

Segurança e Auditoria de Sistemas

Segurança da informação e redes

Prof^a. Ms. Adriane Ap. Loper

- Unidade de Ensino: 1
- Competência da Unidade: Princípios de Segurança da Informação - Confidencialidade, Integridade, Disponibilidade, Vulnerabilidade, Ameaça e Exploit
- Resumo: Principais definições em segurança da informação.
- Palavras-chave: ameaça, vulnerabilidade, cid
- Título da Teleaula: Segurança da informação e redes
- Teleaula nº: 1

Contextualização

- Você é o responsável pela segurança da informação de uma empresa do setor químico, que conta com os maiores cientistas brasileiros.
- A empresa possui unidades em São Paulo, Rio de Janeiro e Salvador, com cooperação internacional com uma empresa chinesa e outra suíça.
- Há grandes investidores financiando seus projetos.
- A sua atividade será focada em um grande projeto em andamento que já chegou a grandes resultados, com os cientistas tendo descoberto um novo composto que será utilizado na indústria agrícola.



Contextualização

- O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.
- Prepare uma apresentação para a diretoria executiva da empresa com a sua visão sobre a necessidade de se tomar ações para a segurança do projeto.
- Pense no que pode acontecer com o projeto do novo produto e a estratégia de marketing.
- A diretoria executiva precisa conhecer a CID, correspondente à confidencialidade, integridade e disponibilidade.



Contextualização

- Neste caminho as informações podem ser vazadas, alteradas ou destruídas (CID).
- Apresente os elementos do risco para a diretoria executiva.
- Além disso, eles devem compreender que é preciso garantir que estas informações estejam sempre acessíveis pelas equipes responsáveis (disponibilidade).
- Para finalizar, apresente um resumo sobre os controles de segurança sugeridos para a prevenção.
- Com a apresentação, você irá iniciar a evolução do nível de maturidade em segurança da informação, principalmente com uma resposta inicial para a pergunta: “Segurança da informação para quê?”.



Introdução à Segurança da Informação

Segurança de Informação

- Segundo Pena (2016), na Era da Informação, há o grande desafio da segurança da informação, sem a qual pessoas, empresas, governos, países e instituições estão sujeitas a sofrerem variados incidentes com uma grande amplitude de impactos.
- A Segurança da Informação pode ser estudada visando-se:
- Segurança de Sistemas (Firewall, Vírus, Cavalos de Tróia , Vermes....) e
- Segurança em Redes: Criptografia, Autenticação, Protocolos, Plataformas.
- A segurança é tão forte quanto o seu elo mais fraco!



Fonte: Shutterstock

Segurança de Informação

- A segurança da informação protege a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos aos negócios e maximizando o retorno dos investimentos e oportunidades. (Norma ABNT ISO/IEC 27002 (2013)).
- Segurança da informação envolve identificação, proteção, detecção, resposta e recuperação (NIST, 2020).



Fonte: Adaptado de NIST (NIST, 2020).



Fonte: Shutterstock

Segurança de Informação

- Nada é 100% seguro porque os elementos do risco são dinâmicos, seja quando novas vulnerabilidades surgem, quando o ambiente muda com novos ativos, ou quando a motivação de um agente de ameaça alcança níveis que aumenta a chance de sucesso de um ataque.
- Assim, o que é seguro hoje pode não ser amanhã. Além disso, pontos de ataques envolvem ativos tecnológicos, humanos e processuais (NAKAMURA, 2016).



Fonte: Shutterstock

Segurança de Informação

- Nada é 100% seguro porque os elementos do risco são dinâmicos, seja quando novas vulnerabilidades surgem, quando o ambiente muda com novos ativos, ou quando a motivação de um agente de ameaça alcança níveis que aumenta a chance de sucesso de um ataque.
- Assim, o que é seguro hoje pode não ser amanhã. Além disso, pontos de ataques envolvem ativos tecnológicos, humanos e processuais (NAKAMURA, 2016).



Fonte: Shutterstock

Pilares da S.I - Confidencialidade

Para a ABNT NBR ISO/IEC 27001:2013 (ISO 27001, 2013),

- É a propriedade de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados.
- Como garantir?
- Somente pessoas autorizadas?
- Evitar acessos?
- Impedir vazamentos?



Fonte: Autora

Pilares da S.I - Integridade

- As informações devem permanecer íntegras, ou seja, não podem sofrer qualquer tipo de modificação .
- Segundo a ABNT NBR ISO/IEC 27001:2013, integridade é a propriedade de salvaguarda da exatidão e completeza de ativos.



Fonte: Autora

Pilares da S.I - Disponibilidade

- Disponibilidade ===➔ Percepção!
- As informações devem estar disponíveis. Ela é logo notada quando há um incidente de segurança.
- Comprometem a disponibilidade são a negação de serviço, com o DoS (Denial of Service) e o DDoS (Distributed Denial of Service).



Fonte: Autora

Autenticidade, Não-Repúdio, Legalidade

- **Autenticidade** - busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser;
- **Não-Repúdio (Irretratabilidade)** - busca-se garantir que o usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação;
- **Legalidade** – O aspecto de legislação e normatização.



Fonte: Autora

CID

1) Ano: 2018 **Banca:** FCC **Órgão:** TRT - 15ª Região (SP) **Prova:** FCC - 2018 - TRT - 15ª Região (SP) - Técnico Judiciário - Segurança

A proteção de três princípios é a razão de ser da segurança da informação. As medidas que garantem que a informação seja mantida nas mesmas condições disponibilizadas pelo proprietário atende ao princípio da ..I.... , a garantia de que estará à disposição dos usuários sempre que eles precisarem é o princípio da ..II.... , ao estabelecer graus de sigilo, no tocante ao conteúdo, visando o acesso apenas a determinadas pessoas observamos o princípio da ..III.... .

