Ameaças e vulnerabilidades à Segurança da Informação

Prof. Anderson Fernandes Pereira dos Santos

Descrição

Conceitos de ameaças e vulnerabilidades, suas classificações e possíveis tratamentos para a mitigação desses problemas. Apresentação de técnicas utilizadas em ataques cibernéticos e exemplos de golpes aplicados na internet.

Propósito

Compreender a importância de identificar ameaças e vulnerabilidades no âmbito da Segurança da Informação para prevenir os danos causados por ataques cibernéticos.

Objetivos

Módulo 1

Conceitos e tipos de ameaças e vulnerabilidades

Identificar os conceitos e os tipos de ameaças e vulnerabilidades de Segurança da Informação.

Módulo 2

Técnicas para ataques cibernéticos

Identificar técnicas utilizadas em ataques cibernéticos.

Introdução

Em meados dos anos 1990, nos laboratórios do CERN (Organização Europeia para a Pesquisa Nuclear), na Suíça, o físico britânico Tim Berners-Lee, em seu computador NExT, começou a escrever algumas linhas de código que transformariam a humanidade. E ali nasceu a internet.

Atualmente, não conseguimos passar um momento sem que façamos algumas interações através da grande rede de computadores. Embora esse sistema seja bastante útil, algumas pessoas e situações têm se aproveitado disso para adquirir vantagem ou demonstrar superioridade técnica.

Assim, deu-se início a uma batalha virtual onde hackers de todo o mundo exploram as fraquezas, também conhecidas como vulnerabilidades, de servidores e serviços utilizados por bilhões de pessoas. Por isso, este conteúd objetiva identificar os conceitos de ameaças e vulnerabilidades de Segurança da Informação e seus possíveis tratamentos. Também serão ressaltados alguns dos golpes mais comuns na internet e apontados caminhos para sua mitigação.

1 - Conceitos e tipos de ameaças e vulnerabilidades

Ao final deste módulo, você será capaz de identificar os conceitos e os tipos de ameaças e vulnerabilidades de Segurança da Informação.

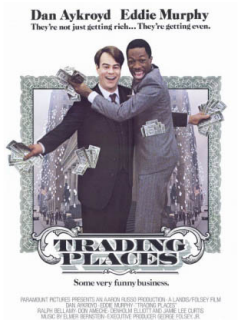
Vamos começar!

Ameaças e vulnerabilidades de software

Confira agora os conceitos de ameaças e vulnerabilidades, bem como os tipos e os tratamentos das ameaças e vulnerabilidades.

Ameaças e vulnerabilidades

Atualmente, a informação é um dos principais ativos das empresas. Por meio das informações, novas tecnologias são obtidas, novos fármacos são ofertados no mercado e salvam vidas. O filme Trocando as Bolas (do inglês, *Trading Places*, de 1983) ilustra bem essa questão.



Pôster do filme *Trading Places*.

O enredo trata de dois corretores bem-sucedidos, os irmãos Duke, que resolvem apostar 1 dólar pela troca de um alto executivo, personagem de Dan Aykroyd, por uma pessoa em situação de rua, interpretado por Eddie Murphy. Com o desenrolar da história, aborda-se o acesso a informações privilegiadas dos irmãos Duke sobre a safra da laranja no mercado norte-americano.

> **Pensando no contexto atual, imagine, agora, quanto seria o valor de mercado de uma empresa que já tivesse a patente da vacina contra o coronavírus no inicio da pandemia.**

As instituições têm o seu valor de mercado calculado a partir de seu *market share*, produtos, patentes, instalações, bens e informações, ou seja, de seus ativos. Os ativos podem ser classificados como **tangíveis**, quando é possível medir o seu valor, e como **intangíveis**, quando é difícil, ou impossível, medir o seu valor.

Para compreender melhor esses conceitos, vejamos alguns exemplos!

Ativos intangíveis

São a imagem de uma organização ou um produto. Algumas operadoras de telefonia tiveram a qualidade de seus serviços prejudicada em função de problemas técnicos de cobertura de sinal. Esse “fantasma” assola os corredores dessas empresas. Que campanha pode ser realizada para mudar tal situação? Percebeu o quão intangível é a imagem de uma companhia?

Ativos tangíveis

São aqueles que conseguimos medir. Eles podem ser classificados como lógicos, quando nos referimos a informações ou softwares; físicos, quando nos referimos a equipamentos ou infraestruturas; e humanos, quando nos referimos a colaboradores e prestadores de serviço.

Vejamos uma explicação mais detalhada de cada ativo tangível:

Ativos tangíveis lógicos

São aqueles que envolvem a informação e sua representação em algoritmos, por exemplo, uma fórmula química, os detalhes sobre a safra da laranja no mercado norte-americano, o algoritmo principal de busca do Google, os detalhes técnicos das baterias dos carros do Elon Musk.

