com uma carteira de clientes, que inclui um data center, uma indústria química, um banco e um fabricante de robôs para a indústria plástica.

Com foco em processos e políticas de segurança, a Conseg-123 irá desenvolver projetos envolvendo aspectos não tecnológicos de segurança da informação, cultura de segurança, aplicação das principais normas de segurança da informação e, também, a criação de cenários de futuro para o setor de segurança da informação.

Seção 4.1

Identificação de fatores de risco

Diálogo aberto

Olá! Seja bem-vindo à aula inicial sobre um assunto que é fundamental para os profissionais de segurança da informação e que complementa a visão necessária para a formação na área: os aspectos não tecnológicos de segurança da informação.

Frases como "o ser humano é o elo mais fraco da corrente", "não é preciso proteger tanto o servidor se ele fica em um local fisicamente inseguro" ou "agora é impossível configurar o *firewall*, pois o administrador responsável não trabalha mais na empresa" são comuns de serem escutadas e, para garantirmos confidencialidade, integridade e disponibilidade de todas as informações em todas as suas variadas formas (física, digital e na cabeça das pessoas), é preciso saber aplicar os processos e as políticas de segurança.

O primeiro desafio da sua empresa de consultoria Conseg-123 é um projeto com um data center, um de seus clientes nessa fase inicial da empresa. O que o data center está demandando é um projeto de consultoria que mapeia os principais riscos envolvidos em seus negócios, com foco em aspectos não tecnológicos.

Realize esse projeto de mapeamento de riscos não tecnológicos do data center utilizando todos os conceitos vistos até agora nesta disciplina.

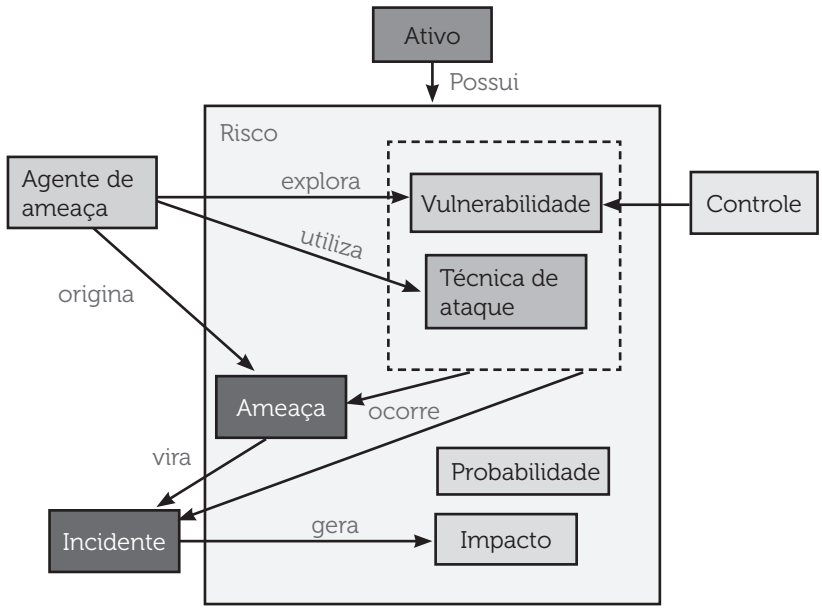
Boa aula!

Não pode faltar

Riscos em segurança da informação

Nós já vimos que risco em segurança da informação é a probabilidade de um agente de ameaça explorar uma vulnerabilidade de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a organização (Figura 4.1) (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007).

Figura 4.1 | Os elementos do risco em segurança da informação



Fonte: elaborada pelo autor.

Os riscos em segurança da informação são compostos por diferentes elementos: probabilidade, impacto, agente de ameaça, ameaça, vulnerabilidade e ativo. Quando avaliamos os riscos não tecnológicos, temos que pensar, principalmente, em algumas categorias.

Um agente de ameaça, que é aquele que provoca um incidente de segurança, pode ser humano, tecnológico ou a própria natureza. Quando um agente de ameaça explora uma vulnerabilidade de um ativo, uma ameaça se torna um incidente de segurança. A ameaça, assim, é algo que "está no ar", que sempre existe e pode virar um evento. Já as vulnerabilidades existem nos ativos, que podem ser humanos, tecnológicos ou físicos.

O foco das aulas até agora foi em aspectos tecnológicos, apesar de termos visto que há outros aspectos envolvidos com a segurança da informação, em especial o aspecto humano e o aspecto físico. São esses dois aspectos que iremos discutir nesta aula, e o interessante disso é que, normalmente, são eles que costumam resultar em grandes impactos para as empresas, algumas vezes maiores do que elas estão acostumadas.

Reflita

Você acha que, em uma empresa que sofre um incidente físico, como o desabamento causado por uma enchente, os impactos são maiores do que um incidente tecnológico, como o vazamento de informações confidenciais de clientes? Por quê?

A organização da aula, seguindo os conceitos dos riscos, vai levar a alguns pontos interessantes, já que há uma forte inter-relação entre os diferentes elementos do risco. A natureza, por exemplo, é um agente de ameaça ou uma ameaça? E uma enchente? E um terremoto? E o congelamento? O mesmo ocorre com os seres humanos. O presidente de uma empresa, por exemplo, é um ativo, um agente de ameaça, uma ameaça ou tudo? Não precisamos nos prender ao purismo, mas vamos seguir, nesta aula, os conceitos discutidos anteriormente. Essa organização é importante para seguirmos adiante e entendermos melhor as nuances que existem nos aspectos não tecnológicos em segurança da informação.

Aspectos não tecnológicos em segurança da informação

Iremos discutir três categorias gerais de aspectos não tecnológicos (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007):

- Aspectos físicos: envolvem elementos do risco que possuem características físicas, tais como data center, servidor ou localização.
- Aspectos humanos: envolvem elementos do risco que possuem características humanas, tais como administrador de sistemas, concorrentes ou *crackers*. Além disso, temos falhas e acidentes.
- Aspectos naturais: envolvem elementos do risco que possuem características naturais, tais como enchentes, terremotos ou altas temperaturas.

Assimile

O que temos que ter em mente é a função da segurança da informação: garantia de confidencialidade, integridade e disponibilidade da informação, que pode existir em diferentes formas: em meio digital, em meio físico ou na cabeça das pessoas.

Ação maliciosa, não intencional ou natural?

Quem realiza uma ação é o agente e, no caso de segurança da informação, quem explora uma vulnerabilidade é o agente de ameaça. O agente de ameaça pode exercer ou provocar ações de três formas gerais (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007):

- Ação maliciosa: algo intencional, como uma invasão, um roubo ou uma destruição.
- Ação não intencional: algo não intencional, como uma falha, engenharia social ou acidente.
- Ação natural: algo que advém da natureza, como terremoto, enchente ou congelamento.

O interessante é a visão que pode ser dada para cada elemento analisado. Por exemplo, no caso de uma ação maliciosa, um roubo (ameaça) é cometido por um ladrão (agente de ameaça), que explora uma vulnerabilidade (porta aberta) de uma casa (ativo). Já no caso de uma ação não intencional, um administrador de rede (ativo) pode ser enganado por engenharia social (ameaça), por um *cracker* (agente de ameaça) que explora a ingenuidade (vulnerabilidade) dele.

No caso do exemplo da ação maliciosa, há aspectos físicos (casa como ativo) e humanos (ladrão como agente de ameaça) envolvidos. Já no caso do exemplo da ação não intencional, há somente aspectos humanos envolvidos, com seres humanos sendo o ativo (administrador de rede) e o agente de ameaça (cracker).

Já em outro exemplo de ação natural, o congelamento (ameaça) de um sistema de supressão de incêndio (ativo) pode ser causado por baixas temperaturas (agente de ameaça).

Reflita

Você tem certeza que os incidentes de segurança são mesmo causados somente por ações maliciosas?

Desastres

A ideia relacionada a desastres é que ela constitui uma das piores consequências que pode existir. Portanto, sendo uma consequência, no linguajar do risco, o desastre é um dos possíveis impactos que uma empresa pode ter. De acordo com essa interpretação, um desastre pode ser tanto resultado de um ataque de *cracker*, como pode também ser resultado de um terremoto. Nessa interpretação do desastre, o valor da gestão de riscos é bastante grande, pois mostra que, para uma empresa, um ataque de *cracker* pode ser um desastre, enquanto para outra empresa o mesmo ataque pode ser apenas um infortúnio.

Isso faz com que tenhamos que pensar que as empresas precisam conhecer muito de seu próprio negócio para estabelecer o que é um desastre, do ponto de vista do impacto.

Exemplificando

Em um hipotético caso de ataque DoS, os serviços de uma empresa digital ficam interrompidos por 1 minuto. O que isso significa para a empresa? Pode haver prejuízos que, no entanto, ficam limitados pelo restabelecimento dos serviços em 1 minuto. O que ocorre se o ataque perdura não por 1 minuto, mas por 2 horas? Os impactos seriam gigantescos, mas será que isso seria um desastre? E se o ataque perdurar por mais de 24 horas? Para algumas empresas, as 24 horas de indisponibilidade podem representar um desastre. Porém, para outras, o único minuto sem os serviços pode representar também um desastre, como no caso de vidas humanas, por exemplo.

Assim, uma visão sobre desastres está na intepretação dos impactos, que podem ser resultantes de ataques de *crackers*, de ataques físicos de terroristas, de falhas, de acidentes ou de perdas com fenômenos da natureza. Outra visão sobre os desastres que também deve ser considerada em segurança da informação é a que considera desastres como parte de fenômenos da natureza.

Os desastres naturais de fato devem ser considerados excluir porque afetam diretamente a informação. Mais do que isso, afetam todas as formas da informação: a que existe em meio digital, a que existe em meio físico e a que existe na cabeça das pessoas. Um terremoto, por exemplo, é um fenômeno da natureza que pode destruir não somente os servidores e todos os seus dados, mas também prédios, data centers e tirar a vida das pessoas.

O potencial do impacto causado por desastres naturais é, com isso, algo bastante grande. Esse impacto é potencializado pelo fato de não termos controle sobre a

natureza. Nesse contexto, os desastres naturais, ou melhor, a natureza, pode ser considerada uma categoria de agentes de ameaça, no linguajar do risco.

Como agente de ameaça, fenômenos da natureza podem levar a desastres. O que é explorada normalmente é a localização, que é a vulnerabilidade, nesse caso.

Alguns fenômenos naturais que podem ser considerados são:

- Enchentes e inundações.
- Terremotos.
- Altas temperaturas.
- Baixa umidade.
- Explosão solar.
- Furacão, tornado, tufão, microexplosão.

Pesquise mais

Veja os principais desastres naturais ao redor do mundo no link da Revista EXAME que consta a seguir. Observe que a localização é a vulnerabilidade, de modo que a mitigação desse tipo de risco deve ser a mudança de endereço ou o uso de controles específicos para aquela ameaça natural.

EXAME. **Desastres naturais**. Disponível em: <http://exame.abril.com.br/topicos/desastres-naturais>. Acesso em: 26 jul. 2016.

