SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

UNIDADE 1 - FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

- **Seção 1**: Parâmetros de informação e segurança da informação
  - Informação (Confidencialidade, Integridade, Disponibilidade) (Vulnerabilidade, Ameaça, Exploit)
- **Seção 2**: Amplitude de proteção de informação
  - Elementos a Serem Protegidos: Pessoas, Informação, Ativos
- **Seção 3**: Mecanismos de Defesa
  - Mecanismos de Defesa: Processos, Tecnologia, Prevenção
- **Seção 4**: Mapeamento de Risco
  - Riscos (Positivos e Negativos), Gestão, Classificação e Contramedidas

UNIDADE 2 - SEGURANÇA DE REDES DE COMPUTADORES

- **Seção 1**: Identificação de vulnerabilidade em redes de computadores
  - Vulnerabilidades de Rede: hardware, software, protocolos, aplicações
- **Seção 2**: Ameaças à Rede
  - Ameaças à Rede: pessoas (hackers), malware, DoS, DDoS
- **Seção 3**: Ferramentas de Segurança I
  - Proteção à Rede (Firewall, IPS, Antimalware)
- **Seção 4**: Ferramentas de Segurança II
  - Proteção à Rede (Tokens, Biometria, Filtros de Conteúdo)

UNIDADE 3 - CRIPTOGRAFIA

- **Seção 1**: Evolução em segurança da informação: criptografia
  - Introdução, Conceitos, Criptografia ao longo da História
- **Seção 2**: Técnicas de Criptografia
  - Principais técnicas : chave privada, chave pública, esteganografia
- **Seção 3**: Soluções de Chave Pública
  - Soluções de Chave Pública: Diffie-Hellman, RSA, assinatura digital, key-escrow
- **Seção 4**: Aplicações de Criptografia
  - Aplicações de Criptografia: cartões de banco, tunelamento VPN, SSL, HTTPS

UNIDADE 4 - PROCESSOS E POLÍTICAS DE SEGURANÇA

- **Seção 1**: Identificação de fatores de risco
  - Ameaças não tecnológicas: desastres, falhas, terrorismo, engenharia social
- **Seção 2**: Definição de políticas de segurança da informação
  - Processo de Segurança, Cultura de Segurança
- **Seção 3**: Normas de Segurança
  - Normas de Segurança: Família ISO 27.000, ISO 22.301
- **Seção 4**: Tendências e futuro em segurança da informação
  - O Futuro da Segurança (Tecnologias Emergentes, Ameaças Emergentes e Futuras)

Bibliografia – Livro Texto

Segurança da Informação e de Redes

Autor: Emílio Tissato Nakamura

Bibliografia complementar

Segurança da Informação: princípios e controle de ameaças

Autor: Felipe Nery Rodrigues Machado

Criptografia e Segurança de Redes: Princípios e Práticas

Autor: William Stallings

Fundamentos de Segurança da Informação – com base na ISO 27001 e na ISO 27002

Autor: Hans Baars

Kees Hintzbergen

Jule Hintzbergen

André Smulders

Segurança de computadores e teste de invasão
Autor: Alfred Basta
Nadine Basta
Mary Brown

Introdução à Segurança de Computadores
Autor: Michael T. Goodrich
Roberto Tamassia

Segurança da Informação – O usuário faz a diferença
Autor: Edison Fontes

O livro dos códigos – A ciência do sigilo – do antigo Egito à criptografia quântica
Autor: Simon Singh

ATENÇÃO À CHAMADA

Provas são individuais

Trabalhos serão aceitos apenas ATÉ a data proposta

CONTATO

Email: milton.santana@anhanguera.com

FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

- Devemos nos preocupar em exigir segurança de produtos e serviços.
- Propriedades básicas definidas devem ser protegidas, fazendo parte de fundamentos importantes do cotidiano.
- Segurança da informação e de redes, mais do que fazer parte de qualquer empresa de qualquer segmento de mercado, faz parte da vida de cada um de nós.
- Hoje em dia tudo é influenciado pela **segurança**: smartphone, internet banking (aplicativos também), compras online, uso de cartão de crédito, computadores, entre vários e vários outros. Concorda?

