INSTITUIÇÃO SENAI “AVAK BEDOUIAN”

LÍVIA GOMES DE CARVALHO

MARIA EDUARDA GIAMPIETRO DOS SANTOS

MARIA JULIA DE SOUZA LEITE

STHEFANY AMANDA MARTINS DE MOURA

CIBERSEGURANÇA:

Protegendo dados em um mundo conectado

Birigui

2024

LÍVIA GOMES DE CARVALHO
MARIA EDUARDA GIAMPIETRO DOS SANTOS
MARIA JULIA DE SOUZA LEITE
STHEFANY AMANDA MARTINS DE MOURA

CIBERSEGURANÇA:
Protegendo dados em um mundo conectado

Pesquisa apresentada ao curso de Desenvolvimento
De Sistemas, na área de T.I., da Instituição do SENAI
“Avak Bedouian”.

Orientador: Igor Cacerez
Coorientadora: Lais Ribeiro Sinatra

Birigui
2024

RESUMO

A cibersegurança é um conjunto de práticas e tecnologias essenciais para proteger sistemas, redes e dados contra ameaças cibernéticas. Um aspecto crucial é a autenticação multifatorial (MFA), que combina diferentes métodos de autenticação, como senhas e biometria, aumentando a segurança contra acessos não autorizados. Após a autenticação, a autorização define quais recursos um usuário pode acessar, utilizando modelos como o controle de acesso baseado em papéis (RBAC) e o controle baseado em atributos (ABAC). A criptografia desempenha um papel fundamental ao proteger dados, convertendo-os em formatos ilegíveis, tanto em trânsito quanto em repouso, garantindo sua confidencialidade e integridade.

O gerenciamento de vulnerabilidades é um processo contínuo que envolve a identificação, avaliação e correção de falhas de segurança, utilizando patches e testes de penetração para simular ataques e detectar fraquezas. A resposta a incidentes inclui a implementação de um plano para detectar e responder a ameaças, além de análises forenses que investigam e documentam os incidentes de segurança. Com o aumento da complexidade das ameaças, a integração de Inteligência Artificial e Machine Learning se torna fundamental para a detecção proativa de ameaças, enquanto a segurança em nuvem é vital para proteger ambientes digitais, especialmente com a crescente adoção da Internet das Coisas (IoT), que demanda normas de segurança robustas.

Além disso, a segurança física e ambiental é essencial para proteger infraestruturas contra desastres naturais e falhas, envolvendo planos de continuidade de negócios, backups regulares e monitoramento de sistemas. A educação e conscientização dos usuários são igualmente importantes para mitigar riscos cibernéticos; programas de conscientização e treinamentos reduzem a vulnerabilidade de indivíduos e organizações, promovendo a conformidade com legislações como a LGPD. Em um cenário de crescente complexidade nas ameaças digitais, a cibersegurança deve ser uma prioridade para garantir a proteção eficaz de sistemas e dados.

Palavras-chave: Cibersegurança. Autenticação Multifatorial. Criptografia. Gerenciamento de Vulnerabilidades. Segurança em Nuvem.

ABSTRACT

Cybersecurity is a set of practices and technologies that are essential for protecting systems, networks, and data against cyber threats. A key aspect is multi-factor authentication (MFA), which combines different authentication methods, such as passwords and biometrics, increasing security against unauthorized access. After authentication, authorization defines which resources a user can access, using models such as role-based access control (RBAC) and attribute-based access control (ABAC). Encryption plays a key role in protecting data by converting it into unreadable formats, both in transit and at rest, ensuring its confidentiality and integrity.

Vulnerability management is an ongoing process that involves identifying, assessing, and remediating security flaws, using patches and penetration testing to simulate attacks and detect weaknesses. Incident response includes implementing a plan to detect and respond to threats, as well as forensic analysis that investigates and documents security incidents. As threats become more complex, the integration of Artificial Intelligence and Machine Learning becomes essential for proactive threat detection, while cloud security is vital to protect digital environments, especially with the growing adoption of the Internet of Things (IoT), which demands robust security standards.

In addition, physical and environmental security is essential to protect infrastructures against natural disasters and failures, involving business continuity plans, regular backups, and system monitoring. User education and awareness are equally important to mitigate cyber risks; awareness programs and training reduce the vulnerability of individuals and organizations, promoting compliance with legislation such as the LGPD. In a scenario of increasing complexity in digital threats, cybersecurity must be a priority to ensure effective protection of systems and data.

Keywords: Cybersecurity. Multi-factor authentication. Cryptography. Vulnerability management. Cloud security.

SUMÁRIO

1. INTRODUÇÃO

Na atualidade, a cibersegurança atua com a função de proteger os dados do mundo que está cada vez mais digitalizado e tecnológico. Com isso, as ameaças à integridade e confidencialidade das informações têm se diversificado e intensificado cada vez mais, colocando em riscos organizações e indivíduos. No entanto, a proteção de dados tornou-se uma prática essencial, não apenas para garantir a privacidade, mas também para preservar a confiança e a integridade dos sistemas digitais.

A cibersegurança é um conjunto de técnicas e ferramentas, desenvolvidas para proteger sistemas e dados contra-ataques, danos e acesso não autorizados. Estes mecanismos são fundamentais para garantir a continuidade das operações e a segurança das informações sensíveis, que são frequentemente alvo de ameaças. Neste caso, é necessário a implementação de estratégias robustas de proteção de dados.

2. FUNDAMENTOS DA CIBERSEGURANÇA

Afinal, o que é cibersegurança?

A Cibersegurança, ou segurança cibernética, é a prática de proteger sistemas de computação, redes, programas e dados contra ataques, danos ou acesso não autorizado. Se trata de um conjunto de ações e técnicas para **proteger sistemas, programas, redes e equipamentos de invasões,** é voltada para **softwares, hardwares e redes**.

Dessa forma, é possível garantir que dados valiosos não vazem ou sejam violados em ataques cibernéticos. Esses ataques podem ter a intenção de **acessar servidores, roubar senhas, sequestrar dados** ou até mesmo fraudar transações financeiras. Portanto, a cibersegurança funciona como um **escudo para blindar toda a parte de TI**, seus dispositivos e suas operações.

2.1. “NÃO UM TRATAMENTO, MAS UMA PROFILAXIA”

Esta citação criada por nosso grupo reflete a resposta para muitas pessoas que acabam por conhecer a cibersegurança tarde demais e por isso tentam aplicá-la depois que os problemas já aconteceram, não conseguindo usufruir de seu efeito preventivo. Isso acontece porque seu principal objetivo é antecipar, identificar e mitigar ameaças e vulnerabilidades que possam comprometer a integridade e a disponibilidade dos sistemas e dados digitais, e não propor um tratamento para problemas que já ocorrem, apesar de poder servir para tanto.

