TUDO SOBRE CIBERSEGURANÇA, SEGURANÇA DA INFORMAÇÃO E PROTE DIGITAL.

SEGURANÇA CIBERNÉTICA

Tudo sobre Segurança Cibernética

by **Mirian Fernandes** há um ano 9 MIN READ

A segurança da informação tem como objetivo tratar e proteger os dados físicos e digitais. Ou seja, **a segurança cibernética ou *cibersegurança***, é uma área que atua no ambiente digital, na prevenção, mitigando e recuperação frente aos ataques cibernéticos.

Neste artigo você vai descobrir:

Tipos de Ataques cibernéticos

Os ataques cibernéticos são ações executadas por criminosos, que usam como vulnerabilidades da rede para atacar e roubar os dados. Dados que são permitidos, e quais são os principais roubados, que causam grandes danos as empresa.

Em 1971, foi criado o primeiro worm de computador, exibindo as palavras “Eu sou o Creeper: pegue-me se puder” a ameaça que abriu os caminhos para os vírus e ataques cibernéticos que passaram a estampar várias manchetes nos últimos anos.

O ano de 2020 ficou marcado por uma explosão de ataques cibernéticos. Um crescimento de 400% no número de ataques registrados, segundo os dados da **Next Generation.**

Já que uma das maneiras de prevenir e manter uma empresa segura é conhecendo as ameaças, vejamos alguns ataques cibernéticos.

Vírus

O **vírus** é um programa ou código de código usado para danificar o computador, corromper os arquivos do sistema e destruir dados. O vírus fica inativo na máquina até que seja executado, ou seja, é necessário executar o programa infectado para contaminar o computador.

A partir disso, ele pode contaminar **outros computadores da rede,** roubar senhas e dados, corromper arquivos, encaminhar spam para contatos de e-mail ou, até mesmo, controlar o computador.

Worms

Adware

Um programa comum de *adware* redireciona as pesquisas do navegador de um usuário para páginas da web com promoções de produtos, aparentemente inofensivas.

O objetivo desse tipo de ataque é obter informações úteis dos usuários como: a localização, detalhes de senhas de acesso (palavras-passe) e endereços IP do computador ou correio eletrônico.

Ransomware

Também conhecido como "*sequestrador digital* " o ransomware é um software que se infiltra em uma máquina, codifica os dados do sistema após a instalação e bloqueia o acesso dos usuários.

Uma vez executado, o atacante pede um resgate para a vítima, geralmente feito em **bitcoin**, que é uma criptomoeda.

O **ransomware** é um dos tipos de ataques que mais ocorre no Brasil, sendo o segundo colocado em número de ataques mundiais de ransomwares. Os dado são da pesquisa Smart Protection Network, da **Trend Micro.**

Cavalo de Troia

Spyware

É um **software de espionagem** praticamente invisível, que funciona em segundo plano, coletando dados ou fornecendo acesso remoto para o cracker.

Em um ataque hacker, o spyware é útil na coleta de informações financeiras, como senhas, contas bancárias e dados de cartão de crédito. Geralmente, esse espião esconde-se em softwares ou em downloads de sites de filmes e músicas.

Confira nossa aba de **vulnerabilidades** aqui no nosso blog, onde contamos mais detalhes sobre esses e outros ataques.

Segurança Cibernética e o valor da informação

Muitos acreditam que somente as grandes e megas empresas são visadas por crackers, que estão à procura de oportunidades para colocar as mãos em informações.

Mas a verdade é que o**s cibercriminosos estão buscando informações**! Independentemente se elas pertencem a grandes empresas ou pequenas, eles procuram oportunidades para roubá-las.

Caso essas informações caiam em mãos erradas, afetarão toda a funcionalidade dos negócios. Um exemplo simples: imagine que uma empresa sofra um ataque que possibilite a exposição dos números de cartões de crédito de seus clientes.

Uma falha como essa poderá gerar ações judiciais por parte dos prejudicados pelo vazamento.

Descubra o valor dos seus dados e como se proteger

Legislações de segurança e privacidade

abriu caminho para criminosos, que muitas vezes conseguem sair impunes. Vazamentos de conversas privadas até invasões de contas bancárias, a internet era vista até então como uma terra sem lei e isso precisava mudar.

Com o objetivo de trazer mais segurança para os usuários e garantir a punição para os cibercriminosos foi criado o **Marco Civil da Internet**.

Em agosto de 2011 foi apresentado a **PL 2126/11**, que viria a ficar conhecida como Marco Civil da Internet. Basicamente, o projeto de lei tem o objetivo de estipular diretrizes dos direitos, deveres, princípios e garantia para o uso da internet em território nacional.

Diferentemente do que muitos podem pensar, o Marco Civil da Internet não impacta apenas empresas de telecomunicações, negócios digitais, entretenimento, startups de tecnologia, educação digital, etc. Talvez o impacto nesses segmentos seja maior, mas todas as empresas precisaram se adaptar.

caso da Cambridge Analytica.