Preenche, correta e respectivamente, as lacunas I, II e III:

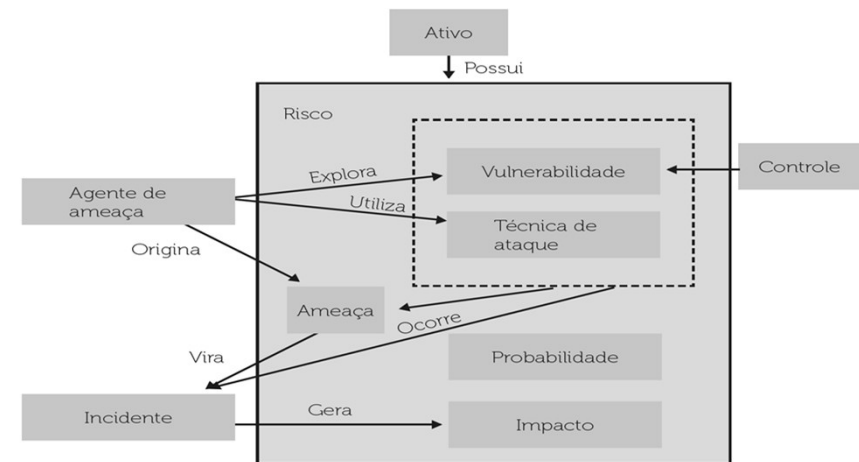
- a) conformidade – confidencialidade – sensibilidade
- b) integridade – disponibilidade – confidencialidade

- c) disponibilidade – confidencialidade – integridade
- d) confidencialidade – disponibilidade – conformidade
- e) integridade – sensibilidade – legalidade

Elementos de Risco

Risco

O **risco** de segurança da informação:
É a probabilidade de um agente de ameaça explorar vulnerabilidade(s) de ativo(s), fazendo com que uma ameaça se torne um incidente de segurança, o que causa impactos e danos a um ativo ou um grupo de ativos da empresa.

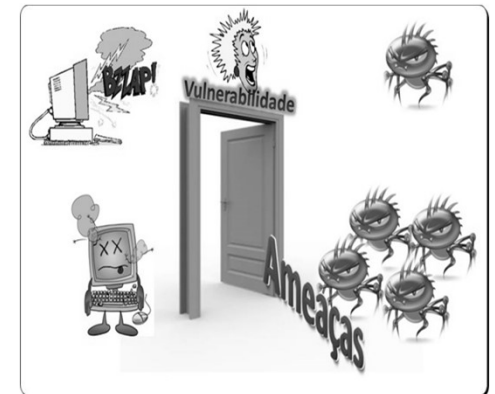


Fonte: Nakamura(2020)

Risco

A vulnerabilidade corresponde a uma falha ou fraqueza em procedimentos de segurança, design, implementação ou controles internos de sistemas, que pode ser disparada acidentalmente ou explorada intencionalmente, resultando em brecha de segurança ou violação da política de segurança do sistema, que existe em ativos.

Os controles de segurança ou os mecanismos de defesa, devem ser aplicados em vulnerabilidades para evitar que sejam explorados pelos agentes de ameaça.



Matriz de riscos

Já a **ameaça** é o potencial de um agente da ameaça explorar uma vulnerabilidade específica, accidental ou intencionalmente. Uma negação de serviço e o vazamento de informações são exemplos de ameaças.

Quando isso ocorre, a ameaça se torna um incidente de segurança, o que resulta em impactos para a organização.

A análise e avaliação de riscos são feitas com o cálculo da probabilidade e do impacto de cada um dos eventos identificados, formando uma matriz de riscos.

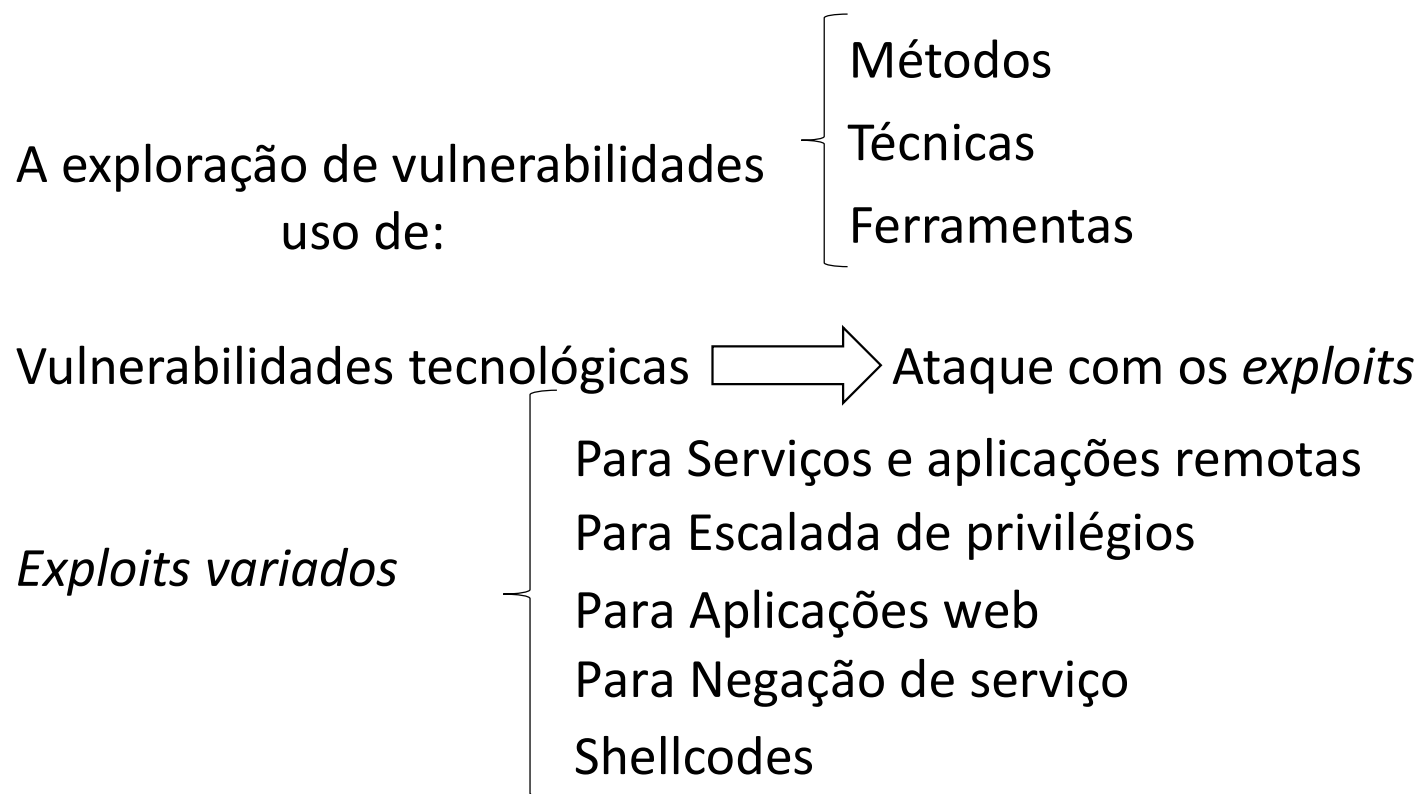
O cálculo da probabilidade disso tudo acontecer representa o risco, segundo cálculo **$R=P*I$** , no qual R=Risco, P=Probabilidade e I=Impacto.

