DIAGNÓSTICO DE SEGURANÇA CIBERNÉTICA

Inspeção de example_report

STYXGUARD

14 de junho de 2024

Conteúdo

1 Descrição da Atividade de Monitoramento Cibernético

Nesta etapa crucial de nossa investigação, mergulhamos profundamente na estrutura digital do seu ambiente online, buscando identificar possíveis vulnerabilidades que não só comprometem a segurança, mas também ameaçam a reputação de sua marca. Nosso objetivo principal foi detectar configurações inadequadas que poderiam expor seus sistemas a ameaças cibernéticas, potencialmente prejudicando a imagem institucional que tanto prezam.

1.1 Indisponibilidade de Serviço

Encontramos potenciais falhas que poderiam resultar em interrupções no serviço, afetando negativamente a experiência dos clientes e minando a confiança na empresa.

1.2 Integridade dos Dados

Observamos vulnerabilidades que poderiam comprometer a integridade dos dados, colocando em risco a confiabilidade das informações gerenciadas pela empresa.

1.3 Danos Reputacionais

Alertamos sobre o risco de danos à reputação da empresa em caso de exploração das vulnerabilidades encontradas por agentes maliciosos.

1.4 Ransomware

Identificamos a possibilidade de ataques de ransomware, representando um perigo significativo para a continuidade dos negócios e a percepção pública da empresa. Apontamos o perigo representado

pelo sequestro de dados digitais por meio de ataques de ransomware, com potencial para causar danos financeiros e operacionais significativos.

1.5 Vazamento de Dados

Destacamos as consequências legais de uma violação da Lei Geral de Proteção de Dados, que podem incluir:

- Multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração.
- Medidas corretivas obrigatórias, como a adoção de políticas de segurança mais rigorosas e a implementação de medidas de proteção de dados adicionais.

Portanto, além das vulnerabilidades técnicas identificadas, é crucial estar ciente dos riscos representados por essas ameaças e implementar medidas proativas para mitigar esses perigos. Ao proteger seus sistemas contra esses tipos de ataques e garantir conformidade com a LGPD, você não apenas protege seus ativos digitais, mas também preserva a confiança e a credibilidade de sua empresa no mercado.

2 Dados do Ambiente Analisado

2.1 Site

example_report

2.2 IP

Não foi possível identificar o IP

2.3 ASN

Não foi possível identificar o ASN

2.4 ISP

Não foi possível identificar o ISP

2.5 Sistema Operacional

Não foi possível identificar o sistema operacional

2.6 Localização

2.6.1 País

Não foi possível identificar o país

2.6.2 Cidade

Não foi possível identificar a cidade

2.6.3 Latitude

Não foi possível identificar a latitude

2.6.4 Longitude

Não foi possível identificar a longitude

2.6.5 Mapa

Não foi possível identificar a localização no mapa

2.7 Categorias

Nenhuma categoria foi encontrada

2.8 Tags

Nenhuma tag foi encontrada

2.9 Nota de Reputação

Não foi possível identificar a reputação

2.10 Portas

Nenhuma porta aberta foi encontrada

2.11 Pichações de Site Conhecidas

Nenhuma pichação de site conhecida foi encontrada

2.12 Informações Atraentes Indexadas no Google

Nenhuma informação possivelmente vulnerável encontrada no Google

2.13 Contas Comprometidas por Vazamentos de Dados

Nenhuma conta comprometida foi encontrada

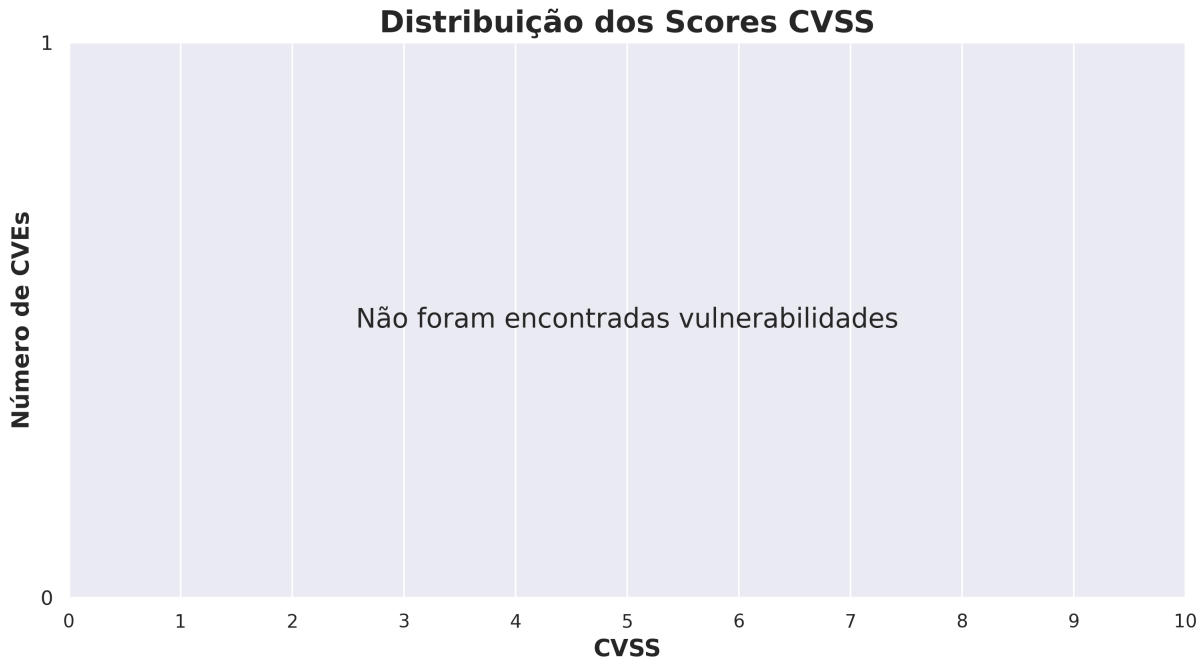
2.14 Menções em Links Públicos Contendo Informações Sensíveis

Nenhuma menção em links públicos contendo informações sensíveis foi encontrada

2.15 Vulnerabilidades Encontradas

Nenhuma CVE foi encontrada

2.16 Descrição das Vulnerabilidades



Nenhuma CVE foi encontrada

2.17 Impacto das Vulnerabilidades

Nenhuma CVE foi encontrada

2.18 Acesso das Vulnerabilidades

Nenhuma CVE foi encontrada

2.19 Subdomínios Encontrados e Vulnerabilidades

Nenhum subdomínio foi encontrado

2.20 Vulnerabilidades KEV

Nenhuma KEV foi encontrada

2.21 Vulnerabilidades com Campanha de Ransomware Conhecidas

Nenhuma vulnerabilidade com campanha de ransomware encontrada

2.22 Detecções em Listas de Distribuição de Malware

Nenhuma distribuição de malware detectada

2.23 Detecções em Listas Negras

2.23.1 IP e Domínio

Detecções: 0

Lista Negra	None	example_report
APEWS-L2	Não Encontrado	Não Encontrado
AZORult Tracker	Não Encontrado	Não Encontrado
Anti-Attacks Blacklist	Não Encontrado	Não Encontrado
AntiSpam by CleanTalk	Não Encontrado	Não Encontrado
Backscatterer	Não Encontrado	Não Encontrado
Barracuda	Não Encontrado	Não Encontrado
Blacklists.co	Não Encontrado	Não Encontrado
Blocked Servers	Não Encontrado	Não Encontrado
Blocklist.de	Não Encontrado	Não Encontrado
Blocklist.net.ua	Não Encontrado	Não Encontrado
Botvrij	Não Encontrado	Não Encontrado
Brute Force Blocker	Não Encontrado	Não Encontrado

Lista Negra	None	example_report
CI Army List	Não Encontrado	Não Encontrado
CSpace Hostings IP Blacklist	Não Encontrado	Não Encontrado
Cloudmark CSI: Cloud Abuse	Não Encontrado	Não Encontrado
CruzIT Blocklist	Não Encontrado	Não Encontrado
Cybercrime Tracker	Não Encontrado	Não Encontrado
Darklist.de	Não Encontrado	Não Encontrado
Darren SSH Block List	Não Encontrado	Não Encontrado
EFnet RBL	Não Encontrado	Não Encontrado
Etnetera Blacklist	Não Encontrado	Não Encontrado
FSpamList	Não Encontrado	Não Encontrado
Feodo Tracker	Não Encontrado	Não Encontrado
GPF DNS Block List	Não Encontrado	Não Encontrado
GreenSnow Blocklist	Não Encontrado	Não Encontrado
HoneyDB Blacklist	Não Encontrado	Não Encontrado
IBM Cobion	Não Encontrado	Não Encontrado
IPSpamList	Não Encontrado	Não Encontrado
IPsum	Não Encontrado	Não Encontrado
ISX.fr DNSBL	Não Encontrado	Não Encontrado
InterServer IP List	Não Encontrado	Não Encontrado
JamesBrine IP List	Não Encontrado	Não Encontrado
JustSpam	Não Encontrado	Não Encontrado
LAPPS Grid Blacklist	Não Encontrado	Não Encontrado
Liquid Binary	Não Encontrado	Não Encontrado
M4lwhere Intel	Não Encontrado	Não Encontrado
Malc0de	Não Encontrado	Não Encontrado
Megumin	Não Encontrado	Não Encontrado
Mirai Tracker	Não Encontrado	Não Encontrado

Lista Negra	None	example_report
Myip.ms Blacklist	Não Encontrado	Não Encontrado
NOC RUB DE	Não Encontrado	Não Encontrado
NUBI Bad IPs	Não Encontrado	Não Encontrado
Nginx Bad Bot Blocker	Não Encontrado	Não Encontrado
NordSpam	Não Encontrado	Não Encontrado
OpenPhish	Não Encontrado	Não Encontrado
Passive Spam Block List	Não Encontrado	Não Encontrado
PhishTank	Não Encontrado	Não Encontrado
Plonkatronix	Não Encontrado	Não Encontrado
RJM Blocklist	Não Encontrado	Não Encontrado
Redstout Threat IP List	Não Encontrado	Não Encontrado
Reuteras Scanning Lists	Não Encontrado	Não Encontrado
S.S.S.H.I.A	Não Encontrado	Não Encontrado
S5h Blacklist	Não Encontrado	Não Encontrado
SSL Blacklist	Não Encontrado	Não Encontrado
Sblam	Não Encontrado	Não Encontrado
Snapt NovaSense	Não Encontrado	Não Encontrado
Spamhaus	Não Encontrado	Não Encontrado
Talos IP Blacklist	Não Encontrado	Não Encontrado
Threat Crowd	Não Encontrado	Não Encontrado
Threat Sourcing	Não Encontrado	Não Encontrado
ThreatLog	Não Encontrado	Não Encontrado
Turris Greylist	Não Encontrado	Não Encontrado
URLVir	Não Encontrado	Não Encontrado
URLhaus	Não Encontrado	Não Encontrado
USTC IP BL	Não Encontrado	Não Encontrado
VXVault	Não Encontrado	Não Encontrado

Lista Negra	None	example_report
ViriBack C2 Tracker	Não Encontrado	Não Encontrado
ZeroDot1 Bad IPs	Não Encontrado	Não Encontrado

2.24 Ativos

Nenhum ativo foi encontrado

2.25 Referências para Remediação

Nenhuma CVE foi encontrada

2.26 Domínios nos Certificados Digitais

Nenhum domínio foi encontrado nos certificados digitais

2.27 Histórico e Validade dos Certificados Digitais

Nenhum certificado digital foi encontrado

2.28 Contatos

2.28.1 Emails

Nenhum email foi encontrado

2.28.2 Pessoas

Nenhuma pessoa foi encontrada

2.28.3 Telefones

Nenhum número de telefone foi encontrado

2.28.4 Redes Sociais

Nenhuma rede social foi encontrada

2.29 Tecnologias Utilizadas

Nenhuma tecnologia foi encontrada

2.30 Vulnerabilidades de SSL

Nenhuma vulnerabilidade SSL foi encontrada

2.31 Cifras SSL

Nenhuma informação sobre cifras SSL foi encontrada

2.32 DNS

2.32.1 DNS Reverso

Nenhuma informação sobre DNS reverso foi encontrada

2.32.2 DNSSEC

2.32.2.1 DNSKEY

Não foi encontrada nenhuma informação no DNSSEC sobre

2.32.2.2 DS

Não foi encontrada nenhuma informação no DNSSEC sobre

2.33 IPv6

Nenhum endereço IPv6 foi encontrado

2.34 Registros MX

Nenhum registro MX foi encontrado

2.35 Registros TXT

Nenhum registro TXT foi encontrado

2.36 Servidores de Nomes

Nenhum servidor de nomes foi encontrado

2.37 Registros DMARC

Nenhum registro DMARC foi encontrado

2.38 Registros SPF

Nenhum registro SPF foi encontrado

2.39 Importações no Código Fonte

Nenhuma importação foi encontrada

2.40 Links Extraídos do Código Fonte

Nenhum link foi encontrado

2.41 Análise por Inteligência Artificial de example_report

2.42 OWASP Top 10 Encontradas por Inteligência Artificial

Nenhuma vulnerabilidade do OWASP Top 10 foi encontrada

3 Conclusão

Este diagnóstico visa fornecer uma visão abrangente do estado de segurança do ambiente analisado, destacando as principais áreas de preocupação e fornecendo orientações para mitigar as vulnerabilidades identificadas. A implementação das recomendações sugeridas é essencial para fortalecer a postura de segurança cibernética e proteger os ativos digitais contra ameaças potenciais.

O relatório não identificou nenhuma vulnerabilidade de acordo com as categorias do OWASP Top 10. O website example_report possui uma reputação score de 0.

4 Glossário dos Principais Termos

4.1 Vulnerabilidades

Vulnerabilidades cibernéticas referem-se a fraquezas ou falhas em sistemas de computadores, redes, aplicativos ou dispositivos conectados à internet que podem ser exploradas por agentes maliciosos para comprometer a segurança dos mesmos. Essas vulnerabilidades podem surgir devido a erros de programação, configurações inadequadas, falta de atualizações de segurança ou falhas no design de sistemas tecnológicos. A exploração dessas vulnerabilidades pode resultar em ataques cibernéticos, roubo de dados, interrupção de serviços ou outras formas de comprometimento da segurança digital. A identificação e correção proativa de vulnerabilidades cibernéticas são essenciais para proteger sistemas e dados contra ameaças cibernéticas.

4.2 Reputação da Sua Marca

Refere-se à percepção geral e à imagem pública de uma empresa ou organização no ambiente digital. Esta reputação é moldada pela maneira como a empresa interage online, sua presença nas redes sociais, o conteúdo que compartilha, a qualidade de seus produtos ou serviços digitais, bem como sua capacidade de proteger os dados dos clientes e manter a segurança cibernética. Uma boa reputação de marca cibernética é vital para construir confiança com os clientes, atrair novos negócios e manter uma posição competitiva no mercado digital.

4.3 Ameaças Cibernéticas

Ameaças cibernéticas referem-se a qualquer tipo de perigo ou risco que possa comprometer a segurança e integridade de sistemas, redes ou dados digitais. Essas ameaças podem incluir ataques de malware, como vírus, ransomware e spyware, ataques de phishing, invasões de rede, violações de dados, entre outros. O objetivo das ameaças cibernéticas geralmente é causar danos, roubar informações confidenciais, interromper operações comerciais ou obter acesso não autorizado a recursos

digitais. A mitigação das ameaças cibernéticas é fundamental para implementar medidas eficazes de segurança cibernética e proteger ativos digitais contra possíveis ataques.

4.4 Ransomware

Uma forma de malware que criptografa os dados de um sistema, tornando-os inacessíveis ao usuário legítimo. Os cibercriminosos exigem então um resgate (ou ransom) em troca da chave de descriptografia necessária para recuperar os dados. Esse tipo de ataque pode causar danos financeiros, operacionais e reputacionais significativos para indivíduos e organizações.

4.5 Disponibilidade de Serviço

Disponibilidade de serviço refere-se à incapacidade de um sistema, aplicativo ou recurso digital estar acessível e operacional quando necessário. Essa condição pode ser causada por uma variedade de fatores, incluindo falhas técnicas, ataques cibernéticos, sobrecarga de tráfego ou problemas de infraestrutura. A indisponibilidade de serviço pode resultar em interrupções nas operações comerciais, impactando negativamente a experiência do usuário e a reputação da organização. É crucial para as empresas implementar medidas de redundância e recuperação de desastres para mitigar os efeitos da indisponibilidade de serviço e garantir a continuidade das operações.

4.6 Integridade dos Dados

A integridade dos dados refere-se à qualidade dos dados que são precisos, completos e consistentes ao longo do tempo. Em sistemas de informação, a integridade dos dados é fundamental para garantir que as informações armazenadas não sejam corrompidas, alteradas ou comprometidas de forma não autorizada. Isso envolve a implementação de controles e mecanismos de segurança para proteger os dados contra modificações indevidas, garantindo que apenas usuários autorizados possam realizar alterações e que as informações permaneçam íntegras e confiáveis em todas as etapas de seu ciclo de vida. A integridade dos dados é essencial para a tomada de decisões precisas e confiáveis, bem como para garantir a confiança e a credibilidade dos sistemas de informação em geral.

4.7 Confidencialidade de Dados

A confidencialidade dos dados é um princípio de segurança da informação que se refere à garantia de que as informações sensíveis e restritas estão protegidas contra acessos não autorizados. Isso signi-

fica que somente indivíduos ou sistemas autorizados têm permissão para acessar, visualizar, modificar ou divulgar esses dados. A confidencialidade é essencial para proteger a privacidade e os interesses das partes envolvidas, impedindo que informações sensíveis caiam em mãos indevidas e evitando consequências prejudiciais, como roubo de identidade, fraudes ou violações de privacidade.

4.8 Vazamento de Dados

O vazamento de dados ocorre quando informações confidenciais, sensíveis ou privadas são acessadas, divulgadas, roubadas ou compartilhadas sem autorização. Isso pode acontecer devido a falhas de segurança, ataques cibernéticos, erros humanos ou má configuração de sistemas. Os dados vazados podem incluir informações pessoais, financeiras, médicas ou comerciais, e o vazamento pode ter sérias repercussões, como roubo de identidade, fraudes financeiras, danos à reputação e penalidades legais.

4.9 KEV

É um Catálogo de Vulnerabilidades Conhecidas Exploradas, desenvolvido pelo Cybersecurity and Infrastructure Security Agency (CISA) dos Estados Unidos, é uma compilação de vulnerabilidades de segurança cibernética que são ativamente exploradas por agentes maliciosos. Essas vulnerabilidades representam brechas de segurança significativas que podem ser aproveitadas para comprometer sistemas, redes e dados. O Catálogo fornece informações detalhadas sobre as vulnerabilidades, incluindo descrições, impactos potenciais, contramedidas recomendadas e referências adicionais para auxiliar na mitigação e remediação. Ele é uma ferramenta fundamental para profissionais de segurança cibernética e organizações na identificação e correção proativa de ameaças emergentes e críticas para a segurança da informação.