1

Introdução à Segurança da Informação

Segurança da Informação

Segurança da Informação

Introdução à Segurança da Informação

O que é a segurança da informação?

Segurança da informação (InfoSec) é a proteção de informações importantes contra acesso não autorizado, divulgação, uso, alteração ou interrupção. Ajuda a garantir que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados, permaneçam confidenciais e mantenham sua integridade.

Segurança da Informação

Introdução à Segurança da Informação

O que é a segurança da informação?

Precisamos proteger os ativos de informações, que podem incluir dados financeiros, confidenciais, pessoais ou sensíveis. Esses ativos podem assumir a forma de arquivos e dados digitais, documentos em papel, mídia física e até mesmo fala humana. Durante todo o ciclo de vida dos dados, a InfoSec supervisiona funções como infraestrutura, software, testes, auditoria e arquivamento.

Segurança da Informação

Introdução à Segurança da Informação

O que é a segurança da informação?

Baseada em princípios estabelecidos há décadas, a segurança da informação evolui constantemente para proteger ambientes cada vez mais híbridos e multinuvem em um cenário de ameaças em constante mudança. Dada a natureza evolutiva dessas ameaças, várias equipes precisam trabalhar juntas para atualizar a tecnologia e os processos usados nessa defesa.

A segurança da informação digital, também conhecida como **segurança de dados**, recebe hoje mais atenção dos profissionais de segurança da informação e é o foco deste artigo.

Segurança da Informação

Introdução à Segurança da Informação

Tipos de segurança

Os termos **segurança da informação**, **segurança de TI**, **cibersegurança** e segurança de dados são frequentemente (e incorretamente) utilizadas de forma intercambiável. Embora esses campos se sobreponham e se informem mutuamente, diferem principalmente no escopo.

Segurança da Informação

Introdução à Segurança da Informação

Tipos de segurança

Segurança da informação é um termo abrangente que envolve os esforços de uma organização para proteger as informações. Inclui **segurança física de ativos de TI**, **segurança de endpoints**, **criptografia de dados**, **segurança de rede** e outras.

Segurança da Informação

Introdução à Segurança da Informação

Tipos de segurança

A **segurança de TI** também se preocupa com a proteção de ativos físicos e digitais de TI e data centers, mas não abrange proteção para armazenamento de arquivos em papel e outras mídias. Concentra-se nos ativos tecnológicos e não nas informações em si.

Segurança da Informação

Introdução à Segurança da Informação

Tipos de segurança

A segurança cibernética concentra-se na proteção dos sistemas de informações digitais. O objetivo é ajudar a proteger os dados e ativos digitais contra ameaças cibernéticas. Embora seja um empreendimento enorme, a segurança cibernética tem escopo restrito, pois não se preocupa em proteger dados analógicos ou em papel.

Segurança da Informação

Introdução à Segurança da Informação

Tipos de segurança

Segurança de dados é a prática de proteger informações digitais contra acesso não autorizado, corrompimento ou roubo durante todo o ciclo de vida. Inclui a segurança física de dispositivos de hardware e armazenamento, além de controles administrativos e de acesso. Também abrange a segurança lógica de aplicativos de software e políticas e procedimentos organizacionais.

Segurança da Informação

Introdução à Segurança da Informação

Por que o InfoSec é importante

Os dados impulsionam grande parte da economia mundial e os cibercriminosos reconhecem seu valor. Os ataques cibernéticos que visam roubar informações confidenciais ou, no caso de **ransomware**, manter os dados como reféns, tornaram-se mais comuns, prejudiciais e caros. As práticas e os princípios da InfoSec podem ajudar a proteger os dados diante dessas ameaças.

Segundo o Relatório de custo de uma violação de dados da IBM, o custo total médio de uma violação de dados atingiu um novo patamar de USD 4,45 milhões em 2023. Esse número representa um aumento de 15,3% em relação aos US$ 3,86 milhões do relatório de 2020.

