1

Tipos de Ataque

Segurança da Informação

Segurança da Informação

Tipos de Ataque

O que é um ataque cibernético?

Um ataque cibernético é qualquer esforço intencional para roubar, expor, alterar, desativar ou destruir dados, aplicativos ou outros ativos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital.

Segurança da Informação

Tipos de Ataque

O que é um ataque cibernético?

Os **agentes de ameaças** lançam ataques cibernéticos por todos os tipos de razões, desde pequenos roubos até atos de guerra. Eles usam uma variedade de táticas, como ataques de malware, golpes de engenharia social e roubo de senhas, para obter acesso não autorizado aos seus sistemas alvo.

Os ataques cibernéticos podem perturbar, danificar e até destruir empresas. O custo médio de uma violação de dados é de US$ 4,35 milhões. Este preço inclui os custos de descoberta e resposta à violação, tempo de inatividade e perda de receitas, e os danos à reputação a longo prazo de uma empresa e da sua marca.

Segurança da Informação

Tipos de Ataque

O que é um ataque cibernético?

Mas alguns ataques cibernéticos podem ser consideravelmente mais caros do que outros. Os ataques de ransomware resultaram em pagamentos de resgate de até USD 40 milhões. Os golpes de comprometimento de e-mail comercial (BEC) roubaram até USD 47 milhões das vítimas em um único ataque. Ataques cibernéticos que comprometem os clientes informações de identificação pessoal (PII) podem levar à perda de confiança do cliente, multas regulatórias e até mesmo ações legais. Segundo uma estimativa, o cibercrime custará à economia mundial 10,5 bilhões de dólares por ano até 2025.

Segurança da Informação

Tipos de Ataque

Por que os ataques cibernéticos acontecem?

As motivações por trás dos ataques cibernéticos podem variar, mas existem três categorias principais: criminoso, político e pessoal.

Atacantes com motivação criminal buscam ganhos financeiros por meio de roubo monetário, roubo de dados ou interrupção de negócios. Os criminosos cibernéticos podem invadir uma conta bancária para roubar dinheiro diretamente ou usar golpes de engenharia social para enganar as pessoas a enviar dinheiro para elas. Os hackers podem roubar dados e usá-los para cometer roubo de identidade ou vendê-los na dark web ou mantê-los como resgate.

Segurança da Informação

Tipos de Ataque

Por que os ataques cibernéticos acontecem?

Extorção é outra tática popular. Os hackers podem usar ransomware, ataques de DDoS ou outras táticas para reter dados ou reféns de dispositivos até que uma empresa pague. De acordo com o X-Force Threat Intelligence Index, 27% dos ataques cibernéticos têm o objetivo de extorquir suas vítimas.

Agressores pessoalmente motivados, como atuais ou ex-funcionários descontentes, buscam principalmente retribuição por alguma percepção de menosprezo. Eles podem pegar dinheiro, roubar dados confidenciais ou interromper os sistemas de uma empresa.

Segurança da Informação

Tipos de Ataque

Por que os ataques cibernéticos acontecem?

Os atacantes com **motivação política** são frequentemente associados à guerra cibernética, ao terrorismo cibernético ou ao "hacktivismo." Na guerra cibernética, os atores dos estados-nação geralmente têm como alvo as agências governamentais ou a infraestrutura crítica de seus inimigos. Por exemplo, desde o início da Guerra Russia-Ucrânia, ambos os países experimentaram uma erupção cutânea de ataques cibernéticos contra instituições vitais (link reside fora de ibm.com). Os hackers ativistas, chamados de "hacktivistas", podem não causar danos extensos aos seus alvos. Em vez disso, eles normalmente buscam atenção para suas causas divulgando seus ataques ao público.

Segurança da Informação

Tipos de Ataque

Por que os ataques cibernéticos acontecem?

Motivações de ataques cibernéticos menos comuns incluem espionagem corporativa, em que hackers roubam a propriedade intelectual para obter uma vantagem injusta sobre os concorrentes, e hackers vigilantes que exploram as vulnerabilidades de um sistema para avisar os outros sobre eles. Alguns hackers simplesmente hackeiam por esporte, saboreando o desafio intelectual.

Segurança da Informação

Tipos de Ataque

Quem está por trás dos ataques cibernéticos?

Organizações criminais, atores estaduais e pessoas privadas podem lançar ataques cibernéticos. Uma forma de classificar os agentes de ameaças é categorizá-los como ameaças externas ou internas.

Ameaças externas não estão autorizadas a usar uma rede ou um dispositivo, mas entram de qualquer maneira. Os agentes externos de ameaças cibernéticas incluem grupos criminosos organizados, hackers profissionais, agentes patrocinados pelo Estado, hackers amadores e hacktivistas.

