IMPORTÂNCIA E MÉTODOS DE PROTEÇÃO DE DADOS

Data de aceite: 03/06/2024

Diego Bandeira
IFSul Câmpus Santana do Livramento

Diogo Machado
IFSul Câmpus Santana do Livramento

Rebeca Fiss
IFSul Câmpus Santana do Livramento

RESUMO: A segurança de dados de clientes em um centro de dados, banco de dados é um assunto crucial para o desenvolvimento de um sistema ou aplicação, seja um site ou um aplicativo. A proteção de dados desempenha um papel fundamental na sociedade digital de hoje, onde a troca e o armazenamento de informações ocorrem em larga escala. A proteção de dados preserva a privacidade, confidencialidade e integridade das informações pessoais e sensíveis. Medidas de segurança como criptografia, autenticação forte e práticas de codificação segura evitam o acesso não autorizado, exploração de vulnerabilidades e vazamento de dados, construindo confiança entre usuários, empresas e instituições.

PALAVRAS-CHAVE: Segurança, dados, ataques, roubo

IMPORTÂNCIA DA PROTEÇÃO DE DADOS

A segurança de dados de clientes em um centro de dados, banco de dados é um assunto crucial para o desenvolvimento de um sistema ou aplicação. Seja este sistema um site ou aplicativo. Por ser uma questão tão importante, é comum encontrar diversas ferramentas e métodos especificamente voltados à defesa dos dados armazenados.

A proteção de dados desempenha um papel fundamental na sociedade digital de hoje, onde a troca e o armazenamento de informações ocorrem em larga escala. A importância da proteção de dados reside na preservação da privacidade, confidencialidade e integridade das informações pessoais e sensíveis. Através de medidas de segurança adequadas, como criptografia, autenticação forte e práticas de codificação segura, é possível evitar o acesso não autorizado, a exploração de vulnerabilidades e o vazamento de dados. Além de salvaguardar os direitos individuais, a proteção de dados

também contribui para a construção da confiança entre usuários, empresas e instituições, promovendo a inovação segura e o desenvolvimento sustentável em um mundo cada vez mais interconectado.

MÉTODOS EFICIENTES PARA DEFENDER INFORMAÇÕES CONFIDENCIAIS NA INTERNET

Quando enviamos dados como e-mail e senha para um formulário na internet, essas informações costumam passar por diversos processos para que cheguem com segurança ao local em que podem ser recuperados posteriormente através de requisições, funcionando através de uma aplicação com conexão à internet, com objetivo de validar um login. Já esses locais, conhecidos como bancos de dados, onde todas as informações presentes neles são armazenadas, sempre devem possuir alguma camada de proteção pela qual devem passar.

VALIDAÇÃO DE ENTRADA DE DADOS

A validação de dados no lado do cliente e no lado do servidor são duas abordagens distintas, mas complementares, para garantir a integridade e segurança dos dados em um sistema web. A validação de dados no lado do cliente é rápida e interativa, fornecendo *feedback* instantâneo aos usuários, mas não é suficiente para garantir a segurança dos dados. A validação de dados no lado do servidor é a linha de defesa final e deve ser sempre realizada, independentemente da validação no lado do cliente. Idealmente, as duas abordagens devem trabalhar juntas para criar uma experiência de usuário suave e segura. A validação no lado do cliente melhora a usabilidade, enquanto a validação no lado do servidor garante que apenas dados válidos e seguros sejam processados e armazenados.

A validação de dados de formulários é um processo que verifica se os dados inseridos pelo usuário em um formulário estão no formato correto e dentro das restrições definidas pela aplicação. Utilizando como exemplo uma página aberta em um navegador, a validação de campos em branco, informações erradas nos formulários no lado do cliente é feita antes de enviar os dados para o servidor. Isso permite que o usuário corrija os dados imediatamente, sem esperar pela resposta do mesmo. Se os dados chegarem ao servidor e forem rejeitados, isso causará um atraso perceptível por causa da ida e volta entre o cliente e o servidor e o processo esperado não irá acontecer, como a tentativa de um login com credenciais incorretas.

