SEGURANÇA DA INFORMAÇÃO

eBook 1

A segurança da informação é um pilar fundamental para qualquer organização, independentemente do tamanho ou setor de atuação. Com a crescente dependência da tecnologia e o aumento de ameaças cibernéticas, é importante que todas as pessoas dentro da empresa compreendam a importância deste assunto e saibam como agir para proteger as informações da empresa.

Estima-se que mais de 75 bilhões de dispositivos estarão conectados à Internet até o final de 2025.

Os crimes chamados cibernéticos tornaram-se um grande problema para as empresas, à medida que os hackers se tornam mais habilidosos e cada vez mais bem-sucedidos em violar as medidas de segurança de uma empresa por meio de ataques das mais variadas formas.

Porquê os hackers invadem?

O dinheiro, claro, é o maior motivador. Mas alguns também o fazem por razões políticas, para aumentar as tensões entre os países. Ou para espionagem corporativa, para espionar concorrentes e obter vantagens injustas. Ou apenas para entretenimento pessoal.

A frase *"dados são o novo ouro"* tem sido o burburinho da última década, mas com quantidades tão grandes de dados que as organizações coletam, surge o risco de violações, que podem expor ou vazar informações confidenciais.

Proteção e privacidade de dados se enquadram na categoria de coleta, manuseio e armazenamento de dados, que são mecanismos de controle para garantir que os dados não caiam em mãos erradas. No entanto, existem diferenças entre esses dois termos .

A privacidade de dados define as políticas e regulamentos, e a proteção de dados envolve o uso de ferramentas e procedimentos para fazer cumprir as políticas e regulamentos, e impedir o acesso não autorizado ou uso indevido dos dados.

Pode parecer que a proteção de dados e as ameaças à privacidade vêm apenas de fontes externas com intenções maliciosas; no entanto, a desatenção é uma grande ameaça à proteção de dados e à privacidade.

Qualquer um de nós pode enviar por engano um e-mail contendo informações confidenciais para a pessoa errada, transferir dados para contas pessoais para usar seus dispositivos nos fins de semana ou feriados ou, sem saber, ser vítima de ataques externos de phishing.

O custo das ameaças internas aumentou em 44% nos últimos 2 anos, com cada incidente custando em média US$15,4 milhões

Instituto Ponemon, 2022

Principais ameaças à segurança

- Malware: Software malicioso projetado para danificar ou obter acesso não autorizado a sistemas ou informações.
- Phishing: Tentativa de obter informações confidenciais, como senhas ou números de cartão de crédito, por meio de e-mails ou sites falsos.
- Engenharia social: Prática de enganar as pessoas para obter acesso não autorizado a informações ou sistemas.
- Ataques de força bruta: Tentativa de adivinhar senhas ou outros dados confidenciais por meio de repetidas tentativas.
- Roubo de equipamentos: Roubo ou perda de dispositivos que contêm informações confidenciais.

Medidas para garantir a confidencialidade, integridade e disponibilidade das informações e dados

Proteção de dados sensíveis

As empresas lidam com informações confidenciais, como dados financeiros, pessoais e estratégicos, que precisam ser protegidos de acessos não autorizados e ataques cibernéticos.

Cumprimento de leis e regulamentações

As empresas estão sujeitas a diversas leis e regulamentações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a GDPR (General Data Protection Regulation) na União Europeia, que estabelecem regras para a proteção de dados pessoais e informações confidenciais.

Manutenção da reputação

A perda ou vazamento de informações confidenciais pode prejudicar a imagem e reputação da empresa perante clientes, parceiros e a sociedade em geral.

Prevenção de perdas financeiras

A perda ou vazamento de informações confidenciais pode levar a prejuízos financeiros, como multas, indenizações e perda de clientes.

Continuidade dos negócios

A segurança da informação é importante para garantir a continuidade dos negócios da empresa, evitando interrupções parciais ou totais nos processos produtivos e na prestação de serviços.

Normas, regulamentos e Leis brasileiras

- Lei Geral de Proteção de Dados (LGPD), que estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o objetivo de proteger a privacidade e os direitos dos titulares dos dados.
- Norma ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para um Sistema de Gestão de Segurança da Informação em uma organização, e define um conjunto de controles para garantir a confidencialidade, integridade e disponibilidade das informações.
- Norma ABNT NBR ISO/IEC 27002:2013, que oferece diretrizes para a implementação de controles de segurança da informação, abrangendo várias áreas do negócio.
- Marco Civil da Internet, que estabelece princípios, direitos e deveres para uso da internet no país, incluindo a garantia da liberdade de expressão, a privacidade dos usuários e a segurança das informações na rede.
- Lei de Crimes Cibernéticos (Lei nº 12.737/2012), que define os crimes cibernéticos e estabelece as penas para os infratores, com o objetivo garantir a segurança das informações e dos dados pessoais na internet.
- Lei de Proteção e Defesa do Consumidor (CDC), que estabelece os direitos e as obrigações dos consumidores e das empresas, e que tem um capítulo específico que fala da segurança das informações pessoais dos consumidores.
- Lei de Direitos Autorais (LDA), Lei nº 9.610/1998, que tem como objetivo proteger os direitos dos proprietários de obras criativas, como livros, música, filmes, software e outros materiais protegidos por direitos autorais.