Segurança da Informação

Tipos de Ataque

Quem está por trás dos ataques cibernéticos?

Ameaças internas são usuários que têm acesso autorizado e legítimo aos ativos de uma empresa e usam indevidamente ou acidentalmente seus privilégios. Esta categoria inclui funcionários, parceiros de negócios, clientes, prestadores de serviços e fornecedores com acesso ao sistema.

Embora os usuários negligentes possam colocar suas empresas em risco, só haverá um ataque cibernético se o usuário usar intencionalmente seus privilégios para realizar atividades mal-intencionadas. Um funcionário que armazena informações confidenciais de forma descuidada em uma unidade não segura não está cometendo um ataque cibernético, mas um funcionário insatisfeito que conscientemente faz cópias de dados confidenciais para ganho pessoal está.

Segurança da Informação

Tipos de Ataque

Qual é o alvo dos ataques cibernéticos?

Os atores de ameaças normalmente se dividem em redes de computadores porque estão atrás de algo específico. Os alvos comuns incluem:

- Dinheiro
- Dados financeiros das empresas
- Listas de clientes
- Dados do cliente, incluindo informações pessoais identificáveis (PII) ou outros dados pessoais confidenciais
- Endereços de e-mail e credenciais de login
- Propriedade intelectual, como segredos comerciais ou designs de produtos

Segurança da Informação

Tipos de Ataque

Qual é o alvo dos ataques cibernéticos?

Em alguns casos, os cyberattackers não querem roubar nada. Em vez disso, eles simplesmente desejam interromper os sistemas de informação ou a infraestrutura de TI para prejudicar uma empresa, uma agência governamental ou outro alvo.

Segurança da Informação

Tipos de Ataque

Quais efeitos os ataques cibernéticos têm sobre as empresas?

Se bem-sucedidos, os ataques cibernéticos podem prejudicar as empresas. Eles podem causar inatividade, perda de dados e perda de dinheiro. Por exemplo:

- Os hackers podem usar malware ou ataques de negação de serviço para causar falhas no sistema ou servidor. Esse tempo de inatividade pode levar a grandes interrupções no serviço e perdas financeiras. De acordo com o relatório *Cost of a Data Breach*, a violação média resulta em USD 1,42 milhões em negócios perdidos.

- Os ataques de injeção SQL permitem que hackers alterem, excluam ou roubem dados de um sistema.

Segurança da Informação

Tipos de Ataque

Quais efeitos os ataques cibernéticos têm sobre as empresas?

- Os ataques de phishing permitem que hackers enganem as pessoas no envio de dinheiro ou informações confidenciais para elas.
- Os ataques de ransomware podem desativar um sistema até que a empresa pague ao invasor um resgate. De acordo com um relatório, o pagamento médio de resgate é de US$ 812.360.

Segurança da Informação

Tipos de Ataque

Quais efeitos os ataques cibernéticos têm sobre as empresas?

Além de prejudicar diretamente o alvo, os ataques cibernéticos podem ter uma série de custos e consequências secundários. Por exemplo, o relatório Cost of a Data Breach descobriu que as empresas gastam, em média, US$ 2,62 milhões em detecção, resposta e correção de violações.

Segurança da Informação

Tipos de Ataque

Quais efeitos os ataques cibernéticos têm sobre as empresas?

Os ataques cibernéticos também podem ter repercussões para vítimas além do alvo imediato. Em 2021, a gangue de ransomware da DarkSide atacou o pipeline colonial, o maior sistema de pipeline de petróleo refinado nos EUA. Os invasores entraram na rede da empresa usando uma senha comprometida (o link reside fora de ibm.com). Eles fecharam o gasoduto que transporta 45% do gás, diesel e combustível de aviação fornecidos para a costa leste dos EUA, levando à escassez generalizada de combustível.