Acidentes

Os acidentes, que são causados por seres humanos, também podem resultar em incidentes de segurança e, em alguns casos, em desastres. Há uma série de interpretações também sobre os acidentes sob o ponto de vista do risco, já que há um relacionamento direto com os desastres e com as falhas (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007). Um operador que executa um comando equivocado quando aperta um botão errado e derruba um link de telecomunicações ou um tubarão que rompe os cabos submarinos e interrompe a internet, por exemplo, são casos de acidentes que levam à perda de disponibilidade de serviços. Outro exemplo é quando uma informação confidencial é divulgada acidentalmente para o público em geral ao invés de apenas o corpo gerencial por um funcionário que não se atentou para configurações básicas do sistema de divulgação.

Outro exemplo é um caso que muitas vezes é considerado em avaliações de riscos: um avião caindo no data center. Esse desastre pode ocorrer devido a uma falha no avião, por um erro do piloto ou por um ataque terrorista, por exemplo.

Neste ponto, há um conceito importante em segurança da informação e avaliação de riscos: a reação em cadeia. A avaliação deve levar em consideração não apenas eventos isolados, mas também toda a sequência de eventos. Em um exemplo, o roubo da senha de e-mail do presidente da empresa, por exemplo, pode ser avaliado como sendo de um determinado nível de risco. Porém, o roubo da senha de e-mail pode ser apenas o início de um ataque maior, iniciando a reação em cadeia. O *cracker* poderia, por exemplo, se passar pelo presidente da empresa e solicitar as senhas dos servidores que armazenam os dados de todos os clientes. A partir desse acesso, o vazamento dos dados poderia levar à perda de clientes, processos judiciais e à perda de reputação.

Falhas

As falhas, sejam elas humanas ou tecnológicas, também devem ser consideradas, pois podem afetar as propriedades básicas da segurança da informação, confidencialidade, integridade e disponibilidade (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007).

As falhas humanas podem ser causadas por diversos fatores, tais como cansaço ou desatenção. O que devemos considerar, no entanto, é que diferentes ativos poderão ser afetados com uma falha humana. Por exemplo, uma informação confidencial pode ser divulgada sem intenção após uma falha na configuração do servidor, afetando a confidencialidade.

Além da falha humana, sistemas também podem falhar, o que é intrínseco, principalmente em hardware. Uma falha em um disco rígido, por exemplo, pode levar à perda de informações, com a disponibilidade sendo afetada.

Outro tipo de falha que afeta a segurança da informação é a de infraestrutura, como a elétrica. O sistema elétrico pode causar variações elétricas capazes de danificar hardware ou corromper informações, que podem afetar a disponibilidade ou a integridade.

Engenharia social

A engenharia social é uma técnica de ataque utilizada para explorar a natureza humana, como a bondade, a inocência ou o medo. A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que ele não é pela manipulação. Como resultado, o engenheiro social pode

aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia. (MITNICK; SIMON, 2003).

Pesquise mais

Conheça mais sobre a engenharia social na obra de Mitnick e Simon (2003). O livro foca na exploração da natureza humana, afirmando que não há tecnologias (como *firewalls* ou criptografia) que são suficientes para deter um *cracker* decidido a atacar um banco de dados corporativo, ou um funcionário revoltado determinado a paralisar um sistema.

MITNICK, Kevin D.; SIMON, William M. **A arte de enganar**. São Paulo: Makron Books, 2003.

Um dos ataques mais comuns para fraudes financeiras, por exemplo, é o envio de e-mails falsos (*phishing*), em que a vítima acaba passando informações, como senhas ou tokens, para o fraudador, ou mesmo instalando *malwares*, que são utilizados em outros ataques. Em e-mails falsos, a vítima é instigada a abrir a mensagem e a respondê-la, o que leva à contaminação ou à divulgação de informações confidenciais.

Outra técnica de engenharia social bastante utilizada é a realização de ligações telefônicas para centros de relacionamento de serviços diversos, de posse de algumas informações sobre a vítima. Informações críticas podem ser obtidas nessas ligações, como as que foram descobertas em ataque contra um jornalista da revista norte-americana *Wired*. Nesse incidente, o *cracker* utilizou informações cruzadas de diferentes serviços da vítima para roubar a sua conta. Primeiro, ele ligou para a *Amazon* pedindo para adicionar um novo cartão de crédito. A validação foi feita com informações de nome completo, e-mail e endereço de cobrança. Em uma nova ligação, o *cracker* alegou não estar conseguindo o acesso com seu e-mail, e conseguiu cadastrar um novo utilizando informações de nome, endereço de cobrança e cartão de crédito (que ele tinha acabado de cadastrar). Com o novo endereço de e-mail cadastrado, o fraudador recuperou a senha usando o método tradicional (esqueci minha senha). Já na conta da *Amazon*, o fraudador teve acesso aos quatro últimos dígitos do cartão de crédito da vítima, que eram, por sua vez, utilizados para verificação de conta da Apple. Com o acesso à conta do *iCloud*, o fraudador conseguiu recuperar a senha do *Gmail* para depois conseguir a senha do *Twitter* (ARRUDA, 2012).

Pesquise mais

Você já viu antes, neste curso, mas pode relembrar o ataque ao jornalista da Revista *Wired* no link a seguir:

ARRUDA, Felipe. **Saiba como hackers apagaram a vida digital de um jornalista em apenas uma hora**. Disponível em: <http://www.tecmundo.com.br/seguranca/27993-saiba-como-hackers-apagaram-a-vida-digital-de-um-jornalista-em-apenas-uma-hora.htm>. Acesso em: 26 jul. 2016.

Terrorismo

O terrorismo está em voga atualmente, o que é péssimo para o mundo, e exige que tenhamos que considerá-lo em qualquer estratégia de segurança da informação (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007). O terrorismo possui uma ligação direta com a continuidade de negócios, que é uma área da segurança de informação relacionada com a disponibilidade.

Podemos considerar três visões para a questão do terrorismo:

- Ativos físicos sendo destruídos: servidores, data centers ou empresas inteiras sofrendo com um atentado terrorista podem levar a gigantescas perdas patrimoniais, para início dos impactos em cadeia.
- Ativos humanos sendo afetados: com funcionários-chave sendo vítimas de ataques terroristas, a capacidade de continuidade de negócios da empresa pode ser afetada e, portanto, deve ser considerada.
- Terrorismo cibernético: o uso de ataques cibernéticos parece fazer parte da estratégia militar de diferentes países. O terrorismo cibernético possui relação direta, também, com a proteção de infraestruturas críticas, na qual serviços críticos, como energia elétrica, transportes ou telecomunicações podem ser afetados com ataques cibernéticos. Há, ainda, a vertente que, com o avanço tecnológico das armas, utilizam elementos de telecomunicações, por exemplo, os ataques cibernéticos fazem cada vez mais sentido em uma guerra.

Sem medo de errar

O primeiro desafio da sua empresa de consultoria Conseg-123 é um projeto com um data center, um de seus clientes nessa fase inicial da empresa. O que o data center está demandando é um projeto de consultoria que mapeia os principais riscos envolvidos em seus negócios, com foco em aspectos não tecnológicos.

O mapeamento de riscos deve considerar os elementos do risco, que são os agentes de ameaça, as ameaças e as vulnerabilidades, além da probabilidade e do impacto. Para simplificar, os riscos serão mapeados de acordo com os seguintes aspectos:

- Aspectos físicos: envolvem elementos do risco que possuem características físicas, tais como data center, servidor ou localização.
- Aspectos humanos: envolvem elementos do risco que possuem características humanas, tais como administrador de sistemas, concorrentes ou *crackers*. Além disso, temos falhas e acidentes.
- Aspectos naturais: envolvem elementos do risco que possuem características naturais, tais como enchentes, terremotos ou altas temperaturas.

O data center que está sendo avaliado pelo Conseg-123 está localizado em um bairro remoto, próximo a grandes rodovias. Em região montanhosa, no inverno, o frio chega a -30 graus centígrados, enquanto no verão faz calor de 40 graus centígrados.

Alguns dos riscos que podem ser mapeados são:

- Aspectos físicos: desastres naturais, como grandes incêndios ou avalanches, podem resultar em grandes impactos para o data center.
- Aspectos humanos: no caso de bloqueio das rodovias, as pessoas poderão não chegar ao data center, o que pode afetar os negócios.
- Aspectos naturais: frio intenso pode congelar sistema de supressão de incêndio baseado em água, o que pode levar a grandes impactos como consequência de outro risco, o de incêndio.

Atenção

Risco em segurança da informação é a probabilidade de um agente de ameaça explorar uma vulnerabilidade de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que resulta em impactos.

Avançando na prática

Engenharia social leva *malware* para dentro da empresa

Descrição da situação-problema

A engenharia social é um dos principais problemas em segurança da informação, já que afeta diretamente as pessoas, o que muitas vezes é mais simples do que

atacar sistemas. Em um dos casos de exploração da engenharia social, um grupo de *crackers* criou um *malware* específico para um sistema interno da empresa. A forma de contaminação do sistema interno foi fazer com que o *malware* fosse inserido em algum computador interno da empresa. Para tanto, foram espalhados pen drives contaminados com o *malware* no estacionamento da empresa e em áreas em que funcionários iam no horário de almoço.

Descreva como a engenharia social culmina na contaminação da empresa por *malware* nesse contexto.

Lembre-se

O que devemos ter em mente é a função da segurança da informação: garantia de confidencialidade, integridade e disponibilidade da informação, que pode existir em diferentes formas: em meio digital, em meio físico ou na cabeça das pessoas.

Resolução da situação-problema

A engenharia social, nesse caso, envolve a curiosidade humana. Algum funcionário mais curioso pode pegar o pen drive encontrado e vasculhar as informações nele contidas em busca de qualquer coisa. No momento de inserção do pen drive no computador que está dentro da empresa, o *malware* inicia a contaminação. As chances de sucesso existem, pois os locais em que os pen drives foram espalhados foram cuidadosamente estudados e escolhidos. Uma vez contaminados, os sistemas internos e a própria empresa passam a sofrer as consequências do ataque cibernético por *malware*.

Faça você mesmo

Nesse caso da contaminação por *malware* em pen drive, o que a empresa poderia fazer para diminuir as chances de incidentes de segurança?

Faça valer a pena

1. Um incidente de segurança pode levar a impactos para as empresas. Uma ameaça não tecnológica pode afetar a confidencialidade da informação? Por quê?

a) Sim, porque há elementos físicos e humanos.

b) Sim, porque há elementos tecnológicos que podem ser atacados.

c) Sim, porque há o uso da criptografia

d) Não, porque o firewall faz a proteção.

e) Não, porque há elementos não tecnológicos.

2. Em segurança da informação, devemos considerar aspectos tecnológicos e não tecnológicos. Qual das alternativas abaixo engloba os aspectos não tecnológicos em segurança da informação que devemos considerar?

a) Aspectos físicos, humanos e naturais

b) Aspectos físicos, apenas.

c) Aspectos humanos, apenas.

d) Aspectos naturais, apenas.

e) Segurança da informação é só tecnológico.

3. Um incidente de segurança pode levar a impactos para as empresas. Uma ameaça não tecnológica como uma falha pode afetar a integridade da informação? Por quê?

a) Sim, porque a informação pode ser alterada de uma forma não intencional.

b) Sim, porque a informação pode ser apagada de uma forma não intencional.

c) Sim, porque a informação pode ser divulgada sem autorização.

d) Não, porque a informação é digital.

e) Não, porque a informação é segura por natureza.