Segurança da Informação

Introdução à Segurança da Informação

Por que o InfoSec é importante

Uma violação de dados gera custos à vítima de várias maneiras. Tempo de inatividade inesperado leva à perda nos negócios. Muitas vezes, uma empresa perde clientes e sofre danos consideráveis e por vezes irreparáveis à sua reputação quando informações confidenciais dos clientes são expostas. A propriedade intelectual roubada pode prejudicar a rentabilidade de uma empresa e minar a sua vantagem competitiva.

Segurança da Informação

Introdução à Segurança da Informação

Por que o InfoSec é importante

Uma vítima de violação de dados também pode enfrentar multas regulatórias ou penalidades legais. Os regulamentos governamentais, como o **Regulamento Geral de Proteção de Dados (GDPR)** e os regulamentos do setor, como o **Health Insurance Portability and Accountability Act (HIPAA)**, exigem que as empresas protejam as informações confidenciais de seus clientes. Não fazer isso pode resultar em multas pesadas.

Segurança da Informação

Introdução à Segurança da Informação

Por que o InfoSec é importante

As empresas estão investindo como nunca antes em tecnologia e talentos de segurança da informação. De acordo com o Relatório do custo das violações de dados, cerca de 51% das organizações planejam aumentar os investimentos em segurança após uma violação.

Entre as principais áreas identificadas para mais investimentos estavam o planejamento e o teste da resposta a incidentes (RI), treinamento de funcionários e tecnologias de detecção e resposta a ameaças. As organizações que fizeram grandes investimentos em **IA de segurança** e automação relataram uma redução de US$ 1,76 milhão nos custos de violação de dados em comparação com as organizações que não usaram recursos de IA de segurança e automação.

Segurança da Informação

Introdução à Segurança da Informação

Por que o InfoSec é importante

Diretores de segurança da informação (CISOs) que supervisionam os esforços de segurança da informação tornaram-se membros da diretoria executiva da empresa.

Está aumentando a demanda para analistas de segurança da informação com certificações avançadas em segurança da informação, como a certificação **CISSP (Certified Information Systems Security Professional)** do ISC2. O Bureau of Labor Statistics prevê que as vagas para analistas de segurança da informação crescerá 32% até 2032.

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

Sugerida pela primeira vez pelo Instituto Nacional de Padrões e Tecnologia (NIST) em 1977, a tríade da CIA tem como objetivo orientar as organizações na escolha de tecnologias, políticas e práticas para proteger seus sistemas de informação. Os elementos da tríade da CIA são:

- **Confidencialidade**
- **Integridade**
- **Disponibilidade**

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

Confidencialidade significa garantir que as partes **não possam acessar dados para os quais não estão autorizadas**.

Confidencialidade define uma sequência contínua de usuários, desde pessoas internas privilegiadas com acesso a grande parte dos dados da empresa até pessoas externas autorizadas a consultar apenas informações que o público tem permissão para visualizar.

As informações pessoais devem permanecer privadas. Dados confidenciais são confidenciais. Se uma pessoa não autorizada obtiver uma senha para dados protegidos, isso será uma violação de confidencialidade.

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

Integridade significa garantir que todas as informações contidas nos bancos de dados da empresa sejam completas e precisas.

Os esforços de integridade visam impedir que as pessoas adulterem os dados, como por meio de adições, alterações ou exclusões não autorizadas. A integridade dos dados se aplica à prevenção tanto de adversários que alteram intencionalmente os dados quanto de usuários bem-intencionados que alteram os dados de forma não autorizada.

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

Disponibilidade significa garantir que os usuários possam acessar as informações a que estão autorizados a acessar quando precisarem.

A disponibilidade determina que as medidas e políticas de segurança da informação não devem interferir no acesso autorizado a dados. Grande parte da disponibilidade é direta, como trabalhar para garantir a robustez do hardware e do software para evitar que os sites de uma organização fiquem inativos.