Os criminosos cibernéticos exigiram um resgate de quase USD 5 milhões em criptomoedas bitcoin, que a Colonial Pipeline pagou (link reside fora de ibm.com). No entanto, com a ajuda do governo dos EUA, a empresa eventualmente recuperou USD 2,3 milhões do resgate.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Os cibercriminosos usam muitas ferramentas e técnicas sofisticadas para lançar ataques cibernéticos contra sistemas de TI corporativos, computadores pessoais e outros alvos. Alguns dos tipos mais comuns de ataques cibernéticos incluem:

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Malware

Malware é um software malicioso que pode tornar os sistemas infectados inoperáveis. O malware pode destruir dados, roubar informações ou até mesmo apagar arquivos essenciais para a execução do sistema operacional. O malware vem em muitas formas, incluindo:

- Os **Cavalos de Tróia** disfarçam-se como programas úteis ou escondem-se dentro de software legítimo para enganar os utilizadores a instalá-los. Um Trojan de acesso remoto (RAT) cria um backdoor secreto no dispositivo da vítima, enquanto um Trojan dropper instala malware adicional assim que consegue uma posição segura.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Malware

- O **Ransonware** é um malware sofisticado que usa criptografia forte para manter o host de dados ou sistemas. Os criminosos cibernéticos exigem o pagamento em troca da liberação do sistema e da restauração da funcionalidade. De acordo com o X-Force Threat Intelligence Index da IBM, o ransomware é o segundo tipo mais comum de ataque cibernético, representando 17% dos ataques.

- O **scareware** usa mensagens falsas para assustar as vítimas e fazê-las baixar malware ou passar informações confidenciais para um fraudador.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Malware

- **Spyware** é um tipo de malware que coleta informações confidenciais secretamente, como nomes de usuário, senhas e números de cartão de crédito. Em seguida, ele envia essas informações de volta ao hacker.

- **Rootkits** são pacotes de malware que permitem aos hackers obter acesso no nível do administrador ao sistema operacional de um computador ou a outros ativos.

- Os **worms** são códigos maliciosos auto-replicantes que podem se espalhar automaticamente entre aplicativos e dispositivos.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Engenharia social

Os ataques de engenharia social manipulam as pessoas para fazerem coisas que não deveriam fazer, como compartilhar informações que não deveriam compartilhar, baixar software que não deveriam baixar ou enviar dinheiro para criminosos.

Phishing é um dos ataques de engenharia social mais difundidos. De acordo com o Cost of a Data Breach É a segunda causa mais comum de violações. Os golpes de phishing mais básicos usam e-mails falsos ou mensagens de texto para roubar as credenciais dos usuários, exfiltrar dados confidenciais ou espalhar malware. As mensagens de phishing geralmente são projetadas para parecer que vêm de uma fonte legítima. Eles geralmente direcionam a vítima para clicar em um hiperlink que a leva a um site malicioso ou abrir um anexo de e-mail que acaba sendo malware.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Engenharia social

Os criminosos cibernéticos também desenvolveram métodos mais sofisticados de phishing. O **spear phishing** é um ataque altamente direcionado que visa manipular um indivíduo específico, muitas vezes usando detalhes dos perfis públicos da vítima nas redes sociais para tornar o estratagema mais convincente. O **whale phishing** é um tipo de spear phishing que tem como alvo específico os executivos corporativos de alto nível. Em um golpe de **comprometimento de e-mail empresarial (BEC),** os criminosos cibernéticos representam executivos, fornecedores ou outros associados de negócios para enganar vítimas na transferência de dinheiro ou no compartilhamento de dados confidenciais.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques de negação de serviço

Ataques de negação de serviço (DoS) e negação de serviço distribuída (DDoS) inundam os recursos de um sistema com tráfego fraudulento. Esse tráfego sobrecarrega o sistema, impedindo respostas a solicitações legítimas e reduzindo a capacidade de execução do sistema. Um ataque de negação de serviço pode ser um fim em si mesmo ou uma configuração para outro ataque.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques de negação de serviço

A diferença entre ataques DoS e ataques DDoS é simplesmente que os ataques DoS usam uma única fonte para gerar tráfego fraudulento, enquanto os ataques DDoS usam várias fontes. Os ataques DDoS geralmente são realizados com uma botnet, uma rede de dispositivos conectados à internet e infectados por malware sob o controle de um hacker. Os botnets podem incluir laptops, smartphones e dispositivos de Internet of Things (IoT). As vítimas geralmente não sabem quando um botnet invadiu seus dispositivos.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Comprometimento da conta

Comprometimento da conta é qualquer ataque em que hackers invadem a conta de um usuário legítimo para realizar atividades maliciosas. Os cibercriminosos podem invadir a conta de um usuário de várias maneiras. Eles podem roubar credenciais por meio de ataques de phishing ou comprar bancos de dados de senhas roubadas na dark web. Eles podem usar ferramentas de ataque de senha como Hashcat e John the Ripper para quebrar criptografias de senha ou realizar ataques de força bruta, nos quais executam scripts automatizados ou bots para gerar e testar senhas em potencial até que uma funcione.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques man-in-the-middle

