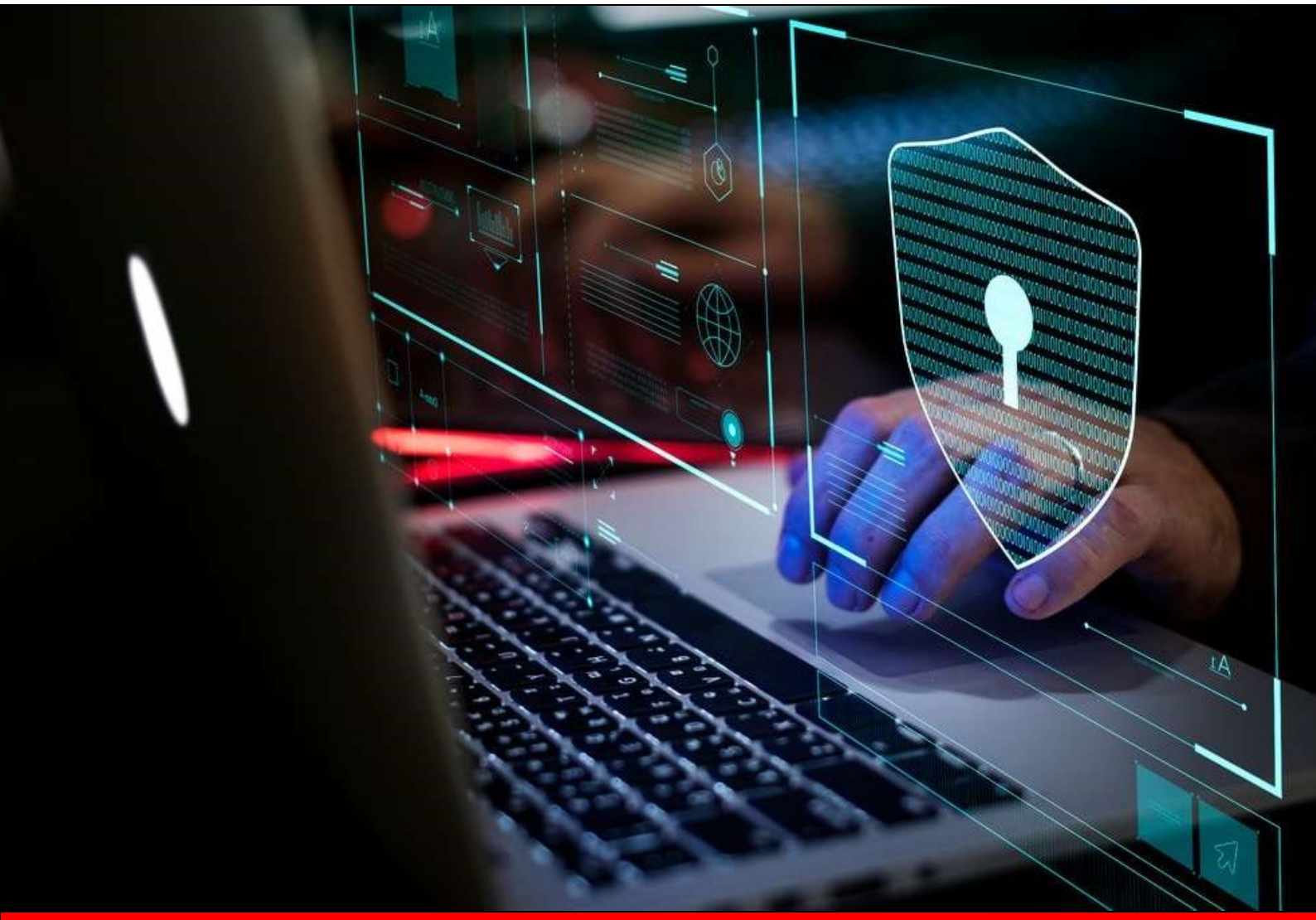
PRO-AUDIT



SEGURANÇA CIBERNÉTICA

Outubro/2020

PRO-AUDIT

❖ Introdução

No mundo atual, que é gerenciado por conexões de tecnologia e rede, é crucial saber o que é segurança cibernética e poder usá-la de maneira eficaz. Sistemas, arquivos importantes, dados e outras coisas virtuais importantes estão em risco se não houver segurança para protegê-los. E não estamos a falar apenas de uma empresa de TI, todas as empresas devem ser protegidas de igual forma. Com o aprimoramento da nova tecnologia em segurança cibernética, os atacantes também não ficam atrás. Eles estão usando técnicas de hacking cada vez melhores e têm como alvo os pontos fracos de muitas empresas por aí.

A cibersegurança é um processo de proteção de dados confidenciais, redes e aplicativos de software contra-ataques cibernéticos. Os ataques cibernéticos podem ser considerados uma exploração de recursos, acesso não autorizado aos sistemas, ataques de ransomware para criptografar dados e extrair dinheiro.

❖ Por que a segurança cibernética é importante?

Não apenas é crucial saber o que é cibersegurança, mas também entender por que é importante. O jogo foi levado a outro nível pelos hackers, para que as organizações e seus funcionários saibam o que está em risco se não for tratado.