2.2. POR QUE APLICAR CIBERSEGURANÇA?

Em um mundo cada vez mais digital, onde a dependência de tecnologia é crescente, a cibersegurança se tornou crucial para garantir a integridade, confidencialidade e disponibilidade das informações. Assim, o mundo globalizado impõe a necessidade de cibersegurança devido a uma série de fatores interconectados que aumentam a exposição e a vulnerabilidade das informações e sistemas. Dentre estes fatores podemos citar: A facilitação do acesso remoto e do trabalho à distância e a expansão gradativa do comércio digital (que envolve as transações online e, consequentemente, a segurança das plataformas digitais).

2.2.1. DE OLHO NO CENÁRIO ATUAL

Globalmente, convergindo com fatos já descritos, os ataques cibernéticos **aumentaram 16%** desde o início do conflito entre Rússia e Ucrânia em fevereiro de 2022. Assim, no Brasil, as ameaças são particularmente preocupantes em setores críticos como saúde, tecnologia, energia e governo, todos apresentando vulnerabilidades específicas e sendo alvos atraentes para criminosos cibernéticos.

Ainda neste tópico, vale ressaltar que, no âmbito global, o Brasil é o segundo país do mundo com mais ataques cibernéticos, atrás apenas dos Estados Unidos, com 1.168.456 de ataques; e a Coreia do Sul em terceiro, com 333,516 registros.

De acordo com o Instituto Internacional de Estudos Estratégicos (IISS, na sigla em inglês), os EUA são a única potência cibernética de nível um no mundo, com base na capacidade de ataque, defesa e influência.

Como supracitado, o **crescimento do trabalho remoto**, foi um dos agravantes impulsionadores para que organizações enfrentassem desafios adicionais, já que violações de dados relacionadas a essa modalidade de trabalho tendem a ser mais custosas e difíceis de conter. Para comprar isto, segundo a **pesquisa da Tessian**, enquanto trabalhavam de casa, 47% dos seus colaboradores atribuíram à distração a razão para serem vítimas de golpes de phishing.

Ainda a exemplo do pressuposto, a saúde, enfrentou um **crescimento de 5%** nos incidentes de ransomware entre 2021 e 2022, colocando em risco **dados sensíveis** dos seus pacientes.

Diante desse panorama, a conscientização sobre práticas de segurança, **investimentos em tecnologias de proteção** e a implementação de políticas rigorosas são essenciais para mitigar riscos e garantir a resiliência digital frente às ameaças cibernéticas crescentes.

2.3. CIBERSEGURANÇA X SEGURANÇA DA INFORMAÇÃO

São constantemente confundidos. A segurança da informação é **um pouco mais abrangente,** pois **se preocupa com a proteção de todos os dados da empresa.** Ou seja, **desde o armazenamento físico de informações até os dados** que são geridos por pessoas.

Com isso, as atividades para garantir a segurança da informação são as mais variadas. Elas passam por regras para transporte de computadores e equipamentos de trabalho, acesso remoto à rede da empresa, política de troca de senhas, garantir que os funcionários estão usando senhas fortes e até mesmo manuais sobre **quais informações podem ser fornecidas a quais pessoas**.

3. PRINCÍPIOS DE SEGURANÇA

Os princípios de segurança são diretrizes fundamentais, que orientam a proteção de sistemas e dados contra ameaças e vulnerabilidades. Eles são essenciais para a construção da base para construir estratégias e políticas de segurança eficazes. A confidenciabilidade, integridade e disponibilidade, contribuem para uma estratégia de segurança robusta.

A confidenciabilidade limita o acesso à informação, sendo permitido somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário, protege informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

A integridade garante a veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e tratamento, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que fique exposta ao manuseio por uma pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

A disponibilidade garante o acesso das pessoas devidamente autorizadas à informação sempre que necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

4. TIPOS DE ATAQUES

Um ataque cibernético trata-se de qualquer esforço intencional para roubar, expor, alterar, desativar ou destruir dados, aplicativos ou outros ativos por meio do acesso não autorizada a uma rede, sistema de computador ou dispositivo digital. Existem vários tipos de ataques cibernéticos, entre eles o Phishing, o Malware, o DoS (Ataque de Negação de Serviço) e DDoS (Ataque de Negação de Serviço Distribuído) e o Ataque Man-In-The-Middle (MITM).

4.1. PHISHING

O Phishing trata-se de um ataque de engenharia social para obter informações sensíveis. Ou seja, consiste no envio de mensagens fraudulentas, normalmente por e-mail ou SMS, que parecem ser de fontes confiáveis com o objetivo de roubar dados pessoais como informações de login ou de cartões de crédito. O phishing divide-se entre 3 tipos: Spear Phishing, Whaling e Smishing.

4.1.1. SPEAR PHISHING

Direciona-se a pessoas e empresas específicas e tem como objetivo o roubo de dados críticos como credenciais de acesso, dados bancários e informações de mercado.

4.1.2. WHALING

Tem um alvo bem definido: executivos sêniores e cargos de alto escalão. Desse modo, conseguem roubar dados estratégicos, dinheiro e mesmo acessar sistemas para executar outro ataque.

4.1.3. SMISHING

Essa ameaça funciona de modo que o hacker envia mensagens fraudulentas para que o usuário forneça seus dados pessoais: senhas, endereço, nome de usuários e número de cartão de crédito. Na maioria dos casos, eles finger ser seu banco.

4.2. MALWARE

O Malware consiste em vírus, worms, trojans, spyware e adware. Em suma, trata-se de um software malicioso que pode se passar por um programa ou anexo de e-mail confiável cujo objetivo consta em enviar um vírus que permite o acesso de hackers a uma rede de computadores. Ele divide-se em 5 tipos principais: Ransomware, Trojans, Spyware, Worms e Keyloggers.

4.2.1. RANSOMWARE

Inicia-se com o envio de links suspeitos em e-mails de phishing ou em vulnerabilidades não corrigidas. Desse modo, o hacker “captura” os dados, aplica uma criptografia avançada e exige um resgate para liberar o acesso.

4.2.2. TROJANS

Trata-se de um tipo de malware que se assimila a um software confiável e inofensivo e, ao ser instalado, dá acesso a dados e gera inúmeros danos.

4.2.3. SPYWARE

Infecta o dispositivo e passa a coletar dados a respeito do usuário de modo imperceptível.

4.2.4. WORMS

Atinge o computador por meio de phishing e técnicas de engenharia social e, após infectar o dispositivo pode modificar e excluir dados além de injetar outros softwares e se replicar até sobrecarregar o sistema.

4.2.5. KEYLOGGERS

Nesse ataque o invasor consegue visualizar o que é digitado pelo usuário podendo, desse modo, extrair senhas e dados sigilosos de forma maliciosa.

4.3. DOS E DDOS

Os ataques *DoS* e *DDoS* tratam-se da saturação de serviços para torná-los inacessíveis. Desse modo o *DoS* funciona de modo a sobrecarregar um servidor ou computador para deixá-lo indisponível para o usuário. Enquanto o *DDoS* usufrui de milhares ou milhões de computadores para atacar um único site ou sistema.

