Cinco aplicações dos conteúdos de base que será estudado

Felipe Cadena de Souza	**RA: 825114852**
Hugo Felipe Diniz	**RA: 82515555**
Gustavo Ferreira Cavalcante	**RA: 82512399**
Guilherme Garcia Lenke	**RA: 824222500**

Firewall

Um firewall é um sistema de segurança de rede que monitora e controla o tráfego de dados entre redes, como a internet e uma rede interna, com o objetivo de impedir acessos não autorizados e proteger contra ameaças externas.

Para que serve um firewall?

O firewall atua como uma barreira de proteção, permitindo apenas o tráfego autorizado e bloqueando tentativas de acesso mal-intencionadas. Ele é essencial para:

- Proteger dados sensíveis contra roubo e acesso não autorizado.
- Impedir a entrada de malware e outras ameaças.
- Garantir a integridade e a confidencialidade das informações transmitidas pela rede.

Como funciona um firewall?

O funcionamento de um firewall envolve a inspeção do tráfego de rede com base em um conjunto de regras predefinidas. Ele pode operar de diferentes maneiras:

- Filtragem de pacotes: Analisa pacotes individuais de dados e decide se devem ser permitidos ou bloqueados com base em critérios como endereços IP, portas e protocolos.

-Inspeção de estado: Verifica o estado das conexões e permite apenas pacotes que correspondam a conexões estabelecidas ou autorizadas.

- Inspeção profunda de pacotes (DPI): Examina o conteúdo dos pacotes para identificar e bloquear ameaças que possam estar ocultas, oferecendo uma camada adicional de segurança.

Além disso, firewalls mais avançados podem incluir recursos como:

- Filtragem de conteúdo: Identifica e bloqueia conteúdos indesejados ou prejudiciais, como sites maliciosos ou materiais inapropriados.

- Detecção e prevenção de intrusões: Monitora atividades suspeitas e tenta identificar e bloquear ataques em tempo real.

Em resumo, um firewall é uma componente fundamental na infraestrutura de segurança de redes, garantindo que apenas tráfego autorizado possa acessar sistemas e dados sensíveis, protegendo contra uma variedade de ameaças cibernéticas.

Pirataria de Software

Podemos dizer que a pirataria de software é uma cópia, seja sob uma venda não autorizada de programas protegidos por direitos autorais ou até mesmo distribuído de forma gratuita em sites e até mesmo usar cracks para remover restrições de licença ou distribuir cópias sem permissão que podem colocar riscos nos seus dados pessoais e até no seu próprio negócio e caracterizando um crime digital.

Muita gente acredita que ao piratear um programa não causa danos, mas na realidade a pirataria de software traz diversas consequências negativas. Empresas de tecnologia sofrem prejuízos financeiros, o que pode reduzir investimento em inovação e segurança. Além disso, usuários que utilizam programas piratas correm riscos de segurança, como infecções por vírus, malwares e roubo de dados pessoais.

Outro ponto importante é a falta de suporte técnico e atualizações, tornando o software mais vulnerável a falhas e ataques cibernéticos. Além disso a pirataria é considerado crime em muitos países, podendo resultar em multas e penalidades legais para quem a pratica.

Principais tipo de pirataria de software

- **Cópia não autorizada:** Instalar um software em mais dispositivos do que a licença permite.
- **Cracks e keygens:** Uso de programas para desbloquear software pago ilegalmente.
- **Venda de software pirata**: Comercialização de programas falsificados ou modificados.
- **Downloads ilegais**: Baixar programas de sites não oficiais.

Riscos da pirataria:

- **Malwares e vírus**: Softwares piratas podem conter códigos maliciosos que se replica e infecta outros arquivos ou sistemas.
- **Falta de suporte e atualizações**: Programas ilegais não recebem melhorias de segurança.
- **Consequências legais**: Uso de software pirata pode resultar em multas e processos judiciais.

Riscos de pirataria de Software

Riscos de Segurança

- **Malwares e vírus**: Softwares piratas frequentemente contêm vírus, trojans e ransomwares que podem roubar dados ou danificar o sistema.
- **Roubo de dados pessoais**: Hackers podem usar programas piratas para capturar senhas, informações bancárias e arquivos sensíveis.
- **Falta de atualizações e suporte**: Softwares ilegais não recebem correções de segurança, deixando o sistema vulnerável a ataques.