Ativos tangíveis físicos

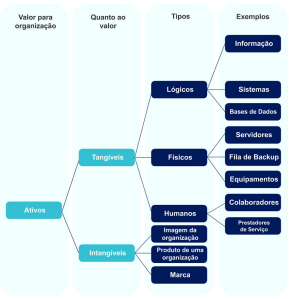
São aqueles que conseguimos tocar, como a usina hidrelétrica de Itaipu, a ponte Golden Gate e o Cristo Redentor. Esses são exemplos de infraestruturas cuja ausência poderá provocar uma perda significativa que ficará marcada na memória. Provavelmente, você se lembra de onde estava no dia 11 de setembro de 2001. Em termos de equipamentos, podemos citar

as prensas de papel moeda da Casa da Moeda; o supercomputador Santos Dumont, que permite fazer o sequenciamento do genoma de diversos seres vivos etc.

Ativos tangíveis físicos

São aqueles referentes aos colaboradores e prestadores de serviço, como, por exemplo, a troca de jogadores de futebol e técnicos nos clubes e as cifras astronômicas que circulam nesse mercado. A mesma situação ocorre em outros esportes, como automobilismo, basquete etc.

De maneira geral, os ativos tangíveis e intangíveis se posicionam e se desdobram desta maneira:



Fluxograma do posicionamento dos ativos tangíveis e intangíveis.

A perda ou a danificação desses ativos poderia acarretar problemas financeiros gigantescos.

Exemplo

Vamos analisar o caso da Apple. Em 1997, Steve Jobs (1955-2011) retornou para a Apple e, até o seu falecimento, as ações da empresa aumentaram 9000%. Em termos comparativos, nos últimos dois anos de vida de Jobs, os valores das ações mais do que dobraram, enquanto os da Microsoft subiram 5,1% e os da Intel valorizaram 14% no mesmo período. Quando Jobs faleceu, as ações da Apple tiveram uma queda, não tão acentuada, mas ainda assim uma queda. Trata-se de um claro exemplo de um ativo humano e da perda financeira causada quando ocorre um problema desse tipo. Do mesmo modo, pode ocorrer também a hipervalorização quando um novo ativo é obtido.

Para proteger esses ativos, precisamos criar barreiras de proteção aos diversos tipos de problemas que possam acontecer. Os controles de Segurança da Informação, também conhecidos como medidas de proteção, são as ferramentas, os equipamentos, as metodologias e os processos que usamos para proteger um ativo contra uma ameaça e a(s) sua(s) vulnerabilidade(s) associada(s).

> **Como relacionar uma ameaça e uma vulnerabilidade? Vamos pensar em um exemplo baseado em um desenho infantil, o Papa-Léguas.**

Na animação, o coiote tentava jogar uma bigorna em cima do pássaro, mas vamos trocar nossos atores. Em vez do pássaro, imaginemos um refrigerante, cuja fórmula está salva em um dispositivo de armazenamento externo (*pen drive*). Nesse caso, a bigorna é uma ameaça contra o nosso dispositivo. Para proteger o nosso *pen drive*, podemos colocá-lo dentro de uma caixa de

metal hiper-resistente. Certamente, criamos uma proteção (controle) contra a ameaça (bigorna).

Vamos agora trocar o *pen drive* por uma folha de papel. Uma bigorna é uma ameaça contra uma folha de papel? Não necessariamente. Mas o fogo seria uma ameaça antes e continua sendo agora. Então, nesses dois casos, o fogo persiste e provavelmente o controle anterior não protegeria o *pen drive* nem a folha de papel contra essa ameaça. Podemos perceber, portanto, que, para explorar a vulnerabilidade de um ativo, pode existir uma ou mais ameaças. Da mesma forma, contra uma vulnerabilidade pode haver uma ou mais ameaças. A imagem, a seguir, representa bem essa situação:

Ameaça contra a vulnerabilidade de um ativo.

O ativo corresponde à forma estrelada central. Cada sulco é uma vulnerabilidade que pode ser explorada por uma ameaça. Cada ameaça tem uma chance (probabilidade) de acontecer, representada na imagem pelo tamanho da seta. Assim, há ameaças com grande probabilidade (setas maiores) de acontecer e outras com pouca probabilidade de acontecer (setas menores).

Os semicírculos vermelhos correspondem aos controles que podem proteger o ativo contra uma ou mais ameaças.

Exemplo

Um incêndio e uma enchente são ameaças físicas para um servidor em um data center. Mais do que isso, são pesadelos para os melhores administradores de TIC. Um sistema anti-incêndio com sprinklers, detectores de fumaça, extintores e uma brigada contra incêndio com treinamentos periódicos correspondem a bons controles que podem envolver equipamentos, pessoas e processos.

IC

Significa Tecnologia da Informação e Comunicação. Essa sigla foi utilizada pela primeira vez em uma proposta de currículo escolar elaborado no Reino Unido, no fim dos anos 90. TIC também pode ser definida como um conjunto de recursos tecnológicos utilizados de maneira integrada, tendo como objetivos o processamento de informação e o auxílio na comunicação. A TIC se faz presente na indústria (no processo de automação), no comércio (no gerenciamento, nas formas de publicidade), no setor de investimentos (informação simultânea, comunicação imediata), na educação (como ferramenta de auxílio ao ensino e aprendizagem, na Educação a Distância), dentre outros setores da sociedade.