Seção 4.2

Definição de políticas de segurança da informação

Diálogo aberto

Olá! Nesta aula você terá contato com um dos principais controles de segurança da informação, que é especialmente destinado às pessoas: a política de segurança da informação. Já vimos que devemos proteger confidencialidade, integridade e disponibilidade das informações, que existem em meios digitais, em meios físicos e, também, na cabeça das pessoas. A política de segurança é destinada às pessoas, que devem seguir diretrizes, normas, processos e procedimentos.

Nesta seção, iremos discutir sobre os objetivos, a estrutura, as formas de divulgação a cultura e sobre como desenvolver uma política de segurança da informação.

Você é sócio da Conseg-123, que é uma consultoria em segurança da informação com foco em processos e políticas de segurança, e desenvolve projetos envolvendo aspectos não tecnológicos de segurança da informação, cultura de segurança, aplicação das principais normas de segurança da informação e, também, a criação de cenários de futuro para o setor de segurança da informação.

O cliente da Conseg-123 a ser trabalhado nesta aula é uma indústria química, a Kimik, possuidora uma grande equipe que desenvolve novos produtos a partir de resultados de projetos de pesquisa e desenvolvimento. Buscando aumentar a competitividade, a Kimik contratou a Conseg-123 para trabalhar em uma política de segurança da informação. Desenvolva uma linha geral da política de segurança para a Kimik.

Boa aula!

Não pode faltar

Objetivos de uma política de segurança

A segurança é de responsabilidade de todos, e não apenas da área de segurança da empresa. De fato, basta um incidente para que toda a empresa seja comprometida: vírus, vazamentos ou desenvolvimento de produtos vulneráveis que levam à má reputação (NAKAMURA; GEUS, 2007).

Como já vimos neste curso, as informações podem existir em meio digital, em meio físico ou na cabeça das pessoas. A segurança da informação deve buscar a manutenção da confidencialidade, da integridade e da disponibilidade dessas informações, para tanto, os controles de segurança, como *firewalls*, antivírus ou criptografia podem ser aplicados para proteger informações que existem em meios digitais (NAKAMURA; GEUS, 2007; ISO 27001, 2013; ISO 27002, 2013).

Já para as informações que existem em meios físicos, como em papéis, e também para as informações que estão na cabeça das pessoas, é necessária uma política de segurança. Mesmo os controles tecnológicos dependem da política de segurança, que estabelece as diretrizes para que a proteção seja efetiva (NAKAMURA; GEUS, 2007; PCI, 2013; ISO 27001, 2013; ISO 27002, 2013).

Assim, a política de segurança possui um dos papéis mais importantes em organizações de qualquer natureza. Segundo PCI (2013, p. 111), em seu Requisito 12, temos: "Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles". Além disso, a norma ainda diz: "Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los". O PCI DSS (*Payment Card Industry Data Security Standard*), padrão para a segurança de dados da indústria de cartões, adotado em todo o mundo, torna claro um dos principais conceitos que uma política de segurança deve seguir: de que ela existe para direcionar a segurança da informação de uma empresa, sendo necessário que todos colaboradores tenham conhecimento sobre ela e cumpram o que nela está estabelecido.

Exemplificando

O PCI DSS (*Payment Card Industry Data Security Standard*) é um padrão de segurança para a indústria de cartões, que deve ser seguido por todas as entidades que processam, armazenam ou transmitem dados de cartões. O PCI DSS é um ótimo balizador para a área de segurança, primeiro porque é largamente adotado em vários países e, em segundo lugar, por empresas de diferentes segmentos de mercado, como bancos, processadores de cartões, lojas virtuais e comércio. Isso faz com que o

padrão seja adotado de fato e implementado na prática das empresas. Além disso, o PCI DSS é bastante abrangente, contemplando de uma forma integrada os vários assuntos de segurança da informação, como a política de segurança.

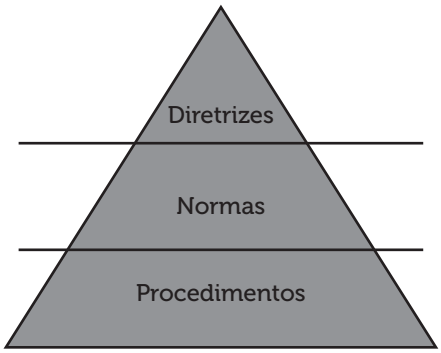
PCI. **Requisitos e procedimentos da avaliação de segurança. Versão 3.0**. 2013. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/PCI_DSS_v3.pdf>. Acesso em: 22 ago. 2016.

Estrutura de uma política de segurança

A política de segurança é composta por um conjunto de documentos ou capítulos que devem ser lidos, compreendidos e seguidos pelos respectivos responsáveis. A política em si, que possui as diretrizes gerais para a segurança da informação na organização, deve ser acessada e seguida por todos. Além disso, há as normas. Já os processos e procedimentos específicos, como o de desenvolvimento de software, ou o de administração de sistemas, por exemplo, devem ser seguidos pelos respectivos responsáveis, não sendo necessário, por exemplo, que o administrador de *firewall* tenha acesso aos processos e procedimentos de gestão de identidades (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

Assim, a política de segurança é composta por diretrizes, objetivos, direcionadores e normas, enquanto os processos e procedimentos se destinam a aspectos específicos (Figura 4.2). Com isso, a política possui uma estrutura que deve facilitar o acesso de todos da organização para os documentos ou capítulos que são de responsabilidade de cada um.

Figura 4.2 | Estrutura de uma política de segurança



Fonte: elaborada pelo autor.

Pesquise mais

Veja uma política de segurança da informação de uma instituição brasileira, a BM&F Bovespa, que trata das diretrizes gerais de segurança da informação da organização, que devem ser lidas, compreendidas e seguidas por todos.

BM&F BOVESPA. **Política de segurança da informação**. Disponível em: <http://ri.bmfbovespa.com.br/fck_temp/26_39/file/Nova%20Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%202014%20-%20final.pdf>. Acesso em: 18 nov. 2016.

Como tornar conhecida uma política de segurança

Uma política de segurança só possui utilidade se for conhecida de seus funcionários. Há três estratégias básicas para que todos da empresa tenham conhecimento da política de segurança (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013):

1. Termo assinado de que o funcionário leu a política de segurança e que se compromete a cumpri-la: as empresas adotam o termo normalmente em conjunto com a assinatura do contrato de trabalho, na admissão.

2. Campanhas e tecnologias: as empresas podem criar quadros para enfatizar a política de segurança espalhadas em pontos estratégicos da empresa. Além disso, tecnologias como protetores de tela de computadores ou mensagens direcionadas também ajudam na disseminação da política de segurança na empresa. Outra ação importante é a realização de campanhas de conscientização, como as relacionadas a senhas ou ao acesso a sites duvidosos, por exemplo. Essas campanhas resultam em diminuição do número de incidentes, contribuindo para a segurança da organização.

3. Ser direta e objetiva: o documento deve ser simples de entender e direto nos seus objetivos, de modo que todos que o leiam percebam sua importância e o memorizem.

4. Treinamentos periódicos em segurança da informação: normas e procedimentos podem ser discutidos e trabalhados em grupos específicos, como o dos desenvolvedores de sistemas ou dos profissionais de suporte e TI. Outro treinamento mais geral pode ser feito para o público mais amplo.

Reflita

Uma política de segurança engavetada, de difícil acesso ou destinada apenas aos profissionais de segurança da informação consegue proteger a organização contra os riscos existentes?

O que direciona uma política de segurança

Cada organização deve ter a sua própria política de segurança, que deve ser desenvolvida de acordo com suas próprias características, linguajares e contextos específicos. Assim, os seguintes aspectos devem ser utilizados para a definição da política de segurança de uma organização (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013):

- Análise de riscos: os riscos de segurança da informação devem ser mapeados para direcionar as ações que devem constar na política de segurança.
- Estratégia e requisitos de negócios: diferentes negócios requerem diferentes níveis de segurança, que direcionam o conteúdo da política de segurança. Uma empresa que quer vender a imagem de privacidade, por exemplo, direcionará a política de segurança para esses aspectos específicos.
- Requisitos legais: alguns setores possuem obrigações legais a serem cumpridas com relação à segurança da informação, que refletem diretamente na política de segurança.

Exemplificando

Um exemplo de requisito legal é a Resolução nº 3.380, do Banco Central do Brasil (BACEN, 2006), que estabelece a necessidade de gerenciamento de risco operacional, levando à necessidade de controles de segurança da informação como o plano de continuidade de negócios, que atua na disponibilidade.

BANCO CENTRAL DO BRASIL. **Resolução nº 3.380, de 29 de junho de 2006**. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em <http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf>. Acesso em: 29 ago. 2016.

Cultura em segurança da informação

Um dos principais fatores que resulta em proteção concreta da organização, em conjunto com uma política de segurança efetiva, é a cultura em segurança da

informação (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

A cultura de segurança é importante porque é voltada para as pessoas, e não para as tecnologias.

Assimile

A segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção de confidencialidade, integridade e disponibilidade da informação.

Em cultura de segurança da informação, a percepção de todos é fundamental. Caso o funcionário de uma organização tenha a percepção de que o presidente é de fato zeloso quanto à proteção da informação, naturalmente ele irá também agir com cuidado para proteger as informações.

A segurança da informação, assim, deve começar pelo topo, em uma abordagem top-*down*, que auxilia na construção de uma cultura forte em segurança da informação.

Além disso, a cultura pode ser estabelecida com ações constantes ao invés de ações isoladas, que na prática indica correções em curso, e não uma legítima preocupação com a segurança da informação.

A cultura deve buscar também o engajamento de todos, para tanto, a política de segurança e as ações definidas devem estar inseridas nas tarefas do dia a dia, influenciando o que a empresa vende, e deve ser incorporada nos produtos. Uma cultura em segurança da informação é persistente, integrada em tudo o que é feito pela empresa.

O que auxilia na construção de uma cultura em segurança da informação é o envio de uma mensagem positiva para todos da empresa, como a participação direta de executivos em campanhas de conscientização ou a certificação profissional de funcionários. Outra ação importante é a criação de uma comunidade de segurança da informação ou comitê de segurança.

Desenvolvendo uma política de segurança da informação

Cada organização é única e possui uma política de segurança única. O tom da política de segurança é estabelecido com base em diferentes aspectos, como estratégia, requisitos de negócios, requisitos legais e resultados da análise de riscos (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

Assim, diretrizes de segurança da informação, normas e procedimentos devem seguir os objetivos de negócios, objetivos legais e os riscos daquela organização específica.

A análise de riscos irá direcionar os principais controles de segurança necessários, que podem ser baseados em normas como a NBR ISO/IEC 27002, que define controles de segurança da informação.

A gestão de segurança da informação, definida na norma NBR ISO/IEC 27001, também indica caminhos para o desenvolvimento de uma política de segurança da informação, incluindo outros aspectos para a proteção efetiva da organização.

Algumas perguntas que a política de segurança deve responder são:

- Os usuários sabem em quais links não devem clicar?
- Os funcionários da empresa sabem o que devem publicar em redes sociais sobre a empresa?
- Há preocupações sobre vazamento durante as discussões de novos produtos ou serviços?
- Quais são as regras para uso de dispositivos móveis?

Após a elaboração da política, é fundamental que ela seja aprovada pelos principais executivos da organização, o que ajuda na criação de uma cultura forte em segurança da informação.

As normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002, além de outras que são importantes para a segurança da informação e de redes, serão vistas na próxima aula.

Sem medo de errar

A Conseg-123 é uma consultoria em segurança da informação com foco em processos e políticas de segurança. Para a Kimik, um cliente da indústria química, o objetivo é desenvolver uma linha geral da política de segurança.