- Segurança da informação é prevenir-se contra ataques, é detectar um ataque em andamento ou é se recuperar após um incidente de segurança?

- **Segurança da Informação** “é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios” [ISO 27002].

- Imagine a seguinte situação: você é um profissional que está preocupado com as possíveis consequências de um ataque cibernético, porém, os diretores da empresa não estão muito interessados no alto investimento.

- Como convencê-los de que a segurança é importante (essencial)?

- Todas as informações estão armazenadas em servidores e sistemas da empresa.

- Estas informações, além de ficarem nos computadores pessoais dos funcionários trafegam pela rede, o que permite possíveis ataques.

- Você deverá preparar uma apresentação que contenha respostas para as seguintes questões:
  - ✓ Em caso de ataque cibernético na empresa, quais propriedades básicas de informações podem ser comprometidas?
  - ✓ Por que você acha que alguém realizaria um ataque cibernético contra sua empresa?

- Antes de responder essas perguntas, precisamos saber o que é Segurança da Informação? O que é Segurança de Redes? E mais importante, o que é **Informação**?

- Como já vimos, Segurança da Informação “é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios”, segundo a ISO 27002.

- Segurança de redes é a parte da informática que lida com as estratégias implementadas por uma empresa para proteger seus ativos computacionais.

- Em um contexto maior podemos dizer que a segurança de redes está relacionada com a segurança da informação que visa proteger o ativo mais importante da empresa que são as informações.

- Mas por que são as informações são os ativos mais importantes da empresa? Existe algo mais importante?

- O que pode gerar insegurança?
  - Assegurar a informação é uma tarefa complicado e extremamente complexa pois abrange diversas situações diferentes, como:
    - Erros;
    - Displicência
    - Ignorância do valor da informação
    - Acesso indevido
    - Roubo
    - Fraude
    - Sabotagem
    - Causas da natureza