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

  Disponibilidade significa garantir que os usuários possam acessar as informações a que estão autorizados a acessar quando precisarem.

  A disponibilidade determina que as medidas e políticas de segurança da informação não devem interferir no acesso autorizado a dados. Grande parte da disponibilidade é direta, como trabalhar para garantir a robustez do hardware e do software para evitar que os sites de uma organização fiquem inativos.

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

- **A tríade CIA**

O processo contínuo de obtenção da confidencialidade, integridade e disponibilidade de dados em um sistema de informação é conhecido como "garantia da informação"

Segurança da Informação

Introdução à Segurança da Informação

Princípios do InfoSec

Não repudiação

Não repudiação significa que um usuário não pode negar (ou seja, repudiar) ter feito uma transação, como alterar dados ou enviar uma mensagem, porque o usuário precisava passar pela autenticação para realizar a transação em primeiro lugar.

Embora não seja tecnicamente parte da tríade da CIA, o não repúdio combina aspectos de confidencialidade e integridade das informações. O não repúdio envolve garantir que somente usuários autorizados trabalhem com dados e que eles só possam utilizar ou modificar dados de maneiras autorizadas.

Segurança da Informação

Introdução à Segurança da Informação

Programas de segurança da informação

- **Avaliação de risco**

  Uma **avaliação de risco** de segurança da informação audita todos os aspectos do sistema de informações de uma empresa. A avaliação ajuda os profissionais de segurança da informação a entender os riscos exatos que enfrentam e a escolher as medidas de segurança e tecnologias mais apropriadas para mitigar os riscos.

Segurança da Informação

Introdução à Segurança da Informação

Programas de segurança da informação

- **Identificação de vulnerabilidades**

  Uma vulnerabilidade é qualquer ponto fraco na infraestrutura de TI (tecnologia da informação) que os adversários possam explorar para obter acesso não autorizado aos dados. Por exemplo, os hackers podem aproveitar os erros de um programa de computador para introduzir um malware ou código malicioso em um aplicativo ou serviço legítimo.

  Os usuários humanos também podem constituir vulnerabilidades em um sistema de informação. Por exemplo, cibercriminosos podem manipular os usuários para compartilhar informações confidenciais por meio de ataques de engenharia social, como phishing.

Segurança da Informação

Introdução à Segurança da Informação

Programas de segurança da informação

- **Identificação de ameaças**

Uma ameaça é qualquer coisa que possa comprometer a confidencialidade, integridade ou disponibilidade de um sistema de informação.

Uma ameaça cibernética é uma ameaça que explora uma vulnerabilidade digital. Por exemplo, um ataque de negação de serviço (DoS) é uma ameaça cibernética em que os cibercriminosos sobrecarregam parte do sistema de informação de uma empresa com tráfego, causando falhas.

As ameaças também podem ser físicas. Desastres naturais, ataques físicos ou armados e até mesmo falhas sistêmicas de hardware são considerados ameaças ao sistema de informação de uma empresa.

Segurança da Informação

Introdução à Segurança da Informação

Programas de segurança da informação

- **Planejamento de resposta a incidentes**

  Um plano de resposta a incidentes (IRP) normalmente orienta os esforços de uma organização na resposta a incidentes.

  As equipes de resposta a incidentes de segurança de computadores (CSIRT) geralmente criam e executam IRPs com a participação de partes interessadas de toda a organização. Os membros do CSIRT podem incluir o diretor de segurança da informação (CISO), diretor de IA (CAIO), centro de operações de segurança (SOC), equipe de TI e representantes jurídicos, de gerenciamento de riscos e outras disciplinas não técnicas.

Segurança da Informação

Introdução à Segurança da Informação

Programas de segurança da informação

- **Planejamento de resposta a incidentes**

Os IRPs detalham as etapas de mitigação que uma organização adota quando uma ameaça significativa é detectada. Embora os IRPs variem de acordo com as organizações que os elaboram e as ameaças que visam, as etapas comuns incluem:

- Reúna a equipe de segurança, seja virtualmente ou pessoalmente.
- Verifique a origem da ameaça.
- Atue para conter a ameaça e detê-la o mais rápido possível.
- Determine qual dano ocorreu, se houver.
- Notifique as partes interessadas da organização, os acionistas e os parceiros estratégicos.