Diversos episódios de vazamento de dados ou mesmo o uso indevido de informações se tornaram públicos nos últimos anos. Tais escândalos trouxeram tanto impacto que impulsionaram a aprovação da **Lei Geral de Proteção de Dados**, (LGPD) como é mais conhecida aqui no Brasil.

A principal influência para a criação e maturação da LGPD, foi o GDPR (General Data Protection Regulation), que entrou em vigor no dia 25 de maio de 2018, regulamentando questões de privacidade para os países europeus.

A LGPD tem como intenção garantir ao usuário mais privacidade e controle sobre seus dados, com o fim de evitar mal-uso por parte de terceiros.

Ela também serve para esclarecer quando uma empresa pode tratar um dado pessoal, ou seja, armazenar, processar e transferir esses dados.

A aprovação da **LGPD** foi impulsionada por esse escândalo, já que a Cambridge Analytica planejava atuar nas eleições brasileiras de 2018, além de expor a necessidade de uma lei que regulasse o tratamento de dados pessoais.

tornem uma pessoa identificável. Necessidade de uma base para tratar os dados: para que a organização seja capaz de tratar os dados dos usuários corretamente, será necessária uma base legal, com o consentimento de todas as pessoas.

- **Autoridade regulatória:** para que todas as empresas se adéquem à nova norma, uma nova autoridade será criada para fiscalizar a nova lei, a ANPD.
- **Impacto financeiro nos negócios:** a lei terá grandes impactos nos negócios das empresas, já que elas precisaram se reformular para garantir que suas responsabilidades sejam cumpridas. Caso alguma exigência seja ignorada, os prejuízos podem ser altos.

Mediante a tamanhos impactos e abrangência da LGPD e Marco Civil, fica claro que essas questões são cruciais e não poderão ser ignoradas por sua empresa, seja qual for seu setor ou tamanho.

Por isso que a prevenção é o melhor caminho. Contudo, muitas empresas só enxergam os riscos e sua dimensão depois que já foram lesadas.

Descubra agora a algumas dicas para você garantir a Segurança Cibernética da sua empresa.

Segurança Cibernética para empresas

Crie uma política de Segurança Elabore um documento detalhado com os aspectos mais importantes para a rotina da empresa. Uma dica é utilizar a ISSO/IEC 17799:2005 como norma de base sobre o conceito de segurança da informação.

1. Firewall

O objetivo do firewall é de proteger sua rede dos ataques externos. Ele fica na borda, na ponta da rede, impedindo que todos os IPs que não são autorizados não entrem.

2. IDS/IPS

Esses dois complementam o trabalho do firewall. O **IDS** identifica todo e qualquer tipo de atividade estranha, incomum na rede. Por exemplo: um download excessivo de arquivos, após fazer isso ele manda essa informação de alerta para **IPS** que vai tomar as ações de bloqueio dos Ips que está fazendo esse tipo de download excessivo.

3. Webfilter

Nem todos ataques são externos, na verdade, existem muitos ataques que vem de dentro da sua rede. A função do webfilter é proteger quem está dentro da sua rede: os computadores, usuários com acesso liberado para mexer dentro da sua rede. Eles podem trazer vulnerabilidades para os ataques.

O **webfilter** faz o gerenciamento do que pode ou não pode ser acessado pelas suas máquinas, ou usuários que são parte da sua rede. Com essa ferramenta você pode aplicar a

notebook em casa, acessando dados e fazendo transações na empresa.

Para que esse acesso seja seguro faz-se necessário a criação da **VPN**, que é basicamente um túnel seguro entre o usuário de fora autorizado a acessar o que tem na rede.

É importante a utilização dessa ferramenta para o monitoramento dos visitantes da rede, pessoas que irão participar de uma reunião ou alguma conferência e para usuários que acessam a rede wifi, se for o caso da empresa ter o mesmo liberado para acesso.

5. Antivírus

Alguns ataques são tipos de softwares que se instalam nas máquinas dos usuários da rede, para coletar dados. O **antivírus** é um software bem mais poderoso que esses ataques, que inibe que eles aconteçam. A função do antivírus é proteger a sua máquina, o usuário específico.

6. Backup

É uma cópia de todos os dados da empresa que permitirá a sobrevivência da mesma, caso um ataque aconteça. E deve ser feito regularmente.

Tenha um bom plano de ação

o cenário torna-se complicado. O ideal é contar com **ajuda especializada** e que ofereça suporte para o seu negócio.

Nós da Starti desenvolvemos o **Starti Security**, uma solução desenvolvida para PMEs, capaz de mitigar vulnerabilidades e impedir acessos indevidos à rede, proteger, otimizar e controlar a navegação dos usuários e elevar a produtividade e disponibilidade do negócio.

Uma ferramenta completa para seus clientes. Clique no banner abaixo e descubra como alcançar bons resultados ofertando essa solução de segurança.

Conclusão

A segurança cibernética é uma aliada indispensável para as empresas que pensam na continuidade dos seus negócios, por isso apresentamos todas essas informações para você.