AMEAÇAS COMUNS À SEGURANÇA DIGITAL

À medida que a sociedade se torna cada vez mais dependente da tecnologia digital, a segurança digital emerge como uma preocupação fundamental. Com o aumento da conectividade e a proliferação de dispositivos inteligentes, surgem também novas e sofisticadas ameaças que visam comprometer a segurança e privacidade dos usuários. Neste artigo, exploraremos algumas das ameaças mais comuns e impactantes à segurança digital atualmente. Desde ataques de phishing e malware até violações de dados em larga escala, examinaremos os desafios enfrentados pelos indivíduos e organizações na proteção de seus ativos digitais. Além disso, forneceremos insights e estratégias essenciais para mitigar essas ameaças e fortalecer as defesas contra ataques cibernéticos. Esteja preparado para mergulhar no complexo e dinâmico mundo da segurança digital.

- **Ataques de phishing**

Phishing é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito. Como em uma verdadeira pescaria, há mais de uma maneira fisgar uma vítima, mas uma tática de phishing é a mais comum. As vítimas recebem um e-mail ou uma mensagem de texto que imita (ou “engana”) uma pessoa ou organização em que confiam, como um colega de trabalho, um banco ou um órgão governamental. Quando a vítima abre o e-mail ou o texto, eles encontram uma mensagem assustadora que induz a deixar o bom senso de lado ao deixá-los com medo. A mensagem exige que a vítima acesse um website e execute uma ação imediata ou assuma um risco por algum tipo de consequência.

- **Malware**

Malicious software ou, em português, software malicioso. A combinação dessas duas palavras gerou o termo malware, o que já ajuda bastante a entender o seu significado. Trata-se do nome que utilizamos para nos referir a qualquer tipo de programa que pode gerar danos aos seus dados ou ao seu dispositivo.

O que torna o malware tão perigoso, além das óbvias implicações de um programa estranho acessar suas informações, é que ele pode afetar qualquer sistema conectado ao computador infectado.

- **Ataques de negação de serviço (DDoS)**

Os ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído (DDoS). Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa.
O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto.

- **Engenharia social**

Os ataques de engenharia social manipulam as pessoas para compartilhar informações que não deveriam compartilhar, baixar software que não deveriam baixar, visitar sites que não deveriam visitar, enviar dinheiro para criminosos ou cometer outros erros que comprometam sua segurança pessoal ou organizacional.

REFERÊNCIAS

Principais ameaças a segurança digital - GestãoPRO **-** Marcos -FlexiTyre / Flexi-Rodas.
Disponível em: https://gestaopro.com.br/blog/seguranca/principais-ameacas-a-seguranca-da-informacao-nas-empresas-e-como-se-proteger

Tudo sobre pushing – Malwarebytes
Disponível em: https://br.malwarebytes.com/phishing/

Malware/Segurança – Rockcontent
Disponível em: https://rockcontent.com/br/blog/malware/

DDOS attacks – kaaspersky
Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks

Engenharia social - IBM
Disponível em: https://www.ibm.com/br-pt/topics/social-engineering

PROTEÇÕES AMEAÇAS DIGITAIS

A segurança digital tornou-se uma preocupação primordial em um mundo cada vez mais interconectado e dependente da tecnologia. Com a proliferação de dispositivos conectados e a constante troca de informações online, proteger dados sensíveis e salvaguardar a privacidade tornou-se uma necessidade premente para indivíduos e organizações. Com base nisso listamos as três principais ferramentas de segurança digital para proteção de informações e segurança digital:

1. Uso do firewall

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

2. Softwares de monitoramentos

Um software de monitoramento digital é uma ferramenta projetada para rastrear e registrar atividades realizadas em dispositivos digitais, como computadores, smartphones e tablets. Esses softwares são frequentemente utilizados por pais, empregadores e indivíduos preocupados com a segurança online para acompanhar o uso desses dispositivos e garantir a conformidade com políticas de segurança e privacidade.

3. Backup inteligente

A digitalização dos processos empresariais trouxe consigo a necessidade de se armazenar um volume crescente de dados. Todos os dias, empresas produzem e processam informações que são essenciais para o seu funcionamento.

Esses dados, se perdidos, podem causar não só prejuízos financeiros, mas também impactar a reputação e a operação da organização. O backup inteligente surge como resposta a essa demanda. Mais do que uma simples cópia de segurança, ele representa uma abordagem proativa e estratégica na gestão de dados.

REFERÊNCIAS

Proteção ameaças digitais - BaseSafeBrasil
Disponível em: https://www.besafebrasil.com.br/6-ferramentas-de-seguranca-da-informacao-que-sua-empresa-precisa-ter/

Firawall – Cisco
Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html

Software de monitoramento – Digitaliza.ai
Disponível em: https://digitaliza.ai/seguranca-digital

Backup inteligente – Targetso
Disponível em: https://www.targetso.com/2023/08/09/backup-inteligente/