No entanto, a verificação de informações em um formulário pelo front-end (aplicativos, páginas abertas no navegador) é relativamente fácil de contornar, por isso é necessário haver uma segunda camada de verificação. Esta camada se encontra em uma área que não pode ser acessada pelo usuário diretamente, sendo esta o servidor. A validação de informações em um servidor é um processo que verifica se os dados enviados

pelo usuário em um formulário ou em outra forma de requisição estão de acordo com as regras e os critérios definidos pela aplicação. Isso é importante para garantir a segurança e a consistência dos dados que serão armazenados ou processados pelo servidor. A validação de informações em um servidor é uma medida de segurança essencial para qualquer aplicação web justamente por ser eficiente em dificultar o acesso a dados por um indivíduo mal-intencionado.

PRINCÍPIO DO MENOR PRIVILÉGIO

O princípio do menor privilégio, também conhecido como “princípio do privilégio mínimo” ou “princípio do mínimo necessário”, é um conceito fundamental em segurança da informação e gerenciamento de acesso. Esse princípio se baseia na ideia de que indivíduos, programas ou sistemas devem receber apenas os privilégios ou permissões mínimos necessários para realizar suas tarefas específicas. Um sistema de computador ou aplicação pode permitir que exitam diferentes níveis de acesso e permissões. Cada usuário ou componente do sistema recebe acesso apenas ao que é estritamente necessário para realizar suas funções. Isso ajuda a limitar os riscos e reduzir a superfície de ataque, minimizando as oportunidades para abuso ou falhas de segurança.

Para aplicar este princípio, é necessário que hajam alguns níveis de permissão como por exemplo:

- Um usuário sem registro: Os visitantes do site que ainda não se registraram não têm acesso a recursos sensíveis, como informações de pagamento ou configurações da conta. Eles podem apenas visualizar produtos cadastrados no site ou aplicativo.
- Usuário cadastrado: Quando alguém se registra, ele recebe acesso adicional para realizar compras, adicionar itens ao carrinho e configurar sua conta.
- Administradores: A equipe de administração tem acesso total à aplicação, incluindo dados de clientes, configurações do site e funções de manutenção.

Cada usuário apenas terá acesso a aquilo que realmente precisa para desempenhar alguma função dentro daquele sistema. Em resumo, o princípio do menor privilégio é uma estratégia de segurança essencial que ajuda a reduzir riscos e proteger sistemas, garantindo que os usuários e componentes do sistema tenham apenas o acesso necessário para realizar suas funções específicas, limitando, assim, os danos potenciais em caso de falhas ou ataques.

CRIPTOGRAFIA

Uma das formas mais utilizadas para garantir uma camada extra de segurança em sistemas de informação, a criptografia é uma parte essencial no processo de proteção de dados, consistindo na arte de comunicar, escrever, desenvolver formas de transmitir mensagens de maneira que apenas o destinatário pretendido possa compreender. No nosso caso, maneiras de transmitir ou armazenar dados de forma que eles não possam ser interceptados ou compreendidos em sua totalidade por pessoas mal-intencionadas. Assim como podem ser usados para garantir a integridade de certos arquivos ou dados importantes em processos computacionais. Um exemplo seriam as senhas que são usadas em redes sociais, comumente armazenadas em Bancos de Dados não em sua forma legível mas encriptadas, assim dificultando o roubo de informações sensíveis.

A criptografia funciona transformando os dados em um formato ilegível chamado de cifra, que só pode ser revertido para o formato original usando uma chave secreta. Existem dois tipos principais de criptografia: simétrica e assimétrica. A criptografia simétrica usa a mesma chave para cifrar e decifrar os dados. Enquanto a assimétrica é mais complexa, sendo dividida em duas partes chamadas de chave pública e chave privada. De uma forma bastante simples, transforma um caracter “A” em uma sequência de caracteres “YDNTQIEURHJJ”, ou uma sequência de caracteres (criptografados ou não) em mais um texto cifrado. Apenas um programa específico ou um código executável em uma máquina que entende como funciona aquela criptografia poderá decifrar o texto criptografado em questão.

Esta forma de proteção de dados é mais interessante em ser usada na troca de mensagens por aplicativo ou quando estiver acessando um site e ser aplicada a criptografia quando é feita uma requisição para acessar os sites na web. Para guardar informações em bancos de dados, há uma forma mais eficiente que pode ser utilizada. Nesse caso, hashes são muito mais eficientes para proteger dados pela simples razão de não poderem mais ser recuperados após serem criptografados. Isso porque um hash não é uma simples sequência de caracteres que é atribuído a cada elemento de um texto. Os hashes são melhores nesse quesito também por sempre possuírem um comprimento fixo e possuírem letras e números atribuídos a cada texto encriptado aleatoriamente. O fato de ser impossível recuperar um texto criptografado por hash não invalida a capacidade de validar uma senha que está criptografada no banco de dados. Já que para conferir se a senha digitada pelo usuário está certa, basta apenas pegar a senha que o cliente digitou no formulário da página e comparar com a senha criptografada por hash na base de dados do servidor.