O ponto principal é que a política de segurança seja direcionada pela estratégia e por requisitos de negócios da Kimik, bem como por requisitos legais e, também, pelos resultados da análise de riscos.

Outro ponto importante é considerar que a estrutura da política de segurança deve conter as diretrizes, as normas, os processos e os procedimentos.

Com o desenvolvimento de produtos a partir de resultados de projetos de pesquisa e desenvolvimento, a Kimik possui como estratégia e requisitos de negócios a confidencialidade dos resultados dos projetos de pesquisa e desenvolvimento, tanto durante o desenvolvimento quanto depois da finalização dos projetos. Além disso, o desenvolvimento dos projetos também deve seguir com a máxima confidencialidade, que cresce a cada dia com o aumento da concorrência.

Outro ponto a ser considerado é a discussão no governo sobre uma regulamentação da indústria química que envolve a existência de um plano de continuidade de negócios.

Já os resultados da análise de riscos da Kimik indicaram que há riscos altos de vazamentos de resultados de projetos de pesquisa e desenvolvimento, reforçados por um caso ocorrido que resultou em perdas significativas de mercado.

A política de segurança da Kimik deve seguir linhas gerais que possuem como diretriz a preservação da confidencialidade das informações, com foco no desenvolvimento de produtos e, também, nos projetos de pesquisa e desenvolvimento. Normas direcionam o uso correto das tecnologias, o armazenamento dos resultados e os cuidados com informações em papéis e no que pode ser discutido em locais públicos. Já os processos e os procedimentos definem as atividades específicas de configuração e uso das tecnologias de segurança.

Atenção

A política de segurança é um conjunto de documentos que devem ser destinados ao público correto para ser efetiva. Assim, diretrizes são para o público em geral, enquanto processos e procedimentos são específicos, como no caso do administrador do servidor de arquivos, que deve seguir o procedimento de configuração segura e rastreabilidade do serviço, por exemplo.

Avançando na prática

Política de senhas

Descrição da situação-problema

Senhas podem ser adivinhadas, descobertas ou quebradas em diferentes ataques, o que leva a uma série de consequências para as empresas. Uma política de senhas, com uma norma que define as regras das senhas, é de fundamental importância para a segurança da informação.

Além das regras das senhas, o que deve ser levado em consideração é que uma política muito restritiva pode ter efeito inverso, os usuários podem apresentar dificuldades em escolher e memorizar suas senhas, tendo que recorrer a métodos como a escrita das senhas em pedaços de papéis. Por isso, é recomendável que a política de senhas possua também elementos que ajudem os usuários a escolherem suas senhas de uma forma segura.

Indique os parâmetros que devem existir em uma política de senhas.

Lembre-se

Cada empresa possui suas próprias estratégias, seus próprios requisitos de negócios, seus próprios requisitos legais e seus próprios conjuntos de riscos. Assim, cada política de segurança é única, apesar de seguirem estruturas similares.

Resolução da situação-problema

A política de senhas deve definir a norma que define os parâmetros, tais como:

- Tamanho mínimo da senha.
- Mistura entre caracteres numéricos, alfanuméricos e/ou caracteres especiais.
- Tempo de validade de cada senha.
- Número de senhas que podem ser repetidas a cada alteração.

É a partir dessa norma que os procedimentos são desenvolvidos, como o procedimento para o administrador dos sistemas, que deve implantar as regras definidas.

Faça você mesmo

Veja como o PCI DSS define como os requisitos mínimos para as senhas de sistemas relacionadas a cartões, em PCI (2013), nos controles 8.2. Com base nesses requisitos mínimos, estabeleça agora uma política de senhas para dois perfis: (i) usuários dos sistemas da organização e (ii) administradores dos sistemas.

PCI. **Requisitos e procedimentos da avaliação de segurança. Versão 3.0**. 2013. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/PCI_DSS_v3.pdf>. Acesso em: 22 ago. 2016.

Faça valer a pena

1. A política de segurança é um dos principais controles de segurança da informação. Ela é composta por diretrizes, normas, processos e procedimentos. Considere as seguintes opções:

I. Conscientização.

II. Treinamento.

III. Criptografia.

IV. Engenharia social.

Para ser efetiva, uma política de segurança deve utilizar quais das opções acima?

a) Apenas I.

b) Apenas II.

c) Apenas III.

d) Apenas I e II.

e) Apenas III e IV.

2. A política de segurança é um dos principais controles de segurança da informação. Ela é composta por diretrizes, normas, processos e procedimentos. Considere as seguintes opções:

I. Política de senhas.

II. Política de registro de entrada em data center.

III. Política de acesso a informações confidenciais.

Quais opções acima podem fazer parte de uma política de segurança?

a) Apenas I.

b) Apenas II.

c) Apenas III.

d) Apenas I e II.

e) I, II e III.

3. A política de segurança é um dos principais controles de segurança da informação. Ela é composta por diretrizes, normas, processos e procedimentos. Considere as seguintes opções:

I. Senhas.

II. Regras de *firewall.*

III. Uso de criptografia.

Qual (is) da (s) opção (ões) acima devem fazer parte de uma política de segurança da informação?

a) Apenas I.

b) Apenas II.

c) Apenas III.

d) Apenas I e II.

e) I, II e III.

Seção 4.3

Normas de segurança

Diálogo aberto

Olá! Nesta aula iremos complementar e integrar todos os conceitos sobre segurança da informação, com o enfoque na organização das ações que devem ser tomadas nas organizações. O que direciona as ações são as normas de segurança da informação, que auxiliam na definição de uma visão sobre o que deve ser feito para a efetiva proteção dos ativos da organização. Para tanto, as normas definem sistemas de gestão e, também, uma coleção de medidas de segurança que podem ser tomadas em situações específicas. O foco da aula está nas principais normas de segurança da informação, de gestão de riscos e de gestão de continuidade de negócios.

Você é sócio da Conseg-123, que é uma consultoria em segurança da informação, com foco em processos e políticas de segurança, e desenvolve projetos envolvendo aspectos não tecnológicos de segurança da informação, cultura de segurança, aplicação das principais normas de segurança da informação e, também, a criação de cenários de futuro para o setor de segurança da informação.

O cliente da Conseg-123 a ser trabalhado nesta aula é um banco, o Bank$$$, que se baseia em uma plataforma totalmente digital, sem nenhuma agência física própria. Ciente de que o negócio de um banco é baseado fortemente em confiança, o Bank$$$ contratou a Conseg-123 para definir um direcionamento sobre quais normas ele deve seguir para reforçar a sua imagem de um banco moderno e preocupado com os aspectos de segurança da informação, que é uma exigência cada vez maior dos clientes de serviços financeiros.

Desenvolva, nesta aula, um direcionamento para o Bank$$$ com relação às normas que ele deve seguir a fim de a se consolidar no mercado.

Os objetivos desta aula estão relacionados com:

- Objetivos de normas e padrões.
- Principais normas e padrões.

- Normas de gestão de segurança da informação, de gestão de riscos, de gestão de continuidade de negócios, de governança de TI e de gestão de serviços de TI.

Boa aula!

Não pode faltar

Objetivos de normas e padrões

As organizações definem suas estratégias de segurança de acordo com as suas próprias características específicas, que incluem requisitos legais (a existência de obrigação de guarda de *logs*, por exemplo), requisitos regulatórios (como regulamentações setoriais do mercado financeiro) requisitos de negócios (alta disponibilidade, por exemplo), estratégia de negócios (como o uso de monitoramento de segurança como diferencial competitivo) e cultura organizacional (como todos da empresa seguirem a preocupação do presidente em ter a segurança em mente) (PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

As normas e os padrões de segurança da informação exercem um papel importante para as organizações, sob dois pontos de vista principais. Primeiramente, as normas e os padrões auxiliam as organizações na definição dos controles de segurança e também no estabelecimento do sistema de gestão que, por sua vez, é o responsável pelo ciclo efetivo da segurança da informação. Além da segurança da informação, é importante considerar também a gestão de riscos e a gestão de continuidade de negócios, que possuem um relacionamento direto entre elas, com intersecções compostas por controles equivalentes.

O segundo ponto de vista sobre a importância das normas e padrões é que elas demonstram a abordagem mais comprometida da organização com a segurança da informação, que é alcançada com a obtenção de certificação. A certificação mais conhecida em segurança da informação é a ISO/IEC 27001, que atesta organizações que possuem um sistema de gestão de segurança da informação.

Principais normas e padrões

A segurança da informação faz parte de todas as organizações, e há um conjunto de normas (e padrões) que são mais utilizadas, sendo algumas delas específicas, enquanto outras tratam de assuntos diferentes, incluindo uma parte referente à segurança da informação (ISO 27001, 2013; ISO 27002, 2013; ISO 27005, 2011; ISO 22301, 2013; ISO 31000, 2009; TUPPENCE, 2010; PCI, 2013; CHIARI, 2016).

A segurança da informação, os riscos e a continuidade de negócios possuem relação direta, sendo que os dois últimos até mesmo fazem parte da segurança da informação. A gestão de riscos busca proteger a organização dos riscos existentes, com a implementação de controles de segurança (gestão de segurança da informação). Caso um risco se torne um incidente de segurança, com um agente de ameaça explorando uma vulnerabilidade de um ativo, o plano de contingência, que deve ser criado antes do incidente ocorrer, é ativado (gestão de continuidade de negócios).

Outra relação direta existe entre a segurança da informação, a governança de TI e a gestão de serviços de TI. Não é possível alcançar a governança de TI, bem como a gestão de serviços de TI, sem a segurança da informação, de modo que as normas e os padrões sobre esses fatores possuem partes que envolvem a segurança da informação.

As principais normas e os padrões que envolvem a segurança da informação, que serão discutidos nesta aula, são:

- Segurança da informação: ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.
- Riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011.
- Continuidade de negócios: ABNT NBR ISO/IEC 27031:2015 e ABNT NBR ISO 22301:2013.
- Governança de TI: COBIT.
- Serviços de TI: ITIL.

Pesquise mais

Uma grande fonte de documentação sobre segurança da informação, em inglês, é o do *National Institute of Standards and Technology* (NIST). O NIST estabelece padrões para os demais órgãos americanos e conta com um centro especializado em segurança computacional, o *Computer Security Resource Center* (CSRC). Veja os documentos de padronização do NIST, em inglês, em NIST (2016).

NIST. **Computer Security Resource Center (CSRC)**. Disponível em: <http://csrc.nist.gov/publications/PubsSPs.html>. Acesso em: 29 ago. 2016.