Riscos Legais

- **Crime de violação de direitos autorais**: No Brasil, a pirataria de software é crime (Lei nº 9.610/98 e Código Penal, Art. 184).
- **Multas e penalidades**: Empresas e indivíduos podem ser processados e obrigados a pagar indenizações.
- **Risco de bloqueio do software**: Muitas empresas desenvolvedoras podem detectar o uso ilegal e bloquear o programa remotamente.

Riscos para Empresas

- **Danos à reputação**: Empresas que usam softwares piratas podem perder credibilidade e confiança no mercado.
- **Multas e processos judiciais**: Empresas flagradas com software ilegal podem pagar altas multas.
- **Baixa produtividade**: Softwares piratas são instáveis, podem travar e não oferecem suporte técnico adequado.

Riscos Financeiros

- **Perda de dinheiro**: Ataques cibernéticos causados por software pirata podem resultar em prejuízos financeiros.
- **Extorsão digital (ransomware)**: Se um malware sequestrar arquivos importantes, a vítima pode ser forçada a pagar um resgate para recuperá-los.

Alternativas ao uso de Software Pirata

Uma opção é utilizar **softwares gratuitos e de código aberto**, como LibreOffice (para edição de documentos), GIMP (para edição de imagens) e Linux (como sistema operacional). Uma alternativa são os **softwares freemium ou educacionais**, que oferecem versões gratuitas ou com descontos para estudantes e professores, como Microsoft Office 365 Education e Autodesk.

Além disso, muitas empresas disponibilizam **assinaturas acessíveis** que permitem pagar um valor mensal ou anual, tornando o software mais acessível. Também é possível aproveitar **períodos de teste gratuitos**, que permitem usar um programa por tempo limitado sem custo.

Por fim, empresas e profissionais podem buscar **licenças com descontos**, especialmente para pequenos negócios, ONGs e startups. Dessa forma, é possível utilizar programas de forma segura e legal, sem recorrer à pirataria e seus riscos.

Fonte: https://www.hostmidia.com.br/blog/pirataria-de-software/

https://www.jusbrasil.com.br/artigos/pirataria-virtual-download-e-comercializacao-e-sua-penalizacao/564850613

Autentificação de usuário

Autenticação é o processo que as empresas usam para confirmar que apenas as pessoas, serviços e aplicativos certos com as permissões certas podem obter recursos organizacionais. É uma parte importante da segurança cibernética, pois a prioridade número um de um invasor é obter acesso não autorizado aos sistemas. Eles fazem isso roubando o nome de usuário e as senhas dos usuários que têm acesso.

O processo de autenticação inclui três etapas principais:

- Identificação: normalmente, os usuários estabelecem quem são por meio de um nome de usuário.
- Autenticação: normalmente, os usuários provam que são quem dizem ser digitando uma senha (algo que apenas o usuário deve saber), mas para fortalecer a segurança, muitas organizações também exigem que provem sua identidade com algo que possuem (um telefone ou dispositivo de token) ou algum identificador físico (impressão digital ou leitura facial).
- Autorização: o sistema verifica se os usuários têm permissão para o sistema que estão tentando acessar.

Como funciona a autenticação

Para usuários, a autenticação envolve a criação de um nome de usuário, senha e outros métodos de verificação, como biometria ou um código PIN. Para garantir a segurança, as senhas não são armazenadas diretamente nos bancos de dados. Em vez disso, elas passam por um processo de hashing, onde são convertidas em um código irreversível antes de serem salvas. Quando um usuário digita sua senha, o sistema gera um novo hash e o compara com o armazenado. Se ambos coincidirem, o acesso é concedido.

No caso da autenticação biométrica, como leitura facial e impressão digital, os dados são criptografados e armazenados no próprio dispositivo, garantindo maior segurança.

Tipos de métodos de autenticação

Na autenticação moderna, o processo de autenticação é delegado a um sistema de identidade separado e confiável, em oposição à autenticação tradicional, em que cada sistema verifica sua própria identificação. Também houve uma mudança no tipo de métodos de autenticação usados. A maioria dos aplicativos requer um nome de usuário e senha, mas como os agentes mal-intencionados ficaram mais hábeis em roubar senhas, a comunidade de segurança desenvolveu vários novos métodos para ajudar a proteger as identidades.

