SEGURANÇA DA INFORMAÇÃO

eBook 4

O ponto mais importante no âmbito da Segurança da Informação são os crimes cibernéticos, que impactam tanto no nosso dia-a-dia pessoal quanto no das empresas.

E os temas que tratam da prevenção do avanço desse problema é a atenção que damos para as vulnerabilidades, a frequência e prática do monitoramento das ameaças e o quanto aprendemos e melhoramos a partir de auditorias e testes de segurança.

Gestão de vulnerabilidades

Ou seja, a vulnerabilidade de sistemas de informação se refere a fraquezas ou brechas em um sistema ou rede, que pode permitir que um invasor comprometa a segurança, acessando, modificando, destruindo ou roubando informações.

Essas vulnerabilidades podem ser exploradas por meio de técnicas de ataque, como exploração de falhas de segurança, injeção de código malicioso, *phishing* ou engenharia social, e podem ocorrer em diferentes camadas do sistema, como o software do sistema operacional, aplicativos, redes e servidores.

E para evitar essas fraquezas brechas e falhas, as empresas adotam as melhores práticas de gestão de vulnerabilidades em sistemas e aplicativos, que inclui a identificação, a priorização, a gestão, o monitoramento constante e a conscientização dos funcionários. E muitas empresas tem inclusive uma equipe dedicada para tudo isso.

Monitoramento de ameaças

E o monitoramento de ameaças é um processo contínuo de identificação, análise e resposta a ameaças de segurança cibernética, que possam comprometer os sistemas redes e dados.

É uma atividade crítica para garantir a segurança da informação que envolve, entre outras, a coleta e análise de informações de diferentes fontes, como logs de eventos de segurança, dados de tráfego de rede, alertas de segurança e fontes de inteligência de ameaças.

E as empresas adotam boas práticas e recomendações para monitorar e responder às ameaças de segurança em tempo real, tais como:

O monitoramento em tempo real, para permitir que as empresas detectem ameaças de segurança imediatamente e tomem medidas para respondê-las antes que ocorram violações de segurança.

Alertas para que a equipe de segurança seja notificada sobre atividades suspeitas, como tentativas de login malsucedidas, downloads de arquivos incomuns ou outras atividades fora do padrão.

Políticas de resposta a incidentes estabelecidas e testadas, que incluem etapas claras para identificar, isolar e responder a ameaças de segurança em tempo real, mitigando os riscos identificados.

Análises de segurança regulares para identificar possíveis vulnerabilidades e ameaças, que inclui testes de penetração e análises de segurança de aplicativos.

E controles de segurança adicionais para monitorar e detectar ameaças de segurança em tempo real, como firewalls, sistemas de detecção de intrusão e autenticação multifator.

> “56% DOS ATAQUES ANALISADOS FORAM CAUSADOS POR NEGLIGÊNCIA DE FUNCIONÁRIOS OU CONTRATADOS, CUSTANDO EM MÉDIA US$ 484.931 POR INCIDENTE.”

O Relatório Global de Custo de Ameaças Internas publicado em 2022 pelo Instituto Ponemon dos Estados Unidos, aponta que as pessoas que tem acesso de dentro são a causa raiz da maioria dos incidentes.

Auditorias e testes de segurança

As auditorias e os testes de segurança ajudam a prever para se antecipar a ameaças, reduzindo significativamente o risco de violações.

Nas empresas, as boas práticas em auditorias e testes de segurança para identificar vulnerabilidades e avaliar o nível de segurança dos sistemas e aplicativos incluem:

Testes
regulares de segurança, incluindo testes de penetração, testes de vulnerabilidades, avaliações de risco e análises de segurança de aplicativos.

Ferramentas
de testes automatizadas, que podem ser usadas para acelerar o processo de auditoria e teste de segurança.

Estar atualizado
com as ameaças atuais, que significa que as empresas devem estar cientes de novas técnicas de ataque e vulnerabilidades recém-descobertas.

Documentar
e relatar descobertas, que vai permitir que os responsáveis pela segurança tomem medidas para remediar quaisquer problemas de segurança identificados.

Implementar
as correções necessárias, inclusive a instalação de patches de segurança, verificações automatizadas de segurança através do antivírus atualizações periódicas de software e reconfiguração de sistemas.