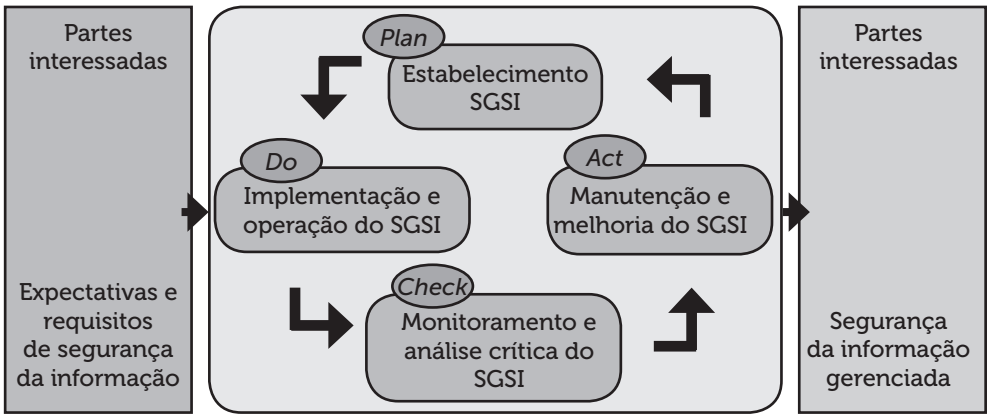
Norma de gestão de segurança da informação: ABNT NBR ISO/IEC 27001:2013

A principal norma de segurança da informação é a ABNT NBR ISO/IEC 27001:2013, que define os requisitos para Sistemas de Gestão da Segurança da Informação (SGSI) e faz parte da família de normas ISO 27000, que possui o foco em segurança da informação (ISO 27001, 2013).

Uma característica da ISO 27001 é que uma organização pode ser certificada na norma, o que indica que ela possui e segue um sistema de gestão de segurança da informação.

O sistema de gestão de segurança da informação deve seguir o ciclo PDCA, de Planejar (*Plan*), Executar (*Do*), Verificar (*Check*) e Agir (*Act*), assim como outros sistemas de gestão. A Figura 4.3 mostra que o ciclo de melhoria contínua parte de expectativas e requisitos de segurança da informação, de modo que há a segurança da informação gerenciada.

Figura 4.3 | Estrutura de uma política de segurança



Fonte: elaborada pelo autor.

O SGSI deve seguir alguns processos básicos para o seu estabelecimento e a consequente certificação da organização na ISO 27001 (ISO 27001, 2013):

1. Definir o escopo do SGSI, considerando os negócios, os ativos, a localização e as tecnologias, justificando as exclusões do escopo.

2. Definir uma política do SGSI, que define a estratégia e direciona as ações da organização, que deve ter aprovação executiva. Possui relação com a política de segurança da informação.

3. Definir a abordagem de avaliação de riscos da organização, com metodologias e critérios.

4. Identificar os riscos, de acordo com a abordagem de avaliação de riscos.
5. Analisar e avaliar os riscos, aplicando os critérios da abordagem de avaliação de riscos.
6. Identificar e avaliar as opções para o tratamento dos riscos.
7. Selecionar os objetivos de controles e os controles para o tratamento dos riscos.
8. Obter aprovação gerencial para os riscos residuais.
9. Obter autorização gerencial para implementar e operar o SGSI.
10. Preparar a declaração de aplicabilidade com as justificativas para os controles que deverão ser implementados e para os que foram excluídos.

É importante ter em mente que há uma relação direta entre a gestão de segurança da informação e a gestão de riscos, dessa forma, os processos de 3 a 8 dizem respeito à gestão de riscos, o que torna a norma ABNT NBR ISO/IEC 27005:2011 bastante relevante para as organizações que buscam a certificação ISO 27001.

Assimile

Uma organização pode ser certificada na norma ISO 27001, o que indica que ela possui e segue um sistema de gestão de segurança da informação. O processo de certificação é feito por empresas de auditoria independentes.

Norma de código de prática para controles de segurança da informação: ABNT NBR ISO/IEC 27002:2013

A importância da norma ABNT NBR ISO/IEC 27002:2013, que trata do código de prática para controles de segurança da informação, existe devido aos processos 6 e 7 do estabelecimento do SGSI, que identificam e selecionam os controles de segurança para o tratamento dos riscos. Os objetivos de controles da ISO 27002 incluem (ISO 27002, 2013): política de segurança da informação; conformidade; gestão de continuidade do negócio; gestão de incidente de segurança da informação; aquisição, desenvolvimento e manutenção de sistemas de informação; controle de acessos; gerenciamento de operações e comunicações; segurança física e do ambiente; segurança de recursos humanos; gestão de ativo; organização da segurança da informação.

Além da ISO 27001 e da ISO 27002, há outras normas da família ISO 27000 que merecem destaque e tornam evidente a abrangência da segurança da informação

(ABNT, 2016). Há, no total, cerca de 30 normas que tratam de diferentes assuntos, tais como: vocabulários; métricas; auditorias; guias; aplicações em setores específicos, como telecomunicações, financeiro, nuvem, energia e saúde; aspectos econômicos; continuidade de negócios; segurança de redes; incidentes de segurança; forense computacional; IDS e IPS; armazenamento.

Reflita

As normas e os padrões relacionados à segurança da informação crescem a passos largos. A ISO já trata de assuntos mais específicos de segurança da informação, como a segurança de redes e a forense computacional, além de auxiliar organizações de setores específicos. A segurança da informação possui ou não importância para organizações de quaisquer naturezas?

Normas de gestão de riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011

A gestão de riscos possui uma estreita relação com a segurança da informação, de modo que para a obtenção de uma certificação ISO 27001 é preciso que a organização tenha estabelecida a gestão de riscos. Há duas normas principais que direcionam a gestão de riscos (ISO 27005, 2011), (ISO 31000, 2009):

- ABNT NBR ISO 31000:2009, que estabelece princípios e diretrizes da gestão de riscos de uma forma mais ampla, sem ser específico para a segurança da informação.
- ABNT NBR ISO/IEC 27005:2011, que estabelece a gestão de riscos de segurança da informação.

As normas ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011 tratam dos processos de gestão de riscos:

- Estabelecimento e definição de contexto.
- Identificação de riscos.
- Estimativa e análise de riscos.
- Avaliação de riscos.
- Tratamento de riscos.
- Comunicação e consulta de riscos.
- Monitoramento, revisão e análise crítica de riscos.

Além da ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011, outras normas relacionadas à gestão de riscos são relevantes (ABNT, 2016):

- ABNT ISO GUIA 73:2009, que trata do vocabulário da gestão de riscos.
- ABNT ISO/TR 31004:2015, que é um guia para implementação da ABNT NBR ISO 31000.
- ABNT NBR ISO/IEC 31010:2012, que trata de técnicas para o processo de avaliação de riscos.

Normas de gestão de continuidade de negócios

A gestão de continuidade de negócios possui uma relação direta com a segurança da informação, com foco na disponibilidade, visando à manutenção e ao restabelecimento dos negócios após um incidente de segurança, que também é tratado pela gestão de riscos e pela gestão de segurança da informação (ISO 22301, 2013).

As duas principais normas são a ABNT NBR ISO 22301:2013, que trata do sistema de gestão de continuidade de negócios, de uma forma mais ampla, e a norma ABNT NBR ISO/IEC 27031:2015, que foca na continuidade dos negócios com enfoque na tecnologia da informação e comunicação.

Uma organização pode ser certificada em gestão de continuidade de negócios, com a aplicação da norma ABNT NBR ISO 22301:2013, que especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão de continuidade de negócios, destinado à proteção, redução da probabilidade de ocorrência, preparação, resposta e recuperação. O ciclo PDCA, de Planejar (*Plan*), Executar (*Do*), Verificar (*Check*) e Agir (*Act*), deve ser seguido.

Um sistema de gestão de continuidade de negócios deve possuir pelo menos os seguintes documentos:

- Escopo e objetivos do sistema de gestão de continuidade de negócios.
- Política de continuidade de negócios.
- Descrição de regras e responsabilidades.
- Resultados da avaliação de riscos e da análise de impacto nos negócios.
- Plano de continuidade de negócios.
- Plano de comunicação, treinamento e conscientização.
- Procedimentos de exercícios e testes.

- Procedimentos de avaliação, revisão gerencial e auditoria.
- Ações preventivas e corretivas.

Exemplificando

Uma empresa que buscou a certificação ISO 22301 é a operadora de telecomunicações Vodafone. A certificação ISO 22301 demonstra os esforços da Vodafone do Reino Unido para oferecer aos seus clientes um serviço mais consistente e confiável, independente das circunstâncias. Além disso, proporciona à empresa um serviço diferenciado e vantagem competitiva, bem como capacidade de atender às exigências legais e civis (BSI, 2016).

BSI. **ISO 22301 - Gestão de Continuidade dos Negócios**. Disponível em: <http://www.bsigroup.com/pt-BR/ISO-22301-Continuidade-dos-Negocios/>. Acesso em: 30 ago. 2016.

Norma e padrão de governança de TI

O COBIT (*Control Objectives for Information and Related Technology*) é um *framework* composto por ferramentas, recursos e guias para a governança e gerenciamento de TI. O COBIT é formado por duas camadas principais: a de governança corporativa de TI e a de gestão corporativa de TI.

A camada de governança é composta por cinco processos no domínio "Avaliar, Direcionar e Monitorar (*Evaluate, Direct and Monitor,* EDM)", que tratam de definição de um *framework* de governança, do estabelecimento das responsabilidades em termos de valor para a organização, de fatores de risco e recursos, bem como da transparência da TI para as partes interessadas (CHIARI, 2016).

Já a camada de gerenciamento é definida por quatro domínios:

- Alinhar, Planejar e Organizar (*Align*, *Plan* and *Organize*, APO): relacionada à identificação de como a TI pode contribuir com os objetivos de negócios.
- Construir, Adquirir e Implementar (*Build*, *Acquire* and *Implement*, BAI): relacionada aos investimentos e projetos para tornar concreta a estratégia de TI.
- Entregar, Servir e Suportar (*Deliver*, *Service and Support*, DSS): relacionada à entrega dos serviços de TI necessários para atender à estratégia e à tática.
- Monitorar, Analisar e Avaliar (*Monitor*, *Evaluate* and *Assess*, MEA).

Relacionados diretamente à segurança da informação estão os processos APO12, para gerenciar riscos, e o APO13, para gerenciar segurança. Além disso, há os processos DSS04, para gerenciar continuidade, e o DSS05, para gerenciar serviços de segurança.

Além do COBIT, a norma ABNT NBR ISO/IEC 38500:2009 também trata a governança corporativa de tecnologia da informação.

Norma e padrão de gestão de serviços de TI

O ITIL (*Information Technology Infrastructure Library*) é um conjunto de cinco livros que definem processos para o gerenciamento de serviços de TI. Apesar de não ser focado em segurança da informação, estão relacionados ao assunto os processos de gerenciamento da continuidade do serviço e, também, o gerenciamento da segurança da informação (TUPPENCE, 2010).

Além do ITIL, são importantes as seguintes normas de gestão de serviços (ABNT, 2016):

- ABNT NBR ISO/IEC 20000-1:2011, requisitos do sistema de gestão de serviços.
- ABNT NBR ISO/IEC 20000-2:2013, um guia de aplicação do sistema de gestão de serviços.
- ABNT ISO/IEC TR 20000-5:2011, exemplo de um plano de implementação da ABNT NBR ISO/IEC 20000-1.

Sem medo de errar

A Conseg-123, que é uma consultoria em segurança da informação, com foco em processos e políticas de segurança, deve desenvolver para o Bank$$$ um direcionamento sobre quais normas ele deve seguir para reforçar a sua imagem de um banco moderno e preocupado com os aspectos de segurança da informação, que é uma exigência cada vez maior dos clientes do mercado financeiro.

Para mostrar ao mercado que o Bank$$$ é de fato comprometido com as informações de seus clientes, a Conseg-123 colocou como objetivo principal a busca da certificação ISO 27001. Como há uma relação direta da ISO 27001 com a gestão de riscos, que é também necessária para o sistema de gestão de segurança da informação, outra norma recomendada para o Bank$$$ é a ISO 27005.