Os dias em que bastava ter apenas uma senha forte já se foram, e nossos dados pessoais e profissionais estão expostos a muitos perigos. Por que é tão importante protegê-lo?

O custo das ameaças cibernéticas está no nível mais alto de todos os tempos e as violações dos sistemas de segurança podem ser descobertas por meses. Por exemplo, ameaças persistentes e avançadas são contínuas para tentar invadir os sistemas de computadores, obter acesso e permanecer dentro por meses, rastreando e monitorando as ações das organizações antes que elas sejam notadas.

Vamos analisar mais detalhadamente por que a segurança cibernética é tão importante:

- **O custo das violações de dados**. Como todos sabemos, muitos regulamentos foram criados para proteger os dados dos usuários. Isso é extremamente importante para as organizações que lidam com os dados dos usuários e precisam intensificá-las para protegê-los. De acordo com o GDPR da UE e outras leis de privacidade emergentes, as empresas podem ser multadas com surpreendentes e enormes quantias em dinheiro. Podendo atingir até 20 milhões de euros ou 4% do faturamento global anual, dependendo de qual for maior. No entanto, as empresas que expõem os dados de seus usuários devido à sua irresponsabilidade podem perder sua reputação e danificar sua imagem.
- **Ataques cibernéticos podem ser prejudiciais.** Aqueles que se expõem como aqueles que não sabem o que é cibersegurança e quais são seus custos podem se tornar vítimas de crimes financeiros. O ganho financeiro é uma motivação comum para a maioria dos hackers, mas não se engane, não é a única. Os cibercriminosos podem usar suas habilidades para obter uma vantagem política, ética, social ou intelectual.

A cibersegurança não é apenas essencial para organizações empresariais e instituições governamentais. Deveria ser para todos que estão usando dispositivos digitais, como computadores, telefones celulares, tablets etc. Esses dispositivos contêm muitas informações pessoais que os ladrões digitais gostariam de ter. O que também é importante é que, se suas informações forem expostas a hackers, eles poderão usar você como isca para atrair seus amigos ou familiares para uma fraude digital.

Tudo o que está conectado à Internet, usado para comunicação e outros fins, pode ser afetado por uma violação da segurança. Podendo ser:

- Sistemas financeiros, que consistem em contas bancárias, empréstimos, contracheques.
- Bancos de dados governamentais, que incluem números de previdência social, licenças e registros fiscais.
- Sistemas de comunicação, como emails, mensagens de texto, chamadas.
- Sistemas médicos com seus equipamentos e registros médicos.
- Sistemas educacionais, que podem afetar notas, boletins e informações pessoais dos estudantes.
- Sistemas de transporte, como controle de tráfego, navegação de aviões e motores de veículos.

Ter as medidas corretas de segurança cibernética é a principal defesa contra esse tipo de erros e ataques maliciosos; portanto, saber o que é segurança cibernética e por que é importante é crucial para todos.

❖ Qual é o conceito principal da segurança cibernética?

A segurança cibernética, por si só, tem um termo muito amplo e pode ter muitas definições que giram em torno do mundo digital. Para entender o termo segurança cibernética, vamos ver três conceitos fundamentais são conhecidos como "A tríade da CIA".

A tríade da CIA é um acrônimo de palavras como confidencialidade, integridade e disponibilidade (availability). Este modelo foi desenvolvido para orientar a organização com as políticas de segurança cibernética.

- *Confidencialidade* . É o processo que exclui o acesso à informação para certas pessoas. É uma medida para impedir que informações confidenciais caem em mãos erradas. Em uma organização, as pessoas têm acesso permitido ou negado às informações de acordo com sua ocupação e posição. Esse tipo de pessoa recebe treinamento e regras adequados sobre o compartilhamento de segredos confidenciais, protege suas contas com senhas adequadamente fortes. Alguns dos pontos principais da cibersegurança cibernética são a autenticação de dois fatores, classificação de dados, criptografia de dados, verificação biométrica etc.
- *Integridade* . O processo de integridade garante que os dados no sistema sejam consistentes, verificados, precisos e confiáveis. Isso significa que os dados não podem ser alterados, alterados, excluídos ou acessados sem permissão. É por isso que é importante acompanhar as permissões de arquivo e o acesso do usuário. Outra coisa importante para manter a integridade dos dados é ter um backup seguro. Os backups em nuvem são um dos mais confiáveis no momento.
- *Disponibilidade .* Em termos de componentes necessários, como hardware, redes, software, dispositivos e equipamentos, a disponibilidade significa que tudo deve ser atualizado e dado manutenção. A razão pela qual a disponibilidade é importante é que ela fornece um funcionamento e acesso fáceis aos dados sem interrupções. Utilitários como firewalls, servidores proxy, soluções de backup e planos de recuperação são pontos-chave contra ameaças cibernéticas

❖ Quais são as ameaças mais comuns à segurança cibernética?

Já conversamos sobre os resultados da falta de segurança cibernética. Pode causar problemas financeiros, médicos, governamentais ou até desastres. Mas o que exatamente os causa ?