- O que pode gerar insegurança?
  - Erro

- O que pode gerar insegurança?
  - Displicência

- O que pode gerar insegurança?
  - Ignorância do valor da informação

- O que pode gerar insegurança?
  - Acesso indevido/roubo

- O que pode gerar insegurança?
  - Fraude/Sabotagem

- O que pode gerar insegurança?
  - Causas da natureza

- Precisamos saber do que e de quem nos proteger

- Precisamos saber do que e de quem nos proteger

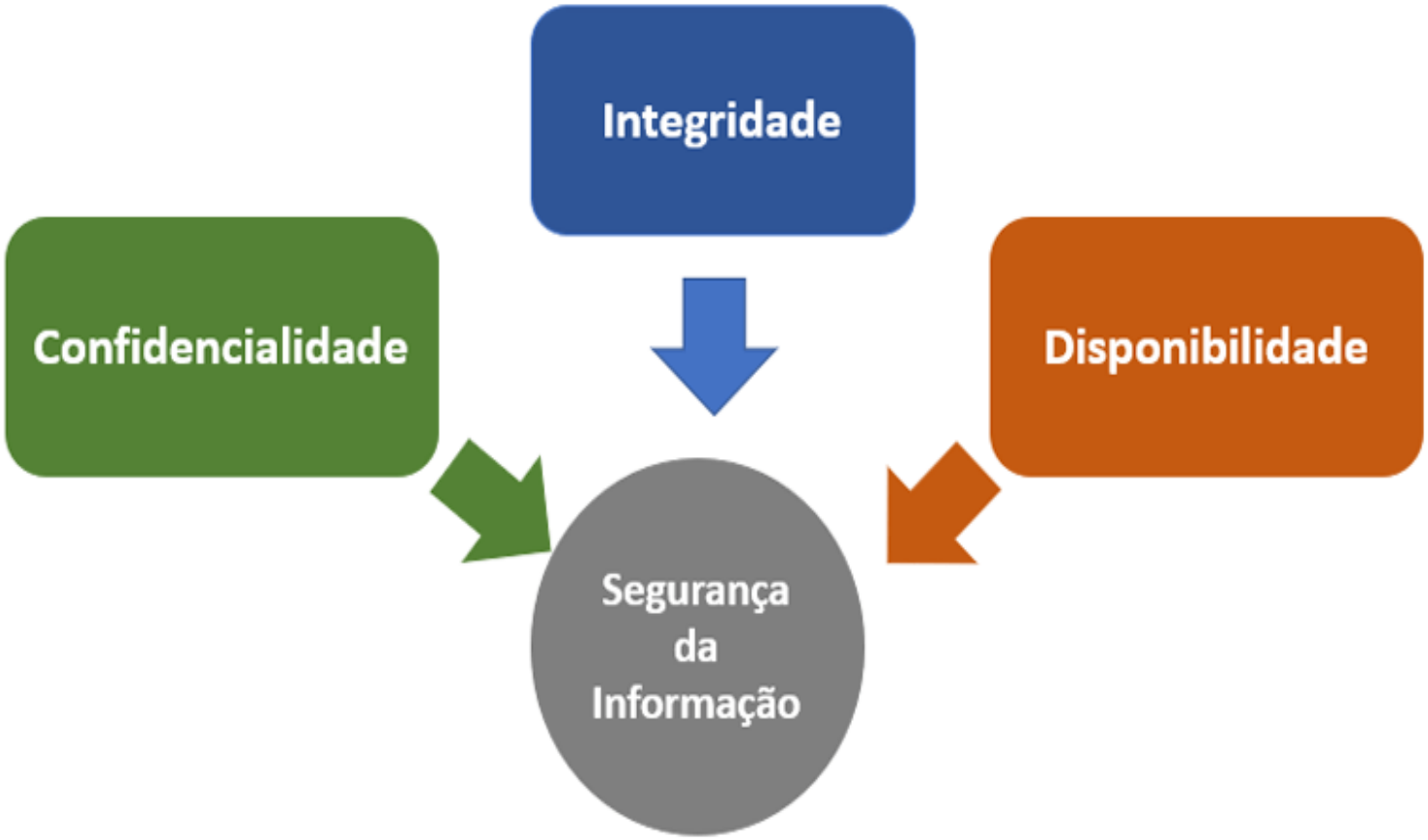
- As informações podem existir em diversas formas.
- O mesmo ocorre com as vulnerabilidades (falhas de segurança) e ameaças.
- A pergunta é: O que e como devemos proteger?

- “O único sistema verdadeiramente seguro é aquele que está desligado, desplugado, trancado num cofre de titanium, lacrado, enterrado em um bunker de concreto, envolto por gás nervoso e vigiado por guardas armados muito bem pagos. Mesmo assim, eu não apostaria minha vida nisso.”

- **Gene Spafford**
  - Diretor de operações de computador, Auditoria e Tecnologia da Segurança Purdue University, França

- “Você vê algumas informações e a maneira como as coisas são formuladas, e então começa a ter alguma compreensão da empresa e das pessoas responsáveis pelo sistemas de TI. E havia essa ideia de que entendiam de segurança, mas talvez estivessem fazendo alguma coisa errada.” **[Arte de Invadir]**

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO



PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade**: é a capacidade de garantir que o nível necessário de sigilo seja aplicado em cada junção de dados em processamento. Além disso, trata-se da prevenção contra a divulgação não autorizada dos mesmos.
- Proteger as informações contra acesso de qualquer pessoa não devidamente autorizada pelo dono da informação, ou seja, as informações e processos são liberados apenas a pessoas autorizadas.
- O grande desafio da segurança da informação é, além de entender essa propriedade, fazer com que ela seja cumprida. Como garantir a confidencialidade das informações? Como permitir que somente pessoas autorizadas tenham acesso a elas? Como evitar acessos não autorizados às informações? Como impedir vazamentos ou ataques cibernéticos que comprometem a confidencialidade?