Probabilidade		1	2	3
Impacto	B	1	2	3
	M	2	4	6
3	A	3	6	9
	E	4	8	12

Risco (P x I)	1	Insignificante
	2 e 3	Baixo
	4 e 6	Médio
	8 e 9	Alto
	12	Extremo

Fonte: Autora

Vulnerabilidades

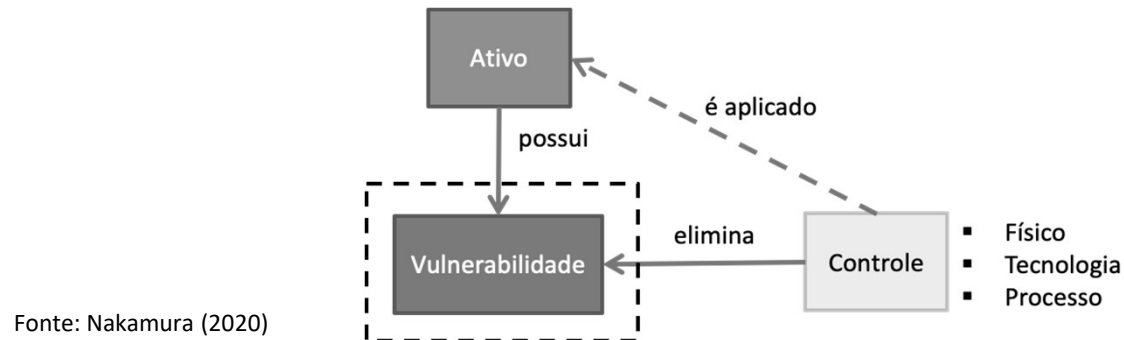


Fonte: Shutterstock

Prevenção contra os riscos

A proteção, que visa a prevenção contra os riscos identificados, analisados e avaliados, é feita pela definição e implementação de controles de segurança, que engloba mecanismos de defesa e uso de medidas e técnicas de segurança de redes.

Os controles de segurança podem ser físicos, tecnológicos ou processos, e são aplicados nos ativos para remover as vulnerabilidades conforme o fluxo de controle :



Apresentação aos diretores

A estrutura da apresentação pode ser como esta sugestão:

Iniciar um trabalho que começa com uma visão organizada de todos os principais conceitos da segurança da informação:

- A segurança da informação envolve identificação, proteção, detecção, resposta e recuperação;
- É preciso garantir os princípios da segurança da informação: confidencialidade, integridade, disponibilidade;
- É preciso trabalhar com os elementos do risco: ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade, impacto;
- A aplicação dos mecanismos de defesa, controles de segurança e técnicas de segurança de redes é definida a partir de uma visão de riscos.

A estrutura da apresentação pode ser como esta sugestão:

Essa visão organizada é fundamental para que uma cultura de segurança se inicie e possibilite uma evolução constante do nível de maturidade da empresa, começando pela diretoria executiva. Ao final da apresentação, ficará mais claro para todos o que está envolvido com a questão “Segurança da informação para quê?”

1. Resumo do projeto da empresa;
2. Ativos envolvidos no projeto, não se esquecendo que eles podem ser as pessoas, os equipamentos e artefatos físicos, os processos e os sistemas e tecnologias. Não é necessário citar todos, mas uma boa representatividade é importante;
3. Considere *crackers* e concorrentes como agentes de ameaça. Cite uma ameaça de cada tipo que afeta a C, I e D.

A estrutura da apresentação pode ser como esta sugestão:

4. Justifique que os ativos podem ter vulnerabilidades, explicando sobre elas;
5. Explique sobre impactos em caso de uma ameaça se tornar um incidente de segurança. Você deve considerar a tríade CID e descrever impactos incrementais, que iniciam com a equipe e incluem o projeto, indo até a empresa e as perdas financeiras, de mercado e de reputação, por exemplo;
6. Faça uma relação entre os elementos do risco, juntando as informações anteriores;
7. Defina uma proposta de implementação de controles de segurança, mecanismos de defesa e técnicas de segurança de redes. Aponte quais são eles;

A estrutura da apresentação pode ser como esta sugestão:

- Atenção para os princípios da segurança da informação: confidencialidade, integridade e disponibilidade.
- São eles que precisam ser protegidos, como um todo. Uma falha comum é focar em apenas um dos aspectos da segurança da informação, negligenciando os outros.
- Há muitas ameaças rondando o ambiente da empresa, e as vulnerabilidades precisam ser identificadas.
- Com a sua apresentação, você estará respondendo a uma série de questões, dentre as quais:

Compreendera os pilares e o riscos da segurança da informação?



Fonte: <https://gifer.com/en/XIOL9>

Controles de segurança

Sua missão

Você irá detalhar os seguintes elementos:

- Pontos de ataques, representados por sistemas compostos por diferentes aspectos, que possuem vulnerabilidades: *hardware*, *software*, protocolos, aplicações;
- Pontos de ataques indicando os ativos humanos e físicos envolvidos;
- Agentes de ameaça, ameaças e técnicas de ataques;
- Controles de segurança para a autenticação dos usuários;
- Controles de segurança de rede.