Os cibercriminosos se tornam altamente sofisticados quando se trata de suas táticas, portanto, eles criam muitas ameaças ou "armadilhas" que podem atrair pessoas inocentes a ciberameaças.

1. **Vírus.** O mais popular que provavelmente todos já encontraram ao longo de suas vidas. Embora muitos se refiram a todas as ameaças à segurança cibernética como um vírus, isso não é totalmente verdade. O vírus é um pedaço de código malicioso carregado em um computador sem a permissão dos usuários. Ele pode se conectar a outros arquivos e se espalhar por toda a rede. Esse é um dos principais objetivos da cibersegurança - evitar esse tipo de ameaça.
2. **DDoS** (negação de serviço distribuída). Essa ameaça tenta interromper o tráfego normal da Web e colocar um site offline, inundando o sistema com mais solicitações do que ele pode suportar.
3. **Malware**. Este é um termo que significa um programa criado para danificar um computador. Ele abrange vírus, spyware, cavalos de Troia, engenharia social e worms.
4. **Worms**. Não, não é aquele jogo que todos nós gostávamos. É uma ameaça semelhante a um vírus. Ele pode se auto-replicar como um vírus, mas não precisa se conectar a um programa de computador. Eles procuram vulnerabilidades em um computador e as denunciam ao criador, que executa as ações adequadamente.
5. **Trojan.** Outra ameaça popular da qual provavelmente todos já ouviram falar. É um tipo de malware que se disfarça de software legítimo. Ele pode ter a forma de programas de remoção de vírus, mas realiza atividades maliciosas quando instalado e executado.
6. **Engenharia social**. É uma ameaça usada para enganar e manipular usuários para obter suas informações e obter acesso ao seu computador. Isso é obtido por meio de links maliciosos ou pelo acesso físico ao computador. Isso pode causar problemas enormes para muitas organizações se elas não souberem o que é segurança cibernética.
7. **Phishing**. É uma forma de ameaça de engenharia social, que tenta adquirir informações sensíveis ou confidenciais dos usuários.
8. **Spyware**. Ele monitora a atividade do computador e coleta informações pessoais. Spyware ou adware podem ser instalados em um dispositivo por meio de links, software ou anexos maliciosos.

9. Ransomware. Isso pode ser considerado como a ameaça cibernética que mais cresce. É um tipo de malware que exige pagamento após criptografar os arquivos dos usuários, tornando-os inacessíveis. Note-se que o pagamento do resgate não garante a recuperação dos dados criptografados, portanto, tenha cuidado.
10. MITM (o homem do meio). Essa ameaça ocorre quando o usuário se expõe à rede não segura. É chamado MITM porque o cibercriminoso se insere entre o usuário e o servidor. O usuário passará as informações para o hacker sem saber.
11. SQL Injection. Isso acontece quando o invasor insere código malicioso em um servidor que usa o Structured Query Language. As SQL Injections só são bem-sucedidas quando existe vulnerabilidade de segurança. Nesse caso, o ataque forçará o servidor a fornecer acesso ou modificar dados.

❖ Quais são os elementos de segurança cibernética?

Agora que analisamos o conceito do que é cibersegurança e por que é tão importante, é importante aprender sobre seus elementos. Uma rede de segurança cibernética forte consiste em muitos recursos:

- **Segurança de aplicativos**. Os aplicativos de sites são um ponto comum para os cibercriminosos e sua vulnerabilidade pode causar muitos problemas. As organizações que administram uma empresa nos sites devem garantir sua segurança para proteger seus clientes, suas informações financeiras e pessoais.
- **Segurança de rede**. É o processo de proteger servidores e resolver problemas de segurança em servidores, hosts, dispositivos e serviços de Internet. A segurança da rede é feita protegendo a usabilidade e a integridade dos dados na rede.
- **Segurança operacional**. Ele protege as principais funções da organização. A segurança operacional é importante para rastrear informações críticas e os ativos que interagem com ela para identificar vulnerabilidades.
- **Educação do usuário final.** A estratégia de segurança cibernética das empresas é tão forte quanto o elo mais fraco da equipe. É por isso que todos os funcionários precisam saber quais medidas são necessárias e como identificar as ameaças recebidas.
- **Envolvimento da gerência**. O último, mas não menos importante, elemento do que é cibersegurança, é o compromisso da gerência das organizações de estar preparado para investir em cibersegurança. Os supervisores precisam entender que é importante contratar pessoas qualificadas, adquirir recursos e tecnologia apropriados de segurança cibernética.

❖ CONCLUSÃO...

Um dos elementos mais problemáticos da segurança cibernética é a natureza em constante evolução dos riscos de segurança. A abordagem tradicional tem sido concentrar os recursos em componentes cruciais do sistema e proteger contra as maiores ameaças conhecidas, o que significa por vezes não proteger os sistemas contra riscos menos críticos.

Gostaria de saber mais?

ESPERAMOS TER AJUDADO!

E NOS COLOCAMOS AO SEU DISPOR

Pro-Audit Consultoria e Serviços
Leandro Áureo Azambuja
Gerente de Projetos e P&D&I
Microsoft Certified Professional
Compliance Specialist
leandro@pro-audit.eti.br