CAIXAVERSO - 02 | Agente de Segurança Cibernética - III

Proposta de Melhoria de Segurança Cibernética para a FinTechSecure

Recife/PE

Ricardo Rodrigues Rocha

Proposta de Melhoria de Segurança Cibernética para a FinTechSecure

Este relatório apresenta uma proposta estratégica para o fortalecimento da segurança cibernética da empresa FinTechSecure, uma fintech especializada em serviços financeiros digitais. A partir da análise dos desafios enfrentados pela organização, são sugeridas ações integradas envolvendo testes de intrusão contínuos, implantação de um Security Operation Center (SOC), gestão de vulnerabilidades, proteção de dados sensíveis e gerenciamento seguro de segredos corporativos.

Recife/PE

Sumário

1. Introdução 4
2. Pentest como Processo 4
2.1 Pré-engajamento 5
2.2 Coleta de informações 5
2.3 Modelagem de ameaças 5
2.4 Análise de vulnerabilidades 6
2.5 Exploração 6
2.6 Pós-exploração 6
2.7 Análise e Relato dos resultados 7
3. Implantação do SOC 7
4. Gestão de vulnerabilidades 9
5. Gestão de dados sensíveis 10
6. Gestão de Segredos 11
6.1 Política Proposta 12
6.2 Ferramentas Recomendadas: 12
6.3 Práticas de Rotação 13
6.4 Controle de Acesso 13
7. Conclusão 13

1. Introdução

A segurança cibernética é um dos pilares fundamentais para a sustentabilidade de empresas do setor financeiro, especialmente das fintechs – Empresas que atuam com tecnologia que oferecem soluções na área de serviços financeiros baseados em plataformas digitais e em tecnologias inovadoras. Diferente dos bancos tradicionais, que possuem infraestrutura consolidada e camadas de segurança mais robustas, as fintechs muitas vezes enfrentam o desafio de crescer rapidamente sem comprometer a proteção de seus ativos digitais e a privacidade de seus clientes. Nesse cenário, ataques cibernéticos tornam-se uma ameaça constante, colocando em risco não apenas a continuidade dos serviços, mas também a confiança do consumidor e a reputação da empresa.

A FinTechSecure, objeto de estudo deste trabalho, é uma empresa em expansão que atua com serviços financeiros digitais, oferecendo soluções como banco online e pagamentos digitais. Az organização sofreu uma tentativa de invasão em seus sistemas, o que evidenciou fragilidades em sua postura de segurança cibernética. Esse episódio acendeu um alerta para a necessidade de maior maturidade nos processos de defesa digital, abrangendo desde a detecção de ameaças até a gestão de dados sensíveis e segredos corporativos.

Diante desse contexto, a empresa se encontra em fase de implantação de um Security Operation Center (SOC), visando estruturar um programa contínuo de gestão de vulnerabilidades e para isso necessita reforçar suas políticas de proteção de dados. O momento é estratégico para que a FinTechSecure alinhe sua segurança cibernética a padrões reconhecidos internacionalmente, de forma a garantir conformidade regulatória, mitigar riscos e consolidar a confiança de seus clientes em um mercado altamente competitivo.

2. Pentest como Processo

O Teste de Intrusão – Pentest, quando tratado como um processo contínuo, é uma prática essencial para garantir a segurança cibernética das organizações. Diferente de ações pontuais, ele deve ser integrado à rotina de segurança, funcionando em ciclos regulares que permitem identificar, corrigir e reavaliar

vulnerabilidades de forma constante. A seguir, são apresentadas as principais etapas desse processo.

2.1 Pré-engajamento

O primeiro passo consiste na definição do escopo do teste, ou seja, quais sistemas, aplicações, redes ou dispositivos serão analisados. Também é necessário estabelecer os objetivos, como validar controles de segurança, simular um ataque direcionado ou verificar a resiliência da infraestrutura. Essa fase inclui ainda a obtenção de autorizações formais, garantindo a legalidade da atividade, bem como a escolha da metodologia a ser adotada (ex.: OWASP, PTES, NIST). O planejamento deve prever a periodicidade dos testes, que podem ser trimestrais, semestrais ou contínuos, dependendo do nível de criticidade do ambiente.