Autenticação baseada em senha

A autenticação baseada em senha é a forma mais comum de autenticação. Muitos aplicativos e serviços exigem que as pessoas criem senhas que usam uma combinação de números, letras e símbolos para reduzir o risco de que um agente mal-intencionado as adivinhe. No entanto, as senhas também criam desafios de segurança e usabilidade. É difícil para as pessoas inventar e memorizar uma senha única para cada uma de suas contas online, e é por isso que muitas vezes elas reutilizam as senhas. E os invasores usam muitas táticas para adivinhar ou roubar senhas ou induzir as pessoas a compartilhá-las involuntariamente. Por esse motivo, as organizações estão substituindo as senhas por outras formas mais seguras de autenticação.

Autenticação baseada em certificado

A autenticação baseada em certificado é um método criptografado que permite que dispositivos e pessoas se identifiquem para outros dispositivos e sistemas. Dois exemplos comuns são um cartão inteligente ou quando o dispositivo de um funcionário envia um certificado digital para uma rede ou servidor.

Autenticação biométrica

Na autenticação biométrica, as pessoas verificam sua identidade usando recursos biológicos. Por exemplo, muitas pessoas usam o dedo ou o polegar para entrar em seus telefones, e alguns computadores escaneiam o rosto ou a retina de uma pessoa para verificar sua identidade. Os dados biométricos também estão vinculados a um dispositivo específico, portanto, os invasores não podem usá-los sem também obter acesso ao dispositivo. Esse tipo de autenticação é

cada vez mais popular porque é fácil para as pessoas, elas não precisam memorizar nada, e é difícil para agentes mal-intencionados roubarem, tornando-o mais seguro do que senhas.

Autenticação baseada em token

Na autenticação baseada em token, um dispositivo e o sistema geram um novo número exclusivo chamado TOTP (PIN avulso por tempo limitado) a cada 30 segundos. Se os números coincidem, o sistema verifica que o usuário está com o dispositivo.

Senha avulsa

As OTP (senhas avulsas) são códigos gerados para um evento de credenciais específicas que expiram logo após serem emitidos. Elas são entregues por meio de mensagens SMS, email ou token de hardware.

Notificação por push

Alguns aplicativos e serviços usam notificações por push para autenticar usuários. Nesses casos, as pessoas recebem uma mensagem em seus telefones solicitando que aprovem ou neguem a solicitação de acesso. Como às vezes as pessoas aprovam notificações por push acidentalmente, mesmo que estejam tentando entrar nos serviços que enviaram a notificação, esse método às vezes é combinado com um método OTP. Com o OTP, o sistema gera um número único que o usuário deve inserir. Isso torna a autenticação mais resistente a phishing.

Autenticação por voz

Na autenticação por voz, a pessoa que tenta acessar um serviço recebe uma chamada telefônica, na qual é solicitada a inserir um código ou a identificar-se verbalmente.

Autenticação multifator

Uma das melhores maneiras de reduzir o comprometimento da conta é exigir dois ou mais métodos de autenticação, que podem incluir qualquer um dos

métodos listados anteriormente. Uma melhor prática eficaz é exigir quaisquer dois dos seguintes itens:

- Algo que o usuário sabe, geralmente uma senha.
- Algo que o usuário possua, como um dispositivo confiável que não é facilmente duplicado, como um telefone ou um token de hardware.
- Algum fator físico do usuário, como uma impressão digital ou uma leitura facial.

Por exemplo, muitas organizações solicitam uma senha (algo que o usuário sabe) e também enviam um OTP via SMS para um dispositivo confiável (algo que o usuário possui) antes de permitir o acesso.

Autenticação de dois fatores

A autenticação de dois fatores é um tipo de autenticação multifator que requer duas formas de autenticação.

Autenticação versus autorização

Embora a autenticação, às vezes chamada de AuthN, e a autorização, às vezes chamada de AuthZ, sejam frequentemente usadas de forma intercambiável, elas são duas coisas relacionadas, mas separadas. A autenticação confirma que o usuário que está acessando a conta é quem diz ser, enquanto a autorização confirma que ele tem as permissões corretas para acessar as informações que deseja. Por exemplo, alguém do departamento de recursos humanos pode ter acesso a sistemas confidenciais, como folha de pagamento ou arquivos de funcionários, que outras pessoas não podem ver. Tanto a autenticação quanto a autorização são essenciais para permitir a produtividade e proteger dados confidenciais, propriedade intelectual e privacidade.