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

Os programas de segurança da informação utilizam várias ferramentas e técnicas diferentes para lidar com ameaças específicas. As ferramentas e técnicas comuns do InfoSec são:

- **Criptografia**
- **Data loss prevention (DLP)**
- **Detecção e resposta de endpoint (EDR)**
- **Firewalls**
- **Sistemas de detecção de intrusão (IDS) e prevenção de intrusão (IPS)**
- **Sistemas de gerenciamento de segurança da informação (ISMS)**
- **Gerenciamento de informações e eventos de segurança (SIEM)**
- **Centros de Operações de Segurança (SOC)**
- **Medidas de autenticação fortes**
- **Inteligência de ameaça**
- **Análise de comportamento de usuários e entidades (UEBA)**

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

- **Criptografia** - utiliza algoritmos para ocultar as informações para que somente pessoas com permissão e capacidade de descriptografá-las possam lê-las.

- **Data loss prevention (DLP)** - As estratégias e ferramentas de DLP rastreiam o uso e a movimentação de dados em uma rede e aplicam políticas de segurança granulares para ajudar a evitar vazamentos e perdas de dados.

- **Detecção e resposta de endpoint (EDR)** - As soluções de EDR monitoram continuamente arquivos e aplicativos em cada dispositivo, buscando atividades suspeitas ou maliciosas que indiquem malware, ransomware ou ameaças avançadas.

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

- **Firewalls** - Um firewall é um software ou hardware que impede a entrada ou saída de tráfego suspeito de uma rede, permitindo a passagem de tráfego legítimo. Os firewalls podem ser implantados nas bordas de uma rede ou usados internamente para dividir uma rede maior em sub-redes menores. Se uma parte da rede for comprometida, os hackers serão impedidos de acessar o restante.
- **Sistemas de detecção de intrusão (IDS) e prevenção de intrusão (IPS)** - Um IDS é uma ferramenta de segurança de rede que monitora o tráfego de rede de entrada e dispositivos contra atividades suspeitas ou violações de política de segurança. Um IPS monitora o tráfego de rede contra ameaças em potencial e as bloqueia automaticamente. Muitas organizações utilizam um sistema combinado chamado **sistema de detecção e prevenção de intrusão** (IDPS).

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

- **Sistema de gerenciamento de segurança da informação (ISMS) -** Um ISMS contém diretrizes e processos que ajudam as organizações a proteger seus dados confidenciais e responder a uma violação de dados. Ter diretrizes em vigor também ajuda na continuidade se houver grande rotatividade de pessoal. ISO/IEC 27001 é um ISMS amplamente utilizado.

- **Gerenciamento de informações e eventos de segurança (SIEM) -** Os sistemasSIEM ajudam as equipes de segurança da empresa a detectar comportamentos anômalos de usuários e a utilizar a inteligência artificial (IA) para automatizar muitos dos processos manuais associados à detecção de ameaças e à resposta a incidentes.

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

- **Centro de Operações de Segurança (SOC) -** Um SOC unifica e coordena todas as tecnologias e operações de segurança cibernética sob uma equipe de profissionais de segurança de TI dedicados a monitorar a segurança da infraestrutura de TI o tempo todo.

- **Medidas de autenticação fortes -** A autenticação de dois fatores (2FA) e a autenticação multifatorial (MFA) são métodos de verificação de identidade nos quais os usuários devem apresentar várias evidências para provar suas identidades e obter acesso a recursos confidenciais.