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade**: a informação que precisa ser protegida passa por uma série de elementos ou ativos, tais como pessoas que estão trabalhando no projeto, softwares e hardwares que armazenam, processam ou transmitem essas informações.
- Qualquer um desses pontos pode ser alvo de vazamento ou ataque cibernético.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade - Exemplos**
  - Steve Jobs é um ícone também no que tange à confidencialidade dos produtos da Apple. Ele utilizava segmentação de informações, na qual um profissional realizava uma tarefa específica em uma parte específica, sem saber especificamente do produto. Além disso, um livro sobre ele (BEAHM, 2011) mostra como encarava a confidencialidade, segundo um executivo da Apple: “Nunca falamos sobre produtos futuros. Havia um ditado na Apple: Não é engraçado? Um navio que vaza pelo topo. Não quero que aconteça o mesmo comigo. Por isso, realmente não posso dizer”.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade - Exemplos**
  - Alguém obtém acesso não autorizado ao seu computador e lê todas as informações na sua declaração de Imposto de Renda.
  - Alguém consegue acesso à sua conta no facebook e “posta” informações comprometedoras.
  - Em uma transferência bancária de valor x durante o trajeto existem vários equipamentos e pessoas má intencionadas que podem tentar capturar o pacote. Se o pacote estiver seguro (criptografado) a pessoa não enxergará nada. O pacote deve ser de conhecimento apenas para quem envia e quem recebe.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Integridade**: Propriedade de manter a informação acurada, completa e atualizada.

- Princípio de segurança da informação através do qual é garantida a autenticidade da informação.

- O usuário que armazena dados espera que o conteúdo de seus arquivos não seja alterado por erros de sistema

- 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.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Integridade - Exemplos**: Durante a transmissão da informação sobre um determinado produto são alterados os preços do mesmo. Se for para cima, pode ocorrer um problema para venda do produto (valor muito alto). Se for para baixo, a empresa pode ter prejuízo. De um jeito ou de outro, a informação perde sua exatidão.

- Voltando ao exemplo da transferência bancária, esse pilar se preocupa em não haver alterações no pacote. Supondo que a pessoa tenha acesso, ela poderia adicionar 3 zeros no valor a ser transferido, por exemplo. A integridade se preocupa em diagnosticar que se um pacote ao ser enviado ao destino sofreu alterações no caminho, então deve-se descartar esse pacote.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Integridade - Exemplos**: Alguém obtém acesso não autorizado ao seu computador e altera as informações da sua declaração de Imposto de Renda.

- Um funcionário que altera seu salário no banco de dados sem o RH tomar conhecimento.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Disponibilidade**: Propriedade de manter a informação disponível para os usuários, quando estes dela necessitarem.

- A disponibilidade deve garantir que as pessoas autorizadas tenham acesso, com base nas restrições determinadas, sempre que necessitarem.

- Diferentemente da dificuldade que é perceber quando a confidencialidade ou a autenticidade é comprometida, a disponibilidade é logo notada quando há um incidente de segurança. Nos outros casos, o incidente de segurança só é percebido normalmente quando a empresa perde clientes ou quando é passada para trás pela concorrência.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Disponibilidade**:

- Está relacionada diretamente com redundância. Se um usuário ficar sem acesso a um servidor do facebook, outro deve entrar em ação para que o usuário não perca o acesso.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Disponibilidade - Exemplos**: Os ataques clássicos que comprometem a disponibilidade são a negação de serviço, com o DoS (Denial of Service) e o DDoS (Distributed Denial of Service). Nesses ataques, que podem ocorrer com a aplicação de diversas técnicas, que vão desde o nível de rede quanto o nível de aplicação, os serviços se tornam indisponíveis, com o comprometimento do acesso à informação.

- Determinado servidor que você está tentando acessar sobre uma sobrecarga de dados e você fica impossibilitado de acessar a informação.

- O servidor pegou fogo.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Exemplos**: O ataque à TJX (grupo varejista) é considerado um dos casos mais emblemáticos de segurança da informação. Com prejuízos estimados em mais de R$ 1 bilhão (na cotação atual), o ataque foi feito a partir de redes sem fio que utilizavam um protocolo reconhecidamente vulnerável de acesso à rede, o WEP.

- Os intrusos que invadiram os sistemas de pagamento da TJX permaneceram incólumes por 18 meses, tempo durante o qual baixaram 80 GB de dados de cartões.

