Proposta de Estratégia de Segurança Cibernética
Preparado para: LojaZeta

Preparado por:
Marco Aurélio
Consultor de Segurança Cibernética

Data:
28 de setembro de 2025

Versão:
1.1 (Revisão Final)

Sumário

1. Resumo Executivo

A LojaZeta, um e-commerce em franca expansão, encontra-se num ponto de inflexão crítico onde o seu crescimento de negócio superou a sua maturidade de segurança. A empresa está atualmente sob ataque ativo (SQLi, XSS, Força Bruta), operando com visibilidade de segurança limitada e sem garantia de recuperação em caso de desastre. Esta

vulnerabilidade representa um risco direto à continuidade do negócio, à confiança do cliente e à conformidade com a LGPD.

Esta proposta detalha uma estratégia de segurança pragmática e faseada, focada na implementação de uma arquitetura de Defesa em Profundidade. A solução prioriza controlos de alto impacto e baixo custo, utilizando primariamente tecnologia open-source para proteger, detetar e responder a ameaças.

A implementação deste plano em três fases (Ganhos Rápidos, Monitorização e Fortalecimento) irá reduzir drasticamente a superfície de ataque, fornecer visibilidade acionável sobre ameaças e estabelecer um processo robusto de resposta a incidentes. O resultado será um ambiente operacional mais resiliente e seguro, protegendo a receita e a reputação da marca LojaZeta.

2. Escopo e Metodologia
2.1. Escopo:
Esta proposta foca na proteção da plataforma de e-commerce da LojaZeta, hospedada em ambiente de nuvem IaaS. O escopo inclui a análise e recomendação de controlos para os servidores de aplicação (Nginx, Node.js), banco de dados (PostgreSQL) e mecanismos de autenticação. Não fazem parte do escopo a segurança física do provedor de nuvem ou a análise de código-fonte da aplicação.

2.2. Metodologia:
A análise e as recomendações foram desenvolvidas utilizando o framework NIST Cybersecurity Framework (CSF) como guia, com foco nos pilares de Identificar, Proteger, Detetar e Responder. A estratégia de implementação prioriza o princípio 80/20, buscando os maiores ganhos de segurança com o menor impacto operacional e financeiro inicial.

2.3. Assunções:

A equipe da LojaZeta (2 Devs, 1 Ops) será responsável pela implementação dos controlos recomendados, com nosso suporte.

As soluções propostas serão primariamente baseadas em software open-source para respeitar o orçamento limitado.

O ambiente de nuvem permite a instalação de agentes e a configuração de regras de firewall/rede.

3. Arquitetura de Defesa (Camadas)

"A arquitetura de defesa proposta está representada visualmente no diagrama constante no Anexo B."

Com base nos requisitos da LojaZeta, propomos uma arquitetura de Defesa em Profundidade com foco em controlos pragmáticos e de alto impacto para o ambiente de e-commerce.

3.1. Camada de Perímetro (Web Application Firewall - WAF):

Diagnóstico: A LojaZeta sofre com tentativas de SQLi e XSS.

Controlo: Implementação de um WAF com o OWASP Core Rule Set (CRS).

Justificativa: Este controlo mitiga de forma direta e eficaz a grande maioria de ataques à camada de aplicação web, servindo como primeira linha de defesa.

Solução Recomendada: ModSecurity, por ser um módulo open-source e nativo para o servidor web Nginx, já utilizado pela LojaZeta.

3.2. Camada de Host (Servidor e Identidade):

Diagnóstico: Tentativas de força bruta no /login e falta de controlos nos servidores.

Controlos:

Proteção contra Força Bruta: Implementação de um sistema que bane IPs após múltiplas tentativas de login falhas.

Hardening do SO: Aplicação de melhores práticas de segurança nos sistemas operacionais dos servidores para reduzir a superfície de ataque.

Gestão de Identidade: Implementação de Autenticação de Múltiplos Fatores (MFA) para todos os acessos administrativos (SSH, painel da nuvem, etc.).

Soluções Recomendadas: Fail2ban para proteção de força bruta; uso de checklists como CIS Benchmarks para o hardening; e soluções de MFA baseadas em TOTP (ex: Google Authenticator) para identidade.

3.3. Camada de Dados:

Diagnóstico: Backups existentes, mas sem garantia de funcionalidade.

Controlo: Criação de uma rotina de testes de restauração de backup.

Justificativa: Um backup não testado não é um backup confiável. Em caso de um incidente grave (como ransomware), a capacidade de restaurar o serviço é o controlo mais crítico para a continuidade do negócio.