4.4. MAN-IN-THE-MIDDLE (MITM)

O ataque Man-In-The-Middle permite ao invasor espionar os dados enviados entre duas pessoas, redes ou computadores. Encontra-se na categoria “ataques baseados em identidade” e possibilita ao hacker induzir as vítimas a executar alguma ação como uma transação bancária.

4.5. CASOS DE ATAQUES CIBERNÉTICOS

Conforme o vídeo *Cibersegurança: conceito, implicações e importância* (MEIO&MENSAGEM, 2024) alguns casos de ataques cibernéticos incluem:

4.5.1. ATAQUE DA VAREJISTA DA RENNER

O ataque ocorreu em agosto de 2021 derrubando parte do sistema da Renner e deixando o site fora do ar.

4.5.2. ATAQUE À SUBSIDIÁRIA BRASILEIRA DA JBS

O ataque ocorreu em junho de 2021 e cobrou 11 milhões de dólares para restabelecer a segurança.

4.5.3 ATAQUE ÀS AMERICANAS

Causou um prejuízo de quase 1 bilhão de reais após um ataque hacker que comprometeu o funcionamento do seu site por 5 dias.

4.5.4. ATAQUE À RECORD TV

A Record TV enfrentou uma invasão em seu sistema de arquivos bloqueando o acesso ao seu acervo e conteúdo.

4.5.5. ATAQUE A INSTITUIÇÕES NACIONAIS

É mencionado também o ataque a instituições nacionais como o Ministério da Saúde, o Tesouro Naional e o Supremo Tribunal de Justiça.

5. COMPLIANCE E REGULAMENTAÇÃO

É de extrema importância compreender sobre a Auditoria de Segurança, principalmente para aqueles que acessam os meios digitais. A partir disso, é possível garantir a proteção de dados pessoais, bem como a segurança do indivíduo, diante de vírus e pessoas mal-intencionadas. Paralelamente, a Legislação e as Normas, fazem um papel crucial para a tomada e elaboração diretrizes rigorosas. Portanto, assim é possível proteger a privacidade dos cidadãos e assegurar que as informações sejam tratadas de forma segura e ética. Dessa maneira, é capaz a identificação de vulnerabilidades presentes no meio tecnológico.

A Auditoria de Segurança tem como papel identificar as ameaças presentes nos meios digitais, identificando riscos e falhas, que podem comprometer a integridade e confiabilidade de uma empresa. Além disso, é uma prática fundamental e preventiva para garantir a segurança de informações pessoais.

A LGPD (Lei Geral de Proteção de Dados), foi criada em 18 de setembro de 2020 no Brasil, com o objetivo de garantir a liberdade e privacidade de todos os cidadãos, padronizando os tratamentos dos dados pessoais, informando a eles algumas de suas garantias, como, a possibilidade de solicitação para que as suas informações sejam excluídas, e assim, seja possível o fortalecimento da segurança jurídica no ambiente virtual.

Ademais, há a presença de dois tratamentos de dados, como o controlador, o qual é uma pessoa natural ou jurídica, em que seu direito pode ser privado ou público, e tem como função decidir como e por que os dados pessoais são coletados e utilizados. Já o operador, que também pode ser considerada uma cidadã natural ou jurídica, porém ela é responsável por realizar o tratamento de dados pessoais em nome e sob as instruções do controlador. Entretanto, caso a empresa não realizar a sua função de proteger os dados desse indivíduo, poderá levá-la a uma multa de até 2% do faturamento da empresa, a qual é limitada a R$ 50 milhões por infração.

Já o GDPR (Regulamento Geral de Proteção de Dados), um Regulamento da União Europeia que entrou em vigor em maio de 2018, tem o mesmo objetivo, proteger os dados dos cidadãos e garantir a segurança dos dados pessoais, o qual deve ser transparente em suas informações, deixando claro aos indivíduos, informando quais os dados coletados e a sua finalidade, assim, empoderar a segurança dos europeus.

Dessa maneira, poderá levar a multas de até € 20 milhões ou 4% da receita anual global, o que for maior, para a empresa que não assegurar a lei.

O CCPA (Lei de Privacidade do Consumidor da Califórnia), se trata de uma lei estadual da Califórnia, que entrou a vigor em 2020, e tem como intuito, promover a privacidade dos cidadãos do local. A lei estabelece alguns direitos a sua população, como o Direito do saber, informando as informações coletadas e como são utilizadas; Direito do apagar, em que é possível a solicitação para excluir as informações pessoais; Direito de optar pela não venda, ou seja, é possível opinar por não vender e divulgar informações pessoais. Além de penalidades caso a lei não for cumprida, podendo levar a multas de US$ 2.500 para cada violação acidental e US$ 7.500 para cada violação intencional.

Sendo assim, é de extrema relevância a segurança meios tecnológicos, pois os dados fornecidos para os sites e empresas, devem estar seguros, contribuindo para todos os cidadãos e para a própria empresa, utilizando os seus bens para outros fins, sem se preocupar com pagamentos de multas, pois não irá ser preciso, caso as normas sejam seguidas, conforme a lei.

6. SEGURANÇA DE REDES

Segurança de rede é um aspecto crucial da cibersegurança que se concentra em proteger a infraestrutura de rede contra diversas ameaças e ataques. Envolve a implementação de políticas, controles e tecnologias para garantir a confidencialidade, integridade e disponibilidade dos dados enquanto viajam pela rede.

Os *firewalls* são componentes essenciais da segurança de rede, projetados para proteger redes e sistemas contra acessos não autorizados e ataques. Eles monitoram e controlam o tráfego de entrada e saída com base em um conjunto de regras de segurança predefinidas.

O S*istemas de Detecção e Prevenção de Intrusões (IDS/IPS)*, são ferramentas de segurança de rede usadas para identificar e mitigar atividades suspeitas e maliciosas. Eles desempenham um papel essencial na proteção das redes contra ameaças e ataques cibernéticos. *O Sistema de Detecção de Intrusões (IDS)*, é responsável por monitorar a rede para detectar atividades suspeitas ou maliciosas e gera alertas. *Não bloqueia ataques, apenas avisa os administradores,* trata-se de um modelo parecido com um firewall, onde o próprio administrador pode configurar as atividades de proteção. O *Sistema de Prevenção de Intrusões (IPS)*, é responsável monitorizar a rede e toma ações automáticas para bloquear ou interromper ataques em tempo real, evitando que causem danos, e possui autonomia para bloqueá-las automaticamente, conforme as permissões configuradas, além disso, pode emitir alertas de possíveis ataques para os administradores, bloqueia sites que provem programas maliciosos, e recupera a conexão com outros serviços. A diferença entre ambos os sistemas de prevenção é que IDS tem o foco em alerta e detecção, já IPD tem ênfase na prevenção automática e detecção, portanto juntos proporcionam uma melhor segurança para a proteção de redes.