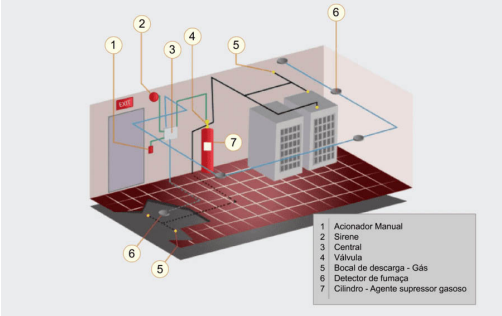
Em um incêndio, os itens citados são boas formas de proteção. Mas e em uma enchente? Esses controles são totalmente ineficientes. E durante a falta de energia elétrica? Ou mesmo em uma sobrecarga de energia elétrica? O que seria mais usual de acontecer: incêndio, enchente, falta de energia elétrica ou sobrecarga de energia elétrica?

> **Certamente, isso dependeria de uma análise geográfica do local de instalação do data center.**

Se ele estivesse instalado no cerrado nordestino, seria razoável pensar em uma enchente? Ou se o data center estivesse instalado em uma região de mangues mato-grossenses, seria razoável pensar em uma enchente? Ou em uma região da Amazônia conhecida pelo elevado número de descargas atmosféricas que ocorrem por ano?

O correto seria a análise e avaliação dos riscos associados à instalação de data centers na região, devendo obedecer a critérios específicos de probabilidade de ocorrência e sorte, afinal de contas, qual seria a probabilidade de dois aviões colidirem em duas torres de um mesmo prédio?

Veja, a seguir, um sistema de combate a incêndio:



Após a análise e avaliação do risco e a sua probabilidade de ocorrência, podemos adotar uma metodologia como a identificação dos ativos e o cálculo do seu valor. Será mesmo que precisamos usar todo e qualquer controle para proteger o ativo? E se o ativo valer menos do que o controle, ainda seria vantajoso implementar esse controle? Com a definição do valor do ativo, a análise e avaliação do risco e os custos para implementar as proteções necessárias, começam as decisões.

Uma boa comparação está no seguro de um automóvel. Ao contratarmos uma seguradora, o valor da franquia do seguro nos é apresentado. Se ocorrer um sinistro e ele for mais barato do que o valor da franquia, valerá a pena acionar o seguro? Não, pois pagaremos mais caro.

Um risco na carroceria é o suficiente para acionar o seguro? E uma batida frontal? E quando o carro sofre perda total? A seguradora decide pagar o valor segurado, pois é mais barato do que mandar consertar.

Tipos de ameaças e vulnerabilidades

Tipos de ameaças e vulnerabilidades - Física e Lógica

Tipos de ameaças e vulnerabilidades - medidas de prevenção

A segurança da informação é fundamentada em três aspectos:

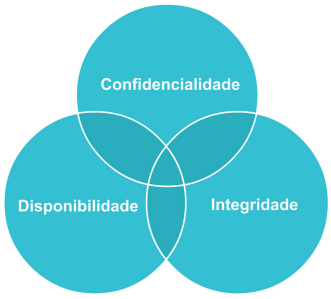
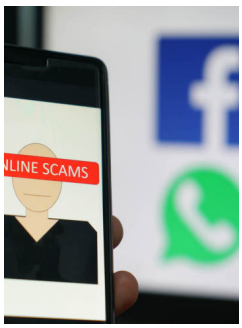


Diagrama dos três aspectos da segurança da informação.

Tomando por base esses três aspectos, pode-se classificar alguns **tipos de ameaças** e os respectivos **controles** que podem ser adotados.

Nos últimos meses, as ocorrências de pessoas relatando problemas de invasão nas contas de WhatsApp multiplicaram. Esse incidente permite que alguém se aproprie da conta do serviço de mensagem de outra pessoa para pedir dinheiro em nome do dono da conta. Podemos perceber o acesso não autorizado, que poderia ser corrigido pelo uso de senhas, evitando possíveis problemas de alteração de dados, ou pela adoção de métodos múltiplos de autenticação.

São exemplos clássicos de perdas de confidencialidade e integridade. Poderá haver recuperação de dados dos usuários por meio de backups realizados pelo sistema. Para esse problema, recomenda-se o uso da confirmação em duas etapas.



Outro exemplo que podemos citar é o armazenamento de documentos eletrônicos. Atualmente, em termos de aplicações que conseguem colocar o rosto de uma pessoa em outra, alterar documentos torna-se uma ação simples de ser realizada. Logo, uma forma de proteger o documento eletrônico é guardar um selo de autenticidade para assegurar que o documento está íntegro. Uma ferramenta bem disseminada é o uso de funções de hashes.