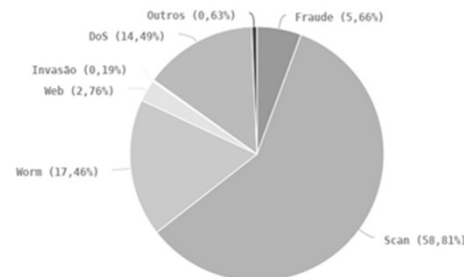
Atualidade

- Em agosto de 2020, a bolsa de valores da Nova Zelândia sofreu paralização de suas operações em virtude de ataques de negação de serviços por quatro dias (CPOM, 2020).
- E ataques de *ransomware*, que sequestram dados de servidores e usuários com finalidade de resgates, continuam fazendo vítimas em todo o mundo (CRN, 2020).
- Estes dois casos mostram que os ataques de *crackers*, ou ataques cibernéticos, continuam acontecendo e evoluindo numa alta velocidade, atingindo desde pequenos negócios até infraestruturas críticas de países.

CERT.br

- O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.
- É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. (CERT, 2020).

Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020
Tipos de ataque



Fonte: CERT.BR, 2021. Disponível em: < <https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html>.
Acesso em: 01mar21.

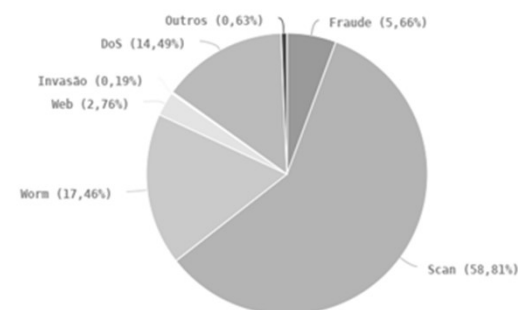
© CERT.br -- by Highcharts.com

CERT.br

worm	notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
DoS (Denial of Service)	notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
invasão	um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
web	um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
scan	Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
fraude	Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
outros	notificações de incidentes que não se enquadram nas categorias anteriores

Fonte: (CERT.BR, 2020).

Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020
Tipos de ataque



Fonte: CERT.BR, 2021. Disponível em:
< <https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html>.
Acesso em: 01mar21.

Lei Geral de Proteção de Dados Pessoais (LGPD)


- Com a Lei Geral de Proteção de Dados Pessoais (LGPD), os dados pessoais devem ser protegidos para a garantia da privacidade.
- Ataques podem ser realizados para vazar dados pessoais e comprometer a privacidade, e ataques podem ocorrer com dados em processamento (DIU), dados em transmissão (DIM) ou dados armazenados (DAR).
- Ataques a banco de dados visam os dados armazenados, enquanto ataques à rede visam os dados em transmissão. Já os dados em processamento podem sofrer ataques mais sofisticados

Agentes de Ameaça, Ameaças e Técnicas de Ataques

- Os agentes de ameaça são elementos importantes para o entendimento dos riscos e da segurança.
- Os agentes de ameaça mais comuns são as pessoas, que possuem facetas diferentes, de acordo com o ambiente em avaliação. Por exemplo, os crackers, um funcionário mal-intencionados, fraudadores.
- Há ainda os agentes de ameaça naturais, que podem comprometer a disponibilidade da informação em caso de uma inundação de datacenter.
- Um agente de ameaça bastante crítico, que pode ser considerado também uma ameaça, é o malware, ou o código malicioso.

Os Pontos de Ataques

Em um portal de fornecedores, pontos de ataque podem ser:

- 
- Na aplicação
 - No banco de dados
 - No middleware
 - No sistema operacional
 - No servidor
 - Nas comunicações
 - Na rede
 - Nos administradores que possuem acesso

Vulnerabilidades

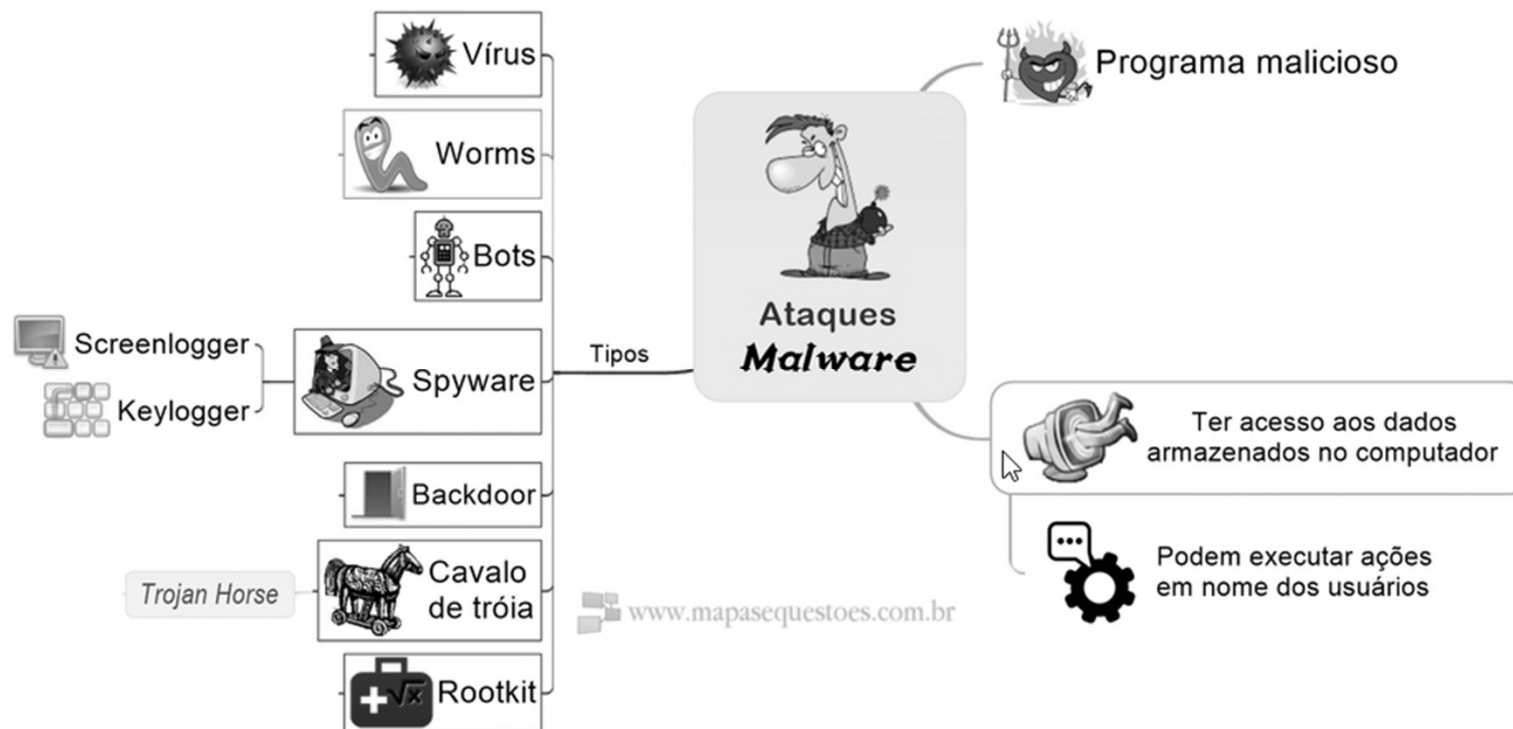
Em um portal de fornecedores, vulnerabilidades podem estar:

- No hardware - servidor, disco rígido
- No software - aplicação, middleware, banco de dados, S.O
- Nos protocolos - TCP/IP ou outro utilizado pela aplicação
- Na rede - e a aplicação está na camada 7 da pilha de protocolos TCP/IP

Os pontos de ataques também devem ser avaliados de acordo com o estado da informação:

- Data-In-Use (DIU) - em processamento
- Data-In-Motion (DIM) - em transmissão
- Data-At-Rest (DAR) - armazenada

Malwares

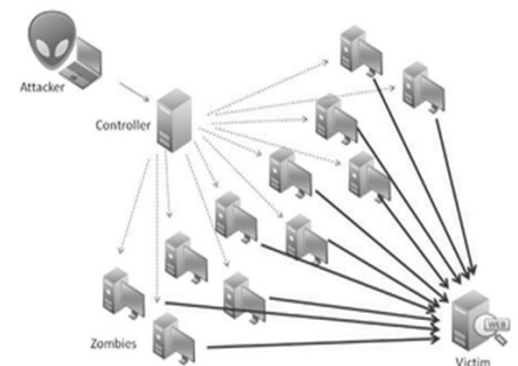


<http://clickpicx.pw/Mapa-Mental-sobre-Malware-informtica-t-Segurana.html>

Ataque – DoS/DDoS

Denial of service: é a negação de serviço ou o processo que torna um sistema ou aplicação indisponível. Ex.: bombardeamento de solicitações que consomem todos os recursos disponíveis do sistema ou da transmissão de dados de entrada defeituosos que podem acabar com o processo de uma aplicação.. Ex.: *SYN Flooding*: causa o *overflow* da pilha de memória e *Smurf*: envio de pacotes específicos.

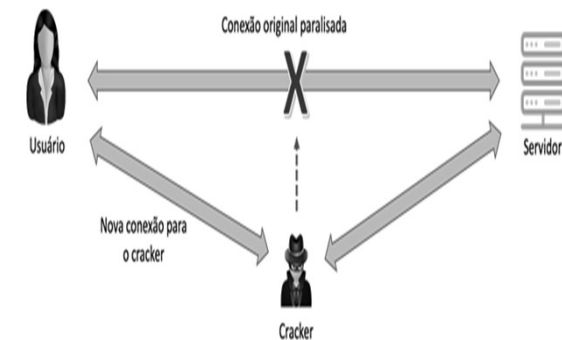
Quando há uma coordenação para que as requisições sejam enviadas simultaneamente a partir de diferentes pontos, o ataque é conhecido como *Distributed Denial-of-Service (DDoS)* - o atacante utiliza masters e daemons para o ataque distribuído e coordenado à vítima. Os masters são máquinas controladas diretamente pelo atacante, enquanto os daemons são controlados pelos masters. Os daemons realizam efetivamente o ataque à vítima.



Fonte : <https://www.binyod.com/security/ddos/>

Ataque - Man-In-The-Middle (MITM)- Sequestro de Conexões

- É ativo, ou seja, a manipulação ocorre em tempo real, com o agente de ameaça tendo o controle dela, redirecionando as conexões TCP para uma determinada máquina.
- Além de permitir a injeção de tráfego, permite ainda driblar proteções geradas por protocolos de autenticação, comprometendo assim a confidencialidade (tendo acesso às informações em trânsito), a integridade (alterando ou injetando informações na conexão) e mesmo a disponibilidade (descartando informações que deixam de chegar ao seu destino).



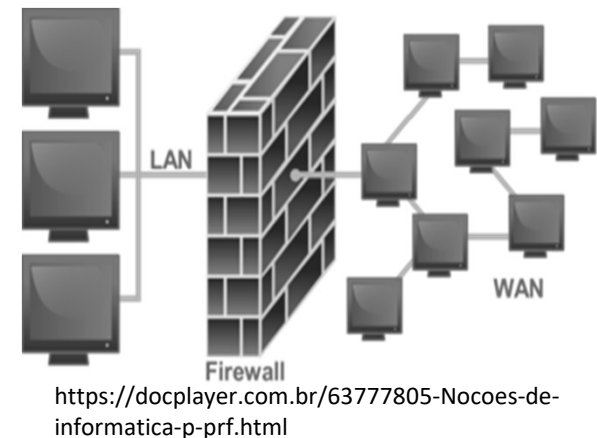
Fonte: Autora

Controles de Segurança e Proteção - DMZ

- A **proteção à rede** considera que, no fluxo da informação, todo acesso passa pela rede, sendo este, portanto, um bom local para controles de segurança.
- Uma boa estratégia de segurança deve levar em consideração a rede, com uma arquitetura de redes segura, considerando segmentação, uso de zonas desmilitarizadas (DesMilitarized Zone, DMZ), controle de acesso de rede e detecção de ataques (OLIVEIRA, 2017).
- A técnica de DMZ é uma rede específica que fica entre uma rede pública como a internet e a rede interna. Com esta segmentação, a rede interna conta com uma camada adicional de proteção, pois os acessos são permitidos para os serviços disponibilizados na DMZ, mas não para a rede interna.

