E-fólio B | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

NOME: Ricardo Alexandre Castro Lopes Lobo

N.º DE ESTUDANTE: 2100622

CURSO: Licenciatura Engenharia Informática

DATA DE ENTREGA: 19 Dezembro 2024

RESOLUÇÃO

Questão 1: Distribuição Segura de Código-Fonte

Considerando que o código-fonte é o principal ativo da empresa, é crucial implementar medidas para reduzir o risco económico associado a fugas de informação e perda de integridade do software. O desafio é particularmente significativo dado o modelo de trabalho híbrido da empresa, onde a maioria dos colaboradores trabalha remotamente. Assim, é necessária uma solução completa e integrada para garantir a segurança durante o ciclo de desenvolvimento, da distribuição inicial do código até à sua devolução à infraestrutura central.

Para tal, propõe-se a implementação de um sistema integrado que combine controlo de versões, automação de processos de segurança e gestão rigorosa de acessos. Este sistema deve assegurar a confidencialidade, integridade e autenticidade das transferências de código.

1.1 Controlo de Versões

No centro da distribuição segura do código-fonte está a implementação de um sistema de controlo de versões Git hospedado em servidores *on-premise*. Este sistema centralizado permite gerir com segurança todo o ciclo de distribuição e devolução do código entre a infraestrutura central e os colaboradores remotos. O acesso aos repositórios é estritamente controlado através de conexões SSH ou HTTPS cifradas, garantindo a confidencialidade e integridade das transferências.

1.2 Políticas de *Branching* e *Code Review*

A implementação de uma política rigorosa de gestão de *branches* protege o fluxo de trabalho no repositório. As *branches* principais (master, development) são protegidas, exigindo revisões de código (*code review*) e validações automatizadas antes de qualquer fusão (*merge*). Isto previne alterações diretas não validadas e estabelece um processo formal de revisão que fortalece a qualidade e segurança do código.

1.3 Integração e Entrega Contínua

Os *pipelines* de CI/CD (*Continuous Integration / Continuous Delivery*) automatizam a validação e integração segura do código. Cada submissão passa por verificações automatizadas incluindo análise estática, verificação de assinaturas digitais e *scanning* de dependências. As credenciais necessárias são armazenadas em cofres de segredos (*vaults*) integrados com o sistema IAM (*Identity and Access Management*), que será apresentado na Questão 2.

1.4 Assinatura de Código

A assinatura digital das alterações de código é totalmente integrada com o *pipeline* de CI/CD em Jenkins, criando um processo contínuo de verificação de autenticidade. Quando um programador submete código, este deve ser assinado com sua chave privada pessoal. O *pipeline* de CI/CD verifica automaticamente esta assinatura antes de iniciar qualquer processo de *build* ou teste. Se a assinatura for inválida ou estiver ausente, o *pipeline* é interrompido imediatamente e um alerta é gerado. Para alterações válidas, o *pipeline* executa testes automatizados e, após sua conclusão bem-sucedida, o código é novamente assinado, desta vez com uma chave de *build* controlada pelo sistema CI/CD. Esta assinatura dupla garante a rastreabilidade desde o programador individual até o processo de *build*, criando uma cadeia de confiança verificável. As chaves de assinatura são protegidas por módulos de segurança de hardware (HSMs) e geridas através do sistema central de gestão de identidades.

1.5 Infraestrutura de Desenvolvimento Híbrida e Mitigação de Ameaças

A infraestrutura de desenvolvimento híbrida foi projetada especificamente para mitigar várias ameaças comuns ao desenvolvimento distribuído. O repositório Git central, mantido *on-premise*, é protegido por múltiplas camadas de segurança que previnem ataques *Man-in-the-Middle* durante a transferência de código. Todas as conexões são realizadas através de túneis SSH ou HTTPS com certificados válidos e verificação bilateral de certificados, eliminando o risco de servidores falsos. O tráfego é monitorizado por sistemas de detecção de intrusão que identificam padrões suspeitos de transferência de dados. Para os ambientes na

cloud, são utilizadas conexões dedicadas e cifradas entre a infraestrutura *on-premise* e os serviços *cloud*, com *firewalls* específicas para controlar este tráfego. Esta arquitetura híbrida também protege contra ataques de negação de serviço (*DoS - Denial of Service*), uma vez que os sistemas críticos podem continuar a operar mesmo quando os componentes na *cloud* forem afetados. A separação física entre ambientes de desenvolvimento e produção previne que comprometimentos num ambiente afetem os demais.

