SEGURANÇA EM REDES DE COMPUTADORES

SEGURANÇA EM ACESSOS SEM FIO, ATAQUES E CONTRAMEDIDAS

Autor: Me. Paulo André Zapparoli
Revisor: Rafael Rehm

INICIAR

introdução

Introdução

Nesta unidade, estudaremos a segurança de rede wireless e como suas características de funcionamento impactam na segurança da rede. Entenderemos quais são as medidas de segurança que devemos adotar para minimizar esses impactos. Descobriremos como os dispositivos móveis provocam mudanças no ambiente das redes e, consequentemente, na segurança de rede. Iremos compreender quais são os fatores de segurança que devem ser considerados na adoção desses dispositivos para os colaboradores de uma organização e como os atacantes utilizam os códigos maliciosos em uma invasão, além das contramedidas a esses ataques. Por fim, analisaremos leis e seus impactos, principalmente no que tange à privacidade dos dados pessoais.

Segurança em Redes *Wireless*

As redes sem fio (*wireless*) foram a evolução natural das redes com fios e trouxeram com ela uma série de problemas de segurança inerentes às suas características, bem como dos dispositivos *wireless* que as utilizam.

Os fatores principais das redes *wireless* que aumentam os riscos à segurança são: o canal, por envolver comunicação broadcast; mobilidade, que permite a portabilidade dos dispositivo *wireless* ; recursos de hardware limitados, apesar de sistemas operacionais complexos; e acessibilidade, ou seja, a possibilidade dos dispositivos estarem em ambientes isolados e hostis.

Simplificando, podemos dizer que são três componentes do ambiente wireless que oferecem ponto de ataque: o **cliente wireless** (o dispositivo equipado com Wi-Fi); o **ponto de acesso wireless** (o dispositivo que fornece a conexão); e o **meio de transmissão** (que transporta as ondas de rádio).

Algumas das ameaças de segurança às redes wireless estão listadas a seguir:

Associação acidental : as LANs ou pontos de acesso *wireless* da empresa para LANs com fios nas proximidades (por exemplo, no mesmo prédio ou em

prédios vizinhos) podem criar sobreposição de alcances de transmissão. Um usuário que deveria se conectar a uma LAN pode, inadvertidamente, se ligar a um ponto de acesso *wireless* de uma rede vizinha. Embora a falha de segurança seja acidental, ela expõe recursos de uma LAN a um usuário acidental.

Associação maliciosa : nessa situação, um dispositivo *wireless* é configurado para parecer ser um ponto de acesso legítimo, permitindo que o operador roube senhas de usuários legítimos e depois penetre em uma rede com fios por meio de um ponto de acesso *wireless* legítimo.

Redes ocasionais : essas são redes ponto a ponto entre computadores *wireless* , sem um ponto de acesso entre eles. Essas redes podem impor uma ameaça à segurança por causa da falta de um ponto de controle central.

Redes não tradicionais : redes e enlaces não tradicionais, como dispositivos *bluetooth* de rede pessoal, leitoras de código de barras e PDAs portáteis, impõem um risco à segurança em termos de espreita e falsificação.

Roubo de identidade (falsificação de MAC): isso ocorre quando um invasor é capaz de estreitar o tráfego da rede e identificar o endereço MAC de um computador com privilégios na rede.

Ataques de man-in-the-middle : no contexto do protocolo de troca de chave Diffie-Hellman. Em um sentido mais amplo, esse ataque envolve persuadir um usuário e um ponto de acesso a acreditarem que estão falando um com o outro, quando, na verdade, a comunicação está passando por um dispositivo de ataque intermediário. As redes *wireless* são particularmente vulneráveis a esses ataques.

Negação de serviço (DoS, do acrônimo em inglês para *Denial of Service*): no contexto de uma rede sem fios, um ataque de DoS ocorre quando um invasor bombardeia continuamente um ponto de acesso *wireless* ou alguma outra porta *wireless* acessível com diversas mensagens de protocolo criadas para consumir recursos do sistema. O ambiente *wireless* permite esse tipo de ataque, pois é muito fácil para um invasor direcionar inúmeras mensagens wireless para o alvo.

Injeção na rede : um ataque de injeção visa aos pontos de acesso *wireless* que estão expostos ao tráfego de rede não filtrado, como mensagens de protocolo de roteamento ou mensagens de gerenciamento de rede. Um exemplo desse tipo de ataque é aquele em que comandos de reconfiguração falsos são usados para afetar roteadores e switches para degradar o desempenho da rede.

Medidas de Segurança em Redes Wireless

Podemos agrupar as medidas de segurança *wireless* como aquelas que lidam com transmissões, pontos de acesso e redes (consistindo em roteadores *wireless* e pontos finais).

Protegendo transmissões wireless

As principais ameaças à transmissão wireless são captura, alteração ou inserção de mensagens e interrupção. Para lidar com a captura, dois tipos de contramedidas são apropriadas:

- Técnicas de ocultação de sinal: as empresas podem tomar uma série de medidas para tornar mais difícil para um invasor localizar seus pontos de acesso *wireless* , incluindo desligar o broadcasting do identificador de dispositivo de serviço (SSID) pelos pontos de acesso *wireless* ; atribuir nomes enigmáticos aos SSIDs; reduzir a intensidade do sinal para o nível mais baixo que ainda ofereça uma cobertura suficiente; e posicionar os pontos de acesso wireless no interior do prédio, longe de janelas e paredes externas. A maior segurança pode ser obtida pelo uso de antenas direcionais e de técnicas de blindagem de sinal.
- Encriptação: a encriptação de toda a transmissão *wireless* é eficaz contra captura desde que as chaves de encriptação sejam protegidas.

O uso da encriptação e protocolos de autenticação é o método padrão de combater tentativas de alterar ou inserir transmissões.

As empresas podem reduzir o risco de ataques de DoS não intencionais.

Análises feitas no local podem detectar a existência de outros dispositivos usando a mesma faixa de frequência, para ajudar a determinar onde os pontos de acesso *wireless* deveriam ser posicionados. As intensidades de sinal podem ser ajustadas, e a blindagem ser usada em uma tentativa de isolar um ambiente *wireless* contra transmissões vizinhas concorrentes.

Protegendo pontos de acesso wireless

A principal ameaça envolvendo pontos de acesso *wireless* é o acesso não autorizado à rede. A técnica principal para impedir esse acesso é o padrão IEEE 802.1X para o controle de acesso à rede baseado em porta. O padrão oferece um mecanismo de autenticação para dispositivos que queiram se conectar a uma LAN ou rede *wireless* .

O uso do 802.1X pode impedir que pontos de acesso maliciosos e outros dispositivos não autorizados se tornem *backdoors* desprotegidos.

Protegendo redes wireless

São recomendadas as seguintes técnicas para a segurança da rede wireless:

1. Use encriptação. Os roteadores wireless normalmente são equipados com mecanismos de encriptação embutidos para o tráfego de roteador a roteador.

2. Use software antivírus e antispyware, além de um firewall. Esses recursos deverão estar ativados em todos os pontos finais da rede wireless.

3. Desligue o broadcasting de identificador. Os roteadores wireless normalmente são configurados para transmitir um sinal de identificação, de modo que qualquer dispositivo dentro do alcance possa descobrir a existência do roteador. Se uma rede for configurada de modo que dispositivos autorizados conheçam a identidade dos roteadores, essa capacidade pode ser desativada, a fim de afastar os intrusos.

4. Mude o identificador padrão do seu roteador. Novamente, essa medida afasta os intrusos que tentarão obter acesso a uma rede wireless usando identificadores padrão do roteador.

5. Mude a senha predefinida para administração do seu roteador. Essa é outra medida prudente.

6. Permita somente que computadores específicos acessem sua rede wireless. Um roteador pode ser configurado para se comunicar somente com endereços MAC aprovados. Naturalmente, os endereços MAC podem ser falsificados, de modo que esse é apenas um dos elementos de uma estratégia de segurança completa.

praticar

Vamos Praticar

Uma rede sem fio (*wireless*) permite que os dispositivos de comuniquem sem a necessidade do uso de cabos. A transmissão de dados e informações é feita através de ondas de rádio. Esse tipo de comunicação não possui uma fronteira tão bem definida como as redes cabeadas que são totalmente controladas. Sendo assim, é possível que o sinal de uma rede se expanda além dos limites físicos de uma corporação. As principais ameaças apresentadas à transmissão de uma rede wireless são captura, alteração ou inserção de mensagens e interrupção.

Selecione a alternativa que indica corretamente dois tipos de contramedidas para a captura de informação *wireless* .

- **a)** Mudar a senha administrativa e encriptação.
- **b)** Técnicas de ocultação de sinal e encriptação.
- **c)** Técnicas de ocultação de sinal e mudar a senha administrativa.
- **d)** Mudar a senha administrativa e usar software antivírus e antispyware.
- **e)** Usar software antivírus e antispyware e encriptação.

Segurança em Dispositivos Móveis

O ambiente de tecnologia da informação tem uma grande mudança com a adoção do smartphone nas corporações. Antes, vemos um ambiente com fronteiras claramente definidos, no qual os computadores ou notebooks operam dentro dos limites da rede física. Esses perímetros ajudavam na criação de políticas de segurança e de uso dos dispositivos. Também auxiliava na definição dos recursos que deviam ser protegidos de acesso indevido dentro da organização. As aplicações eram controladas para fornecer servidor dentro desses limites. Agora, vemos grandes mudanças nesses aspectos, e as seguintes características devem ser acomodadas pelas redes de uma organização:

Uso cada vez maior de novos dispositivos : os colaboradores das organizações estão sendo incentivados a utilizar dispositivos finais diversos, principalmente móveis, em suas atividades diárias.

Aplicações baseadas em nuvem : as aplicações que atendem aos colaboradores da organização passaram a fazer parte de uma gama de serviços utilizados em nuvem. Os formatos colaborativos das aplicações em nuvem facilitam a comunicação de desenvolvimento dos serviços a distância.

Somam-se a essas aplicações diversas outras desenvolvidas para o uso pessoal que passaram a ser ferramentas de trabalho também profissional.

Remoção do perímetro : com a mobilidade das aplicações e a proliferação de dispositivos em nuvem, aquela noção de perímetro de rede fica ultrapassada. Exige agora que determinemos inúmeros perímetros de rede, que, além de diversos, passam a ser dinâmicos, em constante adaptação às condições de ambiente em constante mudança.

Requisitos de negócios externos : abrem-se condições para uma diversidade de acesso às redes por parceiros e colaboradores externos, com o uso de diferentes dispositivos e a partir de inúmeros locais.

O grande motivador de toda essa revolução é o dispositivo de computação móvel. Equipamentos como tablets e smartphones permitiram o aumento de produtividade em razão de sua conveniência. Devido à crescente adoção desses dispositivos móveis e de suas características tecnológicas, a segurança da informação precisa adaptar as políticas de segurança e normas de utilização de dispositivo a essa nova realidade. Além disso, implementar nossas medidas visando ao controle e à gestão da segurança nos dispositivos móveis.

Ameaças à Segurança

As mudanças provocadas com a utilização de dispositivos móveis invocam novas medidas de proteções que sejam especializadas de acordo com as características desses dispositivos. A Nist (National Institute of Standards and Technology) fez a publicação especial “Diretrizes para gerenciar a segurança de dispositivos móveis no empreendimento” (Guidelines for Managing the Security of Mobile Devices in the Enterprise – SP 800-124), que, entre outras informações, lista sete importantes aspectos de segurança que devemos considerar quando utilizamos dispositivos móveis:

1. **Falta de controles de segurança física** : o local em que esse dispositivo trafegava dentro ou fora da organização e quem está em posse do dispositivo

foge ao controle da equipe de segurança. Assim, a política de segurança deve ter suas regras para dispositivos móveis baseadas na hipótese de que o dispositivo pode ser utilizado para fins maliciosos, ou até mesmo roubado.

2. **Uso de dispositivos móveis não confiáveis** : a organização deve levar em conta que, além dos dispositivos que são controlados, todos os seus colaboradores também possuem smartphones e tablets. Como esses últimos não estarão com os controles propostos pela política de segurança, devem ser considerados não confiáveis.

3. **Uso de redes não confiáveis** : os dispositivos móveis poderão estar conectados através da rede *wireless* da empresa, ou através da Internet de uma outra rede *wireless* , ou pela rede celular que possui vulnerabilidade que foge ao controle da equipe de segurança. Dessa forma, a política de segurança deve basear-se na possibilidade de que as utilizadas por esses dispositivos móveis não são confiáveis.

4. **Uso de aplicações criadas por partes desconhecidas** : muito comum será encontrar, além das aplicações da organização, outras desenvolvidas por terceiros. Temos a clara possibilidade de instalação de softwares maliciosos. A política de segurança deve estar preparado para lidar com essas ameaças.

5. **Interação com outros sistemas** : um risco que deve ser mensurado pela organização é a sincronização de dados dos dispositivos móveis com a nuvem. Se a organização não tiver controle de todos os dispositivos envolvidos na sincronização, haverá riscos de introdução de *malware* e de vazamento de dados por armazenamento em local inseguro.

6. **Uso de conteúdo não confiável** : outro cuidado que se deve ter é quanto ao uso de conteúdo que outros dispositivos computacionais não encontram, porque pode induzir o usuário a instalar ou acessar softwares maliciosos.

7. **Uso de serviços de localização** : a capacidade dos dispositivos móveis de GPS pode ser usada para manter um conhecimento do local físico do dispositivo. Para que esse recurso possa ser útil para uma organização como uma parte de um serviço de presença, ele cria riscos à segurança. Um atacante pode usar a informação de local para determinar onde o dispositivo

e o usuário estão localizados, o que pode ser de proveito para o atacante.

Medidas de Segurança

Baseando-se nas ameaças apresentadas, desenvolveu-se uma estratégia de segurança para dispositivos móveis, fundamentada em três categorias que veremos a seguir:

Segurança da barreira

A organização deverá ter mecanismos de segurança para proteger a rede contra acesso não autorizado. A estratégia de segurança também pode incluir políticas de *firewall* específicas ao tráfego de dispositivo móvel. Políticas de *firewall* podem limitar o escopo dos dados e o acesso à aplicação para todos os dispositivos móveis. De modo semelhante, sistemas de detecção e prevenção de intrusão podem ser configurados para ter regras mais rígidas para o tráfego de dispositivo móvel.

Segurança do tráfego

> *A segurança do tráfego é baseada nos mecanismos normais para encriptação e autenticação. Todo o tráfego deverá ser encriptado e trafegar por meios seguros, como SSL ou IPv6. As redes privadas virtuais (VPNs) podem ser configuradas de modo que todo o tráfego entre o dispositivo móvel e a rede da organização seja feito por uma VPN (STALLINGS, 2015, p. 445).*

Deverá ser usado um protocolo de autenticação forte, para limitar o acesso do dispositivo aos recursos da organização. Frequentemente, um dispositivo móvel tem um único autenticador específico do dispositivo, pois considera-se que o dispositivo tenha apenas um usuário. Uma estratégia preferível é ter um mecanismo de autenticação em duas camadas, o que envolve autenticar o dispositivo e depois autenticar o usuário dele.

Segurança do dispositivo

As organizações que fornecem dispositivos móveis para uso dos empregados farão pré-configuração desses dispositivos de acordo com a política de segurança da empresa. Mas algumas organizações podem achar conveniente ou mesmo necessário adotar uma política do tipo "traga seu próprio dispositivo", que permite que os dispositivos móveis pessoais dos empregados tenham acesso aos recursos corporativos. Os gerentes de TI devem ser capazes de inspecionar cada dispositivo antes de permitir o acesso à rede. A TI deverá estabelecer diretrizes de configuração para sistemas operacionais e aplicações. Por exemplo dispositivos móveis não podem armazenar contatos corporativos no armazenamento local. Seja um dispositivo pertencente ou não à organização, esta deverá configurá-lo com controles de segurança (STALLINGS, 2015, p. 444-445).

praticar

Vamos Praticar

Uma organização optou pela utilização de dispositivos móveis, porém decidiu que não seria utilizado de forma irrestrita. Somente alguns departamentos teriam os acessos liberados a esses dispositivos. A política de segurança foi adaptada a essa nova condição. Porém, durante a implementação dos acessos, a equipe de TI deixou aberto o acesso à rede sem fio que conectava os dispositivos e colaboradores indevidos conectaram seus smartphones.

Selecione a alternativa que indica corretamente qual o aspecto de segurança essa falha representa.

- **a)** Uso de redes não confiáveis.
- **b)** Interação com outros sistemas.

- **c)** Uso de dispositivos móveis não confiáveis.
- **d)** Uso de serviços de localização.
- **e)** Falta de controles de segurança física.

Código e Atividade Maliciosa

> *Em termos simples, software malicioso é qualquer programa que execute ações que você, como usuário do computador, não queira. Frequentemente, o objetivo de software malicioso é causar prejuízo a seu sistema. Software malicioso, ou malware, se movimenta pela Internet da mesma forma que uma serpente desliza pela grama. Atacantes o utilizam para roubar senhas e informações confidenciais, excluir informações de seu sistema ou ainda reformatar discos rígidos. Infelizmente, você não pode controlá-lo apenas com software antivírus, pois há outros elementos no código malicioso além de vírus, e algum malware pode escapar de detecção (KIM; SOLOMON, 2014, p. 259).*

No início dos sistemas computacionais um *malware* somente se espalhava através dos disquetes, como era um processo manual se convencionou chamar de redes de pessoas furtivas (sneaker net). Com essa forma de transmissão, um vírus demora meses para se espalhar pelo mundo. Atualmente, os vírus se espalham pelas redes de computadores e Internet, viajando pelo mundo em minutos. Essa diferença deve-se principalmente à evolução da comunidade de escrita de vírus, que desenvolveram formas mais

sofisticadas de disseminação. Existem diversas técnicas diferentes adotadas para a disseminação de um vírus, às vezes mais de uma foi empregada em um mesmo vírus.

Décadas de 1970 e início de 1980: pesquisa acadêmica e UNIX – Utilização de Vermes

Década de 1980: primeiros vírus em PCs

Década de 1990: primeiros vírus em LANs

Meados da década de 1990: aplicativos inteligentes e a Internet – programação dos *malwares* através de softwares de distribuição em massa (por exemplo, e-mail)

2000 até o presente – códigos maliciosos com ataques combinados.

Fonte: Kim e Solomon (2014, p. 273-274).

Os motivos principais para uma organização focar esforços na detecção, atenuação e recuperação de ataques são que as ameaças de malware podem se originar de diversas fontes diferentes, desde pequenos incidentes, pouco sofisticados, que envolvem um único atacante, até ataques complexos e estruturados de grupos organizados, com diversos alvos simultâneos. Geralmente, essas ameaças partem de fora da infraestrutura de TI de uma organização.

Outra preocupação são as ameaças que têm origem interna, seja por políticas de segurança mal feitas ou impróprias, seja por práticas indevidas dos usuários. Entender a natureza e significados e criar métodos de controle para essas ameaças é responsabilidade da área de segurança da informação de TI.

Tipos de Ameaças

Os códigos maliciosos são preocupações constantes das organizações e podem afetá-las de diversas maneiras:

- **Ataques contra confidencialidade e privacidade** : conseguir acesso a informações restritas e, muitas vezes, sigilosas sobre os indivíduos ou sobre o negócio da organização.
- **Ataques contra a integridade de dados** : alteração indevida ou destruição de informações da organização. No caso de informações confidenciais, o resultado pode ser devastador.
- **Ataques contra disponibilidade de serviços e recursos** : ataques de negação de serviço podem trazer muito prejuízo a uma organização. Quanto maior a dependência dos serviços de Internet, maiores os prejuízos nesse caso.
- **Ataques contra produtividade e desempenho** : em diversos postos de trabalho, os colaboradores de uma organização precisam trabalhar on-line. Existem diversas códigos maliciosos que consomem recursos da máquina, além de distrair os usuários.
- **Ataques que criam responsabilização legal** : a responsabilidade pode ser legal, ou seja, o dever de agir na correção de vulnerabilidade pode afetar o relacionamento com parceiros comerciais e até mesmo com clientes (por exemplo, LGPD).
- **Ataques que prejudicam reputação** : a difusão de informações sigilosas ou a fragilidade do sistema destacada em uma invasão pode afetar a reputação de uma organização e levar a prejuízos também financeiros.

Geralmente, as ameaças à segurança que partem de fora da organização recebem maior atenção, mas não podemos esquecer de promover a segurança dentro da rede, que começa com uma boa política de uso e implementação de ferramentas que coíbam a utilização dos sistemas computacionais quando a ação estiver em desacordo com a política de uso.

Algumas das práticas inseguras são consideradas normais pelos usuários da rede, mas podem representar vulnerabilidades de segurança. Devemos estar atentos a práticas como:

- Utilização de mídia de disco não confiável.
- Instalação de software sem autorização ou registro, seja aplicativo ou SO.

- Download de arquivos da Internet não monitorado.
- Disseminação de anexos de e-mail não controlado.

Essas vulnerabilidades se estendem também a políticas de pessoas que podem ser fracas ou mal implementadas. Essas brechas podem permitir:

- Acesso não autorizado a recursos de sistema e de rede.
- Escalada de privilégios.
- Roubo, destruição ou disseminação não autorizada de dados.
- Uso de recursos de rede corporativos para iniciar ataques hostis contra alvos externos.
- A liberação acidental ou intencional de código malicioso em segmentos internos de rede não protegidos por controles de perímetro e contramedidas de detecção de intrusão.

Ataques

Há algum tempo, o atacante era caracterizado como um “nerd” que desenvolvia suas próprias ferramentas movido, muitas vezes, pelo conhecimento e reconhecimento. Hoje em dia, a figura é bem diferente. O atacante pode ser mais que uma pessoa, com softwares sofisticados para fazer o ataque, e tem como motivações: dinheiro fama ativismo social e propagação de ideias e valores. Mas existem outras motivações, por exemplo a raiva e procura por vingança.

Geralmente, os ataques têm por finalidade principal:

- **Negação de disponibilidade** : o objetivo desses ataques é impedir acessos legítimos aos sistemas atacados, por exemplo DoS ou de DDoS.
- **Modificação de dados** : nesse tipo de ataque, o objetivo é acessar os dados para excluir, modificar ou substituir por novo.
- **Exportação de dados** : roubar a informação é o objetivo desse ataque, encaminhando para o atacante através da Internet ou e-mail. Alguns cavalos de Troia são exemplos desse ataque, pois eles

encaminham as informações de usuário e senha ao atacante.
- **Ponto de lançamento** : nesse ataque, a visita será usada como um ponto de lançamento para outro ataque ou disseminação de vírus.

De acordo com as motivações e as finalidades, o atacante ou grupo de atacantes se dividem em quatro tipos de ataques principais:

1. **Ataques não estruturados** contra recursos são, geralmente, executados por atacantes com habilidade moderada. Obtendo-se sucesso, o atacante pode passar a níveis mais maliciosos. Sua motivação inicial, em geral, são gratificações pessoais, como o desafio.

2. **Ataques estruturados** são tecnicamente mais qualificados, exigindo o uso de ferramentas complexas e esforços concentrados. O ataque, muitas vezes, é organizado em fase com objetivos específicos. São atacantes que agem em grupos ou sozinhos que possuem a capacidade de desenvolverem técnicas de invasão com potencial de causar danos sérios a redes. Sua motivação pode ser política, raiva ou dinheiro.

3. **Ataques diretos** têm como característica principal a ação em tempo real. A ação pode ter objetivo simples, como uma pichação em site por hacktivismo, ou pode ser utilizada como porta de entrada para ataques mais maliciosos, como a implantação de um cavalo de Troia para reconhecimento da rede e dispositivos. Esses ataques podem ser não estruturados quando feitos por novatos através de ferramentas de hacker, buscando explorar o ambiente por tentativa e erro. E também podem ser ataques estruturados, por grupos de crackers ou individuais, por um método previamente construídos para alcançar objetivos definidos.

4. **Ataques indiretos** são os resultados obtidos pela exploração de código hostil pré-programados, como worms e vírus de Internet. Mesmo explorando vulnerabilidades específicas, seja de um sistema operacional, seja de um aplicativo, sua transmissão e replicação acontecem de forma indiscriminada e sua propagação é muito rápida. Muitas vezes, o ataque direto é utilizado para iniciar um ataque indireto que atingirá uma população mais ampla.

Uma parte fundamental dos ataques estruturados é o planejamento do

ataque. Esse planejamento possui etapas definidas (Figura 4.1) para se obter êxito no ataque. Vamos ver mais detalhes sobre essas etapas:

Figura 4.1 - Fase de um ataque
Fonte: Kim e Solomon (2014, p. 279).

Reconhecimento e sondagem : análise do alvo em busca de vulnerabilidade. Essa fase é a mais importante porque a boa coleta de informações indicará a melhor forma de atacar, que terá o método mais furtivo. Nessa fase, utilizam-se, muitas vezes, ferramentas comuns, porque elas são baseadas no funcionamento do protocolo e, dessa forma, é possível, se bem planejado, coletar informação sem ser notado.

Escalada de acesso e de privilégio : depois de entender o ambiente do alvo, o trabalho é localizar uma vulnerabilidade dentre as possíveis que permita acesso ao sistema do alvo. A ideia é buscar uma conexão inicial que permita reconhecimentos adicionais. Para isso, na maioria das vezes, é necessário ganhar direitos administrativos no sistema.

Cobrindo seus rastros : essa fase visa dificultar a detecção do ataque. Essas ações vão variar de acordo com os sistemas invadidos, mas seguirão algumas etapas básicas: manter os arquivos o mais próximo possível do ambiente pré-

ataque, removendo arquivos utilizado e restaurando os modificados na medida do possível, e limpar os rastros de arquivos de histórico e auditoria (muitas vezes, será necessário atacar seus sistemas). Todo esforço adotado para limpar rastros é válido, pois aumenta as chances de evitar a detecção do ataque.

Contramedidas

Implementar contramedidas é tarefa essencial dos profissionais de segurança de TI. Essa implementação deve possuir um ciclo de monitoração, teste e melhoria contínua para se tornarem defesas efetivas.

> *Defesa em profundidade é a prática de dispor defesas em zonas para aumentar o nível de proteção geral e fornecer mais tempo de reação para responder a incidentes. Defesa em profundidade combina as capacidades de pessoas, operações e tecnologias de segurança, com o intuito de estabelecer várias camadas de proteção, eliminando linhas de defesa isoladas e efetivamente aumentando o custo de um ataque. Ao lidar com contramedidas individuais como parte de um conjunto integrado de medidas de proteção, você poderá garantir que tratou de todas as vulnerabilidades. Gerentes precisam fortalecer essas defesas em locais críticos, monitorar ataques e reagir a eles rapidamente (KIM; SOLOMON, 2014, p. 283).*

As contramedidas estão divididas em duas partes: prevenção de ataques e detecção de ataques.

Prevenção de Ataques

Na prevenção, as principais ações visam manter seguros os ativos que integram a infraestrutura da rede, que é composta pelos dispositivos intermediários (*switches, access point e roteadores*), dispositivos finais (computadores, smartphones e tablets) e servidores (serviços e aplicações). Para essa manutenção, é essencial o controle também sobre o comportamento dos usuários desses recursos.

A seguir, descrevemos os principais pontos a serem abordados pela prevenção de ataques segundo Kim e Solomon (2014).

Defesas de aplicativo : é necessário para proteger qualquer aplicativo que tenha a função de fornecer acesso a dados, pois são comuns ataques que visam acessar ou danificar dados sensíveis. Recomenda-se a implantação de controles para proteger qualquer software aplicativo que execute em qualquer computador. Alguns desses controles incluem:

- Filtros antivírus em todos os sistemas computacionais.
- Atualização do antivírus deve ser garantida e monitorada.
- Exame obrigatório em toda unidade de mídia removível.
- *Firewall* pessoal e IDS em sistemas computacionais são recomendáveis.
- Software de auditoria, históricos e detecção de mudanças.
- Controles de uso de e-mail e checagem de anexos.
- Política para instalação e atualização de software.
- Garantir origens confiáveis para obtenção, instalação e atualização software.

Defesas de sistema operacional : todo sistema computacional utiliza um sistema operacional para gerenciar o uso do hardware pelos softwares aplicativos. Comprometido o sistema operacional, o atacante, além de conseguir acesso aos sistemas l de armazenamento de dados locais, utiliza o computador para outras finalidades. Proteger os sistemas operacionais é muito importante. Alguns controles para o sistema operacional são:

- Software para a detecção de mudança, auditoria, histórico e verificação de integridade em todos os servidores.
- Certificar-se da atualização de todos os sistemas operacionais pelo fornecedores.
- Garantir origens confiáveis.
- Instalar somente aplicativos necessários.
- Remover serviços e processo desnecessário de SO.

Defesas de infraestrutura de rede : a maioria dos computadores de uma

organização trabalha diretamente conectada à rede ou de alguma forma fazem essa conexão. Dessa forma, pensar em ambientes de rede que possibilitam e aperfeiçoem a segurança é muito importante. Controles que podemos implementar para a proteção da rede incluem:

- Usar serviços proxy proteção e monitoramento de serviços críticos.
- Filtros de conteúdo de tráfego de rede instalados em pontos críticos.
- Implementar serviços para análise de comportamento dos usuários da rede como IDS e mantê-los atualizados.
- Aplicar patches corretivos de segurança nos dispositivos de rede para mitigar vulnerabilidades.
- Controlar tráfego em segmentos de rede ou serviços específicos.
- Acessos remotos permitidos somente em casos necessários.
- Impossibilitar ou evitar ao máximo que se contornem os sistemas de controle e contramedidas implementados.

Outros pontos importantes para a prevenção são criação de políticas e normas de comportamento e uso dos dispositivos de informática.

Detecção de ataques

Para as contramedidas de detecção de ataque, é necessária a adoção de ferramentas. Sistemas de alerta e análise em sistemas e área de rede críticas são elementos essenciais. As ferramentas permitem implementações de acordo com a análise de criticidade da empresa, permitindo uma flexibilidade de adoção e fornecendo recursos contra atividades maliciosas. Muitas dessas ferramentas possibilitam detecção baseadas em assinatura e em comportamento. Algumas das ferramentas adotadas são:

Software de varredura antivírus : deve ser implantado como requisito de acesso a todos os dispositivos que utilizam a rede da organização. A maioria desses produtos, além de checar vírus, analisa também a intrusão.

O software antivírus pode ser ineficiente se não existir uma contínua atualização de sua lista de assinaturas, que contém as definições de vírus mais atuais. Outras ações que podem comprometer a eficiência do software

antivírus é a ausência de atualizações dos sistemas operacionais e a instalação de software não licenciados ou não, autorizados, principalmente de baixados sem as devidas precauções.

Existem as soluções de antivírus baseado em rede. Com elas, é possível filtrar arquivos e tráfego de mensagens em servidores e análise de anexos nos emails.

Monitores e analisadores de rede : é importante o uso de ferramentas que monitoram o tráfego de rede para verificar se as práticas de segurança continuam efetivas. Sabemos que o atacante fará de tudo para se passar por uma comunicação legítima, e, devido a isso, muitas vezes, é necessário correlacionar informações de diferentes comunicações para poder evidenciar um ataque.

Para complementar a monitoria, é necessário usar ferramentas que fazem a análise de vulnerabilidades, que checam o nível de segurança baseado em vulnerabilidades conhecidas e documentadas, indicando quais são ações corretivas necessárias. É necessário que essas ferramentas sejam executadas regularmente para manter o ambiente seguro. Muitas ferramentas desse tipo são usadas para a realização de ataques. Além de checar as aplicações que fazem parte do ambiente de produção, é importante fazer uma análise geral para checar se não existem novas portas de serviços abertas desnecessariamente.

Software de filtragem e de captura de conteúdo/contexto : para a implementação de análise desse tipo, é imprescindível uma política bem clara sobre condutas e comportamentos de uso dos recursos de informática, porque envolve a difícil tarefa de equilibrar a privacidade e segurança. Análise de conteúdo é uma forte aliada na defesa de códigos maliciosos. As ferramentas desse nível podem checar os anexos em e-mails e conteúdo. Adicionar essas ferramentas políticas de lista de controle de acesso auxilia a segmentar redes de forma segura.

Honeypots e ***honeynets*** : *honeypots* são computadores e serviços utilizados como isca nas bordas de uma rede para atraírem as potenciais invasões.