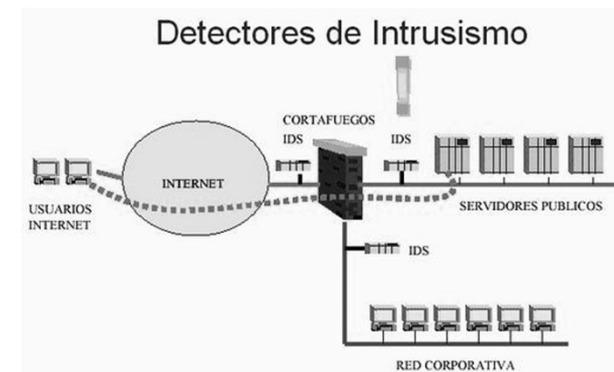
Controles de Segurança e Proteção - Firewall

- O controle de segurança mais famoso é o firewall, que é o responsável pelo controle de acesso de rede.
- Na realidade, o firewall começou funcionando na camada de rede, e atualmente ele atua também na camada de aplicação, realizando a proteção contra ataques que vão além de ataques de rede, com o Web Application Firewall (WAF).
- Enquanto um firewall faz a filtragem do tráfego de rede baseado nos cabeçalhos dos pacotes, o WAF faz o filtro e monitora o tráfego entre os usuários e a aplicação Web, na camada de aplicação HTTP.



IDS – Sistemas de Detecção de Intrusão/ IPS - Sistemas de Prevenção de Intrusão

- IDS - Permitem a detecção de ataques em andamento.
- Monitoramento e análise das atividades dos usuários e dos sistemas.
- Análise baseada em assinaturas de ataques conhecidos
- Análise estatística do padrão de atividadeFuncionam de uma forma mais ativa que um IDS
- IPS -Após a detecção de atividades suspeitas, tomam ações diretas, como o término daquela conexão.
- Atua de uma forma *in-line*, de modo similar ao *firewall*.
- Os sistemas de detecção e prevenção de intrusão atuais incorporam técnicas de inteligência artificial para diminuir a quantidade de falsos positivos (alarmes falsos) e falsos negativos (ataques não detectados).



<http://cloudcomputingbrasil.com.br/author/paulo-boschim-jr/page/2/>

Antimalware

- Antimalware buscam códigos maliciosos, e basicamente funcionam com a verificação de assinaturas ou códigos que identificam um malware já identificado anteriormente e que possuem vacina específica.
- Se por um lado os códigos maliciosos podem alterar seu próprio código ou gerar polimorfismo para não serem detectados pelo antimalware, do outro lado o controle de segurança adota cada vez mais a inteligência artificial para detectar comportamentos anômalos que podem representar perigo para as empresas.

Apresentação aos diretores

A estrutura da apresentação

1. Pense sempre nos pontos de ataque. No caso da loja virtual, você não possui controle sobre os dispositivos de seus clientes, ou os endpoints.
2. O que resta a você é partir para a arquitetura de rede segura, que começa com a segmentação de rede.
3. O servidor deve estar em uma DMZ, para proteger a sua rede interna, que deve estar isolada.
4. A segmentação e o controle de acesso de rede podem ser feitos pelo firewall, que bloqueia tentativas de ataques a portas filtradas. Porém, para as portas liberadas pelo firewall, necessárias para que os clientes cheguem ao servidor, ataques podem ocorrer por ali.

A estrutura da apresentação

5. Outro controle é o IDS, que faz a detecção de ataques. Para que as detecções reflitam em ações como o encerramento das conexões dos ataques, um IPS deve ser utilizado. O problema do IPS é que ele atua na rede, e ataques com construções de pacotes de rede que são mais difíceis de serem detectados podem ser feitos contra a sua empresa.
6. Neste caso, a correlação de eventos, que considera logs de ativos como o servidor de aplicação ou middleware, além da aplicação e das autenticações, podem ser correlacionadas com informações da camada de rede, resultando em detecções mais assertivas.

A estrutura da apresentação

7. Você pode ainda explorar novas tecnologias de detecção que utilizam técnicas de inteligência artificial, que detectam situações como desvios de padrão.
8. E quanto a um cliente que teve a sua identidade roubada, ou seja, tenta realizar uma compra como se fosse uma outra pessoa, o que você faria?

Criptografia

Contextualizando

Sua missão: Prepare uma apresentação para a diretoria executiva da empresa com uma estratégia de segurança que considera as seguintes situações:

- A documentação com os resultados do projeto é armazenada no servidor de arquivos, que está na nuvem.
- O desenvolvimento do projeto é colaborativo, na própria nuvem, entre brasileiros, chineses e suíços.
- Alguns cientistas gravam o documento em seu equipamento para trabalharem no fim de semana na fazenda, que possui limitações de conectividade.
- Outros cientistas gravam os documentos em pendrives para backup.

Contextualizando

- Na apresentação, faça uma correlação dos controles de segurança propostos com a ameaça correspondente, como o vazamento do projeto, a invasão seguida de alteração dos resultados, e a inserção de documentos fraudulentos.
- Não esqueça de inserir em sua apresentação uma explicação breve para a diretoria executiva sobre os algoritmos criptográficos propostos para cada caso.



Fonte: Pixabay. <https://pixabay.com/pt/photos/egito-karni-hier%C3%B3glifos-escrita-3344964/>

Contextualizando

- ✓ 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.
- ✓ Vamos desvendar os mistérios da Criptografia?



Fonte: Shutterstock

Criptografia

- Em 2016, o Federal Bureau of Investigation (FBI) dos EUA tentou de tudo, sem sucesso, para ter acesso às informações de um dispositivo móvel do principal suspeito de um tiroteio que vitimou 14 pessoas em dezembro de 2015 em San Bernardino (KAHNEY, 2019). Esta história mostra o poder de um dos principais controles de segurança, a criptografia.
- Este caso ilustra também que a segurança em camadas é fundamental, já que a criptografia foi utilizada em conjunto com outros controles de segurança, como a autenticação, para proteger os dados do legítimo dono.

