Propagação das ameaças de cibersegurança

Data do Post	@August 30, 2021 9:00 AM (GMT)
Status	Done
Palavras-chave	Ameaças
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Existem especialistas que são inovadores e visionários. Eles constroem os diferentes domínios cibernéticos da Internet. Eles têm a capacidade de reconhecer o poder dos dados e de aproveitá-los. Depois, eles constroem suas empresas e proporcionam serviços, além de proteger as pessoas contra ataques cibernéticos. De maneira ideal, os profissionais de segurança cibernética devem reconhecer a ameaça que os dados representam, se forem usados contra as pessoas.

Dados nas mãos erradas podem resultar em uma perda de privacidade para os proprietários, podem afetar seu crédito ou colocar em risco sua carreira ou relações pessoais.

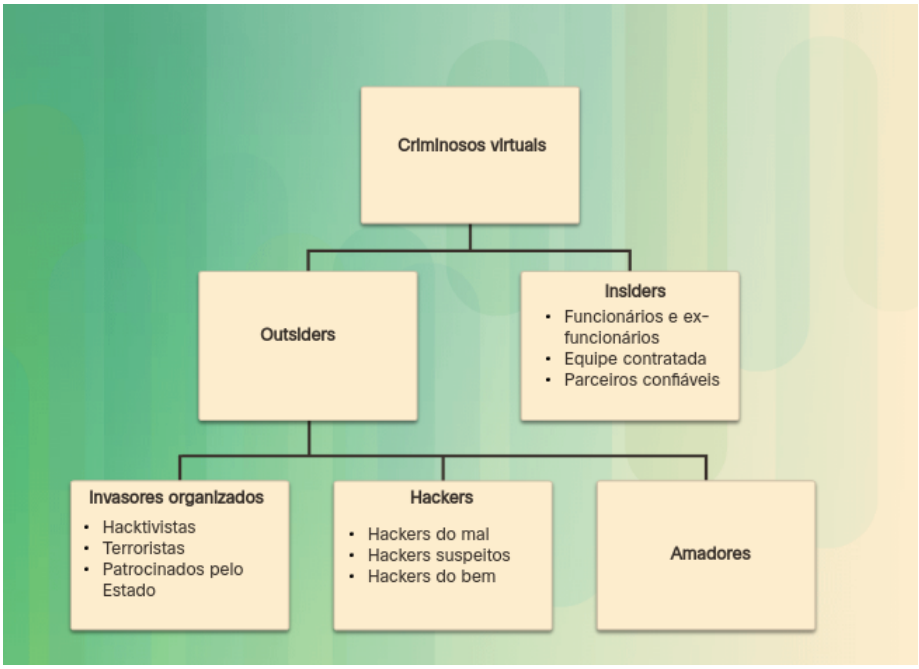
Por esse motivos, é importante que as pessoas físicas e juridicas conheçam as ameaças a que estão expostas. Para isso, nesse artigo, analisaremos como dos dados constituem uma fonte de propagação das ameaças.

Ameaças à segurança interna

Os ataques podem se originar de dentro de uma organização ou de fora da organização, conforme mostrado na figura. Um usuário interno, como um funcionário ou parceiro de contrato, pode, de forma acidental ou intencional:

- Tratar erroneamente os dados confidenciais;
- Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede;
- Facilitar ataques externos conectando mídias USB infectadas no sistema de computador corporativo;
- Convidar acidentalmente malware para a rede por e-mail ou sites mal-intencionados;

Ameaças internas têm o potencial de causar maior dano que as ameaças externas, pois os usuários internos têm acesso direto ao edifício e a seus dispositivos de infraestrutura. Os invasores internos normalmente têm conhecimento da rede corporativa, de seus recursos e de seus dados confidenciais. Eles também podem ter conhecimento de contramedidas de segurança, políticas e níveis mais altos de privilégios administrativos.



Ameaças e vulnerabilidades do usuário comum

O domínio do usuário inclui usuários que acessam o sistema de informações da empresa. Os usuários podem ser funcionários, clientes, prestadores de serviços e outros indivíduos que precisam acessar os dados. Os usuários são frequentemente o elo mais fraco nos sistemas de segurança de informações e representam uma ameaça significativa à confidencialidade, integridade e disponibilidade dos dados da empresa.

As práticas arriscadas ou ruins do usuário normalmente prejudicam, até mesmo, o melhor sistema de segurança. Abaixo, alguns exemplos de ameaças comuns encontradas em muitas empresas:

- **Nenhuma conscientização sobre segurança** – os usuários devem ter consciência dos dados confidenciais, políticas e procedimentos de segurança, das tecnologias e das contramedidas oferecidas para proteger as informações e os sistemas de informação.
- **Políticas de segurança mal aplicadas** – todos os usuários devem conhecer as políticas de segurança e as consequências da não conformidade com as políticas da empresa.
- **Roubo de dados** – o roubo de dados por usuários pode custar às empresas financeiramente, resultando em danos à reputação de uma empresa, ou levar a uma responsabilidade jurídica associada à divulgação de informações confidenciais.
- **Downloads não autorizados** – muitas infecções e ataques de redes e de estações de trabalho estão relacionados a usuários que fazem downloads não autorizados de e-mails, fotos, músicas, jogos, aplicativos, programas e vídeos para estações de trabalho, redes ou dispositivos de armazenamento.
- **Mídia não autorizada** – o uso de mídia não autorizada, como CDs, unidades de USB e dispositivos de armazenamento de rede, pode resultar em infecções e ataques por malware.
- **VPNs não autorizadas** – VPNs podem esconder o roubo de informações. A criptografia normalmente usada para proteger a confidencialidade cega o pessoal de TI para a transmissão de dados sem a autorização adequada.
- **Sites não autorizados** – acessar sites não autorizados pode representar um risco para os dados, dispositivos e para a empresa do usuário. Muitos sites alertam os visitantes quanto a fazer download de scripts ou plugins que contêm código malicioso ou adware. Alguns desses sites podem infectar dispositivos como câmeras e aplicativos.
- **Destruição de sistemas, aplicativos ou dados** – a destruição acidental ou deliberada ou sabotagem de sistemas, aplicativos e dados representa um grande risco para todas as empresas. Ativistas, funcionários descontentes e concorrentes do setor podem excluir dados, destruir dispositivos ou tornar dados e sistemas de informação indisponíveis.