Segurança da Informação

Introdução à Segurança da Informação

Ferramentas e técnicas de InfoSec

- **Inteligência de ameaça -** A inteligência de ameaças ajuda as equipes de segurança a serem mais proativas, possibilitando a tomada de ações eficazes e baseadas em dados para evitar ataques cibernéticos antes de ocorrerem.
- **Análise de comportamento de usuários e entidades (UEBA) -** UEBA é um tipo de software de segurança que utiliza análise comportamental e algoritmos de aprendizado de máquina para identificar comportamentos anormais e potencialmente perigosos de usuários e dispositivos.

Segurança da Informação

Introdução à Segurança da Informação

Ameaças à segurança da informação

As organizações enfrentam uma longa lista de ameaças potenciais à segurança da informação.

- **Ataques cibernéticos**
- **Erro do funcionário**
- **Segurança de endpoint ineficaz**
- **Ameaças internas**
- **Configuração incorreta**
- **Engenharia social**

Segurança da Informação

Introdução à Segurança da Informação

Ameaças à segurança da informação

- **Ataques cibernéticos -** Esses ataques podem tentar comprometer os dados de uma organização de várias direções, incluindo ataques de ameaças persistentes avançadas (APT), botnets (redes de robôs), ataques de negação de serviço distribuídos (DDoS), ataques de download "drive-by" (que baixam código malicioso automaticamente), malware, phishing, ransomware, vírus e worms.
- **Erro do funcionário -** As pessoas podem perder equipamentos móveis carregados com informações confidenciais, visitar sites perigosos em equipamentos da empresa ou utilizar senhas fáceis de decifrar.
- **Segurança de endpoint ineficaz -** Qualquer laptop, dispositivo móvel ou PC pode ser um encriptador do sistema de TI de uma organização na ausência de soluções antivírus ou de segurança de endpoints adequadas.

Segurança da Informação

Introdução à Segurança da Informação

Ameaças à segurança da informação

- **Ameaças internas -** Há dois tipos de ameaças internas:

  - Agentes internos maliciosos são funcionários, parceiros ou outros usuários autorizados que comprometem intencionalmente as informações de uma organização para ganho pessoal ou por despeito.

  - Agentes internos negligentes são usuários autorizados que, sem querer, comprometem a segurança ao não seguir as melhores práticas de segurança.

De acordo com o relatório do X-Force Threat Intelligence , cerca de 32% dos incidentes de segurança envolvem o uso malicioso de ferramentas legítimas. Os incidentes incluem roubo de credenciais, reconhecimento, acesso remoto e exfiltração de dados.

Segurança da Informação

Introdução à Segurança da Informação

Ameaças à segurança da informação

- **Configuração incorreta** - As organizações contam com várias plataformas e ferramentas de TI, incluindo opções de armazenamento de dados na nuvem, infraestrutura como serviço (IaaS), integrações de software como serviço (SaaS) e aplicativos web de vários provedores. Configurações inadequadas de qualquer um desses ativos podem representar riscos de segurança.

  Além disso, mudanças internas ou no provedor podem levar a um "desvio de configuração", em que configurações válidas ficam desatualizadas.

  O X-Force Threat Intelligence Index relatou que, durante os testes de penetração, o risco de aplicativo da web mais observado nos ambientes do cliente foi a configuração incorreta de segurança, representando 30% do total.

Segurança da Informação

Introdução à Segurança da Informação

Ameaças à segurança da informação

- **Engenharia social** - Os ataques de engenharia social induzem os funcionários a divulgar informações confidenciais ou senhas que abrem as portas para atos maliciosos.

  Também pode acontecer que, ao tentar promover uma organização por meio da rede social, os funcionários divulguem erroneamente muitas informações pessoais ou comerciais que podem ser utilizadas pelos atacantes.