- Na época, a TJX divulgou que cerca de 45 milhões de números de cartões pertencentes a usuários de diversos países foram roubados de seus sistemas. Este número pode ser ainda maior: um grupo de bancos que utilizava os serviços da companhia divulgou em outubro que informações de cerca de 94 milhões de cartões ficaram expostas durante a série de intrusões.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Vulnerabilidade**: Além da CID, outro fundamento importante está relacionado também aos riscos: a vulnerabilidade. Esse termo é obrigatório em segurança da informação, por se tratar do elemento que é explorado em ataques. Uma vulnerabilidade é um ponto fraco que, uma vez explorada, resulta em um incidente de segurança. Inclui fraquezas de um ativo ou grupo de ativos que pode ser explorado por uma ameaça.

- Quanto maiores as vulnerabilidades, maiores as fraquezas que podem ser exploradas em ataques. Precisamos conhecer as vulnerabilidades para que elas possam ser eliminadas.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Vulnerabilidade**: Aqui há um conceito bastante relevante sobre a segurança da informação: a segurança de um ativo ou de uma empresa é tão forte quanto o seu elo mais fraco da corrente, ou seja, se houver um ponto fraco (vulnerabilidade), é por lá que o ataque ocorrerá.

- Para o atacante, basta encontrar e explorar uma única vulnerabilidade que ataque sua empresa.

- “Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador” (Comitê Gestor da Internet no Brasil, 2006, pág. 7).

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Vulnerabilidade**: –De acordo com a ABNT (2005) o estudo das vulnerabilidades é algo muito importante para profissionais da área de segurança da informação porque através delas podem-se verificar as falhas e corrigi-las mais rapidamente. *Sites* especializados lançam, diariamente, listas com vulnerabilidades conhecidas. Essas falhas são descobertas pelos próprios pesquisadores ou muitas vezes por usuários comuns que passam horas explorando a rede a procura de falhas.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Vulnerabilidade**: Um ataque só acontece porque vulnerabilidades são exploradas pelos atacantes. Temos que eliminar todos os pontos fracos de nosso ambiente, em todos os níveis. E, em segurança da informação, vulnerabilidades existem em todas as camadas: humano, físico, hardware, protocolo, sistema operacional, aplicação, rede, arquitetura, entre outros. Para complicar, a integração entre diferentes componentes de um ambiente insere complexidade que, como consequência, pode resultar em novas vulnerabilidades.

- São diversos os motivos para um *software* conter uma vulnerabilidade, dentre elas: Configuração do sistema, o próprio sistema com erros, pessoas (um *cracker* pode utilizar Engenharia social para obter informações para facilitar sua invasão), falta de atualização de *software*, etc.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- Normalmente temos 3 tipos de falhas a serem exploradas:
  - Falhas que permitem afetar a disponibilidade do sistema.
  - Falhas que permitem acesso ao sistema.
  - Falhas que permitem a execução de códigos na máquina.
  - Entre outras.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Exploit**: A exploração de vulnerabilidades pelos atacantes é feita com o uso de métodos, técnicas e ferramentas próprias para cada tipo de vulnerabilidade existente. Se há, por exemplo, um ponto fraco na entrada do centro de dados e o atacante vê que pode acessar fisicamente o servidor e roubá-lo por inteiro, ele irá explorar essa vulnerabilidade.

- Para as vulnerabilidades tecnológicas, o ataque é feito com os exploits – softwares que utilizam dados ou códigos próprios que exploram as fraquezas de ativos. Há exploits variados, como aqueles para serviços e aplicações remotas, para aplicações web, para escalada de privilégios, para negação de serviço ou para shellcode.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Exploit**: Os exploits são utilizados APENAS por aqueles indivíduos mal intencionados?

- **IMPORTANTE**: todo e qualquer meio para prejudicar uma empresa também é utilizado para o bem. Sem isso, não saberíamos quais vulnerabilidades existem e quais meios para nos proteger.
- Portanto, profissionais especializados em Segurança da Informação precisam conhecer tanto como se defender e como atacar. Ele se utiliza dessas ferramentas para auxiliá-lo no seu trabalho.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaças**: Ameaça não é vulnerabilidade, e também não é um ataque, bem como não é um risco, além de não ser um agente de ameaça. Ameaça é algo que pode acontecer, é algo que possui potencial de se concretizar. Exemplo: ameaça de um assalto.