Em um ataque man-in-the-middle (MiTM) , também chamado de “ataque de espionagem”, um hacker intercepta secretamente as comunicações entre duas pessoas ou entre um usuário e um servidor. Os ataques MitM são comumente realizados por meio de redes Wi-Fi públicas inseguras, onde é relativamente fácil para os agentes de ameaças espionar o tráfego.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques man-in-the-middle

Os hackers podem ler os e-mails de um usuário ou até mesmo alterar secretamente os e-mails antes de chegarem ao destinatário. Em um ataque de invasão de sessão, o hacker interrompe a conexão entre um usuário e um servidor hospedando ativos importantes, como um banco de dados confidencial da empresa. O hacker troca seu endereço IP com o do usuário, fazendo com que o servidor pense que é um usuário legítimo conectado a uma sessão legítima. Isso dá ao hacker liberdade para roubar dados ou causar estragos.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques à cadeia de suprimentos

Ataques à cadeia de abastecimento são ataques cibernéticos nos quais hackers violam uma empresa visando seus fornecedores de software, fornecedores de materiais e outros prestadores de serviços. Como os fornecedores geralmente estão conectados de alguma forma às redes de seus clientes, os hackers podem usar a rede do fornecedor como um vetor de ataque para acessar vários alvos ao mesmo tempo.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Ataques à cadeia de suprimentos

Por exemplo, em 2020, atores estatais russos hackearam o fornecedor de software SolarWinds e distribuíram malware para seus clientes sob o pretexto de uma atualização de software. O malware permitiu que espiões russos acessassem dados confidenciais de várias agências do governo dos EUA usando os serviços da SolarWinds, incluindo o Tesouro, a Justiça e os Departamentos de Estado.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Scripting entre sites (XSS)** - Os ataques de scripts entre sites (XSS) inserem códigos maliciosos em uma página da Web ou aplicativo da Web legítimo. Quando um usuário visita o site ou aplicativo, o código é executado automaticamente no navegador do usuário, geralmente roubando informações confidenciais ou redirecionando o usuário para um site malicioso e falsificado. Os invasores frequentemente usam JavaScript para ataques XSS.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Injeção de SQL** - Os ataques de injeção SQL usam a linguagem de consulta estruturada (SQL) para enviar comandos maliciosos para o banco de dados back-end de um site ou aplicativo. Os hackers inserem os comandos através de campos voltados para o usuário, como barras de pesquisa e janelas de login. Os comandos são então passados para o banco de dados, solicitando que ele retorne dados privados, como números de cartão de crédito ou detalhes do cliente.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Tunelamento DNS** - O tunelamento de DNS oculta o tráfego mal-intencionado dentro dos pacotes de DNS, permitindo que ele contorne firewalls e outras medidas de segurança. Os criminosos cibernéticos usam o tunelamento de DNS para criar canais de comunicação secretos, que podem usar para extrair dados silenciosamente ou estabelecer conexões entre malware e um servidor de comando e controle (C&C).

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Explorações de dia zero -** As explorações de dia zero aproveitam as vulnerabilidades de dia zero, que são vulnerabilidades desconhecidas pela comunidade de segurança ou identificadas, mas ainda não corrigidas. Essas vulnerabilidades podem existir por dias, meses ou anos antes que os desenvolvedores aprendam sobre as falhas, tornando-as os principais alvos dos hackers.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Ataques sem arquivo -** Ataques sem arquivos usam vulnerabilidades em programas de software legítimos para injetar códigos maliciosos diretamente na memória de um computador. Os criminosos cibernéticos geralmente usam o PowerShell, uma ferramenta de script incorporada aos sistemas operacionais Microsoft Windows, para executar scripts maliciosos que alteram configurações ou roubam senhas.

Segurança da Informação

Tipos de Ataque

Quais são os tipos comuns de ataques cibernéticos?

Outros tipos de ataques cibernéticos

- **Falsificação de DNS -** Os ataques de falsificação de DNS, também chamados de “envenenamento de DNS”, editam secretamente os registros DNS para substituir o endereço IP real de um site por um falso. Quando as vítimas tentam visitar o site real, elas recebem, sem saber, uma cópia maliciosa que rouba seus dados ou espalha malware.

Segurança da Informação

Tipos de Ataque

Prevenção de ataques cibernéticos

Muitas organizações implementam uma estratégia de gerenciamento de ameaças para identificar e proteger seus ativos e recursos mais importantes. O gerenciamento de ameaças pode incluir políticas e soluções de segurança como:

- **Plataformas e políticas de gerenciamento de identidade e acesso (IAM)**, incluindo acesso sem privilégios, autenticação multifatorial e políticas de senha fortes, podem ajudar a garantir que apenas as pessoas certas tenham acesso aos recursos certos. As empresas também podem exigir que os funcionários remotos usem redes privadas virtuais (VPNs) ao acessar recursos confidenciais por meio de Wi-Fi não seguro.