2.2 Coleta de informações

Nesta etapa, ocorre a coleta de informações públicas e acessíveis, muitas vezes sem interação direta com o alvo, utilizando técnicas de OSINT (Open Source Intelligence). São mapeadas informações sobre domínios, endereços de IP, servidores expostos, perfis em redes sociais e outras evidências que ajudam a construir uma visão da superfície de ataque disponível.

2.3 Modelagem de ameaças

Com base nas informações obtidas, é realizada a varredura de portas, serviços e versões de software em execução. Essa análise permite identificar possíveis vulnerabilidades conhecidas e pontos de entrada. Além disso, a enumeração busca descobrir usuários, diretórios, compartilhamentos de rede e banners de serviços, ampliando a compreensão sobre a estrutura do ambiente alvo.

2.4 Análise de vulnerabilidades

Após a identificação de vulnerabilidades, inicia-se a fase de exploração, na qual o analista tenta, de forma controlada, explorá-las para verificar seu real impacto. Podem ser utilizadas ferramentas automatizadas e técnicas manuais para obter acesso indevido, executar comandos não autorizados ou manipular dados. É fundamental que essa etapa seja conduzida com cautela para não comprometer a disponibilidade do ambiente de produção.

2.5 Exploração

A fase de exploração consiste na execução prática das vulnerabilidades previamente identificadas, com o objetivo de obter acesso não autorizado aos sistemas-alvo. Nesta etapa, o pentester utiliza técnicas e ferramentas específicas para validar a existência das falhas e demonstrar seu impacto potencial, sempre respeitando os limites éticos e legais definidos no escopo do teste.

A exploração pode envolver a execução de exploits conhecidos, desenvolvimento de scripts personalizados, manipulação de parâmetros de entrada, injeção de código malicioso ou quebra de autenticação. O foco é comprovar que uma vulnerabilidade pode ser utilizada para comprometer a confidencialidade, integridade ou disponibilidade dos ativos da organização. Ferramentas como Metasploit Framework, Burp Suite, SQLmap, Hydra e John the Ripper são comumente empregadas nesta fase, dependendo do tipo de sistema e da natureza das falhas encontradas

2.6 Pós-exploração

Caso a exploração seja bem-sucedida, o próximo passo é analisar até onde um invasor poderia avançar. Isso inclui escalonamento de privilégios, movimentação lateral dentro da rede, acesso a informações sensíveis e manutenção de persistência. Essa etapa fornece uma visão clara do impacto real que um ataque poderia causar à organização.

2.7 Análise e Relato dos resultados

Todas as descobertas devem ser documentadas de maneira detalhada e clara. O relatório deve conter tanto a descrição técnica das vulnerabilidades e suas evidências (como capturas de tela e logs) quanto uma versão executiva, direcionada a gestores, destacando os riscos e impactos no negócio. A classificação de severidade pode ser realizada por meio de métricas como o CVSS(Sistema padronizado utilizado para avaliar a gravidade de vulnerabilidades de segurança), facilitando a priorização das correções.

3. Implantação do SOC

A implantação de um Centro de Operações de Segurança (SOC) é um passo estratégico para qualquer organização que busca garantir a proteção contínua de seus ativos digitais. Esse processo envolve a combinação de pessoas, processos e tecnologias, de modo a permitir o monitoramento, a detecção e a resposta rápida a incidentes de segurança. O primeiro passo para estabelecer um SOC é o planejamento estratégico, no qual são definidos os objetivos da operação, como monitorar a infraestrutura em tempo real, detectar ameaças, responder a incidentes e atender a requisitos de conformidade regulatória. Nessa fase também é importante avaliar o nível de maturidade de segurança da organização e decidir se o SOC será interno, terceirizado ou híbrido, bem como definir se a operação funcionará em regime de 24 horas por dia, apenas em horário comercial ou sob demanda. Outro aspecto

fundamental é a estrutura organizacional. Um SOC bem estabelecido deve contar com analistas de diferentes níveis de atuação. Os analistas de primeiro nível são responsáveis por realizar o monitoramento contínuo e a triagem de alertas. Já os analistas de segundo nível assumem a investigação detalhada dos incidentes, correlacionando eventos e propondo medidas de mitigação. Por fim, especialistas de nível avançado, conhecidos como threat hunters, atuam na identificação de ameaças mais sofisticadas, análise forense e inteligência de ameaças. Além da equipe técnica, a gestão do SOC deve garantir coordenação eficiente, comunicação com as áreas de negócio e alinhamento com aspectos jurídicos, especialmente em casos relacionados à privacidade de dados e à LGPD.

