FOCO NO MERCADO DE TRABALHO

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Emilio Tissato Nakamura

SEGURANÇA DA INFORMAÇÃO PARA QUÊ?

Entenda na prática por que é necessário investir em segurança da informação.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você é o responsável pela segurança da informação de uma empresa do setor químico e iniciará um trabalho que começará com uma visão organizada de todos os principais conceitos da segurança da informação:

- A segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.
- É preciso garantir os princípios da segurança da informação: confidencialidade, integridade, disponibilidade.
- É preciso trabalhar com os elementos do risco: ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade, impacto.
- A aplicação de mecanismos de defesa, de controles de segurança e de técnicas de segurança de redes é definida a partir de uma visão de riscos.

Essa visão organizada é fundamental para que uma cultura de segurança se inicie e possibilite uma evolução constante do nível de maturidade da empresa, começando pela diretoria executiva. Ao final da apresentação, ficará mais claro para todos tudo o que envolve a questão “segurança da informação para quê?”.

Sugestão de estrutura da apresentação:

1. Faça um resumo do projeto da empresa.
2. Apresente os ativos envolvidos no projeto, não se esquecendo de que eles podem ser as pessoas, os equipamentos, os artefatos físicos, os processos, os sistemas e as tecnologias. Não é necessário citar todos, mas uma boa representatividade é importante.
3. Considere *crackers* e concorrentes como agentes de ameaça. Cite uma ameaça de cada tipo que afeta confidencialidade, integridade e disponibilidade.
4. Justifique que os ativos podem ter vulnerabilidades e explique-as.
5. Disserte sobre impactos em caso de uma ameaça tornar-se um incidente de segurança. Considere a tríade CID e descreva impactos incrementais, que iniciam com a equipe e incluem o projeto, indo até a empresa e as perdas financeiras de mercado e de reputação, por exemplo.
6. Faça uma relação entre os elementos do risco, unindo as informações anteriores.
7. Defina uma proposta de implementação de controles de segurança, mecanismos de defesa e técnicas de segurança de redes e aponte quais são eles.

Atenção para os princípios da segurança da informação: confidencialidade, integridade e disponibilidade — são eles que precisam ser protegidos. Uma falha comum é focar apenas um dos

aspectos da segurança da informação, negligenciando os outros. Há muitas ameaças rondando o ambiente da empresa, e as vulnerabilidades precisam ser identificadas.

Com a sua apresentação, você responderá a uma série de questões:

- No caso de um ataque cibernético contra a empresa, quais princípios de segurança da informação podem ser comprometidos?
- O que pode ser atacado, por que e por quem?
- O que pode acontecer em caso de um incidente de segurança?
- O que pode ser implementado para a segurança da informação?

AVANÇANDO NA PRÁTICA

EVITANDO VAZAMENTO DE INFORMAÇÕES

Devemos, como profissionais de segurança da informação, garantir a confidencialidade da informação, ou seja, permitir que somente pessoas autorizadas tenham acesso àquelas informações. O grande desafio da segurança da informação é, além de entender esse princípio, fazer com que ele seja cumprido. Como garantir a confidencialidade da informação? Como permitir que somente pessoas autorizadas tenham acesso às informações? Como evitar acessos não autorizados às informações? Como impedir vazamentos ou ataques cibernéticos que comprometem a confidencialidade?

De forma complementar, a disponibilidade também é um requisito primordial para a sua empresa, principalmente ao se tratar de uma plataforma de *marketplace* imobiliário. Sem o acesso a essas informações, o andamento dos negócios sofre prejuízos. No caso mais simples, a perda de disponibilidade temporária resulta em perda de tempo. Já nos casos mais complexos, a perda total das informações resulta em prejuízos bem maiores, que inviabilizam todo o andamento da empresa. Como tratar a segurança da informação nesse caso?

RESOLUÇÃO

Inicie a resolução considerando os diferentes tipos de ativos existentes: humanos, físicos, tecnológicos; explore as vulnerabilidades típicas existentes em cada um desses tipos de ativo. Por exemplo, humanos podem ser fonte de vazamento de informações em caso de suborno e um serviço na nuvem pode ser explorado a partir de uma vulnerabilidade da aplicação, que não é de responsabilidade do provedor de nuvem. Frente a isso, explore os possíveis controles de segurança que podem ser aplicados nos ativos para tratar as vulnerabilidades.

Ver anotações 0