ATUALIZAÇÕES E PATCHES

Um aspecto muito subestimado em Sistemas computacionais são as atualizações que apesar de serem desagradáveis em alguns momentos trazem diversos benefícios que podem ser úteis na proteção de seus sistemas/dados. Um dos principais seria a Atualização de ameaças pois conforme as tecnologias vão se aprimorando acabam surgindo ameaças igualmente danosas e com cada atualização o sistema/software se torna mais 'preparado' para lidar com tais ameaças. Claro que temos o aspecto corretivo de patches e atualizações, no caso de erros ou bugs encontrados na vida útil de uma versão a próxima certamente os corrigirá, e quaisquer vulnerabilidades causadas por tais erros não serão uma preocupação novamente.

Como as atualizações e patches são linhas de código novas ou atualizadas que determinam o funcionamento de um sistema operacional, plataforma ou aplicação. Eles são importantes para corrigir erros, falhas e vulnerabilidades que podem comprometer a segurança do software. Os patches podem ser classificados em diferentes tipos, de acordo com sua finalidade e urgência. Por exemplo, os patches de segurança são aqueles que visam proteger o software contra ataques maliciosos, como vírus, hackers e malware. Eles devem ser aplicados o mais rápido possível, pois representam um alto risco para os dados e a integridade do sistema. Os patches também podem melhorar o desempenho e a usabilidade do software, adicionando novos recursos ou otimizando as funcionalidades existentes. Esses tipos de patches podem ser opcionais ou recomendados, dependendo da necessidade e da preferência do usuário.

AUTENTICAÇÃO FORTE

Relativamente recente, a famosa Autenticação de dois fatores utilizada frequentemente em Redes Sociais ou na Google por exemplo que consiste no uso de um fator externo para autenticar o acesso a serviços ou a própria conta. Podendo ser utilizada com uma Senha, PIN ou outra informação compartilhada do usuário com o sistema para liberar o acesso; Com um dispositivo físico como um celular por meio de código ou confirmação; Ou até mesmo com o uso de biometria, muito comum em apps bancários, assim disponibilizando um recurso a mais para a proteção de contas contra roubo/hacking, pois se qualquer atividade suspeita ocorrer sem a confirmação do 2º fator não haverá acesso ao recurso.

GERENCIAMENTO DE SESSÕES

Sessões são uma parte essencial de Sistemas e Ambientes Corporativos, logo a manutenção destas não pode ser deixada para depois, o gerenciamento de sessões auxilia e adiciona uma camada a mais de segurança ao seu sistema. Iniciando com a autenticação/autorização que normalmente se dá por meio de credenciais como login e senha, assim restringindo o acesso a apenas pessoal autorizado, logo após pode ser gerado um identificador único para tornar possível o monitoramento das atividades de um usuário específico, assim como o tempo de uso.

PREVENÇÃO CONTRA CSRF (CROSS-SITE REQUEST FORGERY)

Uma das técnicas mais utilizadas por criminosos cibernéticos para adquirir dados, informações ou contas é a prática de CSRF, que consiste em utilizar de vulnerabilidades presentes em sites confiáveis para atrair usuários legítimos a lhe entregarem seus dados, normalmente sem mesmo nem perceber por causa da natureza 'confiável' dessa prática. Por meio de links, elementos da interface e até formulários eles são capazes de extrair dados de pessoas que não tem a menor ideia que estão sendo enganadas.

Para se prevenir de tais ataques é necessário seguir algumas regras, começando pela REST API que consiste em diretrizes para o uso de métodos em sites, GET deve ser utilizado em casos onde só se acessam dados localizados no servidor(eliminando um dos principais meios de CSRF), POST é usado em casos onde se enviam dados ao/do servidor(aumentando a segurança das transações). Outro método para prevenir ataques são o uso de Cookies anti- csfr que geram um valor único que é utilizado para autenticar a comunicação entre usuário e servidor.