Criptografia

- Da origem para ocultar o significado de uma mensagem até o uso em aplicações como WhatsApp e acesso a websites, passando pelo uso em guerras e por agentes secretos, a criptografia evoluiu de uma arte para uma ciência, e atualmente faz parte de nossas vidas, incluindo os objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, além de dinheiro digital (NAKAMURA, 2016).
- A criptografia deriva de duas palavras gregas: kryptos, que significa oculto, e graphien, que significa escrever.

Criptografia

- Arte de escrever ou resolver códigos.
- Ocultar o significado da informação.
- Antes: o objetivo inicial era a comunicação secreta
- Atualmente: autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, etc.
- Criptografia básica: simétrica ou de chave privada.
 - Chave secreta é a mesma para a cifragem e decifragem, e deve ser compartilhada;
 - Cifragem com algoritmos matemáticos.

Criptografia - Objetivos

- Sigilo: proteção dos dados contra divulgação não autorizada.
- Autenticação: garantia que a entidade se comunicando é aquela que ela afirma ser.
- Integridade: garantia 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

Segurança dos sistemas criptográficos

- ✓ Geração de chaves: geração aleatória de chaves;
- ✓ Mecanismo de troca de chaves: chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras;
- ✓ Taxa de troca das chaves: quanto maior a frequência de troca automática das chaves, maior será a segurança;
- ✓ Tamanho da chave: são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas

Criptografia - exemplos

Vamos brincar?

Um site interessante para se brincar com cifras de César é o **ROT13**: <http://www.rot13.com/>.

Eu te amo

↓

ROT13 ▾

↓

Rh gr nzb

Mais uma experiência:

<http://www.dcode.fr/caesar-cipher>.



Fonte: Shutterstock

Técnicas de criptografia

- A criptografia é baseada em um conjunto de técnicas que incluem a cifragem, funções de *hash* e assinaturas digitais.
- A escolha da técnica depende de critérios:
 - Nível de segurança requerido, métodos de operação dos algoritmos, desempenho, facilidade de implementação.

Criptografia de chave privada

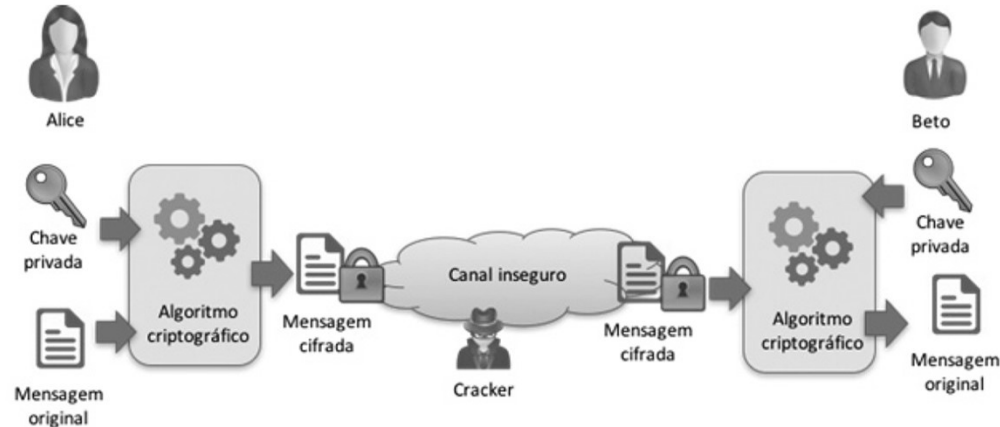
Enviar uma mensagem cifrada

algoritmo criptográfico

chave secreta privada para cifrar a mensagem original.

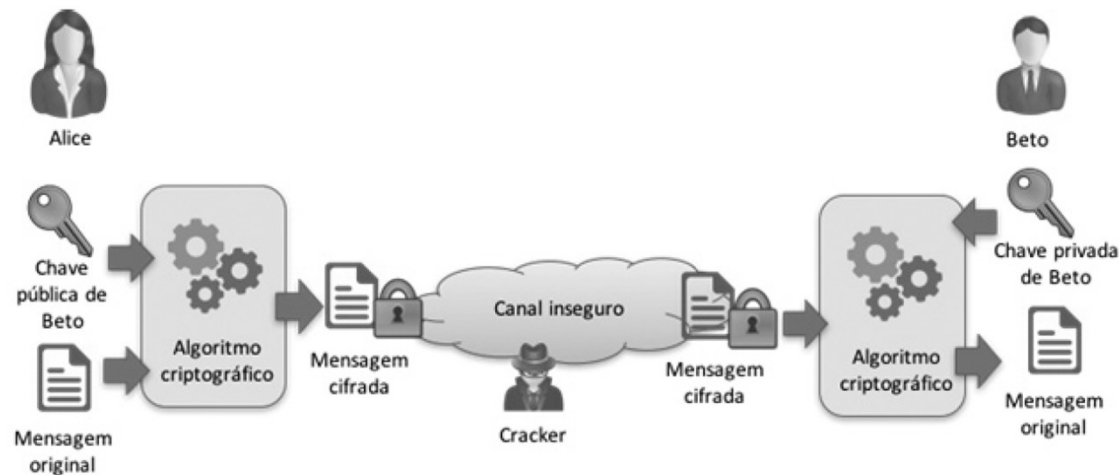
Na mensagem cifrada recebida

Mesma chave secreta para decifrar a mensagem



Criptografia de chave pública

- Utiliza um par de chaves para a troca de mensagens
 - Chave pública: para cifrar a mensagem.
 - Chave privada: decifrar a mensagem (chave exclusiva do receptor)