Recomendação: Realizar um teste de restore completo a cada 3 meses e um teste de restore de arquivos específicos mensalmente.

4. Monitorização & SIEM
4.1. Diagnóstico:
A LojaZeta atualmente carece de visibilidade centralizada sobre a sua segurança. Os logs estão distribuídos pelas instâncias, tornando a deteção e a análise de incidentes uma tarefa manual, lenta e ineficaz.

4.2. Controle:
Implementação de uma solução de SIEM (Security Information and Event Management) para centralizar a recolha, o processamento e a correlação de logs de segurança de todas as fontes críticas.

4.3. Fontes de Log Essenciais:
Para garantir uma visibilidade mínima viável (MVP), as seguintes fontes de log devem ser integradas:

Servidor Web (Nginx): Logs de acesso e de erro.

WAF (ModSecurity): Logs de alertas e bloqueios.

Sistema Operacional (Linux): Logs de autenticação (SSH), comandos executados e eventos de sistema.

Proteção de Força Bruta (Fail2ban): Logs de IPs banidos.

Banco de Dados (PostgreSQL): Logs de queries lentas e erros (pode indicar tentativas de extração de dados).

4.4. Alertas Acionáveis (Casos de Uso Iniciais):
O SIEM será configurado para gerar alertas automáticos para as seguintes condições de alta prioridade:

Múltiplos Alertas de WAF: Mais de 10 alertas de SQLi ou XSS do mesmo IP em 5 minutos.

Força Bruta Detetada: Alerta gerado pelo Fail2ban indicando um IP banido.

Login Administrativo Suspeito: Acesso SSH bem-sucedido fora do horário comercial (ex: 22:00 - 06:00).

Criação de Utilizador com Privilégios: Um novo utilizador sudo é criado num servidor.

4.5. Solução Recomendada:
Wazuh. É uma plataforma open-source robusta que combina funcionalidades de SIEM, XDR e monitorização de integridade de ficheiros. É ideal para o cenário da LojaZeta devido à ausência de custos de licenciamento e à sua vasta documentação e comunidade ativa.

5. Resposta a Incidentes (NIST IR)
5.1. Abordagem:
A capacidade de responder a um incidente é tão crítica quanto a capacidade de o prevenir. Propomos a adoção de um plano de resposta a incidentes (IRP) baseado no framework NIST SP 800-61. Este plano garante uma resposta estruturada, rápida e eficaz para minimizar o impacto de um incidente de segurança.

5.2. Fases do Ciclo de Vida da Resposta:
O plano seguirá o ciclo de vida padrão da indústria:

Preparação: Ter as ferramentas, os processos e as equipas treinadas antes que um incidente ocorra.

Deteção & Análise: Identificar e validar um incidente de segurança.

Contenção, Erradicação & Recuperação: Limitar o dano, eliminar a causa raiz e restaurar a operação normal.

Atividade Pós-Incidente: Aprender com o incidente para fortalecer as defesas.

5.3. Plano Detalhado:
Como parte desta proposta, foi desenvolvido um plano de resposta completo e detalhado, com playbooks técnicos, para o cenário de maior risco para a LojaZeta: uma Violação de Dados via SQL Injection. Este plano encontra-se no Anexo A deste documento.

6. Recomendações (80/20) e Roteiro

A implementação será faseada para garantir ganhos rápidos (quick wins) e respeitar a capacidade da equipa.

Fase	Prazo	Ações Prioritárias (80/20)	Responsável	Custo Estimado
1	30 dias	- Implementar ModSecurity (WAF) em modo DetectionOnly - Instalar e configurar Fail2ban - Realizar o primeiro teste de restore de backup	Equipe de Ops	Horas/Homem
2	90 dias	- Ativar ModSecurity (WAF) em modo Blocking - Implementar o servidor Wazuh (SIEM) - Instalar agentes Wazuh nos servidores web	Equipe de Ops	Horas/Homem
3	180 dias	- Integrar todas as fontes de log no Wazuh - Configurar e afinar os alertas acionáveis - Implementar MFA para todos os acessos administrativos	Equipe de TI	Horas/Homem

7. Riscos, Custos e Assunções
Riscos: A ativação do WAF em modo de bloqueio pode gerar falsos positivos, impactando tráfego legítimo. Mitigação: Manter o WAF em modo de deteção por 30 dias para afinar as regras.

Custos: As soluções recomendadas (ModSecurity, Fail2ban, Wazuh) são open-source, eliminando custos de licenciamento. O principal investimento será em horas/homem da equipa interna para implementação e configuração. Recomenda-se alocar 10 horas semanais da equipa de Ops durante a Fase 1.