Os principais aplicativos usados para autenticação de usuários incluem:

- Geradores de códigos temporários (TOTP): Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile.
- Autenticação por notificação push: Microsoft Authenticator, Duo Mobile, Okta Verify, LastPass Authenticator.

- Gerenciadores de senhas: 1Password, LastPass, Dashlane, Bitwarden.
- Biometria: Apple Face ID, Touch ID, Android Biometrics, Windows Hello.
- Aplicativos bancários e de segurança: Google Smart Lock, Apple iCloud Keychain, apps de bancos (Itaú, Bradesco, Nubank, etc.).

Fonte

- https://blog.bgcbrasil.com.br/autenticacao-de-usuarios
- https://www.microsoft.com/pt-br/security/business/security-101/what-is-authentication

O que é backup?

Backup é o processo de fazer uma cópia dos dados ou das configurações do seu sistema para protegê-los. O backup é uma cópia de segurança que é armazenada separadamente da original, com o fim de evitar perdas ocasionadas por imprevistos, como erros humanos, falhas computacionais e de segurança, ou desastres naturais.

Os imprevistos podem impactar no tempo de inatividade não planejada de um negócio, o que pode resultar rapidamente em perda de receita em muitos setores. Qualquer tempo de inatividade pode inviabilizar interações com o cliente, prejudicar a produtividade de funcionários SAP, destruir dados e interromper processos de negócios.

O que é recuperação de desastres?

Recuperação de desastres refere-se ao plano e aos processos para restabelecer rapidamente o acesso a aplicativos, dados e recursos de TI após uma indisponibilidade ocasionada por um imprevisto.

Esse plano pode envolver migrar para um conjunto redundante de servidores e sistemas de armazenamento até que seu data center principal esteja funcional novamente.

Backup e recuperação de desastres

Backup e recuperação de desastres servem para criar uma cópia de segurança de dados e criar procedimentos para acessar esses dados em caso de imprevistos.

Em caso de que ocorra uma grande indisponibilidade, é essencial ter uma **cópia dos dados (backup)**. Porém, ter apenas o backup não significa que você pode manter sua empresa em funcionamento.

Para assegurar a continuidade dos negócios, também é necessário ter um **plano de recuperação de desastres** robusto e comprovado. Isso ajudará a acessar e utilizar os dados para reestabelecer o funcionamento dos sistemas da empresa.

Jeito mais utilizado para recuperação

- ## Cloud

  As soluções de backup e recuperação de desastres baseadas na cloud estão se tornando cada vez mais conhecidas entre organizações de todos os portes. Muitas soluções na cloud oferecem a infraestrutura para armazenar dados e, em certos casos, as ferramentas para gerenciar processos de backup e recuperação de desastres.

  Ao selecionar uma solução de backup ou recuperação de desastres baseada na cloud, você estará economizando um investimento inicial de capital em infraestrutura, além dos custos de gerenciamento do ambiente. Além disso, você ganha escalabilidade rápida, juntamente com a distância geográfica necessária para manter os dados seguros no caso de um desastre regional.

  As soluções de backup e recuperação de desastres baseadas na cloud oferecem suporte a ambientes de produção tanto no local quanto baseados na cloud. Você pode, por exemplo, optar por armazenar na cloud apenas os

dados de backup ou replicados, enquanto mantém seu ambiente de produção em seu próprio data center. Com esta abordagem híbrida, você ainda terá as vantagens de escalabilidade e distância geográfica, sem ter que migrar seu ambiente de produção.

No modelo cloud-to-cloud, tanto a produção quanto a recuperação de desastres estão localizadas na cloud, porém em locais diferentes, para assegurar suficiente separação física.

Fonte: https://www.ibm.com/br-pt/topics/backup-disaster-recovery

Antivírus

Antivírus é um software projetado para detectar, prevenir e remover malware, como vírus, worms e spyware, de um sistema de computador. Ele funciona monitorando e analisando os arquivos em busca de comportamentos suspeitos ou sinais de malware conhecidos. O antivírus pode realizar varreduras manuais, automáticas e em tempo real, protegendo o sistema contra ameaças.

A eficácia de um antivírus depende de sua base de dados, que é constantemente atualizada para incluir novas ameaças. Além disso, ele pode oferecer funções adicionais, como proteção contra phishing, bloqueio de sites maliciosos, e monitoramento de e-mails.

Fonte: Kaspersky, 2021 [Kaspersky](https://www.kaspersky.com.br/)