PROTEÇÃO DE DADOS SENSÍVEIS

Quando se trabalha com dados sensiveis é importante que eles estejam em um ambiente seguro que não apresente vulnerabilidades, sejam dados pessoais ou dados de outros indivíduos, para isso se apresentam algumas opções para proteção desse tipo de dado, o uso das varias técnicas apresentadas acima são uma delas, elas podem diminuir o risco do possível vazamento desses dados e aumentar o nivel de segurança do ambiente em que estão armazenados. Outra parte importante deste processo é o treinamento da equipe humana pois não existem ameaças somente no mundo digital, um 'hacker social' habilidoso pode conseguir acesso direto ao sistema ou a dados confidenciais assim ultrapassando quaisquer mecanismos de defesa presentes em um ambiente digital, assim se torna imperativo o treinamento do contingente humano.

TESTES DE SEGURANÇA

É importante assegurar a segurança de seu sistema e de sua empresa, e para isso existem os Testes. De nada adianta possuir um sistema de segurança de alto nível e ele cair na primeira 'situação estressante' isso se aplica também para sua equipe. Existem vários tipos de testes possíveis eles podem ser divididos em Testes para o Sistema e Testes para a Empresa: Nos voltados para o Sistema nós temos o 'Red Team' onde um grupo de 'hackers éticos' é contratado pela empresa para simular ataques em seu Sistema descobrindo possíveis falhas e informando o nível de segurança da informação da empresa. Passamos para o teste de invasão mais conhecido como 'pentest' onde o processo é similar ao Red Team mas se utilizam de técnicas de hacking reais para descobrir vulnerabilidades no sistema. Em ares mais simples temos o Teste de Vulnerabilidade onde um programa é utilizado para detectar possíveis falhas no sistema. Passando para os Testes para empresa temos a Avaliação de Postura que avalia as politicas contra ciberataques implementadas pela empresa e o cumprimento delas pelos funcionários, são também consideradas as ações da empresa acerca dessas regras como Palestras, Reuniões, Aulas.

LOGS E MONITORAMENTO

Logs são essenciais para a manutenção de aplicativos e sistemas sendo o principal meio de identificação de erros e bugs. Eles consistem no armazenamento de eventos em um arquivo de texto funcionando como um histórico das ações realizadas em um ambiente digital, normalmente incluindo data e hora para facilitar o monitoramento das ações, podendo ser utilizados para monitorar o funcionamento de um aplicativo ou as ações de um usuário no sistema assim diminuindo a ocorrência de erros se devidamente utilizado. O monitoramento desses arquivos podem servir como provas confiáveis no caso de modificações ou situações indesejadas em um sistema.

POLÍTICAS DE PRIVACIDADE E CONSENTIMENTO

Política de privacidade é um documento que informa ao usuário como a empresa realiza o tratamento de dados pessoais, ou seja, como coleta, usa, armazena e protege essas informações. Consentimento é a manifestação livre, informada e inequívoca pela qual o usuário autoriza a empresa a tratar seus dados. Esses conceitos podem ser aplicados a uma aplicação para melhorar a sua segurança na internet, seguindo as regras e princípios da Lei Geral de Proteção de Dados (LGPD) e outras normas existentes.

Uma política atualizada, detalhada e bem documentada e organizada é eficiente para a proteção dos dados, pois estabelece um padrão para a empresa, organização que usa um serviço e/ou aplicação com o objetivo de servir como base para as decisões sobre a segurança da empresa. Para uma elaboração de uma política de segurança e padronizar os sistemas e normas da organização ou empresa, é preciso seguir uma série de passos. Tais como:

- Definir o escopo, os objetivos, os princípios e as diretrizes da política de segurança;
- Analisar os riscos e as vulnerabilidades da organização em relação à segurança;
- Estabelecer as responsabilidades e as atribuições dos gestores, dos colaboradores e dos terceiros envolvidos na política de segurança;
- Elaborar um plano de ação com as medidas preventivas, corretivas e emergenciais para garantir a segurança da organização;
- Implementar, monitorar, revisar e atualizar a política de segurança periodicamente.

SEGURANÇA DO BANCO DE DADOS

A segurança de um banco de dados é outro elemento importante que entra em ação quando informações são enviados por um formulário e armazenados em um local pré-determinado pela aplicação. Também vale destacar que armazenamento dos dados deve permanecer sobre constante vigilância contra possíveis vulnerabilidades após a inserção de qualquer tipo de informação. As maneiras mais eficientes de proteger um banco de dados dependem de vários fatores, como o tipo de banco de dados, o sistema de gerenciamento de banco de dados (DBMS), o aplicativo associado, o servidor físico ou virtual do banco de dados, a infraestrutura de computação e rede e as ameaças potenciais.