Assunções: Assume-se que a infraestrutura de nuvem atual possui recursos (CPU/RAM) suficientes para hospedar o servidor Wazuh.

8. Conclusão e Próximos Passos
A LojaZeta encontra-se num ponto de inflexão crítico, onde o crescimento do negócio deve ser acompanhado por um amadurecimento da sua postura de segurança. Os incidentes recentes são um claro indicador de que a ausência de controlos básicos representa um risco existencial para a empresa.
Esta proposta detalha um plano de ação pragmático, faseado e de baixo custo que irá reduzir drasticamente a superfície de ataque, aumentar a visibilidade sobre ameaças e preparar a LojaZeta para responder eficazmente a um incidente.
Recomendamos uma reunião de alinhamento para discutir esta proposta e aprovar o início imediato da Fase 1 do roteiro. Os critérios de sucesso serão medidos pela redução de 90%

dos ataques de força bruta e SQLi bem-sucedidos em 90 dias, e a centralização de 100% dos logs críticos no SIEM.

Anexo A: Plano de Resposta a Incidentes – Violação de Dados
1. Preparação
Equipa de Resposta a Incidentes (CIRT):

Incident Commander: CTO (responsável final pela resposta).

Analista Chefe: Líder de Operações (coordena as ações técnicas).

Comunicação: CEO (ponto de contacto para comunicação externa/interna).

Assessoria Jurídica: Contratada externamente (acionada em caso de violação de dados confirmada).

Ferramentas e Recursos:

Acesso administrativo ao provedor de nuvem, servidores e SIEM.

Acesso aos backups.

Canal de comunicação de crise seguro (ex: Signal), separado da infraestrutura principal.

Treinamento: Realizar uma simulação de resposta a incidentes (tabletop exercise) a cada 6 meses.

2. Deteção e Análise
Fontes de Deteção: Alerta do SIEM/Wazuh (ex: "Múltiplos Alertas de SQLi"), comunicação de um investigador de segurança externo, reclamações de clientes sobre fraudes.

Análise Inicial (Primeira Hora):

Validar o Incidente: Confirmar se os alertas são legítimos, analisando os logs do WAF e do Nginx.

Determinar o Escopo Inicial: Identificar o IP de origem do atacante, os servidores-alvo e o período de tempo da atividade suspeita.

Classificar o Incidente: De acordo com a matriz de classificação, uma violação de dados de clientes é sempre de severidade CRÍTICA.

Análise Aprofundada:

Analisar os logs do banco de dados para identificar quais tabelas foram acedidas.

Determinar o volume e o tipo de dados exfiltrados (ex: nomes, e-mails, dados de cartão).

3. Contenção, Erradicação e Recuperação
Contenção (Primeiros 15 minutos):

Bloquear o IP do Atacante: Criar uma regra no firewall da nuvem e no WAF para bloquear imediatamente o IP de origem do ataque.

Isolar o Servidor Comprometido (se necessário): Se houver suspeita de que o atacante ganhou acesso ao servidor, isolá-lo da rede pública para análise forense.

Erradicação:

Corrigir a Vulnerabilidade: A equipa de desenvolvimento deve corrigir a vulnerabilidade de SQL Injection e fazer o deploy da versão corrigida da aplicação.

Reset de Credenciais: Forçar a alteração de todas as senhas de acesso à base de dados e aos sistemas de administração.

Recuperação:

Validar a Integridade dos Dados: Verificar se o atacante não alterou ou apagou dados no banco de dados. Se necessário, restaurar a partir do último backup limpo.

Monitorização Intensiva: Aumentar o nível de monitorização sobre a aplicação e a base de dados por 72 horas para garantir que o atacante não regressa.

4. Atividade Pós-Incidente (Lições Aprendidas)
Comunicação:

Interna: Utilizar o template de comunicação interna para informar as equipas sobre o incidente, as ações tomadas e os próximos passos.

Externa: Se dados sensíveis de clientes (conforme LGPD) foram comprovadamente vazados, acionar a assessoria jurídica para notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados afetados.

Relatório de Lições Aprendidas: Realizar uma reunião em até 7 dias após o incidente para responder:

O que correu bem?

O que correu mal?

O que podemos fazer para evitar que isto aconteça novamente?

O que podemos fazer para melhorar a nossa resposta da próxima vez?

Ações de Melhoria: As saídas da reunião devem gerar tarefas concretas, como "Implementar revisão de segurança no ciclo de desenvolvimento" ou "Melhorar as regras de alerta do SIEM".

Anexo B: Diagrama da Arquitetura Proposta

Este diagrama representa a arquitetura de defesa em camadas recomendada para a LojaZeta.