Segurança da Informação

Tipos de Ataque

Prevenção de ataques cibernéticos

- **Uma plataforma abrangente de segurança de dados e ferramentas de prevenção contra perda de dados (DLP)** podem criptografar dados confidenciais, monitorar seu acesso e uso e aumentar os alertas quando atividades suspeitas são detectadas. As organizações também podem fazer backups de dados regulares para minimizar os danos no caso de uma violação.

- **Firewalls** podem ajudar a impedir que agentes de ameaças entrem na rede em primeiro lugar. Os firewalls também podem bloquear o tráfego mal-intencionado que flui para fora da rede, como um malware que tenta se comunicar com um servidor de comando e controle.

Segurança da Informação

Tipos de Ataque

Prevenção de ataques cibernéticos

- O **treinamento de conscientização sobre segurança** pode ajudar os usuários a identificar e evitar alguns dos vetores mais comuns de ataques cibernéticos, como phishing e outros ataques de engenharia social.

- As **políticas de gerenciamento de vulnerabilidades,** incluindo agendamentos de gerenciamento de patches e testes de penetração regulares, podem ajudar a detectar e fechar vulnerabilidades antes que hackers possam explorá-las.

Segurança da Informação

Tipos de Ataque

Prevenção de ataques cibernéticos

- **As ferramentas de gerenciamento de superfície de ataque (ASM)** podem identificar, catalogar e remediar ativos potencialmente vulneráveis antes que os cyberattackers os encontrem.

- As ferramentas de **Gerenciamento unificado de endpoints (UEM)** podem aplicar políticas e controles de segurança a todos os endpoints na rede corporativa, incluindo laptops, desktops e dispositivos móveis.

Segurança da Informação

Tipos de Ataque

Detectando ataques cibernéticos

É impossível evitar totalmente as tentativas de ataques cibernéticos, portanto, as organizações também podem usar o monitoramento contínuo de segurança e os processos de detecção precoce para identificar e sinalizar ataques cibernéticos em andamento. Estes são alguns exemplos:

- Os **sistemas de gerenciamento de eventos e informações de segurança** (SIEM) centralizam e monitoram alertas de várias ferramentas internas de cibersegurança, incluindo sistemas de detecção de intrusão (IDSs), sistemas de detecção e resposta de endpoints (EDRs) e outras soluções de segurança.

Segurança da Informação

Tipos de Ataque

Detectando ataques cibernéticos

- As **plataformas de inteligência** contra ameaças enriquecem os alertas de segurança para ajudar as equipes de segurança a entender os tipos de ameaças à segurança cibernética que podem enfrentar.
- O **software antivírus** pode verificar regularmente os sistemas de computador em busca de programas maliciosos e erradicar automaticamente o malware identificado.
- **Processos proativos de caça a ameaças** podem rastrear ameaças cibernéticas secretamente na rede, como ameaças persistentes avançadas (APTs).

Segurança da Informação

Tipos de Ataque

Responder a ataques cibernéticos

As organizações também podem tomar medidas para garantir uma resposta adequada a ataques cibernéticos contínuos e outros eventos de segurança cibernética. Estes são alguns exemplos:

- Os **planos de resposta a incidentes** podem ajudar a conter e erradicar vários tipos de ataques cibernéticos, restaurar os sistemas afetados e analisar as causas principais para evitar ataques futuros. Os planos de resposta a incidentes demonstram reduzir os custos gerais de ataques cibernéticos. De acordo com o relatório Cost of a Data Breach, organizações com equipes formais de resposta a incidentes e planos têm, em média, 58% menos custos de violação.

Segurança da Informação

Tipos de Ataque

Responder a ataques cibernéticos

- As **soluções de orquestração, automação e resposta de segurança (SOAR)** podem permitir que as equipes de segurança coordenem ferramentas de segurança diferentes em um semi ou totalmente automatizado playbook para responder a ataques cibernéticos em tempo real.

- As **soluções estendidas de detecção e resposta (XDR)** integram ferramentas e operações de segurança em todas as camadas de segurança: usuários, endpoints, e-mail, aplicativos, redes, cargas de trabalho na nuvem e dados. Os XDRs podem ajudar a automatizar processos complexos de prevenção, detecção, investigação e resposta de ataques cibernéticos, incluindo caça proativa a ameaças.

Referências

- **IBM**

  https://www.ibm.com/br-pt/topics/cyber-attack