A norma ISO 22301 fecha esse direcionamento e visa à continuidade de negócios, garantindo que os serviços do Bank$$$ estejam sempre disponíveis, com o mínimo de interrupções, mesmo após incidentes de segurança.

Atenção

Para uma organização ter um sistema de gestão de segurança da informação, é preciso ter, também, a gestão de riscos, já que é a partir dos resultados da análise e da avaliação de riscos que os controles de segurança da informação são definidos e implementados, fazendo parte do ciclo PDCA dos sistemas de gestão.

Avançando na prática

Tudo ao mesmo tempo

Descrição da situação-problema

Uma nova empresa no setor de pagamentos eletrônicos está sendo montada, a Pag$$$, com o objetivo de investir tudo o que é necessário para prestar serviços em seu estado da arte com a máxima segurança, a máxima disponibilidade e a máxima eficiência operacional tanto interna quanto na relação com seus clientes.

Quais normas e padrões essa empresa deve seguir? Cite as vantagens da adoção, bem como as desvantagens da não-adoção dessas normas e desses padrões.

Lembre-se

Normas e padrões, além de direcionar e organizar as ações específicas daquele assunto, também indicam as intenções das organizações, que podem ser comprovadas com certificações.

Resolução da situação-problema

A Pag$$$ irá buscar três certificações: em proteção de dados de pagamento PCI DSS (PCI, 2013), em gestão de segurança da informação (ISO 27001) e em gestão de continuidade de negócios (ISO 22301). Além disso, a Pag$$$ adotará a ISO 27005 para a gestão de riscos e também o ITIL para a gestão de serviços de TI, que precisa de respostas eficientes. Além disso, sendo um negócio digital, o COBIT também será adotado para a busca da governança de TI.

As vantagens incluem maior visibilidade no mercado como uma empresa preocupada de fato com a segurança da informação e a natural vantagem competitiva no negócio de pagamento eletrônicos, que exige naturalmente a proteção dos dados de cartões. Já a não-adoção torna a Pag$$$ não sustentável a médio e longo prazo, pois incidentes de segurança tendem a acontecer, tornando o negócio inviável.

Faça você mesmo

Utilize os objetivos de controle da norma ABNT NBR ISO/IEC 27002:2013 para estruturar os controles de segurança da organização da Pag$$$. Considere que a empresa é digital, com a sede sendo ocupada pela equipe de desenvolvimento e pela equipe de negócios. A equipe de suporte aos clientes é terceirizada.

Faça valer a pena

1. Normas e padrões são importantes para organizar estratégias e ações relacionadas aos assuntos. Qual das normas relacionadas abaixo possibilita a certificação em gestão de segurança da informação?

a) ISO 27001.
b) ISO 27002.
c) ISO 27005.
d) ISO 22301.
e) ITIL.

2. Normas e padrões são importantes para organizar estratégias e ações relacionadas aos assuntos. Qual das normas relacionadas a seguir possibilita a certificação em gestão de continuidade de negócios?

a) ISO 27001.
b) ISO 27002.
c) ISO 27005.
d) ISO 22301.
e) ITIL.

3. Normas e padrões são importantes para organizar estratégias e ações relacionadas aos assuntos. Qual das normas relacionadas a seguir está relacionada com a gestão de riscos de segurança da informação?

a) ISO 27001.

b) ISO 27002.

c) ISO 27005.

d) ISO 22301.

e) ITIL.

Seção 4.4

Tendências e futuro em segurança da informação

Diálogo aberto

Olá! Chegamos à nossa última aula do curso de segurança da informação e de redes. Já passamos pelos principais assuntos que são essenciais para compreender os desafios e os aspectos envolvidos com a segurança da informação. Desde os princípios básicos de segurança de informação que devem ser protegidos, até os processos e as políticas, passando pelas principais ameaças, pelos mecanismos de defesa, pelo mapeamento de riscos, pela segurança de redes e pela criptografia, você teve a oportunidade de chegar ao entendimento de uma área tão ampla e dinâmica como a segurança da informação.

Agora, chegou a hora de vermos o futuro, discutindo as principais tendências que direcionarão os esforços da evolução natural da segurança da informação e de redes. Nesta aula, alguns conceitos que direcionam a área, como o fato de novas tecnologias trazerem consigo novas vulnerabilidades, serão utilizados como direcionadores, bem como alguns cenários que resultarão em necessidades intrínsecas de segurança da informação, como no caso de carros conectados.

Para exercitar os assuntos discutidos na aula, voltaremos à Conseg-123, que é uma empresa de consultoria focada em processos e políticas de segurança, especializada em projetos envolvendo aspectos não tecnológicos de segurança da informação, cultura de segurança, aplicação das principais normas de segurança da informação e, também, a criação de cenários de futuro para o setor de segurança da informação. O cliente a ser trabalhado nesta aula é a Robplasticx, que é uma fabricante de robôs para a indústria plástica. A Robplasticx possui uma linha de produtos inovadora, mas está se deparando com uma exigência de potenciais clientes quanto à segurança da informação. O objetivo é a criação de um cenário de futuro para a Robplasticx na área de segurança da informação.

Boa aula!

Não pode faltar

Tendências

Nesta seção, iremos explorar alguns aspectos que fazem com que possamos enxergar o futuro da segurança da informação e de redes.

De um lado, a segurança da informação é uma das áreas que mais crescem no mundo, com taxas ascendentes de 9,8% anuais, com estimativas de chegar a US$ 170 bilhões até 2020 (SEGINFO, 2016). Do outro, há a exigência cada vez maior de segurança da informação em produtos e serviços, o que leva ao natural aumento da importância da área em aulas de graduação e pós-graduação, e também em concursos públicos.

Pesquise mais

Veja mais sobre o mercado de segurança cibernética no link a seguir:

SEGINFO. **Mercado de segurança cibernética deve chegar a US$ 170 bilhões em 2020**. Disponível em: <https://seginfo.com.br/2016/01/05/mercado-de-seguranca-cibernetica-deve-chegar-a-us-170-bilhoes-em-2020-2/>. Acesso em: 6 set. 2016.

O que é seguro hoje pode não ser seguro amanhã

Novas vulnerabilidades são descobertas o tempo todo, o que leva ao fato de novos ataques passarem a existir. Somadas a isso, há as ações do crime organizado, que buscam os maiores retornos financeiros, o que faz com que, com os recursos direcionados a alvos específicos, os incidentes de segurança tendam ao crescimento explosivo. Com isso, um ambiente considerado seguro hoje pode não ser seguro amanhã, o que exige uma abordagem de evolução constante de segurança da informação em ciclos (NAKAMURA; GEUS, 2007).

Pesquise mais

Imagine uma vulnerabilidade que pode comprometer grande parte da internet. O *Drown Attack* é uma dessas vulnerabilidades, ao afetar grande parte dos servidores web que utilizam comunicação segura baseada em SSL (*Secure Sockets Layer)*.

CRYPTOSTREAM. **Drown Attack**: **nova vulnerabilidade no SSL**. Disponível em: <https://blog.leverage.inf.br/2016/03/01/drown-attack-nova-vulnerabilidade-no-ssl/>. Acesso em: 8 set. 2016.

Ataques direcionados

Vivemos em um mundo no qual o crime organizado está constantemente em busca de maiores retornos financeiros. Ambientes digitais vulneráveis tendem a se tornar alvos naturais do crime organizado pelo rápido retorno, ainda mais no caso de não representarem muitos riscos para os criminosos. Somados a isso, há os ataques destinados a alvos específicos, por diferentes razões, que vão desde a política até guerras cibernéticas, passando pelos ganhos financeiros (REVA, 2016; UBERDAN, 2012).

De qualquer modo, os ataques direcionados fazem com que a defesa seja muito mais complexa, já que o inimigo irá tentar o ataque até que ele seja efetivo. O conceito aqui é que, para os inimigos, basta encontrar uma fragilidade, enquanto para a defesa é preciso fechar todas as brechas. E, com os recursos necessários, que envolvem tempo e capacitação técnica, um ataque direcionado tende a alcançar o sucesso (NAKAMURA; GEUS, 2007).

Exemplificando

O *Carnanak* é um ataque que causou sérios prejuízos para o mercado financeiro, demonstrando a eficácia de ataques direcionados. Uma citação em Reva (2016, p. 1) reforça isso: "A fase de atividade dos ataques virtuais está se tornando mais curta. Quando os atacantes se especializam em uma operação específica, são necessários apenas alguns dias ou uma semana para conseguirem o que desejam e fugirem."

REVA, João Gustavo. **Depois do *Carbanak*, bancos enfrentam novos ataques**. Disponível em: <http://www.tecmundo.com.br/antivirus/98560-carbanak-bancos-enfrentam-novos-ataques.htm>. Acesso em: 11 set. 2016.

Novas tecnologias trazem consigo novas vulnerabilidades

A complexidade das tecnologias e do seu processo de desenvolvimento possui uma característica intrínseca, que é a possibilidade de condições nem sempre intencionais que levam às vulnerabilidades, que por sua vez podem ser exploradas em ataques. Assim, novas tecnologias trazem consigo novas vulnerabilidades (NAKAMURA; GEUS, 2007). Isso aconteceu com o Wi-Fi (VERÍSSIMO, 2006), com novos bancos de dados (SCITECH, 2005) e com sistemas operacionais (GARCIA, 2015), por mais que existam as maiores preocupações com a segurança. E, atualmente, as vulnerabilidades tornam-se evidentes até mesmo em carros (G1).

Esse fato leva a um dos grandes motes da área, que é a de que a segurança é um processo contínuo, devendo ser aplicada em tempo de projeto, em tempo de desenvolvimento e em tempo de operação ou uso.

Pesquise mais

A vulnerabilidade na primeira versão do Wi-Fi é discutida em Teleco (2016), enquanto um caso envolvendo carros pode ser visto em Silva (2016).

TELECO. **WLAN de Alta Velocidade II: Segurança**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeswlanII/pagina_3.asp>. Acesso em: 11 set. 2016.

SILVA, Carlos L. A. da. **FBI alerta sobre risco de hacking de automóveis**. Disponível em: <http://codigofonte.uol.com.br/noticias/fbi-alerta-sobre-risco-de-hacking-de-automoveis>. Acesso em: 11 set. 2016.

Guerras cibernéticas

Uma nova forma de guerra, baseada não em bombas nucleares, mas em "bombas cibernéticas", é discutida cada vez mais pelos países. Com as preocupações cada vez maiores com as infraestruturas críticas, como as de energia, de telecomunicações ou de transportes, que podem ser afetadas por ataques cibernéticos, a importância dos países com a proteção cibernética aumenta cada vez mais.

Exércitos cibernéticos já fazem parte de vários países, com capacidades tanto ofensivas quanto defensivas. Um exemplo da importância do tema ocorreu no encontro do G20, em 2016, quando o presidente norte-americano Barack Obama discutiu com outros líderes a segurança cibernética (SAPOTEK, 2016).

Pesquise mais

Infraestruturas críticas são cada vez mais o centro nevrálgico dos países nos dias de hoje, já que resultam em impactos imediatos e devastadores aos países (SAPOTEK, 2016).

SAPOTEK. **Dimensão cibernética é crítica para a sobrevivência dos países. Quem o diz é Obama**. Disponível em: <http://tek.sapo.pt/noticias/internet/artigo/a_dimensao_cibernetica_e_critica_para_a_sobrevivencia_dos_paises_quem_o_diz_e_ob-48764qfp.html>. Acesso em: 6 set. 2016.