A arquitetura tecnológica é o pilar que sustenta o funcionamento do SOC. O uso de ferramentas de SIEM (Security Information and Event Management) é indispensável, pois permite centralizar e correlacionar logs de diferentes fontes, como servidores, firewalls, aplicações, endpoints e serviços em nuvem. Além disso, soluções de detecção e prevenção, ajudam a identificar comportamentos maliciosos em diferentes camadas da infraestrutura. Para aumentar a eficiência, muitas organizações integram plataformas de SOAR (Security Orchestration, Automation and Response), que automatizam respostas a incidentes, como o bloqueio imediato de um endereço IP malicioso. Também é recomendada a integração com fontes de inteligência de ameaças (Threat Intelligence), permitindo antecipar riscos por meio da análise de indicadores de comprometimento. Os processos operacionais de um SOC giram em torno do ciclo de resposta a incidentes. Esse ciclo inicia-se com a coleta e centralização de logs pelo SIEM. Em seguida, as regras de correlação detectam atividades suspeitas, que são analisadas inicialmente por analistas de primeiro nível. Se confirmada a relevância do alerta, o caso é encaminhado para investigação mais detalhada, na qual se avaliam contexto, impacto e origem. Quando uma ameaça é confirmada, medidas de mitigação e contenção são aplicadas, como bloqueio de acessos e isolamento de dispositivos. Após essa etapa, a fase de erradicação e recuperação garante que a ameaça seja removida e que os sistemas afetados retornem ao funcionamento normal. Por fim, é conduzida uma análise de lições aprendidas, atualizando regras de detecção, aprimorando processos e reforçando treinamentos.

Do ponto de vista de governança e conformidade, o SOC deve estar alinhado a normas e frameworks de segurança reconhecidos, como a ISO 27001, o NIST

Cybersecurity Framework e a matriz MITRE ATT&CK. A mensuração de indicadores de desempenho, como o tempo médio para reconhecer (MTTA) e responder (MTTR) a incidentes, é essencial para avaliar a eficiência da operação e orientar melhorias contínuas.

A implantação do SOC pode ser dividida em fases. A fase inicial consiste na preparação, com levantamento de requisitos, definição do escopo e aquisição de ferramentas e equipe. Em seguida, na fase de implementação, ocorre a instalação do SIEM e a integração dos primeiros logs. A fase de expansão contempla a adição de controles complementares, como EDR, IDS e automação com SOAR. Por fim, na fase de maturidade, o SOC passa a atuar de forma proativa, incorporando técnicas de threat hunting, inteligência de ameaças e integração com práticas de DevSecOps.

4. Gestão de vulnerabilidades

A gestão de vulnerabilidades é um processo essencial para garantir a resiliência cibernética de uma organização. Trata-se de uma prática contínua que envolve a identificação, avaliação, tratamento e monitoramento de falhas de segurança presentes em sistemas, aplicações, dispositivos e infraestruturas de TI. Para que seja eficaz, a empresa deve adotar uma política formal de gestão de vulnerabilidades, assegurando que o processo esteja integrado à governança de segurança e em conformidade com normas e boas práticas reconhecidas, como ISO 27001, NIST e CIS Controls.