Nenhuma solução técnica, controle ou contramedida torna os sistemas de informação mais seguros do que os comportamentos e processos das pessoas que usam esses sistemas.

Ameaças à segurança externa

Ameaças externas de amadores ou invasores habilidosos podem explorar vulnerabilidades em dispositivos conectados em rede ou podem usar social engineering, como enganações, para ter acesso. Ataques externos exploram fraquezas ou vulnerabilidades para obter acesso a recursos externos.

Dados Tradicionais

Dados corporativos incluem informações pessoais, propriedade intelectual e dados financeiros. Informações pessoais incluem materiais de aplicativos, folha de pagamento, cartas de oferta, acordos de funcionários e todas as informações usadas na tomada de decisões de emprego. Propriedade intelectual, como patentes, marcas registradas e planos de novos produtos, permite que uma empresa obtenha vantagem econômica sobre seus concorrentes. Considere essa propriedade intelectual como um segredo comercial. Perder essas informações pode ser desastroso para o futuro da empresa. Dados financeiros, como declarações de rendimentos, balanços e demonstrações de fluxo de caixa, proporcionam detalhes sobre a saúde da empresa.

Vulnerabilidades de dispositivos móveis

No passado, os funcionários normalmente usavam computadores fornecidos pela empresa conectados a uma LAN corporativa. Os administradores monitoram e atualizam continuamente esses computadores para atender aos requisitos de segurança.

Surgimento da Internet das Coisas

A Internet das coisas (IoT) é o conjunto de tecnologias que permitem a conexão de vários dispositivos à Internet. A evolução tecnológica associada ao advento da IoT está mudando os ambientes comerciais e de consumo. As tecnologias IoT permitem às pessoas conectarem bilhões de dispositivos à Internet. Esses dispositivos incluem aparelhos, bloqueios, motores e dispositivos de entretenimento, para citar apenas alguns. Essa tecnologia afeta a quantidade de dados que precisam de proteção. Os usuários acessam esses dispositivos remotamente, o que aumenta o número de redes que requer proteção.

Com o surgimento da IoT, há muito mais dados a serem gerenciados e protegidos. Todas essas conexões, além da capacidade de armazenamento expandida e de serviços de armazenamento oferecidos na nuvem e da virtualização, levaram ao crescimento exponencial de dados. Essa expansão de dados criou uma nova área de interesse na tecnologia e nos negócios, chamada "Big data".

O impacto do Big data

O big data é o resultado de conjuntos de dados grandes e complexos, tornando os aplicativos de processamento de dados tradicionais inadequados.

Simplificando, big data é um conjunto de dados maior e mais complexo, especialmente de novas fontes de dados. Esses conjuntos de dados são tão volumosos que o software tradicional de processamento de dados simplesmente não consegue gerenciá-los. No entanto, esses grandes volumes de dados podem ser usados para resolver problemas de negócios que você não conseguiria resolver antes.

O big data impõe desafios e oportunidades, com base em três dimensões:

- O volume ou a quantidade de dados
- A velocidade ou a rapidez dos dados
- A variedade ou a gama de tipos e fontes de dados

Embora o big data seja uma grande promessa, ele também traz seus desafios.

Para começar, o big data é grande. Apesar de novas tecnologias terem sido desenvolvidas para o armazenamento de dados, os volumes de dados estão dobrando em tamanho a cada dois anos. As empresas ainda se esforçam para acompanhar a evolução de seus dados e encontrar maneiras de armazená-los com eficiência.

Mas armazenar os dados não é o suficiente. Eles devem ser usados para serem úteis, e isso depende da curadoria. Dados limpos ou relevantes para o cliente e organizados de maneira que permita uma análise significativa exigem muito trabalho. Cientistas de dados gastam de 50 a 80 por cento de seu tempo curando e preparando dados antes de serem usados.

Por fim, a tecnologia de big data está mudando em ritmo acelerado. Há alguns anos, o Apache Hadoop era a tecnologia popular usada para lidar com big data. Em seguida, o Apache Spark foi introduzido em 2014. Hoje, uma combinação das duas estruturas parece ser a melhor abordagem. Manter-se atualizado com a tecnologia de big data é um desafio contínuo.

Há vários exemplos de grandes ataques corporativos de hackers nos jornais. Empresas como Target, Home Depot e PayPal são alvo de ataques altamente divulgados. Como resultado, os sistemas empresariais exigem mudanças drásticas nos designs dos produtos de segurança e atualizações significativas nas tecnologias e nas práticas. Além disso, os governos e as indústrias estão introduzindo mais regulamentações e demandas que exigem melhor proteção dos dados e controles de segurança para ajudar a proteger o big data.