Impactos em vidas humanas

Com a integração tecnológica cada vez maior, que já faz parte da vida de cada vez mais pessoas, incidentes de segurança podem, nos casos extremos, resultar em impactos em vidas humanas. Se até agora um incidente de segurança levava a aborrecimentos ou prejuízos financeiros, a tendência é que as vidas humanas possam

sofrer diretamente com os ataques cibernéticos, sejam eles com a intenção explícita ou não (NAKAMURA, 2016).

Há quatro contextos principais que possuem relação com vidas humanas: as infraestruturas críticas, a Internet das Coisas, os carros conectados e a indústria 4.0.

Reflita

Será que uma vida humana pode mesmo ser comprometida em um ataque cibernético? Pense nas integrações entre o físico e o digital, e também nas interdependências que existem e que aumentam nas nossas tarefas do cotidiano.

Infraestruturas críticas

Como países em guerra podem afetar um ao outro de uma forma rápida, eficiente e devastadora. Atacando suas infraestruturas críticas que, com as integrações e a conectividade, podem sofrer ataques cibernéticos que paralisam serviços críticos, como a energia, as telecomunicações, os transportes ou o financeiro (RIBEIRO et al., 2007).

Os reflexos para vidas humanas podem ser grandes, como acidentes de trânsito causados com confusões em sinalizações após uma invasão no sistema de transportes. No caso da infraestrutura crítica de energia, hospitais ou outras atividades críticas podem sofrer com interrupções no fornecimento de energia, ocasionados por ataques aos sistemas SCADA (*Supervisory Control And Data Acquisition*) de concessionárias de energia, por exemplo (NAKAMURA, 2016).

Pesquise mais

Uma das principais infraestruturas críticas de qualquer país é a de telecomunicações. Veja sobre a identificação de infraestrutura crítica de telecomunicações realizada para os Jogos Pan-Americanos, em 2007, em Ribeiro et al. (2007).

RIBEIRO, Sérgio Luís et al. Aplicação da Metodologia para Identificação da Infraestrutura Crítica (MI2C) no Pan 2007. **Cadernos CPqD Tecnologia**, Campinas, v. 3, n. 2, p. 7-16, jul./dez. 2007. Disponível em: <https://www.cpqd.com.br/cadernosdetecnologia/Vol3_N2_jul_dez_2007/pdf/artigo1.pdf>. Acesso em: 8 set. 2016.

Carros conectados

Os carros autônomos e conectados avançam rapidamente, com vários experimentos sendo realizados ao redor do mundo. O que tem causado preocupações é que eles estão sendo alvos de constantes ataques cibernéticos, em uma demonstração de que vidas humanas podem ser colocadas em risco.

Com o controle remoto de veículos, já foram demonstrados ataques que controlavam funções críticas dos carros, como aceleradores, freios e mesmo direção (G1, 2015).

Em casos mais simples, acessos a carros sem as chaves também envolvem a necessidade de mecanismos de segurança da informação, como a que afeta mais de 100 milhões de veículos da VW (G1, 2016).

Pesquise mais

Saiba mais sobre os ataques cibernéticos a carros da Fiat Chrysler e sobre carros da VW sendo acessados sem as chaves.

G1. **Fiat Chrysler chama 1,4 milhão de carros que podem ser hackeados.** 2015. Disponível em: <http://g1.globo.com/carros/noticia/2015/07/fiat-chrysler-chama-14-milhao-de-carros-que-podem-ser-hackeados.html>. Acesso em: 8 set. 2016.

G1. **Carros com acesso sem chave da VW podem ser hackeados, diz estudo.** 2016. Disponível em <http://g1.globo.com/carros/noticia/2016/08/carros-com-partida-sem-chave-da-vw-podem-ser-hackeados-diz-estudo.html>. Acesso em: 8 set. 2016.

Indústria 4.0

O avanço da Internet das Coisas, o uso de sensores, a conectividade e a inteligência chegam, também, na indústria, que passa a usufruir das vantagens da era digital de uma forma mais prática. Isso resulta em novas oportunidades de ataques cibernéticos, que exigem uma abordagem em segurança da informação (CPQD, 2016).

Na indústria 4.0, projetos podem ser desenvolvidos em uma matriz brasileira para serem produzidos em uma filial europeia, por exemplo. Novas preocupações de segurança da informação passam a existir nesse cenário, como o roubo dos projetos de novos produtos, que podem ser feitos na matriz, na filial ou nos meios de comunicação. Mais desafiador está o fato de as informações dos projetos existirem nos servidores, e também nos robôs das fábricas, que estão todos conectados (CPQD, 2016).

Assimile

Uma das principais tendências em segurança da informação é a integração entre o físico e o digital, o que leva à necessidade de conhecimentos integrados de hardware e de software. Isso é comprovado pelos avanços, principalmente, da Internet das Coisas, dos carros conectados e da indústria 4.0.

Mobilidade e computação em nuvem

O mundo é móvel, com informações trafegando de tal modo que uma pergunta vem à tona: perímetros de rede ainda fazem sentido? A resposta é que sim, e na realidade fazem mais sentido ainda em um mundo móvel, já que o ambiente a ser protegido muda com as informações, não existindo mais somente nos servidores das empresas.

Além da evolução da abordagem de proteção das informações das empresas, outro aspecto que aumenta a complexidade de proteção é que os acessos às informações são feitos de uma forma cada vez mais heterogêneos, a partir de diferentes origens. Com isso, surgem novos vetores de ataques cibernéticos, como os dispositivos móveis.

No caso de bancos, por exemplo, a infraestrutura pode ser considerada bastante segura, de modo que há um mito de que é quase impossível realizar um ataque cibernético atacando um banco. O que ocorre, na prática, é o ataque aos clientes dos bancos, que utilizam seus dispositivos contaminados, os vetores para as fraudes financeiras. O resultado é que há grandes prejuízos com isso.

Assim, uma tendência é que aumente a importância da segurança móvel, bem como a segurança nas pontas (ou *endpoint*), em uma clara abordagem em camadas, que é fundamental em segurança da informação.

Reflita

No caso dos bancos, há o mito de que é quase impossível atacar sistemas do banco. E o Carbanak? O que ele representa para a segurança da informação?

Necessidades de segurança

Durante todo o curso, vários aspectos da segurança da informação e de redes foram visitados e discutidos. Porém, como ficou evidente, há uma série de necessidades de segurança que precisam ser tratadas de uma forma mais efetiva pelas organizações.

Um fato que indica a abrangência da segurança da informação são as próprias equipes das organizações, que agrupam perfis bastante diferentes, tais como administradores de segurança e de redes, especialistas em identidades, desenvolvedores de políticas de segurança, especialistas em avaliações de segurança, analistas de riscos, arquiteto de segurança física ou especialista em criptografia, por exemplo (VENÂNCIO, 2016).

Algumas necessidades de segurança tendem a levar ao crescimento mais acentuado de alguns perfis, tais como Guia (2016), Pimenta (2015) e Nakamura (2016):

Desenvolvedores de software (e hardware) que seguem metodologias de desenvolvimento seguro: cada vez mais o mercado exigirá produtos seguros, que começam no seu desenvolvimento.

- Arquitetos de segurança da informação: apenas com uma visão abrangente de todos os aspectos de segurança da informação, tanto das ameaças quanto de tecnologias disponíveis, é possível fazer as organizações seguirem um caminho que leva à segurança efetiva. Reconhecer que não há uma bala de prata que resolva todos os problemas de segurança de uma só vez é importante para que uma abordagem em camadas seja adotada, com otimização de recursos, ou seja, com o uso de controles de segurança que não excedam as necessidades específicas de cada organização.

- Gestores de segurança da informação: de uma forma similar aos arquitetos, os gestores devem ter uma visão cada vez mais alinhada com as constantes e rápidas mudanças que ocorrem, de modo a definir a melhor estratégia de segurança da informação das organizações. Os gestores devem ter uma capacidade cada vez maior de integração entre diferentes áreas de negócios, que passam a ter relações cada vez mais diretas com os incidentes de segurança. Foco especial para a continuidade de negócios, que passa a agregar cada vez mais exigências de negócios e exigências legais.

- Especialistas em forense computacional: investigações de incidentes de segurança da informação ganharão importância com os avanços legais que ocorrem em todo o mundo. O mundo é digital e os aspectos técnicos e legais dos crimes cibernéticos naturalmente farão parte das organizações.

Sem medo de errar

A Conseg-123 é uma empresa de consultoria focada em processos e políticas de segurança, especializada em projetos envolvendo aspectos não tecnológicos de segurança da informação, cultura de segurança, aplicação das principais normas de segurança da informação e, também, criação de cenários de futuro para o

setor de segurança da informação. A Robplasticx, uma fabricante de robôs para a indústria plástica, necessita de um cenário de futuro para a segurança da informação, principalmente devido à exigência crescente de potenciais clientes.

Os principais pontos que a Conseg-123 pode considerar para a criação de um cenário de futuro para a Robplasticx são:

- O que é seguro hoje pode não ser amanhã, o que exige da Robplasticx uma demonstração de como os seus robôs, que são conectados, estão sendo construídos. Mesmo sem nenhum caso de ataques ainda, o mercado sabe que, no caso de um ataque a um robô da empresa, outros ataques poderão acontecer.
- Ataques direcionados, o que faz com que a Robplasticx tenha que definir quais são os mecanismos de segurança existentes em seus produtos, já que a concorrência pode ser um vetor para espionagem industrial, o que é facilitado com os robôs conectados.
- Novas tecnologias trazem consigo novas vulnerabilidades, o que leva a Robplasticx a entregar robôs que tenham passado por uma avaliação de segurança, incluindo a possibilidade de certificações em segurança da informação.

Atenção

A Robplasticx faz parte da indústria 4.0, que utiliza um conjunto de tecnologias conectadas para uma nova revolução industrial. A primeira revolução veio com o uso de máquinas, vapor e força hidráulica nas fábricas. A segunda revolução trouxe a eletricidade e a produção em massa. Já a terceira revolução veio com o uso de computadores, que permitiu a automação. A quarta revolução vem com o uso de um conjunto de tecnologias que cria um ambiente versátil de produção que integra o físico com o digital. Há sensores inteligentes, robôs conectados que se autoconfiguram, impressoras 3D, análise *big data* e canais de comunicação que trafegam grande quantidade de diferentes tipos de dados. As inovações levam a uma linha de produção mais efetiva, com capacidade de entregar produtos customizados e individuais melhores, mais rápidos e a custos menores. Um dos reflexos da indústria 4.0 é a necessidade de segurança da informação, o que é potencializado pela integração entre o físico e o digital, que pode levar a impactos para vidas humanas (CPQD, 2016).

Avançando na prática

Vidas humanas e a segurança da informação

Descrição da situação-problema

Além da indústria 4.0, que integra o físico com o digital, a infraestrutura crítica e também os carros conectados são exemplos de contextos que levam à possibilidade de reflexos para vidas humanas a partir de ataques cibernéticos.

Faça uma breve descrição sobre a razão que leva um ataque cibernético a causar impactos para vidas humanas nos três contextos citados: indústria 4.0, infraestrutura crítica e carros conectados.