Segurança da Informação

Introdução à Segurança da Informação

Os benefícios do InfoSec

Os benefícios de um forte programa InfoSec podem ajudar equipes em toda a organização:

- **Continuidade de negócios**
- **Conformidade**
- **Economia de custo**
- **Maior eficiência**
- **Proteção de reputação**
- **Redução de risco**

Segurança da Informação

Introdução à Segurança da Informação

Os benefícios do InfoSec

- **Continuidade de negócios -** As informações comerciais críticas podem ser protegidas e armazenadas de forma mais eficaz para serem reiniciadas após um incidente de segurança.
- **Conformidade -** Privacidade de dados e regulamentações de proteção, como HIPAA e PCI-DSS, geralmente exigem a proteção de informações confidenciais. A segurança da informação ajuda a garantir a conformidade e reduzir a responsabilidade legal ou a possibilidade de multas.
- **Economia de custo -** Um sistema de segurança de nível empresarial permite que as organizações tenham medidas adequadas para diversos níveis de dados, com a possibilidade de evitar gastos excessivos com a segurança de dados menos confidenciais.

Segurança da Informação

Introdução à Segurança da Informação

Os benefícios do InfoSec

- **Maior eficiência -** Os funcionários lidam melhor com as informações quando os dados são rotulados com mais clareza quanto ao sigilo e quando há implantados processos mais seguros.

- **Proteção da reputação -** Violações de segurança são ruins para os negócios. Incidentes de segurança podem ter custo imediato, mas também causam a perda da confiança do público.

Segurança da Informação

Introdução à Segurança da Informação

Os benefícios do InfoSec

- **Redução de risco -** Com a existência de planos de resposta a incidentes e um sistema, as medidas de segurança da informação podem ajudar a evitar incidentes de segurança e ataques cibernéticos, como violações de dados e ameaças de negação de serviço (DoS).

  Podem ser aplicadas medidas de autenticação para ajudar a proteger dados pessoais e organizacionais confidenciais, incluindo finanças e segredos comerciais. Os planos de recuperação de desastres podem estar prontos para uma recuperação mais rápida de incidentes de segurança.

Segurança da Informação

Introdução à Segurança da Informação

Os desafios do InfoSec

Além das ameaças diretas à segurança da informação, as organizações enfrentam vários desafios para criar e gerenciar estratégias e sistemas robustos de InfoSec.

- **Complacência**
- **Complexidade**
- **Conexões globais**
- **Inflexibilidade**
- **Integração de terceiros**

Segurança da Informação

Introdução à Segurança da Informação

Os desafios do InfoSec

- **Complacência** - Com um novo sistema implantado, pode haver a tendência de se afastar, satisfeito com a conclusão da tarefa. Mas as técnicas de hackers são aprimoradas constantemente para acompanhar as novas medidas de segurança. A manutenção e a tarefa de proteger os dados raramente são concluídas e são necessárias melhorias constantes nos controles de segurança.

- **Complexidade** - O ambiente tecnológico em constante mudança exige um sistema sofisticado e uma equipe de TI totalmente atualizada para gerenciar esses sistemas cada vez mais complexos. Isso inclui trocar informações com segurança com a Internet das Coisas (IoT) e todos os dispositivos móveis.

  A complexidade pode consumir muito tempo: algumas equipes de TI descobrem que seu principal esforço é reconfigurar e manter constantemente seu sistema de segurança.

Segurança da Informação

Introdução à Segurança da Informação

Os desafios do InfoSec

- **Conexões globais -** Empresas de todo o mundo podem utilizar sistemas de computador diferentes, ter diferentes níveis de segurança da informação e trabalhar sob regulamentações diferentes. Tudo isso torna a troca global de dados segura cada vez mais difícil.

- **Inflexibilidade -** O bloqueio de todas as informações pode interromper todo o progresso dos negócios. O equilíbrio difícil é ter um fluxo de dados construtivo dentro de uma organização, mantendo os dados seguros dentro da organização e utilizando-os corretamente.

- **Integração de terceiros -** Dependendo do nível de segurança, a integração de sistemas de informação com um fornecedor terceirizado ou outro parceiro de negócios pode ser difícil ou criar novos riscos de segurança.

Referências

- **IBM**

  https://www.ibm.com/br-pt/topics/information-security