O comprometimento pode gerar uma perda enorme tanto para os usuários quanto para a empresa. Consequências de uma violação podem incluir perda de propriedade intelectual, danos à reputação da marca, interrupção dos negócios, multas ou penalidades por não conformidade e custos de reparação e notificação. As ameaças à segurança do banco de dados podem vir de fontes internas ou externas, e podem explorar vulnerabilidades no software, na rede, nos aplicativos ou nos dispositivos. Podem ser causadas pela falta de patches, injeção SQL, estouro de buffer, malware, ataques DoS/DDoS e backups inseguros atingidos por um ataque cibernético não previsto. Métodos como:

Separar os servidores de banco de dados dos servidores web, para evitar que um ataque bem-sucedido ao servidor web comprometa o banco de dados.

- Usar firewalls de banco de dados e de aplicação web para filtrar o tráfego malicioso e bloquear tentativas de injeção de SQL ou outros ataques comuns.
- Endurecer o banco de dados, desabilitando ou removendo recursos desnecessários, configurando as permissões corretas e aplicando as atualizações de segurança.
- Realizar testes de penetração para verificar quão seguro é o banco de dados ou usar ferramentas de varredura de vulnerabilidades.

- Criptografar os dados em repouso e em trânsito é uma outra maneira extremamente útil para evitar que sejam lidos por terceiros em caso de roubo ou interceptação.

DESENVOLVIMENTO SEGURO

A maior importância de treinar uma equipe para manter a segurança de dados é evitar ou minimizar os danos causados por ataques cibernéticos e violações de dados que podem comprometer a reputação, a confiança, a competitividade e a conformidade da empresa e suas aplicações na internet. Além disso, treinar uma equipe para manter a segurança de dados pode melhorar a produtividade, a eficiência a inovação por parte dos funcionários, pois eles se sentem mais capacitados, responsáveis e valorizados pela empresa. Portanto, treinar uma equipe para manter a segurança de dados é um investimento que traz benefícios tanto para a empresa ou grupo atuando no trabalho.

A segurança de uma aplicação depende de vários fatores, como o tipo de aplicação, o ambiente de desenvolvimento, as ferramentas utilizadas, as ameaças potenciais e os requisitos regulatórios. Não há uma única estratégia que seja a melhor para todos os casos, mas existem algumas práticas recomendadas que podem ajudar a treinar uma equipe para que implemente soluções de segurança para uma aplicação. Dentre elas está a abordagem de DevSecOps, que integra a segurança em todas as fases do ciclo de vida do desenvolvimento, desde o planejamento até a implantação e a manutenção. Isso permite que a equipe identifique e corrija as vulnerabilidades mais cedo, reduzindo os custos e os riscos. O método de DevSecOps também implica a cooperação entre os programadores, os especialistas em segurança e os consumidores, para assegurar que as soluções de segurança satisfaçam os requisitos.

PREPARAÇÃO PARA INCIDENTES

Um plano de resposta a incidentes é um conjunto de instruções que ajuda a equipe de TI a detectar, responder e se recuperar de incidentes de segurança que afetam diretamente os dados de um servidor. Um plano de resposta a incidentes é importante porque permite que, em caso de um ataque cibernético, o pessoal e os procedimentos adequados estejam em prática para lidar efetivamente com a ameaça. Este plano pode envolver diversas etapas diferentes que vão desde a identificação do problema até recuperação do sistema em caso de uma perda grave. Entrando em mais detalhes, as etapas para organizar um plano de resposta a qualquer ataque contra um sistema e prevenir-se de que seus dados sejam comprometidos seguem essa sequência:

- Preparação: Esta etapa consiste em reconhecer os componentes essenciais da aplicação web, os pontos críticos de falha, as equipes e as funções encarregadas pela resposta, as ferramentas e os recursos imprescindíveis para a detecção e a análise dos incidentes, e os planos de cópia de segurança e recuperação dos dados.
- Identificação: Esta etapa consiste em confirmar e validar um incidente de segurança, determinar sua abrangência, impacto e severidade, e comunicar as informações pertinentes às partes envolvidas.
- Contenção: Esta etapa consiste em isolar o sistema ou a rede afetada pelo incidente, para impedir que ele se propague ou cause mais prejuízos. Isso pode envolver desconectar o sistema da internet, bloquear o acesso aos dados delicados ou desativar certas funções da aplicação.
- Erradicação: Esta etapa consiste em eliminar os elementos nocivos do sistema ou da rede, como malware, portas dos fundos, arquivos danificados ou credenciais violadas. Isso pode envolver limpar ou restaurar o sistema para um estado anterior ao incidente.
- Recuperação: Esta etapa consiste em restaurar o sistema ou a rede para um estado normal e operacional, verificando se não há mais vestígios do incidente e monitorando o desempenho e a segurança da aplicação.
- Análise: Esta etapa consiste em revisar o incidente, identificar suas causas principais, avaliar sua eficácia e eficiência da resposta, documentar as lições aprendidas e as recomendações para melhorias futuras.