As soluções apresentadas foram selecionadas considerando o contexto específico da empresa XPTO e as suas necessidades particulares. O sistema de controlo de versões Git foi escolhido por ser robusto e ter gestão distribuída, essencial para uma equipa predominantemente remota. A escolha de manter o repositório central *on-premise*, combinada com ambientes híbridos para desenvolvimento e testes, equilibra a necessidade de controlo sobre o código-fonte com a flexibilidade operacional.

A implementação de *pipelines* de CI/CD com verificações de segurança automatizadas reduz significativamente o risco de introdução de código malicioso ou vulnerável, enquanto a assinatura digital de código garante a autenticidade e responsabilização por cada alteração. A integração destas soluções com um sistema robusto de gestão de identidades assegura que apenas utilizadores autorizados tenham acesso ao código, com níveis de permissão apropriados às suas funções.

Esta abordagem integrada fornece múltiplas camadas de proteção ao principal ativo da empresa - o código-fonte - enquanto mantém a eficiência do processo de desenvolvimento e permite a colaboração segura entre equipas distribuídas. A solução proposta protege contra ameaças externas e internas, estabelecendo uma base sólida para o desenvolvimento seguro do software.

Questão 2: Perímetro de Rede Seguro

A infraestrutura híbrida da empresa XPTO, combinada com uma força de trabalho predominantemente remota, apresenta desafios significativos para a segurança do perímetro de rede. Com 35 funcionários no escritório central e 85 trabalhando remotamente, é crucial implementar uma estratégia de segurança que proteja tanto o acesso local quanto o remoto, mantendo a flexibilidade operacional necessária.

A solução proposta baseia-se nos princípios fundamentais de segurança apresentados no manual: confidencialidade, integridade e disponibilidade, complementados pelo conceito de defesa em profundidade e pelo modelo Zero Trust, onde nenhuma conexão é automaticamente considerada segura.

2.1 Sistema de Gestão de Identidades e Acessos (IAM)

O núcleo da segurança do perímetro é um sistema IAM (*Identity and Access Management*) híbrido que gere centralmente todas as identidades e acessos. Este sistema unifica o controlo de acesso através de toda a infraestrutura, implementando autenticação forte e autorização baseada em funções (RBAC - *Role-Based Access Control*). O IAM integra-se com todos os sistemas críticos, incluindo VPN, repositórios de código e ambientes cloud.

2.2 Rede Privada Virtual (VPN) Corporativa

A conexão segura dos trabalhadores remotos é estabelecida através de uma VPN (*Virtual Private Network*) corporativa utilizando OpenVPN com cifragem AES-256 (*Advanced Encryption Standard*). A autenticação multifator (MFA - *Multi-Factor Authentication*) é obrigatória, utilizando o Aegis Authenticator em dispositivos *Android* fornecidos pela empresa. Esta configuração garante um túnel seguro para todas as comunicações remotas.

2.3 Firewalls de Próxima Geração

As NGFW (*Next-Generation Firewalls*) implementadas incluem capacidades de DPI (*Deep Packet Inspection*), IPS (*Intrusion Prevention System*) e controlo granular de tráfego. Estas firewalls protegem as interfaces entre ambientes *on-premise* e *cloud*, implementando políticas estritas

de segurança e monitorização contínua de todo o tráfego que atravessa o perímetro da rede. Por exemplo, são implementadas ACLs (*Access Control Lists*) que permitem apenas o tráfego SSH (porta 22) e HTTPS (porta 443) para acesso aos repositórios Git, bloqueando todas as outras portas não essenciais.

Adicionalmente, o tráfego dos ambientes de desenvolvimento é isolado do ambiente de produção através de regras específicas que permitem apenas as conexões necessárias entre serviços predefinidos.