Uma política formal deve estabelecer responsabilidades claras entre as áreas de TI e Segurança da Informação, definindo que todos os sistemas críticos passem por verificações periódicas de vulnerabilidades por meio de ferramentas especializadas, como scanners automáticos (ex.: Nessus, OpenVAS, Qualys) e auditorias manuais em casos específicos. O processo deve abranger também softwares de terceiros, dispositivos de rede, serviços em nuvem e endpoints. O ciclo de atualização de sistemas é um componente fundamental dessa política. Ele deve incluir a varredura periódica de vulnerabilidades, a análise de relatórios gerados pelas ferramentas de detecção, a priorização de falhas identificadas e a aplicação de correções por meio de patches ou reconfigurações de segurança. Recomenda-se que

vulnerabilidades críticas sejam corrigidas em prazos curtos (por exemplo, até 72 horas), enquanto vulnerabilidades de médio e baixo risco podem seguir prazos mais flexíveis, sempre com base em um calendário definido pela política. Além disso, é importante que cada correção seja acompanhada por um processo de reteste, confirmando que a falha foi efetivamente eliminada e que não foram introduzidas novas fragilidades.

Para apoiar a priorização das correções, a empresa pode utilizar métricas de risco padronizadas, como o CVSS (Common Vulnerability Scoring System). Esse sistema atribui uma pontuação de 0 a 10 às vulnerabilidades, levando em conta fatores como facilidade de exploração, impacto na confidencialidade, integridade e disponibilidade dos dados, além de características do vetor de ataque. Dessa forma, vulnerabilidades com pontuação alta (7,0 a 10,0) devem ser tratadas como prioridade imediata, enquanto vulnerabilidades médias (4,0 a 6,9) podem ser planejadas em ciclos de manutenção, e vulnerabilidades de baixo risco (0,1 a 3,9) podem ser resolvidas em etapas posteriores.

A política de gestão de vulnerabilidades deve ainda prever a integração com ferramentas de monitoramento e SIEM, permitindo correlacionar vulnerabilidades conhecidas com tentativas reais de exploração detectadas em tempo de execução. Isso aumenta a capacidade da organização em priorizar não apenas pelo risco teórico (pontuação CVSS), mas também pelo risco contextual, considerando exposição real e criticidade do ativo afetado.

5. Gestão de dados sensíveis

A proteção de dados sensíveis é um dos pilares fundamentais da segurança da informação, especialmente em empresas do setor financeiro como a FinTechSecure, que lidam diariamente com informações pessoais, bancárias e estratégicas. A gestão eficaz desses dados requer políticas claras, controles técnicos robustos e conformidade com normas regulatórias. Segue políticas e controles propostos visando garantir a proteção de dados sensíveis:

- Classificação de Dados: Implementar uma política de classificação que identifique e categorize os dados conforme seu nível de sensibilidade (ex: público, interno, confidencial, restrito). Isso permite aplicar controles proporcionais ao risco.
- Política de Retenção e Descarte: Definir prazos de retenção para cada tipo de dado e procedimentos seguros de descarte, como destruição criptográfica ou sanitização de mídia.
- Conformidade Regulatória: Garantir aderência a normas como LGPD, GDPR e ISO/IEC 27001, com foco em privacidade, consentimento e direitos dos titulares.
- Criptografia:
    - Dados em repouso: utilizar algoritmos como AES-256 para proteger bancos de dados, arquivos e backups.
    - Dados em trânsito: adotar protocolos seguros como TLS 1.2+ para comunicação entre sistemas.
- Controle de Acesso:
    - Autenticação multifator (MFA) para usuários com acesso a dados sensíveis.
    - Princípio do menor privilégio (PoLP) para limitar acessos apenas ao necessário.
    - Segregação de funções para evitar conflitos de interesse e abuso de privilégio.
- Monitoramento e Auditoria:
    - Registro de acessos e alterações em dados sensíveis.
    - Alertas para acessos fora do padrão ou tentativas de exfiltração.
- Tokenização e Mascaramento: Técnicas que permitem o uso de dados substitutos em ambientes de teste ou visualizações, sem expor os dados reais.

6. Gestão de Segredos

A gestão segura de segredos corporativos — como credenciais, chaves de API, tokens de acesso e certificados — é essencial para prevenir acessos não autorizados e mitigar riscos de comprometimento de sistemas críticos. Em ambientes financeiros digitais como o da FinTechSecure, a exposição indevida desses elementos pode resultar em fraudes, vazamentos de dados e interrupções operacionais.