CONCLUSÕES

Em um mundo cada vez mais digitalizado e interconectado, a proteção de dados se tornou uma preocupação crítica para organizações e indivíduos. Este artigo explorou métodos eficientes para proteção de dados, abordando tópicos cruciais para a segurança dos sistemas e dados guardados nele. A proteção de dados é um desafio contínuo que exige uma abordagem multifacetada. Os métodos eficientes abordados neste artigo, quando implementados de maneira integrada e consistente, contribuem para a construção de um ambiente de dados seguro e confiável. À medida que as ameaças digitais continuam a evoluir, a atualização constante dessas práticas se torna crucial para manter a integridade e a confidencialidade dos dados em um mundo cada vez mais digital.

REFERÊNCIAS

Shannon, C. (1948). A Mathematical Theory of Communication Shannon, C. (1949). Communication Theory of Secrecy Systems

Borgis, E. (2020). Qual a importância da atualização de softwares, navegadores e sistemas operacionais? Retirado de: https://tripla.com.br/atualizacao-de-softwares-navegadores-e-sistemas-operacionais/

OneSpan (2022). Autenticação forte. Retirado de: https://www.onespan.com/#:~:text=O%20que%20é%20autenticação%20forte,e%20a%20autorização%20da%20transação.

BugHunt (2022) 5 tipos de testes de segurança. Retirado de: https://blog.bughunt.com.br/tipos-de-testes-de-seguranca/

Netsupport. (2021). Gerenciamento de logs: 3 boas práticas para proteger sua rede Retirado de: https://netsupport.com.br/gerenciamento-de-logs/

The TechCave. (2021). CSRF Explained Retirado de: https://youtu.be/eHqbh0kyRYk?si=iOAO_hrMkisbOae1

docusign.com.br (2021). Como montar uma política de privacidade? Veja 6 dicas! Retirado de: https://www.docusign.com.br/blog/como-montar-uma-politica-de-privacidade

Marcondes, JS. (2022). Política de Segurança: O que é, Qual sua Importância, Como criar. Retirado de: https://gestaodesegurancaprivada.com.br/politica-de-seguranca-o-que-e-qual-sua- importancia-como-criar/

IBM. (sem data). Segurança de banco de dados: um guia essencial Retirado de: https://www.ibm.com/br-pt/topics/database-security

Tripwire. (2023). 10 Database Security Best Practices You Should Know Retirado de: https://www.tripwire.com/state-of-security/database-security-best-practices-you-should-know

IBM. (sem data). O que é DevSecOps? Retirado de https://www.ibm.com/br-pt/topics/devsecops

Diazero Security. (2022). Plano de resposta a incidentes: o que é **e como desenvolver? Retirado de** https://www.diazerosecurity.com.br/pt/blog/plano-de-resposta-a-incidentes-o-que-e-e-como- desenvolver#:~:text=Na%20prática%2C%20o%20plano%20de%20resposta%20a%20incidentes,negócios%20que%20estão%20sendo%20feitos%20após%20o%20incidente.

MDN. (2023). Introdução ao lado servidor. Retirado de https://developer.mozilla.org/pt-BR/docs/Learn/Server-side/First_steps/Introduction

Mendonza, MÁ. (2018). Princípio do menor privilégio: a estratégia de limitar o acesso ao que é essencial. Retirado de https://www.welivesecurity.com/br/2018/07/18/principio-do-menor-privilegio/

IBM. (sem data). O que é **criptografia? Definição de criptografia de dados. Retirado de https://www.ibm.com/br-pt/topics/encryption**

Microsoft. (2023). Visão geral do gerenciamento de ameaças e vulnerabilidades. Retirado de https://learn.microsoft.com/pt-br/compliance/assurance/assurance-vulnerability-management

Durbano, V. (2019). O que é patch e por que fazer o gerenciamento desse programa? Retirado de https://blog.ecoit.com.br/o-que-e-patch/