Pense em três fases principais: na primeira fase, descreva rapidamente quais elementos podem ser vítimas de ataques nos três contextos citados; na fase 2, relacione os tipos de ataques que podem ocorrer sobre os elementos citados na fase anterior; para finalizar, relacione os ativos relacionados na fase 1 com os ataques relacionados na fase 2 para chegar às vidas humanas.

Lembre-se

Novas tecnologias trazem consigo novas vulnerabilidades. Esse fato, no caso dos contextos citados, é potencializado pela conectividade, já que criam as condições para os ataques remotos.

Resolução da situação-problema

Fase 1:

- Indústria 4.0: há robôs, redes, servidores, máquinas industriais e operadores.
- Infraestrutura crítica: há sistemas de controle, elementos físicos, sistemas de energia e toda a população que utiliza esses serviços.
- Carros conectados: há o carro, com sistemas de supervisão e barramentos com sistemas de controle, além do motorista.

Fase 2:

- Indústria 4.0: ataque à rede, ataque aos robôs, ataques a qualquer ponto para roubo de informações de projetos.
- Infraestrutura crítica: ataque a qualquer ponto da infraestrutura, como ao sistema de controle, e também a elementos físicos conectados.

Fase 3:

- Na indústria 4.0, em que a produção é realizada com robôs conectados, há o risco natural de ataques cibernéticos que podem resultar em controle (ou descontrole) dos robôs, o que podem levar a incidentes fatais.
- Na infraestrutura crítica, setores como energia, transportes e telecomunicações podem ser afetados com ataques cibernéticos. Acidentes no trânsito poderão ser causados por ataques dessa natureza, bem como o fornecimento de energia elétrica pode ser interrompido, o que pode afetar hospitais, por exemplo.
- Nos carros conectados, como já foi demonstrado, ataques cibernéticos podem levar ao controle da direção, de funções do motor ou do câmbio. Sequestros e acidentes automobilísticos poderão ocorrer, afetando assim as vidas humanas.

Faça você mesmo

Com os avanços tecnológicos, há uma relação cada vez maior entre ataques cibernéticos e os reflexos na vida humana. Cite algumas situações em que as pessoas passam a sofrer grandes riscos com os ataques cibernéticos.

Faça valer a pena

1. Uma das tendências em segurança da informação é o constante aumento dos ataques cibernéticos. Considere os seguintes fatores:

I. Aumento de conectividade.

II. Aumento de vulnerabilidades.

III. Ganhos financeiros com os ataques.

Quais fatores podem ser considerados relevantes para o aumento dos ataques cibernéticos?

a) Somente I.

b) Somente I e III.

c) Somente II.

d) I, II e III.

e) Somente III.

2. O aumento da conectividade pode levar ao aumento dos ataques cibernéticos. Você concorda com essa afirmação, e por quê?

a) Não, porque não há relação entre conectividade e ataques.

b) Não, porque ataques não exploram conexões de redes.

c) Não, porque basta utilizar firewalls para a proteção.

d) Sim, porque a conectividade aumenta a superfície de ataques.

e) Sim, porque a conectividade torna tudo mais vulnerável.

3. Ataques cibernéticos acontecem quando um agente de ameaça explora uma vulnerabilidade de um ativo, fazendo com que uma ameaça se torne um incidente de segurança. Quanto às vulnerabilidades, você acredita em qual das alternativas abaixo?

a) Vulnerabilidades serão reduzidas no futuro, porque a criptografia será utilizada.

b) Vulnerabilidades serão reduzidas no futuro, porque já foram tratadas.

c) Vulnerabilidades aumentarão, pois novas tecnologias trazem novas vulnerabilidades.

d) Vulnerabilidades aumentarão, pois haverá mais agentes de ameaça para atacar.

e) Vulnerabilidades continuarão no mesmo nível.

Referências

ABNT ISO GUIA 73:2009. **Gestão de Riscos** – Vocabulário. 2009.

ABNT NBR ISO 22301:2013. **Segurança da sociedade** - Sistema de gestão de continuidade de negócios - Requisitos. 2013.

ABNT NBR ISO/IEC 27001:2013. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação** – Requisitos. 2013.

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação**. 2013.

ABNT NBR ISO/IEC 27005:2011. **Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação**. 2011.

ABNT ISO 31000:2009. **Gestão de Riscos - Princípios e Diretrizes**. 2009.

ABNT ISO/TR 31004:2015. **Gestão de riscos - Guia para implementação da ABNT NBR ISO 31000**. 2015.

ABNT NBR ISO/IEC 31010:2012. **Gestão de riscos - Técnicas para o processo de avaliação de riscos**. 2012.

ABNT. **Catálogo**. Disponível em: <http://www.abntcatalogo.com.br/default.aspx>. Acesso em: 30 ago. 2016.

ARRUDA, Felipe. **Saiba como hackers apagaram a vida digital de um jornalista em apenas uma hora**. Disponível em: <http://www.tecmundo.com.br/seguranca/27993-saiba-como-hackers-apagaram-a-vida-digital-de-um-jornalista-em-apenas-uma-hora.htm>. Acesso em: 26 jul. 2016.

BANCO CENTRAL DO BRASIL. **Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional**. 2009. Disponível em: <http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf>. Acesso em: 29 ago. 2016.

CHIARI, Renê. **Compreendendo os principais conceitos do COBIT® 5**. Disponível em: <http://www.itsmnapratica.com.br/compreendendo-os-principais-conceitos-do-cobit-5/>. Acesso em: 7 set. 2016.

CPQD. **Webinar**: segurança cibernética na indústria 4.0. Disponível em: <https://www.youtube.com/watch?v=aSnhmvQHidM>. Acesso em: 29 set. 2016.

G1. **Hackers chineses conseguem controlar carro da Tesla à distância**. Disponível em: <http://g1.globo.com/carros/noticia/2016/09/hackers-chineses-conseguem-controlar-carro-da-tesla-distancia.html>. Acesso em: 29 set. 2016.

G1. **Carros com acesso sem chave da VW podem ser hackeados, diz estudo**. 2016. Disponível em <http://g1.globo.com/carros/noticia/2016/08/carros-com-partida-sem-chave-da-vw-podem-ser-hackeados-diz-estudo.html>. Acesso em: 8 set. 2016.

GARCIA, Daniel. Mac OS X e iOS lideram lista de sistemas operacionais mais vulneráveis, diz estudo. **Revista Exame**, 2015. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/mac-os-x-e-ios-lideram-lista-de-sistemas-operacionais-mais-vulneraveis>. Acesso em: 29 set. 2016.

GUIA da carreira. **Segurança da informação**. Disponível em: <http://www.guiadacarreira.com.br/cursos/seguranca-da-informacao/>. Acesso em: 29 set. 2016.

ISO/IEC 13335-1:2004. **Information technology - Security techniques - Management of information and communications technology security**: concepts and models for information and communications technology security management. 2004.

ITU. **Security architecture for systems providing end-to-end communications**. **X.805**. 2003. Disponível em: <https://www.itu.int/rec/T-REC-X.805-200310-I/en>. Acesso em: 20 mar. 2016.

MITNICK, Kevin D.; SIMON, William M. **A arte de enganar**. São Paulo: Makron Books, 2003.

NAKAMURA, Emilio T. **Vidas humanas dependem cada vez mais de segurança da informação**: **isso é um exagero?** Disponível em: <https://www.linkedin.com/pulse/vidas-humanas-dependem-cada-vez-mais-de-seguran%C3%A7a-da-isso-nakamura>. Acesso em: 29 set. 2016.

NAKAMURA, Emilio T.; GEUS, Paulo L de. **Segurança de redes em ambientes cooperativos**. São Paulo: Editora Novatec, 2007.

NETO, João Sorima. Investimento em segurança da informação cresce mais no país. **O Globo**, 2015. Disponível em: <http://oglobo.globo.com/economia/negocios/investimento-em-seguranca-da-informacao-cresce-mais-no-pais-17645471>. Acesso em: 29 mar. 2016.

PCI. **Requisitos e procedimentos da avaliação de segurança. Versão 3.0**. 2013. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/PCI_DSS_v3.pdf>. Acesso em: 22 ago. 2016.

PIMENTA, Adriano. **7 competências que o mercado espera dos profissionais de segurança da informação**. 2015. Disponível em: <https://www.arcon.com.br/blog/7-competencias-que-o-mercado-espera-dos-profissionais-de-seguranca-da-informacao>. Acesso em: 29 set. 2016.

REVA, João Gustavo. **Depois do Carbanak, bancos enfrentam novos ataques**. Disponível em: <http://www.tecmundo.com.br/antivirus/98560-carbanak-bancos-enfrentam-novos-ataques.htm>. Acesso em: 11 set. 2016.

RIBEIRO, Sérgio Luís et al. Aplicação da Metodologia para Identificação da Infraestrutura Crítica (MI2C) no Pan 2007. **Cadernos CPqD Tecnologia**, Campinas, v. 3, n. 2, p. 7-16, jul./dez. 2007. Disponível em: <https://www.cpqd.com.br/cadernosdetecnologia/Vol3_N2_jul_dez_2007/pdf/artigo1.pdf>. Acesso em: 8 set. 2016.

SAPOTEK. **Dimensão cibernética é crítica para a sobrevivência dos países. Quem o diz é Obama**. Disponível em: <http://tek.sapo.pt/noticias/internet/artigo/a_dimensao_cibernetica_e_critica_para_a_sobrevivencia_dos_paises_quem_o_diz_e_ob-48764qfp.html>. Acesso em: 6 set. 2016.

SCITECH. ***Oracle unbreakable* com *hash* de senhas fraco.** 2005. Disponível em: <https://techberto.wordpress.com/2005/10/22/oracle-unbreakable-com-hash-de-senhas-fraco/>. Acesso em: 29 set. 2016.

SEGINFO. **Mercado de segurança cibernética deve chegar a US$ 170 bilhões em 2020**. Disponível em: <https://seginfo.com.br/2016/01/05/mercado-de-seguranca-cibernetica-deve-chegar-a-us-170-bilhoes-em-2020-2/>. Acesso em: 6 set. 2016.

TND BRASIL. **Adobe flash player apresenta falha de segurança**. 2015. Disponível em: <http://www.tndbrasil.com.br/adobe-flash-player-apresenta-falha-de-seguranca/>. Acesso em: 12 set. 2016.

TUPPENCE. **Vamos desmistificar ITIL**. 2010. Disponível em: <https://tuppencetd.wordpress.com/category/t-i/itil/>. Acesso em: 30 ago. 2016.

UBERDAN, Lúcio. **Cibercrime**: a quarta era do crime organizado não é formada de "jovens hackers". 2012. Disponível em: <https://relatividade.wordpress.com/2012/03/29/cibercrime-a-quarta-era-do-crime-organizado-nao-e-formada-de-jovens-hackers/>. Acesso em: 29 set. 2016.

VENÂNCIO, Rafael. **Por que o futuro da segurança da informação está no foco em pessoas**. Disponível em: <http://computerworld.com.br/por-que-o-futuro-da-seguranca-da-informacao-esta-no-foco-em-pessoas>. Acesso em: 29 set. 2016.

VERÍSSIMO, Fernando. **O problema de segurança em redes baseadas no padrão 802.11**. 2006. Disponível em: <http://www.lockabit.coppe.ufrj.br/artigo/problema-seguranca-em-redes-baseadas-no-padrao-80211>. Acesso em: 29 set. 2016.

Anotações

Anotações

Anotações

ISBN 978-85-8482-594-3