- A ameaça de assalto sempre existe, porém ela só se torna um incidente quando um agente de ameaça explora uma vulnerabilidade de um ativo, concretizando aquele potencial.

- Em Segurança da Informação a ameaça é primordial para o entendimento dos riscos que sua empresa corre.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaças**: Também pode ser definido como todo e qualquer tipo de gesto que tenha como objetivo causar mal para determinada pessoa, bem ou instituição.

- As ameaças exploram falhas de segurança e as causas podem ser naturais ou não naturais.

- **Causas Naturais:**
  - São aquelas causadas pela natureza, sem intervenção humana, como por exemplo, fogo, chuva, terremoto;
- **Causas Não Naturais:**
  - São aquelas que se tem intervenção humana e podem ser divididas em dois grupos:

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaças**:
  - **Intencionais:** furtos de informações, sabotagens, invasões, etc.
  - **Involuntárias:** são muito comuns quando o usuário não tem conhecimento da ferramenta ou sobre o risco de passar informações da empresa

- **Causas internas**:
  - São ameaças vindas de dentro da própria empresa, ou seja, os próprios funcionários podem vazar informação ou contribuir para que aconteçam danos.
  - Os motivos são diversos: desde insatisfação com a empresa quanto a real intenção de prejudicar e obter ganhos com isso.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaças**:
- **Causas externas**:
  - São ameaças mais comuns e estão relacionadas aos vírus de computador e aos crackers, invasões, etc.

- **Exemplos de diferentes tipos de ameaças**:
  - **Indivíduos mal intencionados** – São os mais perigosos. Tem o objetivo de roubar dados, destruí-los, derrubar o sistema, etc.
  - **Indivíduos de Alto-nível** – Deseja apenas invadir o sistema para ter um reconhecimento maior entre os amigos hackers.
  - **Indivíduo curioso** – São aqueles que invadem o seu sistema simples e puramente por curiosidade.
  - **Concorrente** – São indivíduos que procuram conhecer seus dados e seu negócio para obter vantagem no mercado.

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaças**: Exemplos:
  - Vazamento do projeto do novo produto ou da estratégia de marketing.
  - Acesso não autorizado às informações confidenciais.
  - Negação de serviço aos sistemas de TI da empresa.
  - Alteração de informações-chave da estratégia de marketing.

EXERCÍCIOS

- Você trabalha em uma empresa de desenvolvimento de produtos (celulares). Em caso de ataque cibernético na empresa, quais propriedades básicas de informações podem ser comprometidas?

- Por que você acha que alguém realizaria um ataque cibernético contra sua empresa?
- Crie um relatório e descreva, baseado em cada um dos pilares de segurança da informação, quais as ameaças possíveis no cenário acima descrito.

EXERCÍCIOS

1) Um dos ataques cibernéticos que mais afetam as empresas é o DoS, o qual impede que clientes e funcionários acessem seus sistemas. Esse é um tipo de ataque contra qual fundamento da segurança da informação?

a) Confidencialidade.

b) Integridade.

c) Disponibilidade.

d) Vulnerabilidade.

e) Ameaça.

EXERCÍCIOS

2) Em um ataque recente contra um famoso sistema operacional, um malware infectou todas as máquinas que utilizavam uma determinada versão do sistema. A infecção do malware está relacionada a qual fundamento da segurança da informação?

a) Confidencialidade.

b) Integridade.

c) Disponibilidade.

d) Vulnerabilidade.

e) Ameaça.

EXERCÍCIOS

3) Em um ataque recente contra um famoso sistema operacional, um malware infectou todas as máquinas que utilizavam uma determinada versão do sistema. Esta infecção alterou funções importantes do sistema, incluindo funções maliciosas. Estas funções maliciosas estão relacionadas com qual fundamento da segurança da informação?

a) Confidencialidade.

b) Integridade.

c) Disponibilidade.

d) Vulnerabilidade.

e) Ameaça.

RESOLUÇÃO

1) C

2) D

3) B

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

REFERÊNCIAS

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera