Capítulo 5 - Tudo precisa ser protegido

# **Tipos de dados**

Os dados realmente mudaram? Bom, tecnicamente não, os dados gerados por computadores e dispositivos digitais ainda são grupos de 1s e 0s. Isso não mudou. O que mudou foi a quantidade, volume, variedade e urgência dos dados gerados.

Tradicionalmente, as empresas tinham acesso às informações coletadas de formulários, planilhas, aplicativos, compras de cartão de crédito e outros tipos de arquivos. A maior parte das informações era armazenada e analisada posteriormente. Os dados confidenciais ainda eram coletados, armazenados e analisados, mas, tradicionalmente, os hackers estavam mais interessados em invadir os sistemas para obter os segredos corporativos ou governamentais.

Atualmente, os dados coletados estão ganhando novas características. O mundo digitalizado abriu os portões da coleta de dados. Os dispositivos de IoT habilitados para sensores estão coletando cada vez mais dados pessoais. Os rastreadores fitness vestíveis, sistemas de monitoramento residencial, câmeras de segurança e transações de cartão de débito estão coletando dados pessoais, bem como dados comerciais e ambientais. Muitas vezes, os dados são combinados de diferentes fontes e os usuários podem não ter conhecimento disso. Combinar os dados de monitoramento de exercícios físicos com os dados de monitoramento residencial pode produzir pontos de dados que ajudam a mapear os movimentos ou a localização de um proprietário. Esse novo tipo de coleta e agregação de dados pode ser usado para bons propósitos a fim de ajudar o meio ambiente. Também aumenta a possibilidade de invasão de privacidade, roubo de identidade e espionagem corporativa.

Informações de identificação pessoal (PII, Personal indentifiable information) ou informações pessoais confidenciais (SPI, sensitive personal information) são dados relacionados a um indivíduo vivo que podem ser usados por conta própria ou com outras informações para identificar, entrar em contato ou localizar um determinado indivíduo. Os dados coletados por empresas e instituições governamentais também podem conter informações confidenciais sobre segredos corporativos, patentes de novos produtos ou segurança nacional.

Como estamos coletando e armazenando volumes exponenciais de dados confidenciais e informativos, aumentou a necessidade de segurança adicional para proteger essas informações contra desastres naturais, hackers e uso indevido.

# **Quem quer nossos dados?**

**Os Caras Bons**

Empresas legítimas tem um contrato estabelecido, que dá permissão para usar os dados coletados sobre você para fins de melhorar os negócios. Lembra daqueles documentos de "Termos e condições" ou "Termos de serviço e contratos" para os quais dizemos sim, mas que normalmente não lemos? Na próxima vez que se deparar com um, leia. O conteúdo pode ser surpreendente.

Outros usuários legítimos de nossos dados seriam empresas que usam sensores em seus próprios dispositivos ou veículos. Governos que têm sensores ambientais e cidades que têm sensores instalados em trens, ônibus ou semáforos também têm direito aos dados gerados.

Alguns hackers, chamados de hackers “white hat”, são pagos por empresas legítimas e governos para testar a segurança de um dispositivo ou sistema. Seu objetivo não é roubar ou modificar os dados, mas ajudar a protegê-los.

**Os Caras Maus**

Outros hackers, chamados de hackers "black hat", querem acesso aos dados coletados por muitas razões desonestas:

* Para vender as informações para terceiros.
* Para modificar os dados ou desativar a funcionalidade em um dispositivo.
* Para interromper ou danificar a imagem de uma empresa legítima.
* Para acessar dispositivos, páginas da Web e dados para criar tumultos políticos ou fazer uma declaração política.
* Para acessar as IDs de usuário e senhas a fim de roubar identidades.
* Para acessar dados para cometer um crime.
* Para invadir sistemas só para provar que podem fazê-lo.

# **Práticas recomendadas de segurança**

Proteger a rede envolve todos os protocolos, tecnologias, dispositivos, ferramentas e técnicas que protegem dados e reduzem ameaças. A segurança da rede é amplamente orientada pelo esforço de permanecer um passo à frente de hackers mal intencionados. Assim como médicos tentam evitar novas doenças, enquanto tratam problemas atuais, os profissionais de segurança da rede tentam evitar possíveis ataques e minimizar os efeitos dos ataques em tempo real. As redes estão sob ataque rotineiramente. É comum ler as notícias sobre outra rede que foi comprometida.

Políticas, procedimentos e normas de segurança devem ser seguidos no design de todos os aspectos de toda a rede. Isso deve incluir os cabos, dados em trânsito, dados armazenados, dispositivos de rede e dispositivos finais.

Realizar a avaliação de risco: Saber o valor do que você está protegendo ajudará a justificar as despesas de segurança. Criar uma política de segurança: Criar uma política que define claramente as regras da empresa, os deveres e as expectativas do trabalho. Medidas de segurança física: Restringir o acesso a armários de rede, locais de servidor, bem como supressão de fogo. Medidas de segurança de recursos humanos: Os funcionários devem ser devidamente pesquisados com verificações de antecedentes.. Executar e testar backups: Fazer backups regulares e teste de recuperação de dados de backups. Manter patches de segurança: Atualizar regularmente o servidor e os sistemas operacionais e programas de dispositivos de rede e do cliente. Empregar controles de acesso: Configurar funções de usuário e níveis de privilégio, bem como autenticação forte ao usuário. Testar regularmente a resposta a incidentes: Empregar uma equipe de resposta a incidentes e testar cenários de resposta a emergências. Implementar uma rede de monitoramento, análise e ferramenta de gerenciamento: Escolher uma solução de gerenciamento de segurança que se integra a outras tecnologias. Implementar dispositivos de segurança de rede: Use roteadores, firewalls e outros dispositivos de segurança de última geração. Implementar uma solução abrangente de segurança de endpoints: Use software antivírus e antimalware de nível corporativo. Treinar os usuários: Treinar os usuários e funcionários nos procedimentos seguros. Criptografar dados: Criptografar todos os dados confidenciais da empresa, incluindo e-mail.

# **Segurança Física**

Os data centers atuais armazenam enormes volumes de informações confidenciais, essenciais para a empresa; portanto, a segurança física é uma prioridade operacional. A segurança física não só protege o acesso às instalações, como também protege as pessoas e equipamentos. Por exemplo, alarmes de incêndio, sprinklers, racks de servidor reforçados contra atividades sísmicas e aquecimento redundante, ventilação e ar-condicionado (HVAC), bem como os sistemas de nobreak são implantados para proteger as pessoas e equipamentos.

A segurança física dentro do data center pode ser dividida em duas áreas, externa e interna.

* **Segurança fora do perímetro** - Pode incluir segurança no local, cercas, portões, vigilância contínua por vídeo e alarmes de violação de segurança.
* **Segurança dentro do perímetro** - Pode incluir vigilância contínua por vídeo, detectores eletrônicos de movimento, traps de segurança e sensores biométricos de acesso e de saída.

Os traps de segurança fornecem acesso aos data halls em que os dados do data center são armazenados. Semelhantes a um bloqueio de ar. Uma pessoa deve primeiro entrar no trap de segurança, usando seu cartão ou crachá com ID de proximidade. Depois que a pessoa entrou no trap de segurança, o reconhecimento facial, impressões digitais ou outras verificações de biometria são usados para abrir a segunda porta. O usuário deve repetir o processo para sair do data hall.

# **Desafios da proteção dos dispositivos de IoT**

Os dispositivos de IoT são desenvolvidos com os recursos de conectividade de rede necessários, mas geralmente não implementam uma sólida segurança da rede. A segurança da rede é um fator crítico durante a implantação de dispositivos de IoT. Métodos devem ser usados para garantir a autenticidade, integridade e segurança dos dados, o caminho entre o sensor para o coletor e a conectividade com o dispositivo.

# **Uso de Wi-Fi seguro**

As redes sem fio são populares em todos os tipos e portes de empresas, pois são fáceis de configurar e convenientes de usar. Para funcionários e convidados, a empresa precisa proporcionar uma experiência sem fio que permita mobilidade e segurança. Se uma rede sem fio não estiver devidamente protegida, os hackers dentro do alcance podem acessá-lo e se infiltrar na rede.

A figura destaca os passos para ajudar a proteger uma rede sem fio. Selecione cada passo para obter mais informações.

# **Casas smart**

A tecnologia de casa smart se tornou muito popular e sua popularidade aumenta a cada ano, à medida que a tecnologia evolui. Quem não acha interessante ativar, aumentar ou diminuir o termostato da casa, enquanto está no trabalho, ou ter um refrigerador que faz compras para serem entregues quando você chegar em casa? É legal dar uma olhada no cachorro ou verificar se os adolescentes estão fazendo o dever de casa depois da escola, ativando as câmeras de segurança de sua casa?

À medida que instalamos mais e mais sensores inteligentes em nossas casas, podemos aumentar a possibilidade de problemas de segurança. Geralmente, os sensores estão conectados à mesma rede que os nossos dispositivos domésticos ou de pequenas empresas, de modo que uma violação de um dispositivo pode irradiar para fora e afetar todos os dispositivos conectados. Os sensores também podem propiciar uma forma para que hackers entrem na rede doméstica e obtenham acesso a todos os computadores e dados conectados à rede.

Até mesmo assistentes virtuais, como Apple SIRI, Amazon Echo ou Google Home, podem ser riscos de segurança. As pessoas usam esses dispositivos para ligar o som, ajustar a temperatura do ambiente, fazer compras on-line e obter instruções sobre aonde estão indo. Isso pode causar danos? O vazamento de informações pessoais, como senhas ou informações de cartão de crédito, é possível.

Felizmente, muitas das falhas de segurança dos sensores de tecnologia smart anteriores já foram descobertas. Os desenvolvedores estão trabalhando para corrigir as falhas e melhorar as medidas de segurança para proteger os sistemas contra ataques. Antes de comprar sistemas de segurança doméstica, é muito importante pesquisar o desenvolvedor e os protocolos de segurança e de criptografia que estão em vigor para seus produtos.

# **Hotspots públicos**

Quando você estiver longe de casa, um ponto de acesso de WiFi público permite acessar as informações on-line e navegar na Internet. As atividades comuns em Wi-Fi público incluem entrar em uma conta de e-mail pessoal, inserir informações pessoais identificáveis, fazer login em redes sociais e acessar informações bancárias ou financeiras. Todas essas informações podem ser roubadas se a conexão Wi-Fi não for segura.

Regras de segurança a seguir se você estiver usando um hotspot de Wi-Fi público ou inseguro:

* Não acesse ou envie informações pessoais e confidenciais em uma rede sem fio pública.
* Verifique se o computador está configurado com o compartilhamento de arquivos e mídia e se ele requer autenticação de usuário com criptografia.
* Use os serviços e túneis criptografados de rede privada virtual (VPN). O serviço VPN fornece acesso seguro à Internet, com uma conexão criptografada entre o computador e o servidor VPN do provedor de serviços VPN. Com um túnel VPN criptografado, mesmo se for interceptada uma transmissão de dados, ela não será decifrável.

Muitos dispositivos móveis, como smartphones e tablets, vêm com o protocolo sem fio Bluetooth. Esse recurso permite que dispositivos habilitados para Bluetooth conectem-se entre si e compartilhem informações. Infelizmente, o Bluetooth pode ser explorado por hackers para bisbilhotar alguns dispositivos, estabelecer controles de acesso remoto, distribuir malware e drenar as baterias. Para evitar esses problemas, mantenha o Bluetooth desligado quando você não estiver usando.

# **Configuração de uma VPN em smartphones**

VPN é uma rede segura que usa uma conexão criptografada com a Internet, que atua como um "túnel" seguro dos dados. Pode ser criada na conexão pública com a Internet, para permitir que os usuários ocultem a identidade quando estiverem usando a Internet. Você deve usar um serviço VPN ao se conectar a uma rede Wi-Fi de terceiros (por exemplo, na biblioteca ou em uma cafeteria). Isso impede que outras pessoas nessa rede pública espionem seu uso da Web, quando você estiver usando sites ou comunicações que não são seguros.

Muitas empresas exigem o acesso VPN em suas redes internas, se os funcionários estiverem trabalhando remotamente ou em trânsito. O funcionário receberá o cliente VPN, bem como as informações de ID de usuário e senha. Para quem não tem acesso a uma VPN corporativa, existem diversos aplicativos de serviço de VPN para smartphone, que podem ser baixados gratuitamente ou mediante uma taxa mensal. Os exemplos desses aplicativos de VPN incluem: [ExpressVPN](https://www.expressvpn.com/), [NordVPN](https://nordvpn.com/)e [TunnelBear](https://www.tunnelbear.com/).

Se tiver uma VPN corporativa ou baixar um aplicativo de serviço de VPN, você receberá as informações e o suporte necessários para configurar a VPN.

**Resumo**

Este capítulo começou discutindo os tipos de dados. Informações de identificação pessoal (PII, Personal indentifiable information) ou informações pessoais confidenciais (SPI, sensitive personal information) são dados relacionados a um indivíduo vivo que podem ser usados por conta própria ou com outras informações para identificar, entrar em contato ou localizar um determinado indivíduo. Empresas legítimas tem um contrato (Termos e condições ou termos de serviço), que dá permissão para usar os dados coletados sobre você para fins de melhorar os negócios. Outros usuários legítimos de nossos dados seriam empresas que usam sensores em seus próprios dispositivos ou veículos. Governos que têm sensores ambientais e cidades que têm sensores instalados em trens, ônibus ou semáforos também têm direito aos dados geram.

Alguns hackers, chamados de hackers “white hat”, são pagos por empresas legítimas e governos para testar a segurança de um dispositivo ou sistema. Seu objetivo é não roubar ou modificar os dados, mas ajudar a protegê-los. Hackers "black hat" querem acesso aos dados coletados por muitos motivos, incluindo venda, danos à reputação de uma pessoa ou empresa e causar tumultos políticos.

Em seguida, o capítulo detalhou as melhores práticas de segurança. A segurança inclui proteger fisicamente os perímetros interno e externo de lugares, como data centers, onde os dados são armazenados. A proteção dos dispositivos de IoT é um desafio devido ao grande número deles, o fato de que são encontrados em locais não tradicionais e que muitos deles não podem ser atualizados.

Hackers "black hat" acessam o Wi-Fi disponível frequentemente. Existem várias medidas que você pode adotar para proteger a rede sem fio da empresa. Para proteger os dispositivos, mantenha o firewall ativado, gerencie o sistema operacional e navegador, e use antivírus e antispyware.

Regras de segurança a seguir se você estiver usando um hotspot de Wi-Fi público ou inseguro:

* Não acesse ou envie informações pessoais e confidenciais em uma rede sem fio pública.
* Verifique se o computador está configurado com o compartilhamento de arquivos e mídia e se ele requer autenticação de usuário com criptografia.
* Use os serviços e túneis criptografados de rede privada virtual (VPN). O serviço VPN fornece acesso seguro à Internet, com uma conexão criptografada entre o computador e o servidor VPN do provedor de serviços VPN. Com um túnel VPN criptografado, mesmo se for interceptada uma transmissão de dados, ela não será decifrável.

À medida que instalamos mais e mais sensores inteligentes em nossas casas, podemos aumentar a possibilidade de problemas de segurança. Geralmente, os sensores estão conectados à mesma rede que os nossos dispositivos domésticos ou de pequenas empresas, de modo que uma violação de um dispositivo pode irradiar para fora e afetar todos os dispositivos conectados.