6.1 Política Proposta

A política de gestão de segredos deve abranger os seguintes princípios:

- Centralização e Controle: Todos os segredos devem ser armazenados em repositórios seguros e centralizados, com criptografia forte e controle de acesso granular.
- Segregação de Ambientes: Segredos devem ser separados por ambiente (produção, teste, desenvolvimento), evitando reutilização indevida.
- Auditoria e Monitoramento: Toda ação relacionada a segredos (criação, acesso, modificação, exclusão) deve ser registrada e monitorada em tempo real.
- Automação e Integração: Sempre que possível, o gerenciamento de segredos deve ser integrado a pipelines de CI/CD, evitando exposição manual.

6.2 Ferramentas Recomendadas:

- HashiCorp Vault: Solução robusta para armazenamento, rotação e acesso seguro a segredos, com suporte a políticas dinâmicas e autenticação baseada em identidade.
- AWS Secrets Manager: Ideal para ambientes em nuvem, permite rotação automática de segredos e integração com serviços da AWS.
- CyberArk Conjur: Focado em ambientes DevOps e containers, com forte controle de acesso e auditoria.

6.3 Práticas de Rotação

- Rotação Periódica: Segredos devem ser rotacionados em intervalos definidos (ex: a cada 30 ou 90 dias), mesmo sem evidência de comprometimento.
- Rotação por Evento: Sempre que houver suspeita de vazamento, mudança de pessoal ou alteração de escopo, os segredos devem ser imediatamente substituídos.
- Automação da Rotação: Utilizar ferramentas que suportem rotação automática, reduzindo erros humanos e garantindo conformidade.

6.4 Controle de Acesso

- Princípio do Menor Privilégio (PoLP): Usuários e sistemas devem ter acesso apenas aos segredos estritamente necessários para suas funções.
- Autenticação Forte: Acesso a segredos deve exigir autenticação multifator (MFA) e, preferencialmente, autenticação baseada em identidade (IAM).
- Revisão Periódica de Permissões: As permissões de acesso devem ser revisadas regularmente para garantir que estejam atualizadas e alinhadas com as funções dos usuários.

7. Conclusão

A implantação de um SOC eficaz requer mais do que tecnologia: depende de equipes capacitadas, processos claros e ferramentas que possibilitem visibilidade, automação e resposta eficiente. Quando bem estruturado, o SOC não apenas reduz riscos de ataques cibernéticos, mas também fortalece a governança de segurança da organização, transformando a cibersegurança em um processo contínuo e estratégico.

Gestão de vulnerabilidades deve ser entendida como um processo contínuo, alinhado ao ciclo de vida dos sistemas da empresa. Novas tecnologias, atualizações de software e mudanças na infraestrutura exigem que a análise de vulnerabilidades seja constante, apoiada por relatórios periódicos para a gestão e métricas que comprovem a evolução da maturidade em segurança. Assim, a empresa transforma a resposta a vulnerabilidades de uma atividade reativa para uma prática estratégica de proteção contra ameaças.

A gestão de dados sensíveis envolve políticas e controles para proteger informações críticas da empresa, como dados pessoais, financeiros e estratégicos. Essas medidas garantem confidencialidade, integridade e disponibilidade dos dados, reduzindo riscos de vazamento e violação.

A gestão de segredos envolve três pilares principais: armazenamento seguro, controle de acesso e rotação periódica. Os segredos devem ser mantidos em cofres digitais seguros (como HashiCorp Vault, AWS Secrets Manager ou Azure Key Vault) e nunca incluídos diretamente em código-fonte ou arquivos de configuração acessíveis publicamente. O controle de acesso garante que apenas usuários ou sistemas autorizados possam utilizar os segredos, aplicando princípios de mínimo privilégio e autenticação forte. Já a rotação periódica de senhas e chaves reduz o impacto de possíveis vazamentos, evitando que segredos antigos continuem válidos por longos períodos.

A integração entre SOC, gestão de vulnerabilidades, dados sensíveis e segredos não é apenas desejável — é indispensável. Ela transforma a segurança cibernética de uma série de controles isolados em um sistema inteligente, coordenado e resiliente, capaz de proteger os ativos mais valiosos da organização com agilidade e precisão.