Outro meio importante para segurança de rede é a *Segmentação de Rede*, que é a prática de dividir uma rede de computadores em segmentos menores e distintos para melhorar a segurança, a performance e a gestão da rede. Essa divisão pode ser feita através de várias técnicas e tecnologias, com o objetivo de isolar diferentes partes da rede e controlar o tráfego entre elas. Tem como benefícios além de uma melhoria na segurança, o isolamento de ameaças, ou seja, se um segmento for comprometido a segmentação pode limitar o impacto do ataque prevenindo que ele se espalhe pelas outras redes. O controle de acesso, que ajuda na redução do risco do acesso não

autorizado, através da aplicar políticas de segurança específicas para cada segmento. Disponibiliza um melhor gerenciamento de largura de banda permitindo alocar largura de banda de forma mais eficiente com base nas necessidades de cada segmento. A segmentação de rede controla o tráfego, facilita o desempenho e limita o impacto de possíveis ameaças.

7. SEGURANÇA DE APLICAÇÕES

Assim como redes estão expostas a ataques, o mesmo acontece com os aplicativos que utilizamos, seja no **contexto pessoal ou dentro das empresas**. Desse modo, a segurança de aplicações, dentro do contexto da cibersegurança, refere-se à prática de proteger aplicativos de software contra uma ampla gama de ameaças e vulnerabilidades que podem comprometer a integridade, a confidencialidade e a disponibilidade das aplicações. O objetivo é garantir que as aplicações funcionem de forma segura e eficaz, evitando que sejam exploradas por atacantes para obter acesso não autorizado, roubar dados, ou causar danos.

7.1. SEGURANÇA DE DESENVOLVIMENTO DE SOFTWARE

A segurança de desenvolvimento de software é uma disciplina dentro da cibersegurança que foca em garantir que o software seja criado e mantido de maneira a minimizar riscos e vulnerabilidades. Ela abrange práticas e técnicas que devem ser incorporadas ao longo do ciclo de vida do desenvolvimento de software para proteger as aplicações contra ataques e falhas. Abaixo, citaremos algumas práticas conhecidas para a aplicação da cibersegurança neste âmbito:

7.1.1. VALIDAÇÃO E SANITIZAÇÃO DA ENTRADA

A validação de entrada é o processo de verificar se os dados fornecidos por um usuário ou outra fonte estão corretos, completos e dentro dos parâmetros esperados antes de serem processados ou armazenados pela aplicação. Assim, tem o objetivo de garantir que os dados atendam a requisitos específicos, como formato, tipo, e intervalo, para prevenir erros e proteger de ataques. Já a sanitização de entrada é o processo de modificar dados para garantir que eles não contenham elementos prejudiciais ou maliciosos antes de serem usados pela aplicação, e tem o mesmo objetivo.

7.1.2. USO DE PRINCÍPIO DE MENOR PRIVILÉGIO

A concessão das permissões mínimas necessárias para que uma função ou usuário realize suas tarefas reduz o impacto de uma potencial vulnerabilidade.

7.1.3. TRATAMENTO DE ERROS E EXCEÇÕES

É mister optar por não expor detalhes internos do sistema ou da aplicação em mensagens de erro. É indicado que o administrador forneça mensagens genéricas e registre erros de forma segura para análise posterior.

7.1.4. SEGURANÇA EM DEPENDÊNCIAS E BIBLIOTECAS

Mantenha todas as bibliotecas e frameworks SEMPRE atualizados. Utilize ferramentas para verificar vulnerabilidades conhecidas nas dependências do projeto.

7.1.5. SEGURANÇA NO ARMAZENAMENTO E MANIPULAÇÃO DE DADOS

É recomendável evitar armazenar dados sensíveis desnecessariamente. Adote boas práticas para o gerenciamento seguro de dados, incluindo o uso de políticas de retenção e eliminação adequadas para a proteção destas informações.

7.1.6. ANÁLISE ESTÁTICA DE CÓDIGO

Utilize ferramentas de análise estática (As ferramentas de análise estática de código inspecionam o código em busca de indicações de vulnerabilidade comum, que são então corrigidas antes do lançamento do aplicativo) para examinar o código-fonte em busca de vulnerabilidades e falhas de segurança sem executar o código.

7.2. OWASP

O Open Worldwide Application Security Project (OWASP) é uma organização sem fins lucrativos dedicada à melhoria da segurança de software. O OWASP fornece uma variedade de recursos e ferramentas para ajudar organizações e desenvolvedores a criar aplicações seguras.

7.2.1. OBJETIVO

O principal objetivo do OWASP é aumentar a segurança de software promovendo melhores práticas e oferecendo recursos educacionais. Eles se concentram na segurança de aplicações e na conscientização sobre vulnerabilidades.

7.2.2. PROJETOS

O OWASP desenvolve e mantém uma série de projetos, muitos dos quais são amplamente utilizados na indústria de segurança. Alguns dos projetos mais conhecidos incluem:

7.2.2.1. OWASP TOP TEN

Se trata de uma lista das dez principais vulnerabilidades de segurança em aplicações web, atualizada periodicamente. É um recurso essencial para desenvolvedores e profissionais de segurança.

7.2.2.2. OWASP ZAP (ZED ATTACK PROXY)

Se trata de uma ferramenta de segurança para encontrar vulnerabilidades em aplicações web.

7.2.2.3. OWASP DEPENDENCY- CHECK

Esta também é uma ferramenta que identifica vulnerabilidades, todavia, estas são conhecidas em dependências de bibliotecas de software.

7.2.3. COMITÊS, CAPÍTULOS, DOCUMENTAÇÃO E GUIAS

O OWASP possui uma rede global de capítulos e comitês que trabalham para promover a segurança de software em diferentes regiões e áreas de especialização. Cada capítulo local organiza eventos, encontros e treinamentos. Além disso, ela publica uma ampla gama de documentos e guias para ajudar na implementação de práticas seguras de desenvolvimento. Isso inclui diretrizes sobre desenvolvimento seguro, gestão de riscos e muito mais.

8. CONTROLE DE ACESSO

O controle de acesso cibernético trata-se de uma tecnologia que permite gerenciar e monitorar o uso de dados na internet, além de controlar a permissão de acesso a eles. É fundamental para a cibersegurança dado que protege computadores e dispositivos conectados a uma rede. Ele evita que informações confidenciais, como dados de clientes e propriedade intelectual sejam roubadas por pessoas mal-intencionadas ou usuários não autorizados. Além disso, reduz o risco de exfiltração de dados por funcionários e mantém as ameaças baseadas na web afastadas.

De modo simples, funciona de modo a identificar um usuário com base em suas credenciais e a autorização do nível de acesso apropriado assim que ele for autenticado. Algumas das credenciais comumente usadas incluem senhas, pins, tokens de segurança e verificações biométricas. Nesse processo, depois que a identidade de um usuário for autenticada, as políticas de controle de acesso concedem permissões específicas e permitem que o usuário proceda conforme pretendido.

Deste modo, o controle de acesso pode se dividir entre 3 principais tópicos: a autenticação, a autorização e a criptografia.

8.1. AUTENTICAÇÃO

A autenticação trata-se do processo de verificação da identidade de um usuário com o intuito de garantir que eles é quem afirma ser. Isso pode ocorrer de diferentes formas, dentre elas: através de senhas, da biometria e da autenticação multifatorial (MFA).

8.1.1. SENHAS

O uso de senhas é o método mais comum para provar a identidade do usuário pois utiliza de uma sequência de caracteres propondo facilidade e aplicabilidade. No entanto, tem como desvantagem a susceptibilidade a ataques de força bruta, phishing e uso de senhas fracas.

8.1.2. BIOMETRIA

A biometria é utilizada atualmente por muitos softwares e aplicativos — em especial, por bancos — e utiliza de características físicas ou comportamentais do usuário como impressões digitais, reconhecimento facial, íris ou voz. É um método bastante seguro por ser difícil de imitar e ser geralmente mais conveniente. Entretanto, sua implementação pode gerar altos custos além da possibilidade falsos positivos e negativos.

8.1.3. AUTENTICAÇÃO MULTIFATORIAL (MFA)

Como o próprio nome insinua, a autenticação multifatorial combina dois ou mais métodos de autenticação, como algo aplicável para o usuário (senha), algo que ele possui (token ou smartphone) e algo que ele é (biometria). Esse método aumenta significativamente a segurança e reduz a probabilidade de acesso não autorizado. Por outro lado, pode ser mais complexo e exigir mais esforço do usuário.

8.2. AUTORIZAÇÃO

A autorização trata-se do processo de definir e controlar quais recursos e dados podem ser acessados pelo usuário após sua autenticação. Ela se divide em 4 vertentes: RBAC, ABAC, DAC e MAC.

8.2.1. CONTROLE DE ACESSO BASEADO EM PAPÉIS/FUNÇÃO (RBAC)

Nesse modelo os direitos de acesso são concedidos com base em funções de negócios definidas e não na identidade ou tempo de serviço dos indivíduos. Tem como objetivo fornecer ao usuário apenas os dados que eles precisam para realizar o trabalho/papel designado a ele.

8.2.2. CONTROLE DE ACESSO BASEADO EM ATRIBUTOS (ABAC)

Nesse modelo o acesso é concedido de forma flexível com base em uma combinação de atributos do usuário e condições ambientais, como horário e local. Esse modelo possui um controle de acesso mais granular e ajuda a reduzir o número de atribuições de funções.

8.2.3. CONTROLE DE ACESSO DISCRICIONÁRIO (DAC)

Nesse modelo cada objeto em um sistema protegido tem um proprietário e são estes que concedem acesso aos usuários conforme seus critérios.

8.2.4. CONTROLE DE ACESSO OBRIGATÓRIO (MAC)

Nesse modelo os usuários recebem acesso na forma de uma autorização aonde uma autoridade central regula os direitos de acesso — estes, que já são definidos centralmente e não podem ser alterados pelos usuários — e os organiza em camadas que se expandem uniformemente. É um modelo bastante comum em contextos governamentais e militares.

8.3. CRIPTOGRAFIA

A criptografia trata-se da prática de proteger dados convertendo-os em um formato que só pode ser lido por aqueles que possuem a chave para decifrá-los. É fundamental para garantir a confidencialidade e integridade dos dados. Ela pode se dividir entre 4 vertentes: a criptografia em trânsito, a criptografia em repouso, a criptografia simétrica e a criptografia assimétrica.

8.3.1. CRIPTOGRAFIA EM TRÂNSITO

A criptografia em trânsito protege dados enquanto estão sendo transmitidos através de redes como HTTPS e TLS. Isso impede que os dados sejam interceptados e lidos por terceiros não autorizados.

8.3.2. CRIPTOGRAFIA EM REPOUSO

A criptografia em repouso protege dados armazenados em dispositivos e sistemas como criptografia de discos e arquivos. Desse modo, garante que, mesmo que o armazenamento seja comprometido, os dados permanecem seguros.

8.3.3. CRIPTOGRAFIA SIMÉTRICA

Utiliza da mesma chave para criptografar e descriptografar dados sendo rápida e eficiente para grandes volumes de dados.

8.3.4. CRIPTOGRAFIA ASSIMÉTRICA

Utiliza de um par de chaves sendo uma pública para criptografar e uma privada para descriptografar. Isso permite a comunicação segura sem a necessidade compartilhar chaves secretas.

9. GERENCIAMENTO DE VULNERABILIDADES

O *gerenciamento de vulnerabilidades* é um processo contínuo que tem como objetivo identificar, avaliar, priorizar e corrigir vulnerabilidades de segurança em sistemas e redes. É um componente crucial da cibersegurança, ajudando a proteger a organização contra-ataques que exploram falhas de segurança. Existem alguns métodos de gerenciamento, sendo eles as *aplicações de patches* que seriam as instalações fornecidas pelos fabricantes de softwares, para a correção de vulnerabilidades conhecidas. As *configurações seguras*, que altera as configurações do sistema ou aplicativo para mitigar vulnerabilidades. E o *desenvolvimento de contenção*, que são as implementações de medidas temporárias para proteger sistemas enquanto uma solução permanente é desenvolvida.

As atualizações são de extrema importância para um melhor funcionamento dos sistemas, pois com elas há os lançamentos de software que corrigem os problemas. Atualização frequentes corrigem falhas de segurança, elas otimizam o desempenho do sistema, além de adicionar novos recursos e melhorias. Manter o software atualizado é crucial para garantir que ele continue compatível com outros sistemas e serviços e que receba suporte contínuo do fornecedor.

Os patches, são correções específicas que são aplicadas a software para corrigir problemas ou vulnerabilidades detectados. Eles geralmente se concentram em resolver questões de segurança, bugs ou falhas específicas sem alterar significativamente a funcionalidade principal do software. Os patches são muito importantes para a segurança, correção de bugs, manutenção de integridade e compatibilidade dos softwares.

O *teste de penetração*, ou *pentest* é uma prática de segurança cibernética que faz a simulação de ataques nos sistemas, redes ou aplicativos para identificar vulnerabilidades e fraquezas. Tem como objetivo é avaliar a segurança de um sistema e fornece recomendações para melhorar suas defesas antes que atacantes reais possam explorar essas fraquezas. Existem alguns tipos de teste de penetração, por exemplo em rede que avalia a segurança de redes internas e externas, identificando vulnerabilidades em dispositivos de rede, servidores e comunicações para identificar pontos de entrada e possíveis falhas em firewalls, roteadores e switches. Aplicações da web, que foca na segurança de aplicações web, incluindo servidores web, APIs e interfaces de usuário para identificar vulnerabilidades como SQL injection, cross-site scripting (XSS) e falhas de autenticação. Aplicações móveis, que avalia a segurança

de aplicativos móveis, verificando possíveis vulnerabilidades nas versões para iOS e Android para identificar falhas na lógica do aplicativo, armazenamento inadequado de dados e problemas de comunicação. Sistemas internos que analisa a segurança dos sistemas internos, como servidores e estações de trabalho para identificar vulnerabilidades nos sistemas operacionais, software e configurações. Física, avalia a segurança física de instalações, verificando a proteção contra intrusões físicas para testar o acesso físico a áreas restritas e a segurança física dos equipamentos. Social, que simula ataques baseados em engenharia social para testar a conscientização e a resposta dos funcionários para identificar como os funcionários reagem a tentativas de phishing, chamadas fraudulentas e outros ataques baseados em manipulação. O teste de penetração é importante para identificação de vulnerabilidade, avaliação de segurança, conformidade, aprimoramento da segurança, educação e conscientização.

As *atualizações e patches* são essenciais para manter a segurança, o desempenho e a funcionalidade dos sistemas de computação e redes. Elas ajudam a proteger contra ameaças, melhoram a eficiência do sistema e garantem a compatibilidade com outras tecnologias. Implementar um processo eficaz para gerenciar atualizações e patches é uma prática crítica para qualquer organização que deseja manter um ambiente de TI seguro e confiável. O *teste de penetração* é uma ferramenta essencial, recomendada para qualquer estratégia de segurança cibernética.

10. RESPOSTA A INCIDENTES

Também chamada de “Resposta a Incidentes de Segurança Cibernética”, refere-se aos processos e tecnologias de uma organização com o intuito de detectar e responder a ameaças cibernéticas, violações de segurança ou ataques cibernéticos. Tem como principal objetivo prever ataques e, consequentemente, evitá-los ou mitigá-los. Para que isso ocorra é necessária a realização de um plano de resposta a incidentes e uma análise forense.

10.1. PLANO DE RESPOSTA A INCIDENTES

Normalmente são criados e executados por uma equipe nomeada “computer security incident response team (CSIRT)” composta por stakeholders de diversas áreas da organização: o chief information security officer (CISO), security operations center (SOC) e a equipe de TI, além de representantes das áreas de liderança executiva, jurídica, recursos humanos, conformidade regulatória e gestão de riscos. Um plano de resposta a incidentes geralmente inclui:

- As funções de cada membro da equipe.
- As soluções de segurança, software, hardware e outras tecnologias envolvidas.
- Um plano de continuidade dos negócios destacando os procedimentos de restauração dos sistemas críticos e dados afetados.
- Uma metodologia detalhada de resposta a incidentes delineando as etapas a serem seguidas em cada fase do processo de resposta e quem deve executá-las.
- Um plano de comunicações para informar os líderes, funcionários, clientes e autoridades policiais a respeito dos incidentes.
- Instruções de documentação para coleta de informações e documentação de incidentes para revisão post-mortem e processos judiciais.

10.2. ANÁLISE FORENSE

Trata-se do processo de investigação e análise de incidentes de segurança com o intuito de entender o que ocorreu e como ocorreu para evitar futuros ataques. Isso ocorre através dos seguintes componentes:

10.2.1. COLETA DE EVIDÊNCIAS

Identifica e coleta evidências relevantes incluindo logs de sistema, arquivos, imagens de disco e outros dados usufruindo de ferramentas especializadas para garantir que a coleta de dados seja feita de modo preciso e legalizado.

10.2.2. ANÁLISE DE EVIDÊNCIAS

Analisa as evidências previamente coletadas para identificar a origem e o impacto do incidente tentando recriar a linha do tempo do incidente, entendendo como os ataques ocorreram e quais ações foram realizadas pelos atacantes.

10.2.3. DOCUMENTAÇÃO E RELATÓRIO

Documenta todas as descobertas durante a análise, incluindo métodos de ataque, vulnerabilidades exploradas e qualquer outra informação relevante. Com base nisso, prepara um relatório detalhado que descreve as descobertas com base na análise.

10.2.4. PREVENÇÃO DE FUTUROS ATAQUES

Identifica vulnerabilidades e falhas na segurança exploradas em meio ao incidente e, com base nisso, fornece recomendações para fortalecer as defesas e prevenir ataques semelhantes no futuro.

10.2.5. ASPECTOS LEGAIS E COMPLIANCE

Garante que a análise forense esteja em conformidade com as leis e regulamento aplicáveis e, baseado nisso, pode fornecer suporte em processos legais ajudando a construir um caso com base nas evidências coletadas e analisadas.

11. TENDÊNCIAS E TECNOLOGIAS EMERGENTES

A internet vem-se tornando cada vez mais perigosas, em que os ataques cibernéticos têm avançado rapidamente. De acordo com o levantamento de dados do site “Levantamento Digital”, “foram 1.636 ataques hackers por semana no segundo trimestre de 2024”, o que comprova esse aumento. A Inteligência Artificial é de extrema importância para detectar possíveis ameaças nos meios digitais, identificando atividades suspeitas e maliciosas, através de diferentes análises de dados. Entretanto, é necessário compreender mais sobre a sua funcionalidade e como ela se aplica na segurança desses meios.

A Machine Learning (aprendizado de máquina), é um método e uma técnica da IA responsável pela análise de dados, trazendo grande contribuição na identificação dessas ameaças, pois se trata de um algoritmo, o qual é capaz de realizar análises em tempos reais, e identificar itens suspeitos, como ciberataques. Esse método é capaz de identificar anormalidades, detectando o uso indevido de aplicativos ou tentativas de acesso não autorizado aos diferentes sistemas. Ademais, conforme a gravidade de e as ameaças aumentam, a Inteligência Artificial pode ajustar seus algoritmos e maneiras de defesa para estarem a frente das invasões e com uma maior estruturação.

A segurança em Nuvem é de extrema relevância, pois tem como função proteger os ambientes de computação de maneira, que facilita o gerenciamento para scanear vulnerabilidades e prevenir certas ameaças, além de detectar anomalias e riscos, através de algoritmos. Consequentemente, o indivíduo pode receber alertas de violações em seu perfil. Ademais, muitas empresas fazem o seu uso, para auxiliar em sua segurança, como o Google, Netflix, Sportify, Amazon, entre outros.

Além disso, A Internet das Coisas (IoT) trouxe grandes desafios para manter a segurança nos meios digitais, se tornando cada vez mais crítica, devido ao crescendo do aumento de acesso, também se expandiu o número de ataques cibernéticos. Sendo assim, as organizações começaram a desenvolver normas de segurança para prevenir esses riscos, como exemplo disso possui a norma IEC 62443, que tem como objetivo, fornece diretrizes de segurança para sistemas de automatização industriais.

Diante do aumento exponencial de ataques cibernéticos e da crescente complexidade das ameaças digitais, a integração de Inteligência Artificial e segurança em nuvem torna-se indispensável. A aplicação de Machine Learning para análise em

tempo real e detecção de anomalias proporciona uma defesa proativa contra intrusões e vulnerabilidades. A segurança em nuvem, por sua vez, oferece uma abordagem eficaz para gerenciar e proteger dados, enquanto a expansão da Internet das Coisas (IoT) reforça a necessidade de normas de segurança robustas. Em conjunto, essas estratégias garantem uma proteção eficaz contra riscos emergentes, assegurando a integridade e a continuidade dos sistemas digitais em um cenário cada vez mais desafiador.

12. SEGURANÇA FÍSICA E AMBIENTAL

Se resume na proteção contra desastres naturais e falhas de infraestrutura através da cibersegurança, envolvendo a combinação de medidas de segurança física, planejamento de continuidade de negócios e práticas específicas para garantir a resiliência e a recuperação eficaz dos sistemas e dados.

Algumas abordagens que norteiam um bom desempenho na proteção de infraestrutura física e contra desastres ambientais envolvem:

12.1. BUSINESS CONTINUITY PLAN

O plano de continuidade de negócios (BCP) se baseia em um plano abrangente que inclua procedimentos para resposta a desastres naturais e falhas de infraestrutura. O plano deve cobrir a recuperação de sistemas, dados e operações críticas. Cabe realizar uma avaliação para identificar e priorizar as funções delicadas e os recursos essenciais que precisam ser protegidos e recuperados em caso de desastre.

12.2. BACKUPS E RECUPERAÇÃO DE DADOS

É necessário realizar backups regulares e automáticos dos dados críticos. Armazene cópias de backup em locais seguros e separados da infraestrutura principal para proteger contra lapsos físicos e desastres. Ademais, é preciso testar regularmente os processos de recuperação de dados para garantir que os backups sejam funcionais e que a recuperação possa ser realizada de maneira mais rápida e eficaz.

12.3. SEGURANÇA DE SISTEMAS

A Utilização da segmentação de redes, que consiste em uma técnica usada para dividir uma rede maior em várias sub-redes menores ou "segmentos", é ótima para isolar sistemas críticos e proteger a comunicação entre eles. Isso pode limitar o impacto de falhas e ataques cibernéticos significativamente. Para aumentar o nível de segurança, é importante a implementação de ferramentas de monitoramento para detectar e responder a falhas e incidentes de segurança em tempo real. Isso inclui a vigilância de redes, sistemas e dados.

12.4. PROTEÇÃO CONTRA ATAQUES CIBERNÉTICOS

O uso de criptografia protege dados em trânsito (durante a transmissão entre dois pontos) e em repouso (dados armazenados). E a criptografia nada

mais é que um recurso que transforma informações legíveis em um formato ilegível que só pode ser lido ou revertido por quem tem a chave correta. Isso ajuda a garantir a confidencialidade e integridade dos dados, mesmo em caso de ataques ou falhas.

12.5. ATUALIZAÇÃO DE PLANOS

É sempre muito importante manter planos e procedimentos atualizados com base em mudanças na infraestrutura, novas ameaças e lições aprendidas de exercícios e incidentes anteriores.

12.6. SEGURANÇA EM NUVEM

Se você utiliza serviços em nuvem, certifique-se de que os dados estão protegidos com criptografia e que o provedor de nuvem tem medidas adequadas de continuidade de negócios e recuperação. Do mesmo modo, nunca se esqueça de avaliar as práticas de segurança de fornecedores e prestadores de serviços que têm acesso físico às suas instalações ou equipamentos.

A proteção da infraestrutura física é uma parte crucial da cibersegurança, pois garante que o hardware e os recursos físicos que suportam sistemas e redes permaneçam seguros contra ataques e acessos não autorizados. Essas são algumas outras precauções conhecidas que atuam como prevenções contra violações físicas, mais especificamente:

12.7. SEGURANÇA DE AMBIENTES

Nesse tópico, um dos métodos mais usados é a instalação de câmeras de segurança em áreas críticas para monitorar atividades e registrar eventos. Além disso, no que diz respeito às máquinas de trabalho, é mister manter controle sobre condições ambientais como temperatura, umidade e fumaça para proteger os equipamentos contra danos físicos e falhas. Ainda nesta questão, a busca por supressores de incêndio se torna também importante, e esses devem ser especiais para ambientes de T.I., não danificando eletrônicos (como sprinklers ou sistemas de gás inerte).

12.8. SEGURANÇA DE HARDWARE

Cabe o uso de trancas físicas e suportes para proteger servidores, roteadores e outros equipamentos contra roubo e acesso não autorizado. Um inventário detalhado e etiquetagem de todos os equipamentos para facilitar a rastreabilidade e prevenir perdas são igualmente aconselháveis.

12.9. PROTEÇÃO CONTRA ATAQUES FÍSICOS

Proteger o perímetro das instalações com cercas, barreiras e controle de acesso nas entradas e saídas, assim como as redes de energia e os sistemas de backup de energia (como UPS e geradores) para garantir a continuidade operacional em caso de falhas de energia é fundamental.

13. EDUCAÇÃO E CONSCIENTIZAÇÃO

É de extrema relevância o conhecimento do ambiente digital, pois através do crescente aumento de acesso nesse meio, também houve avanços nos ataques cibernéticos, por isso é importante os indivíduos terem a consciência dos riscos que podem estar correndo, diante da falta de experiência com tais práticas. Dessa forma deve estar atento na proteção de suas informações pessoais.

Além do mais, o e-mail é uma ferramenta crucial para a comunicação empresarial, mas também é um alvo comum para crimes cibernéticos. Entretanto, o Phishing, ransomware e malware são as principais ameaças. O Phishing usa engenharia social para enganar usuários a revelarem informações sensíveis, enquanto o ransomware criptografa dados e exige resgate, já malware pode danificar ou roubar dados através de downloads inseguros e e-mails de spam. Ademais, ameaças internas podem surgir de funcionários ou parceiros que têm acesso a dados críticos. Para mitigar esses riscos, é essencial adotar medidas como treinamento contínuo, backups regulares, uso de antivírus e controles de acesso rigorosos.

Os programas de conscientização são de extrema relevância, pois tem como função diminuir as ameaças que podem ocasionar em violações de dados ou ataques cibernéticos. Ademais, irá favorecer as empresas, contar com colaboradores que possuem práticas com o meio e habilidades de lidarem com a implementação de atividades comerciais seguras, consequentemente, terão mecanismos de defesas maiores para proteger os negócios da empresa. Sendo assim, as organizações necessitam de estrutura capazes de conscientizar os funcionários sobre tais riscos, melhorando em suas decisões, e reduzindo a chance de algum incidente nos meios tecnológicos.

Ademais, a sociedade deve ter conhecimento das inúmeras vantagens para a segurança de todos os cidadãos que acessam o ambiente digital. Dessa forma, irá trazer uma melhor reputação para as empresas, as quais irão estar preparadas para administrar e solucionar qualquer tipo de intervenção. Além disso, também trará maior confiança para os funcionários, reduzindo a possibilidade de erro daquela organização. De acordo com a segunda edição do “Barômetro da Segurança digital”, foi revelado que 64% das empresas brasileiras são alvo de fraudes e ataques digitais com média ou alta frequência, por isso é indispensável que os meios que mitigam ameaças. Além disso, é importante as empresas estarem de acordo em conformidade

com a LGPD (Lei Geral de Proteção de Dados), proporcionando, uma proteção dos direitos fundamentais de liberdade e privacidade da personalidade de cada indivíduo.

O aumento do acesso tecnológico trouxe também um crescimento nos ataques cibernéticos, tornando essencial a conscientização sobre segurança digital. O e-mail, apesar de ser uma ferramenta fundamental para a comunicação, é frequentemente alvo de ataques como phishing, ransomware e malware. Para mitigar esses riscos, é crucial implementar medidas como treinamento contínuo, backups regulares e uso de antivírus. Outrossim, programas de conscientização ajudam a proteger dados, melhoram a segurança das empresas e garantem conformidade com leis como a LGPD. Em um cenário onde grandes empresas brasileiras enfrentam ataques frequentes, adotar práticas de segurança eficazes é vital para manter a integridade e a confiança no ambiente digital.

14. CONCLUSÃO

Em suma, a **cibersegurança** é essencial para proteger informações sensíveis, sistemas e redes contra uma variedade de ameaças digitais cada vez mais sofisticadas decorrentes do panorama de um mundo tão conectado quanto o que vivemos. Com o crescente volume de dados gerados e armazenados em ambientes digitais, bem como a maior dependência da tecnologia em todas as esferas da sociedade, a segurança cibernética tornou-se, não erroneamente, uma prioridade para empresas, governos e indivíduos.

As medidas de cibersegurança, como **segmentação de redes**, **criptografia de dados em trânsito e em repouso**, **controle de acessos**, **firewalls** e **monitoramento contínuo**, são pilares fundamentais para garantir a proteção de sistemas e a confidencialidade, integridade e disponibilidade dos dados. Todas estas ferramentas corroboram, mutuamente ou não, para a proteção contra os vigentes inúmeros ataques diários aos quais podemos estar submetidos, como **phishing**, **malwares**, **ransowares** e **DDoS**.

À medida que as ameaças evoluem, as defesas cibernéticas também precisam ser continuamente aprimoradas e adaptadas. Sem uma estratégia robusta de cibersegurança, organizações e indivíduos ficam vulneráveis a violações de dados, ataques de ransomware, fraudes e perdas financeiras muito significativas. Assim, adotar uma abordagem proativa, com o uso de diversas camadas de proteção e boas práticas de segurança, é essencial para mitigar riscos e preservar a confiança no ambiente digital, não apenas na esfera empresarial, mas em todas elas

15. REFERÊNCIAS BIBLIOGRÁFICAS

Equipe do IBM. **O que é resposta a incidentes?** Disponível em: <https://www.ibm.com/br-pt/topics/incident-response>. Acesso em: 30 jul. 2024.

Equipe do IBM. **O que é um ataque cibernético?** Disponível em: <https://www.ibm.com/br-pt/topics/cyber-attack>. Acesso em: 29 ago. 2024.

Equipe da Microsoft. **O que é controle de acesso?** Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-access-control>. Acesso em: 24 fev. 2021.

Equipe da Fortinet. **Tipos de ataque cibernético.** Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/types-of-cyber-attacks>.

RAMOS, Helber. **7 tipos de ataques cibernéticos mais comuns nas empresas.** Disponível em: <https://blog.tripla.com.br/blog-ataques-ciberneticos/>. Acesso em: 22 dez. 2023.

Equipe da Check Point. **Tipos de ciberataque.** Disponível em: <https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/>. Acesso em: 22 fev. 2024.

FLOWTI, Equipe De Conteúdo . Conheça as principais sanções para quem descumpre a LGPD: A Lei Geral de Proteção de Dados, desde fevereiro de 2023, passa a ser apoiada por um Regulamento de Dosimetria que prevê sanções administrativas para quem descumprir a lei. **Flowti,** 2024. Disponível em: https://flowti.com.br/blog/conheca-as-principais-sancoes-para-quem-descumpre-a-lgpd#:~:text=Por%C3%A9m%2C%20nos%20casos%20de%20m%C3%A1,teto%20de%20R%24%2050%20milh%C3%B5es.. Acesso em: 06 set. 2024.

NONES, Fernanda. LGPD: o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing e vendas: Entenda como a Lei Geral de Proteção de Dados Pessoais afeta a forma com que as empresas e organizações captam, armazenam e utilizam dados de seus clientes, tanto no meio online quanto offline; conheça também um curso da RD University sobre LGPD. RD STATION, 2022. Disponível em: https://www.rdstation.com/blog/marketing/o-que-e-lgpd/. Acesso em: 06 set. 2024.

DE OLIVEIRA, Vinícus . LGPD: Entenda tudo sobre a lei que protege seus dados... - Veja mais em https://www.uol.com.br/tilt/faq/lgpd-entenda-tudo-sobre-a-lei-que-protege-seus-dados.htm?cmpid=copiaecola. Tilt Uol, 2021. Disponível em: https://www.uol.com.br/tilt/faq/lgpd-entenda-tudo-sobre-a-lei-que-protege-seus-dados.htm. Acesso em: 06 set. 2024.

O que é a Lei de Privacidade do Consumidor da Califórnia (CCPA)?. A Lei de Privacidade do Consumidor da Califórnia (CCPA) é uma lei estadual da Califórnia promulgada em 2020 que protege e faz cumprir os direitos dos residentes da Califórnia em relação à privacidade das informações pessoais (IP) dos consumidores. IBM. Disponível em: https://www.ibm.com/br-pt/topics/ccpa-compliance. Acesso em: 06 set. 2024.

TOTVS, Equipe. GDPR: o que é, importância e impactos para brasileiros. **TOTVS,** 2023. Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/gdpr/#:~:text=A%20GDPR%20entrou%20em%20vigor,a%20respeito%20das%20informa%C3%A7%C3%B5es%20pessoais.. Acesso em: 06 set. 2024.

GDPR [Guia Completo]: tudo que você precisa saber sobre a Lei. **FIA,** 2019. Disponível em: https://fia.com.br/blog/gdpr/. Acesso em: 06 set. 2024.

Lei Geral de Proteção de Dados Pessoais (LGPD). **Gov.br.** Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 06 set. 2024

O que é segurança de nuvem? **Check Poin.** Disponível em: https://www.checkpoint.com/pt/cyber-hub/cloud-security/what-is-cloud-security/#:~:text=Prote%C3%A7%C3%A3o%20de%20dados%20aprimorada%20com,configurados%20e%20encerramento%20de%20recursos. Acesso em: 16 set. 2024.

EQUIPE, Verx. A IMPORTÂNCIA DA CONSCIENTIZAÇÃO E EDUCAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO. **Verx,** 2023. Disponível em: https://www.verx.com.br/a-importancia-da-conscientizacao-e-educacao-dos-usuarios-sobre-seguranca-da-informacao/. Acesso em: 16 set. 2024.