Podemos resumir esses exemplos relativos ao data center na tabela a seguir:

Aspecto	Ameaça	Segurança

Aspecto	Ameaça	Segurança
Confidencialidade	Acesso não autorizado	Uso de senhas
	Acesso não autorizado	Uso de criptografia
	Perda de fitas backup durante o transporte	
Integridade	Alteração dos dados por pessoa/software/processo não autorizado	Uso de métodos de autenticação
	Corrupção dos dados	Uso de hashes
Disponibilidade	Fenômenos oriundos de causas naturais, como incêndio e enchentes	Uso de servidores de backup e/ou redundâncias
	Ataques de negação de serviço	Uso de servidores de redundância

Outra forma de abordar as ameaças descritas é utilizando a classificação quanto a ser física ou lógica. Fenômenos naturais e perdas de dispositivos de armazenamento são exemplos de ameaças físicas enquanto as demais são exemplos de ameaças lógicas.

Podemos reorganizar a tabela anterior e reapresentar as ameaças de acordo com a taxonomia física e lógica, obtendo a seguinte tabela:

Classificação	Ameaça	Segurança
Física	Fenômenos oriundos de causas naturais, como incêndio e enchentes	Uso de servidores de backup e/ou redundâncias
	Perda de fitas backup durante o transporte	Uso de criptografia
Lógica	Alteração dos dados por pessoa/software/processo não autorizado	Uso de métodos de autenticação
	Corrupção dos dados	Uso de hashes
	Escuta na ligação ou tráfego de rede	Uso de criptografia
	Ataques de negação de serviço	Uso de servidores de redundância
	Acesso não autorizado	Uso de senhas

Classificação	Ameaça	Segurança

Podemos consolidar da seguinte forma: se ocorrer falha em equipamentos e instalações, a ameaça é **física**. Caso contrário, se estiver relacionada a problemas de software, algoritmos etc., é considerada ameaça **lógica**.

Quando a ameaça tiver algum agente humano, é classificada dessa forma. Caso contrário, como, por exemplo, nos fenômenos oriundos de causas naturais, como incêndio e enchentes, é conhecida como ameaça não humana. Veremos os detalhes na próxima tabela:

Classificação	Ameaça	Segurança
Humano	Acesso não autorizado	Uso de senhas
	Escuta na ligação ou tráfego de rede	Uso de criptografia
	Perda de fitas backup durante o transporte	
	Alteração dos dados por pessoa/software/processo não autorizado	Uso de métodos de autenticação
	Corrupção dos dados	Uso de hashes
	Ataques de negação de serviço	Uso de servidores de redundância
Não Humano	Fenômenos	Uso de servidores de backup e/ou redundâncias

As ameaças humanas são aquelas que foram provocadas por seres humanos, e as não humanas são provocadas pela natureza ou por problemas de infraestrutura. As ameaças provocadas por seres humanos podem ainda ser classificadas das duas formas a seguir:

Colaboradores

As oriundas de colaboradores ou pessoas mal-intencionadas e aquelas oriundas de pessoas ou colaboradores que não possuem o conhecimento adequado (mal treinados). Nesse caso, o colaborador, propositalmente, faz ações que podem provocar incidentes e prejuízos financeiros, seja pela perda de confidencialidade de algum ativo, seja pela adulteração de algum ativo para agente ou processo não autorizado.

×

Hackers

Os oriundos dos hackers que exploram as vulnerabilidades para demonstrar conhecimento e exibir seu feito para a comunidade; ou ainda pelo simples desafio de alcançar o objetivo, como se fosse um jogo; ou mesmo para obter ganhos financeiros a partir da obtenção de ativos das instituições. Exemplo disso são as notícias que circularam em junho de 2020, quando o governo norte-americano alegou terem sido realizadas invasões para o roubo da pesquisa farmacológica de remédios do coronavírus.

As ameaças não humanas podem ainda ser classificadas em ameaças oriundas de desastres ou de problemas de infraestrutura. Essas ameaças podem ser mitigadas pela gestão do risco envolvido na implantação dos ativos.

Por exemplo, na construção do data center, se a região possui enchentes com certa regularidade, é razoável pensar em alternativas concretas para mitigar esses riscos. A enchente é um exemplo de causa natural. Na contramão, um incêndio causado por uma sobrecarga elétrica é um exemplo de uma ameaça não humana, resultante de problemas de infraestrutura.

Quando a ameaça tiver algum agente humano, é classificada dessa forma. Caso contrário, como, por exemplo, nos fenômenos oriundos de causas naturais, como incêndio e enchentes, é conhecida como ameaça não humana. Veremos os detalhes na próxima tabela:

Tipo de classificação	Tipo de ameaça
Quanto ao tipo de ativo envolvido	• Relacionadas com a Confidencialidade • Relacionadas com a Integridadee • Relacionadas com a Disponibilidade
Quanto ao vetor de ataque	• Física • Lógica • Humano • Não Humano

Tipo de classificação	Quanto ao fenômeno que deu origem (subclassificação das não humanas)
	• Desastre naturais
Tipo de ameaça	• Infraestrutura

Essas classificações se sobrepõem e permitem que determinada ameaça possa ser classificada por vários critérios.