Esteganografia

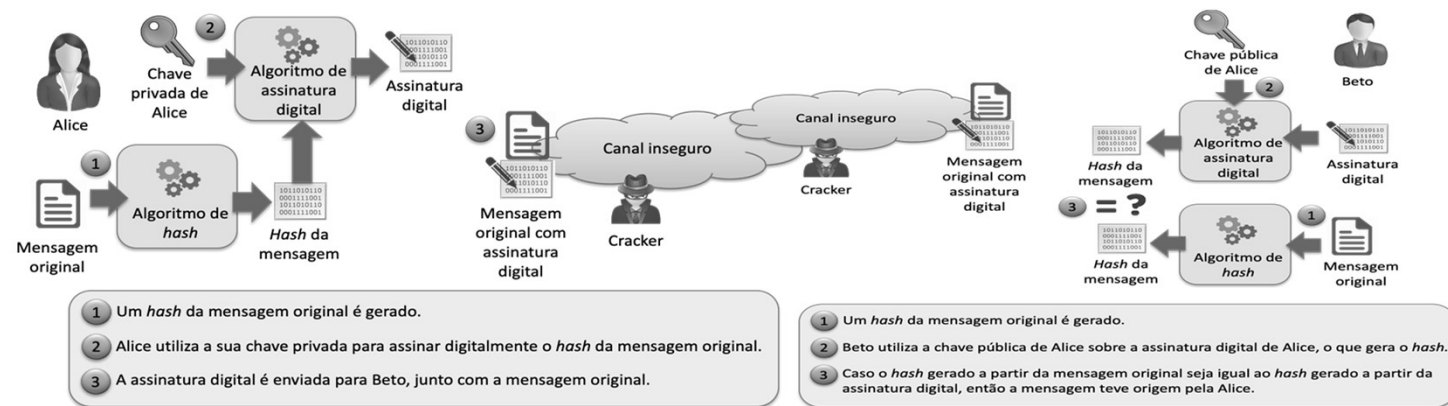
- Uso de técnicas para ocultar a existência de uma mensagem dentro de outra.
- Diferença entre a criptografia e esteganografia
 - Uma oculta o significado da mensagem, enquanto a outra oculta a existência da mensagem.
- Exemplos:
 - Inserção de mensagens nos bits menos significativos de áudios ou imagens; uso de caracteres *Unicode* que se parecem com conjunto de caracteres ASCII



Assinatura digital

A mensagem é “cifrada” com a chave privada - validar a origem de uma mensagem

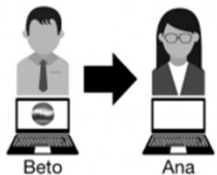
Utiliza a chave pública correspondente para realizar a validação da assinatura.



Blockchain

Como funcionam as transações na **BLOCKCHAIN**

1 Beto quer enviar 1 BTC para Ana



2 A transação é submetida para a rede Blockchain



3 Os mineradores trabalham para validar as transações

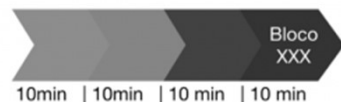


4 O primeiro a resolver o "hash", cria um novo bloco incluindo, entre outras, a transação do Beto para a Ana



E é recompensado com novos Bitcoins e com um fee sobre as transações

5 E o novo bloco é adicionado na blockchain

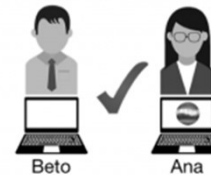


Um novo bloco é criado a cada 10 minutos, e os mineradores passam a trabalhar buscando o próximo bloco

6 A rede reconhece o novo bloco com as transações validadas (consenso)



7 A transação é concluída e o BTC agora pertence à Ana



Diffie-Hellman

1976 - primeiro método criptográfico para troca de chaves.

Compartilhar uma chave secreta em um canal inseguro

Cálculo de logaritmos discretos em um campo infinito.

RSA e Key escrow

RSA:

Geração das chaves pública e privada é feita a partir de dois números primos.

fatoração de inteiros em fatores primos – quebra inviável!

Key escrow (custódia de chaves)

Cópias de chaves criptográficas existam para o acesso a informações cifradas no caso de ordens judiciais, por exemplo.

Um direcionamento pode ser:

- Situação 1: armazenamento de resultados do projeto no servidor de arquivos na nuvem. Servidor de arquivos ou o provedor de nuvem pode ser atacado e a documentação pode ser vazada ou alterada. Envolve confidencialidade e integridade.
- Situação 2: armazenamento de resultados do projeto no serviço de troca de arquivos. Serviço pode sofrer um incidente de segurança e resultar em acesso não autorizado. Envolve confidencialidade e integridade.
- Situação 3: armazenamento de documentação em notebooks e pendrives. Equipamentos e dispositivos podem ser roubados, perdidos ou acessados indevidamente.

Envolve confidencialidade no caso de roubo, perda ou acesso indevido, e integridade no caso de acesso indevido.

- Situação 4: dados do projeto trafegam pela Internet quando são trabalhados de forma colaborativa, quando são armazenados no servidor de arquivos e quando são enviados entre as equipes, via e-mail e serviço de troca de arquivos. Dados podem ser expostos e alterados durante a transmissão. Envolve confidencialidade e integridade.

- Situação 5: dados do projeto trocados via e-mail permanecem nestes servidores, que podem ser atacados. Envolve confidencialidade e integridade.

- Situação 6: origem dos documentos pode ser alterados, de modo que informações falsas podem ser inseridas na empresa.

Envolve integridade, e mais especificamente, autenticidade de origem.

A estratégia de segurança envolvendo a criptografia pode ser definida desta forma:

- Criptografia de chave privada ou simétrica: situações 1, 2, 3, 4, 5 e 6.
- Hash criptográfico: situações 1, 2, 3, 4, 5 e 6.
- Criptografia de chave pública ou assimétrica com assinatura digital: situação 6.

Não se esqueça de incluir um overview sobre os tipos de criptografia na apresentação para a diretoria executiva.

Compreenderam todos os aspectos que devemos proteger?

Muiiiitos!!!

Recapitulando

- ✓ Segurança da Informação
- ✓ Pilares da S.I
- ✓ Risco
- ✓ Controles de segurança
- ✓ Agentes de Ameaça, Ameaças e Técnicas de Ataques
- ✓ Controles de Segurança e Proteção
- ✓ Criptografia