2.4 Segmentação de Rede

A implementação de VLANs (*Virtual Local Area Networks*) e microsegmentação através de SDN (*Software-Defined Networking*) divide logicamente os ambientes críticos, como desenvolvimento, testes e produção. Esta segmentação permite isolar o tráfego dos colaboradores no escritório central dos acessos remotos, além de separar os ambientes de desenvolvimento conforme sua importância. Esta separação limita o movimento lateral em caso de comprometimento e facilita o controlo de acesso granular, seguindo o princípio do menor privilégio.

2.5 Sistema de Monitorização e Resposta

Um SIEM (*Security Information and Event Management*) centraliza a monitorização de segurança, correlacionando eventos de múltiplas fontes. Integrado com capacidades SOAR (*Security Orchestration, Automation and Response*), permite respostas automatizadas a incidentes de segurança. Por exemplo, se o sistema detetar múltiplas tentativas falhadas de autenticação VPN a partir do mesmo endereço IP num curto período de tempo, pode automaticamente bloquear esse IP na firewall e enviar um alerta à equipa de segurança para investigação. Este sistema fornece visibilidade completa sobre todas as atividades no perímetro da rede e permite uma resposta rápida e consistente a potenciais ameaças.

As soluções propostas foram selecionadas pela sua eficácia comprovada na proteção de

perímetros de rede em ambientes híbridos. A implementação em camadas, começando com controlo de identidades forte e estendendo-se através de múltiplos mecanismos de segurança, cria uma defesa robusta e adaptável. O uso de tecnologias modernas como NGFW e microsegmentação permite um controlo granular do tráfego, enquanto a monitorização centralizada garante visibilidade completa e capacidade de resposta rápida a incidentes.

Esta arquitetura de segurança não protege apenas a infraestrutura atual, mas também estabelece uma base sólida para o crescimento futuro da empresa, permitindo a adição segura de novos serviços e utilizadores sem comprometer a segurança do perímetro.

Questão 3: Segurança Interna da Rede

Mesmo com um perímetro de rede robusto, a segurança interna é crucial, especialmente considerando que a XPTO possui informação sensível em forma de código-fonte e opera num modelo híbrido. As ameaças internas, sejam acidentais ou maliciosas, podem comprometer seriamente os ativos da empresa. Por isso, é necessária uma abordagem abrangente de segurança interna que complemente as proteções de perímetro já estabelecidas.

A estratégia proposta baseia-se no princípio de defesa em profundidade, implementando múltiplas camadas de controlo e monitorização dentro da rede, assumindo que o perímetro pode ser comprometido.

3.1 *Hardening* de Sistemas

Práticas rigorosas de fortalecimento (*hardening*) são aplicadas em todos os sistemas internos. Isto inclui a criação de imagens base (*golden images* - modelos padronizados de instalação) para servidores e estações de trabalho com configurações seguras predefinidas. Por exemplo, todos os sistemas têm serviços desnecessários desativados, como o SMBv1 (*Server Message Block version 1* - protocolo de partilha de arquivos ultrapassado), e seguem uma política de palavra-passe robusta com rotação automática a cada 90 dias. A gestão centralizada de

atualizações garante que *patches* de segurança críticos são aplicados dentro de 24 horas do seu lançamento.

3.2 Proteção de Dados

A implementação de DLP (*Data Loss Prevention*) monitoriza e controla o movimento de dados sensíveis dentro da rede. São implementadas políticas estritas de classificação e controlo de dados baseadas em padrões específicos. Por exemplo, o sistema pode detetar e bloquear tentativas de envio de código-fonte por email ou transferência para dispositivos USB não autorizados, protegendo assim a propriedade intelectual crítica da empresa.

3.3 Monitorização e Resposta a Incidentes

O centro das operações de segurança interna é um SIEM, já introduzido na questão anterior, que centraliza e correlaciona registos de toda a infraestrutura. Integrado com capacidades SOAR, este sistema permite respostas automatizadas a ameaças. Por exemplo, se um utilizador tentar aceder a um número anormal de repositórios Git num curto espaço de tempo, o sistema pode automaticamente suspender o acesso dessa conta e alertar a equipa de segurança. A monitorização contínua permite a deteção precoce e mitigação de ameaças internas.