Exemplo

Considere uma chuva torrencial em uma região metropolitana, onde tenha um data center implantado. Nosso país, pela sua geografia, possui locais em que há chuvas em determinadas épocas do ano, em especial as chuvas durante o verão no Rio de Janeiro. Trata-se de um problema que ocorre em diversas capitais brasileiras. Se uma rua inundasse, como ficaria um data center? Já imaginou a perda ocasionada por essa ameaça?

No caso de uma inundação em um data center, o principal problema gerado é a disponibilidade. Dependendo dos controles (proteções) escolhidos pelo gestor, até mesmo problemas de integridade dos dados podem ser gerados. Por isso, sempre é necessário realizar a abordagem em camadas. Nesse cenário, alguns controles simples poderiam ser desenvolvidos como:

- Contingência: desenvolvimento de alguma técnica/metodologia para suprir a ausência ou falha do data center.
- Processo e treinamento do uso da contingência.
- Processo e realizações de cópias de segurança, bem como a verificação do status dessas cópias, inclusive com simulação de desastres.

Comentário

Lógico que não é possível esgotar totalmente o assunto, pois várias situações complementares poderão ocorrer e a lista estaria incompleta, mas, por si só, essas seriam as principais abordagens.

Um exemplo de classificação das ameaças, como uma inundação, pode afetar a disponibilidade e/ou integridade (quanto ao tipo de ativo envolvido), é física e não humana (quanto ao vetor de ataque) e causada por desastre natural (quanto ao fenômeno que deu origem).

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

(IADES – 2019 – CRF-TO – Analista de TI) “[...] é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças” (HINTZBERGEN, 2018). A definição apresentada refere-se ao conceito de:

A Exposição

B Salvaguarda

C Vulnerabilidade

D Risco

E Impacto

Parabéns! A alternativa C está correta.

Como pudemos verificar neste módulo, “vulnerabilidades” e “fraquezas” são conceitos que estão intimamente relacionados.

Questão 2

Considere o ataque às torres gêmeas ocorrido em Nova York. Marque a opção que não apresenta uma possível classificação àquela ameaça.

A Lógica

B Humana

C Infraestrutura

D Terrorista

E Física

Parabéns! A alternativa A está correta.

O ataque às torres gêmeas ocorreu quando aviões comerciais foram sequestrados por grupos terroristas; assim, foi uma ameaça física, humana, que nesse contexto é sinônimo de terrorista e infraestrutura.

2 - Técnicas para ataques cibernéticos

Ao final deste módulo, você será capaz de identificar técnicas utilizadas em ataques cibernéticos.

Vamos começar!

Exploração e mitigação das ameaças

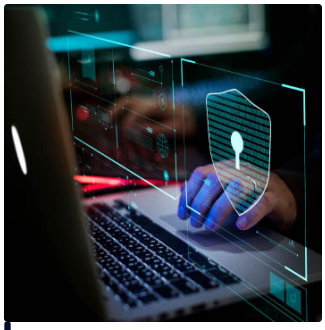
A seguir, exploraremos mais detalhes acerca das ameaças, detalhando alguns golpes clássicos da internet.

Ataques cibernéticos

Definição

Abordaremos as seguintes ameaças cibernéticas: ataques; engenharia social; pichação de sites e softwares maliciosos. Esses tópicos correspondem à maioria das atividades relacionadas com este conteúdo.

Sendo assim, deve-se ter em mente que, por mais que possamos explorar esses itens na sua plenitude, eles nunca estarão totalmente completos porque constantemente são criadas novas técnicas e metodologias envolvidas na atividade hacktivista.



As ameaças cibernéticas são concretizadas por meio do uso de técnicas que normalmente exploram a vulnerabilidade de uma tecnologia, de um processo ou de uma metodologia.

No caso de uma vulnerabilidade relacionada à tecnologia, ela se vincula com a forma de desenvolvimento da ferramenta e, certamente, novas versões daquele software trarão a correção adequada. Um bom exemplo disso é o ping da morte (***ping of death***) que durante muitos anos foi o pesadelo dos gerentes de TI e atualmente não passa de história nos livros sobre segurança.

ing of death

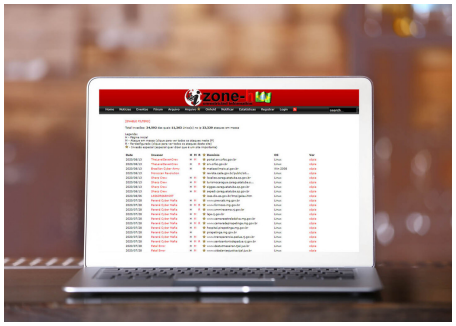
É um tipo de ataque DDoS (*Distributed Denial of Service*, ou Negação de Serviço Distribuído em português). DDoS é um ataque malicioso que age sobrecarregando um servidor ou um computador, a ponto de esgotar os seus recursos (como memória e processamento) e torná-lo indisponível para acesso à internet.

Especificamente sobre o *ping of death*, ele é um ataque que afeta os protocolos de IP e atua através de uma alta frequência de solicitações 'ping' (que são usadas para testar a conexão entre computadores) de tamanho grande (mais de 65.535 bytes, sendo que um 'ping' normal tem cerca de 64 bytes). O computador ou servidor então torna -se incapaz de processar os dados provenientes de tantos *pings of death*, o que resulta na sobrecarga e na falha do sistema.

Ataques cibernéticos são ações maliciosas intencionais, provocadas por hackers ou por funcionários insatisfeitos. Essas ameaças humanas já foram objeto de explicação anteriormente e vimos que as pessoas estão envolvidas. Aqui falaremos do que essas pessoas poderiam realizar.

As razões e motivações já foram explicadas, mas podermos resumi-las ao estímulo de se obter determinada informação (ferindo a confidencialidade), danificar a informação (ferindo a integridade) e interromper o funcionamento de determinado sistema (ferindo a disponibilidade).

No campo do exibicionismo que motiva essas pessoas, podemos exemplificar as informações divulgadas pelo site zone-h, que possui uma lista dos últimos ataques que aconteceram, funcionando como um hall da fama, onde os hackers disputam a quantidade e qualidade dos ataques realizados. Percebe-se que o principal fator é a motivação do hacker em proferir o ataque.



Conquistas de defacement.

Mas como tornar um serviço indisponível por meio de outro tipo de ameaça que não a humana? Outras situações podem gerar a indisponibilidade do serviço, como enchentes etc. Um simples poste caído devido a uma batida de carro pode gerar uma perda de comunicação e a indisponibilidade do serviço.

De qualquer forma, uma boa análise e a avaliação do risco associado devem ser realizadas buscando o desenvolvimento dos controles associados para a criação da contingência necessária.

Dica

Redundâncias e contingências são sempre úteis e, quando possível, devem sempre ser utilizadas.

Ataques de negação de serviço (DOS)

Corresponde a um tipo de ataque que tem por objetivo indisponibilizar determinado sistema ou equipamento. Ou seja, o equipamento pode até estar funcionando, mas seu uso fica prejudicado pela impossibilidade de acesso ao serviço prestado. Nesse tipo de ataque, são exploradas vulnerabilidades de softwares, de equipamentos e de algoritmos/protocolos.

São exemplos o pod (*ping of death*), *syn flood*, *udp flood* e o *tcp flood*. Esses ataques exploram vulnerabilidades na implementação de algum serviço de rede, sistema operacional ou protocolo utilizado. Foram muito famosos no início de disseminação desse tipo de ataque e atualmente são utilizados com mais de um agente (fonte), caracterizando assim uma nova classe de ataques, os distribuídos, que é interpretada como uma variante do DOS quando a fonte do ataque é distribuída, ou seja, quando há mais de uma fonte de emissão de sinais de ataques destinados para uma ou mais vítimas.

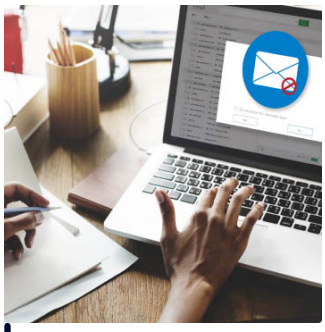
Antes eram utilizados os mesmos tipos de ataques para cada fonte. Atualmente, é comum encontrarmos situações em que cada fonte possui um tipo de ataque diferente, utilizando vulnerabilidades em implementação, sistema operacional ou protocolo. Assim, fica claro que há uma coordenação que determina a sincronicidade e o momento que os ataques serão proferidos. A necessidade de coordenação tornou urgente o desenvolvimento de uma infraestrutura de ataque e que diversas etapas predecessoras fossem criadas, situação esta denominada botnet.

Engenharia social

Situação em que são usadas as fraquezas humanas para se obter informação (ferir a confidencialidade) de uma pessoa ou organização.

Normalmente, comenta-se que o elo mais fraco, exatamente aquele que poderá ser o primeiro a ser explorado, é o humano.

Em uma organização é difícil que todos os colaboradores tenham o mesmo entendimento e a mesma maturidade com relação ao sigilo de informações.



> **O exemplo mais comum desse tipo de ataque é o phishing, comumente utilizado para obter dados de cartões de crédito, visando ao ganho financeiro.**

Ações de phishing podem acontecer de diversas formas. Pode ser um e-mail semelhante ao de uma instituição financeira, um SMS com um link para regularizar uma situação, uma página (ou post) em uma rede social e até mesmo um site inteiro clonado.

Outro exemplo bem comum na década de 1990 eram dispositivos, que possuíam várias formas e partes diferentes, que liam os cartões de crédito (naquela época sem chip) para copiar a tarja magnética. No Brasil, eles ganharam o apelido de chupa-cabra, fazendo menção a uma situação ocorrida em Minas Gerais, que era creditada à presença de alienígenas naquela região, na mesma época da aparição desses mecanismos.

O que chama bastante atenção é o **grau de sofisticação** usado pelos fraudatários na construção dos dispositivos de fixação e com aparência bem próxima aos dos bancos.

Pichação de site

Corresponde à técnica mais utilizada e se caracteriza pela alteração não autorizada de determinado site na internet. Também conhecido como defacement, essa técnica objetiva a adulteração do portal, sem o consentimento do proprietário. São exploradas as vulnerabilidades dos portais e, por meio disso, são realizadas as modificações.

Esse ataque é mais popular pela repercussão gerada após a sua realização. É relativamente fácil encontrá-lo em ferramentas de gestão de conteúdos (CMS), onde o proprietário do site apenas customiza determinados assuntos no portal, ou faz uso de plug-ins para ofertar novas formas de interação com o usuário.

Comentário

Inicialmente, apresentamos a imagem do zone-h, onde são exibidas as conquistas de defacement.

Botnets

Também conhecido como rede zumbi, é um conjunto de equipamentos que sofreu um ataque, resultando no controle do equipamento pelo hacker. O ataque é realizado através de um software chamado bot, que explora uma vulnerabilidade do equipamento e faz a instalação nele.

Na botnet, existem alguns equipamentos cuja finalidade é orquestrar o ataque, permitindo a manutenção do sigilo do hacker. Esses equipamentos são chamados de centros de comando e controle. Os bots se assemelham aos worms no que se refere à forma de proliferação, porém divergem por acatarem às ordens dos centros de comando e controle. Através de botnets é possível fazer ataques de negação de serviço, envios de e-mails em massa e vários outros.

Outros tipos de ataques cibernéticos

Ataques de Negação de Serviço

Engenharia social

Técnicas aplicadas

Veja, a seguir, outras técnicas utilizadas em ataques cibernéticos:

Ip spoofing

Ocorre quando o atacante forja o seu endereço IP, colocando outro valor nesse campo, fingindo ser a fonte dos dados de outra origem. É muito comum por explorar a vulnerabilidade do protocolo.

Pharming ou dns cache poisoning

Ocorre quando os servidores de DNS são atacados, visando alterar a troca dos nomes de domínios por endereços IPs e, assim, destinando a vítima para equipamentos e softwares falsos. Explora vulnerabilidades em determinadas implementações e marcas de equipamento. É uma técnica difícil de ser identificada pelo usuário final.

Ip session hijacking

Ocorre quando a conexão entre o cliente e o servidor na internet é realizada através de troca de comandos HTTP de requisição e resposta, por exemplo. Durante esse processo, é comum ter alguma sessão de usuário (HTTP Session) configurada e em execução, visando identificar o usuário que está acessando o portal.

Uma das técnicas utilizadas, seja para quebrar a confidencialidade do usuário, ou para realizar um ataque ao portal, é o sequestro de sessão do usuário. Logo, o invasor captura essa troca de informações e se faz passar por um dos equipamentos. Trata-se de uma técnica com certo grau de sofisticação e difícil de ser identificada por gerentes de rede e usuários finais.

Ip session hijacking

Ocorre quando as senhas nos sistemas de informação ficam codificadas no servidor. A codificação pode ser realizada por meio de técnicas proprietárias do sistema, onde são desenvolvidos algoritmos específicos de codificação, ou por meio de funções de condensação, também conhecidas como hash.

As quebras de senha podem usar conjuntos especiais de tabelas, conhecidas como rainbow tables, ou até mesmo a testagem de todas as combinações possíveis, chamada de força bruta. Nessa técnica, o grau de conhecimento do atacante determinará a eficácia do ataque.

Hash

Ocorre quando alguns algoritmos são criados usando manipulações algébricas que transformam os dados de entrada em um conjunto finito de números hexadecimais, chamado de hash do dado. Essas manipulações impedem que os

valores iniciais sejam recuperados a partir dos dados gerados.

Vamos ver como isso acontece? Faça download do documento.

Trashing dumpster diving

Ocorre quando são realizadas buscas nos lixos corporativos na expectativa de ter sido realizado algum descarte de forma inapropriada. Isso nos remete ao primeiro módulo, onde tratamos do ciclo de vida da informação. Se o descarte não for feito de forma apropriada, técnicas como essa permitem a recuperação da informação direto do lixo. Em muitos países, não há legislação que torne essa técnica ilegal.

Wardriving

Ocorre quando a pesquisa de locais físicos contém sinal de Wi-Fi desprotegido visando à exploração da vulnerabilidade encontrada. Nessa técnica, o invasor percorre os espaços públicos procurando os sinais desprotegidos, podendo ser a pé, de carro ou utilizando drones.

Softwares maliciosos

Malwares são softwares maliciosos que objetivam a infecção dos ativos de TI. Nessa categoria, há uma variação muito grande e com diversos tipos. Podemos citar os vírus Cavalos de Troia relacionados com propaganda, ferramentas de suporte usadas indevidamente, exploits e worms.

avalo de Troia

Inspirado no exemplo histórico que deu origem à técnica, mascara-se um vetor de ataque, normalmente um malware, dentro de um documento ou ferramenta, enganando a vítima do ataque.

xploits e worms

São as aplicações construídas especificamente para explorar determinadas vulnerabilidades existentes e os worms, muitas vezes confundidos com os vírus, utilizam as estruturas de comunicação para sua disseminação.

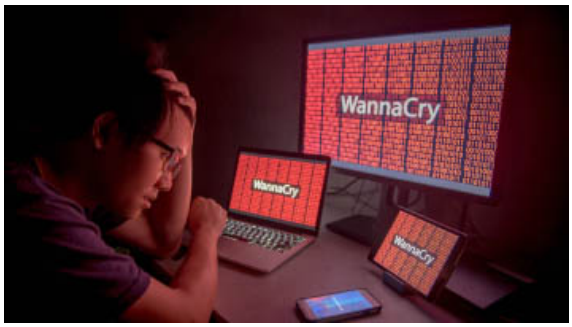
Há divergências entre as formas de classificação dos tipos de malwares. Porém, de maneira geral, pode-se dizer que os vírus são os malwares que precisam de um ambiente para a sua execução.

Os vírus relacionados com propaganda, como os **spywares** (por exemplo, aplicações que capturam tudo o que é digitado pelo usuário, conhecidas como keyloggers) e **adwares** (aplicações que trazem propaganda para o usuário, sem sua autorização) monitoram o usuário de alguma forma, visando explorar o aspecto comportamental humano.

Ainda há o uso mal-intencionado de ferramentas de suporte, como **sniffers** (farejadores) de rede e **port scanners**. O primeiro permite analisar o tráfego de rede e o segundo permite verificar quais são as portas de comunicação dos protocolos da camada de transporte que estão disponíveis para conexão.

Ransomware

Software malicioso, com alto poder de reprodutibilidade, que invade a máquina da vítima, criptografa os seus dados e solicita um resgate. Nos últimos anos, esse tipo de ataque tem sido bem frequente, tendo como caso emblemático o **WannaCry**.



Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

(IBFC – 2018 – Câmara de Feira de Santana-BA – Técnico de Suporte em Informática) É um software nocivo do tipo spyware, cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins. Essa é a descrição técnica do:

A Datalogger

B Keycutter

C Datacutter

D Keylogger

E Trashing hash

Parabéns! A alternativa D está correta.

As letras B e C não existem e Datalogger e Trashing hash não está relacionado com segurança.

Questão 2

(CESGRANRIO – 2018 – Transpetro – Analista de Sistemas Júnior – Infraestrutura) O código malicioso que visa criptografar os dados das vítimas e cobrar pagamento de resgate pela chave e pelo código de decriptação é classificado como um:

A Worm

B Spyware

C Ransomware

D Trojan Horse

E Wardriving

Parabéns! A alternativa C está correta.

Worm é um malware que se prolifera sozinho através de compartilhamentos de rede. Spyware captura o comportamento do usuário e envia para um atacante. Cavalo de Troia, ou trojan horse, é uma técnica em que um software malicioso se faz passar por outro software.

Considerações finais

Neste conteúdo, apresentamos os conceitos de ameaça e vulnerabilidade. Foram explorados os tipos de cada um e como é o relacionamento deles com os ataques e os controles, ou as ferramentas de proteção. Também abordamos ataques cibernéticos e técnicas de ataques, como DDoS, defacement e malware. No tocante aos malwares, falamos sobre conceitos, desde worm até ransomware.

Podcast

Ouça agora um resumo sobre os principais assuntos abordados.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. NBR ISO/IEC 27.002:2013. **Tecnologia da informação** — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

BARRETO, J. S.; ZANIN, A.; MORAIS, I. S.; VETTORAZZO, A. S. **Fundamentos de Segurança da Informação**. Porto Alegre: Sagah, 2018.

HINTZBERGEN, J. *et al*. **Fundamentos de Segurança da Informação**. Rio de Janeiro: Brasport, 2018.

MACHADO, F. N. R. **Segurança da Informação** – Princípios e Controles de Ameaças. 1 ed. São Paulo: Érica, 2019.

NIST, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 180-4, ***Secure Hash Standards*** (SHS). Publicado em: ago. 2015.

Explore +

Confira a sugestão que separamos especialmente para você!

Leia o artigo **Bitcoin: A Peer-to-Peer Electronic Cash System**, de Satoshi Nakamoto, que apresentou ao mundo não apenas mais

Leia o artigo **Bitcoin: A Peer-to-Peer Electronic Cash System**, de Satoshi Nakamoto, que apresentou ao mundo não apenas mais um modelo de moeda digital, mas também toda a técnica de blockchain, trazendo a ideia de armazenar informações de forma segura para evitar fraude. Pouco depois, descobriram que Satoshi Nakamoto não é uma pessoa, e sim um avatar de um grupo de pessoas ligadas ao mundo cibernético. Ainda não se sabe qual a sua verdadeira identidade.