Configurados para parecem reais, fazem parte de uma rede segregada, chamada *honeynet* . Esse é um ambiente controlado e permite que se analise e detecte facilmente um ataque.

praticar

Vamos Praticar

O analista de segurança utiliza uma ferramenta de varredura e de mapeamento de porta chamada NMAP. Essa ferramenta permite ao analista de segurança identificar todos os *hosts* da rede, dispositivos que estão conectados à rede com um IP válido em seu range, e também checar se nesse *hosts* existe algum serviço ativo. Obtidas essas informações, ele checa se confere com o ambiente de produção proposto e verifica motivos de eventuais divergências. Essa ferramenta, muitas vezes, é utilizada por um atacante.

Selecione a alternativa que indica corretamente a fase do ataque que seria utilizada essa ferramenta.

- **a)** Cobrindo rastro.
- **b)** Reconhecimento e sondagem.
- **c)** Mantendo acesso.
- **d)** Ganhando acesso.
- **e)** Escalando privilégio.

Conformidade

Novas ameaças para cidadãos e organizações surgiram com a utilização do ciberespaço. Em nenhuma outra época, compartilharam-se tantos dados pessoais como hoje em dia. Na rede, as pessoas compartilham seus dados com os amigos e para adquirir bens e serviços. Esses dados são coletados e usados por organizações para realizar negócios. Para atender aos cidadãos com seus serviços, os governos estadual e federal coletam e utilizam informações das pessoas.

Com o aumento indiscriminado da coleta de dados, surgem questões sobre seu uso apropriado. Pessoas exigem que as organizações detentoras de seus dados confidenciais tomem medidas para protegê-los. Quando as organizações não protegem esses dados voluntariamente, as pessoas normalmente dizem que “deveria haver uma lei”. O Brasil tem a Lei nº 13.709, aprovada em agosto de 2018 (BRASIL, 2018, on-line), que trata do assunto, chamada de Lei Geral de Proteção de Dados Pessoais (LGPD). Ela entra em vigência a partir de agosto de 2020. Essa lei exige que organizações utilizem controles de segurança para proteger os diferentes tipos de dados que coletam. As leis não são opcionais. Se uma lei se aplicar a uma organização,

ela deverá segui-la. Às vezes, as empresas devem seguir diversas leis de proteção de dados.

saiba mais

Saiba mais

O Brasil possui a LGPD, a qual versa sobre o tratamento de dados pessoais que incluem os meios digitais. Essa lei visa proteger os dados dos cidadãos, dando a eles o direito à privacidade. Ela indica que os cidadãos têm o direito de saber o que se fará com seus dados e optar se desejam que seus dados sejam excluídos. Para saber mais, acesse a LGPD disponível em:

ACESSAR

Faz parte da atividade da maioria da organizações o uso e armazenamento de muitos dados, e, para muitas delas, a informação é um de seus ativos mais importantes. Elas utilizam a informação para realizar negócios, para rastrear preferências de produtos de clientes e também usam esses mesmos sistemas de tecnologia de informação (TI), com seus bando de dados enormes, para gerenciar os produtos e serviços que oferecem a clientes. As organizações utilizam os dados e os transferem a outras empresas, além de constantemente coletar mais dados, os quais podem ser usados para identificar uma pessoa, e muitos os consideram confidenciais.

Infelizmente, organizações, às vezes, não realizam um bom trabalho de proteção dos dados privados. Elas podem perder os dados por conta de uma brecha de segurança e também podem usá-los de maneira que seus consumidores e clientes não aprovem. Quando as organizações não protegem a privacidade voluntariamente, os governos criam leis para forçá-las a fazer isso. Uma vez que as leis sejam decretadas, as empresas deverão segui-las. É o que se chama de conformidade.

Conformidade também pode ser descrita como rastreabilidade, obrigação, flexibilidade, tolerância e obediência. Resumindo, uma organização deve observar seus próprios regulamentos internos, bem como as leis do país e os requisitos da legislação e regulamentos locais (HINTZBERGEN et al., 2015, p. 155).

Conformidade é um conceito importante. No sistema jurídico, é o ato de seguir leis, regras e regulamentações que se apliquem a você. Para uma organização, conformidade envolve não apenas seguir leis e regulamentações, mas também as próprias políticas e procedimentos da empresa. Uma organização deverá documentar as respectivas atividades de conformidade. Não é suficiente para uma empresa apenas afirmar que está em conformidade com as leis. Ela precisará provar.

reflita

Reflita

Uma pequena loja de rua, para atrair novos clientes e conseguir uma lista de contatos para comunicar por novidade e descontos, decidiu fazer um sorteio. Para participar, era necessário informar uma série de dados pessoas e privados. O proprietário do negócio não possui funcionário da área de TI ou contato com alguém que trabalhe com segurança da Informação. Reflita como a LGPD pode impactar nesse negócio e o que deve fazer para estar em conformidade.

Fonte: Elaborado pelo autor.

Organizações utilizam diversas atividades diferentes para mostrar conformidade, incluindo:

- Criar políticas e procedimentos para agir de acordo com requisitos legais e regulamentares.
- Comparar requisitos de conformidade com as práticas diárias da organização e modificá-las de acordo com a necessidade.

- Desenvolver e usar sistemas de monitoramento em sistemas computacionais para alertar a organização se há controles de segurança, legalmente exigidos, comprometidos.
- Criar atividades de treinamento e conscientização que instruam os funcionários sobre requisitos de conformidade.

Conformidade não apenas inclui o estado real de estar de acordo, mas também as etapas e processos tomados para estar em conformidade. Em geral, é preciso fazer as seguintes perguntas: Quais são as regras? Como devem ser seguidas? Se uma organização deixar de cumprir suas obrigações, ela poderá estar sujeita a penalidades.

praticar

Vamos Praticar

Para provar que está em conformidade, uma organização deve apresentar evidências de que está seguindo rigorosamente as leis que regem suas atividades. Durante uma auditoria sobre a segurança das informações, uma determinada organização apresentou algumas evidências, de acordo com as solicitações feitas pelo auditor, para comprovar que está em conformidade. Os seguintes documentos foram apresentados:

I. Políticas e procedimentos do uso de sistemas computacionais.

II. *Logs* do sistema de monitoramento em sistemas computacionais.

III. Lista de presença de treinamento e conscientização de reciclagem.

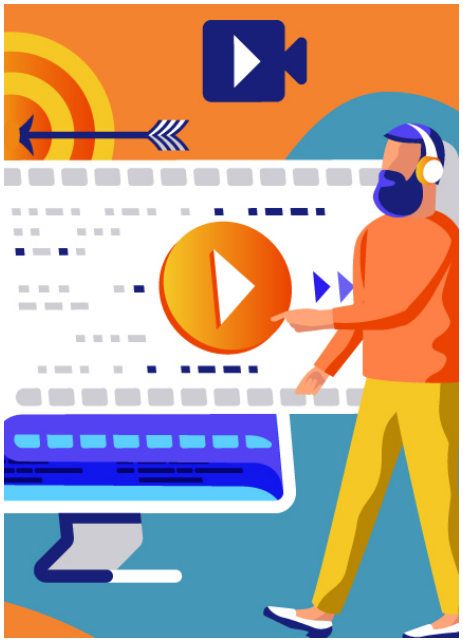
IV. *Logs* e históricos de backup e restore.

Selecione a alternativa que indica corretamente as evidências de conformidade em segurança da informação.

- **a)** I, II, III e IV.
- **b)** I, II e III, apenas.
- **c)** I, III e IV, apenas.
- **d)** I, II e IV, apenas.
- **e)** II, III e IV, apenas.

indicações

Material Complementar



FILME

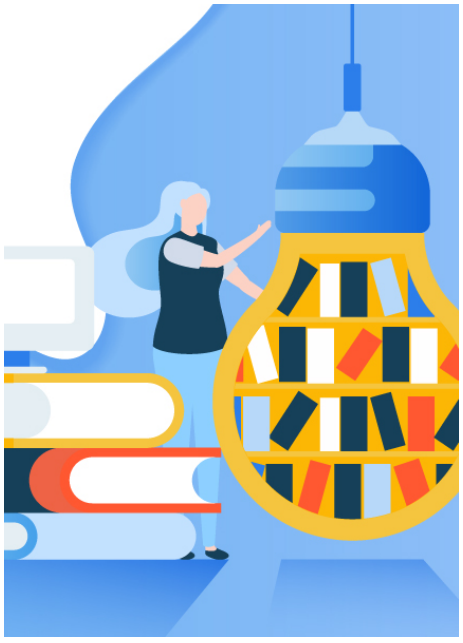
Nome : Privacidade hackeada

Ano : 2019

Comentário : O filme é um documentário que apresenta o caso Cambridge Analytica/Facebook, empresa que fez a campanha de Donald Trump e o Brexit. No filme, é exposto como eles fizeram uso de dados pessoais, privados, sem autorização e evidencia a necessidade das pessoas obterem o direito de controle sobre suas informações privadas.

Para conhecer mais sobre o filme, acesse o trailer disponível em:

TRAILER



LIVRO

Nome do livro : *A arte de invadir*

Editora : Pearson Education do Brasil

Autor : Kevin Mitnick e William Simon

ISBN : 978-8576050551

Comentário : Kevin Mitnick é considerado o hacker mais famoso do mundo. Ele escreve este livro apresentando um caso de sucesso de invasões cibernéticas. Apresenta também como esses ataques poderiam ser evitados, o que deveria ter sido adotado

como contramedida em cada um dos casos.

conclusão

Conclusão

Nesta unidade, entendemos quais são os tipos de ataques, suas fases e motivações. Vimos os elementos necessários para uma contramedida de ataque, tanto para detectar quanto para prevenir o ataque, e que as leis, sempre que aplicáveis a uma organização, devem nortear suas atividades. Estudamos sobre a criação de planos e políticas que regulam e evidenciam que as atividades da organização funcionam conforme a lei, que chamamos de conformidade, e compreendemos que as redes sem fio e dispositivos móveis motivaram grandes mudanças no ambiente de tecnologia da informação. Por fim, aprendemos a criar medidas que controlem os ambientes sem fio e de mobilidade.

referências

Referências Bibliográficas

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Diário Oficial da União** . Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm . Acesso em: 30 jan. 2020.

HINTZBERGEN, J.; HINTZBERGEN Hi., K.; SMULDERS, A.; BAARS, H.

Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002. 3. ed. São Paulo: Brasport, 2015.

KIM, D.; SOLOMON, M. G. **Fundamentos de segurança de sistemas de informação** . Rio de Janeiro: LTC, 2014.

MITNICK, K.; SIMON, W. **A arte de invadir** . São Paulo: Pearson Education do Brasil, 2005.

NIST. **Guidelines for managing the security of mobile devices in the Enterprise** , jun. 2013. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final . Acesso em: 30 jan. 2020.

PRIVACIDADE HACKEADA | Trailer oficial | Netflix (2 min. 16 seg.). Disponível em: https://www.youtube.com/watch?v=wjXYCrxRWqc . Acesso em: 30 jan. 2020.

STALLINGS, W. **Criptografia e segurança de redes** : princípios e práticas. 4. ed. São Paulo: Pearson Education do Brasil, 2015.