3.4 Auditorias e Revisões

Um programa contínuo de auditorias internas e testes de penetração avalia regularmente a eficácia das medidas de segurança. São realizadas verificações mensais de conformidade, incluindo análise de *logs* de acesso aos repositórios Git e revisão de privilégios de utilizador. Os testes de penetração trimestrais simulam tentativas de movimento lateral na rede, identificando potenciais vulnerabilidades antes que possam ser exploradas.

3.5 Gestão de Backups e Recuperação

Uma estratégia robusta de *backups* protege os dados críticos da empresa. São realizados *backups* incrementais diários e completos semanais, com retenção *offline* de 30 dias. A

infraestrutura de *backup* é segregada da rede principal, com autenticação independente e monitorização dedicada. São realizados testes mensais de recuperação para validar a integridade dos *backups* e os procedimentos de restauro.

3.6 Formação e Consciencialização

Um programa abrangente de formação em segurança é implementado para todos os colaboradores. São realizadas sessões mensais de consciencialização, incluindo simulações de tentativas de *phishing* (tentativas fraudulentas de obter informações sensíveis) e exercícios de resposta a incidentes. A análise dos resultados das simulações pode dar origem a ações corretivas personalizadas.

As soluções propostas foram selecionadas para criar uma defesa interna robusta e em profundidade. A combinação de monitorização contínua, controlos técnicos rigorosos e formação regular dos colaboradores cria múltiplas camadas de proteção. Cada componente foi desenhado para complementar os outros, criando um sistema de segurança resiliente que protege os ativos críticos da empresa mesmo em caso de comprometimento do perímetro.

Esta abordagem abrangente não só protege contra ameaças atuais, mas também estabelece uma base sólida para a segurança interna à medida que a empresa continua a crescer e evoluir.

Questão 4: Proteção contra *Malware*

O ambiente de trabalho predominantemente remoto da XPTO, com colaboradores a trabalhar fora do escritório e atualmente com permissões de administração local nos seus computadores, apresenta um risco significativo de infecção por *malware*. Esta situação é particularmente crítica considerando que os computadores têm acesso ao principal ativo da empresa - o código-fonte. É necessária uma abordagem abrangente que combine redução de privilégios, proteção ativa e capacidade de resposta a incidentes.

4.1 Endpoint Detection and Response (EDR)

A implementação do CrowdStrike EDR fornece proteção avançada contra *malware* nos *endpoints* (laptops, telemóveis, tablets, etc). Esta solução monitoriza continuamente os dispositivos, detecta e bloqueia ameaças em tempo real, e permite respostas rápidas a incidentes de segurança. Por exemplo, se um processo tentar encriptar múltiplos ficheiros rapidamente (comportamento típico de ransomware), o EDR pode automaticamente terminar o processo e isolar o sistema da rede.

4.2 Gestão de Privilégios

A remoção de direitos administrativos locais e implementação de PAM (*Privileged Access Management*) reduz significativamente a superfície de ataque. Os acessos privilegiados passam a ser estritamente controlados através de um processo de elevação temporária de privilégios, onde cada pedido é avaliado, aprovado e registado. Por exemplo, quando um programador necessita de instalar uma nova ferramenta de desenvolvimento, deve solicitar elevação temporária de privilégios através do sistema PAM, que regista a atividade e revoga automaticamente os privilégios após a conclusão da tarefa.

4.3 Proteção de E-mail e Web

Filtros avançados de e-mail, incluindo análise em *sandbox* (ambiente isolado de testes) e proteção contra *phishing*, previnem a entrada de *malware* através do vetor mais comum de ataque. Todos os anexos de email são automaticamente analisados em ambiente seguro antes de serem entregues. Adicionalmente, é implementada filtragem de conteúdo web através de um *proxy* seguro, bloqueando acesso a domínios maliciosos conhecidos e analisando downloads em tempo real.

4.4 Gestão de Atualizações

Um sistema centralizado de gestão de *patches* garante que todos os sistemas permaneçam atualizados contra vulnerabilidades conhecidas. As atualizações de segurança são aplicadas

automaticamente seguindo uma política rigorosa: *patches* críticos são instalados dentro de 24 horas, atualizações importantes dentro de uma semana, e atualizações regulares mensalmente. O estado de conformidade de cada dispositivo é monitorizado continuamente.

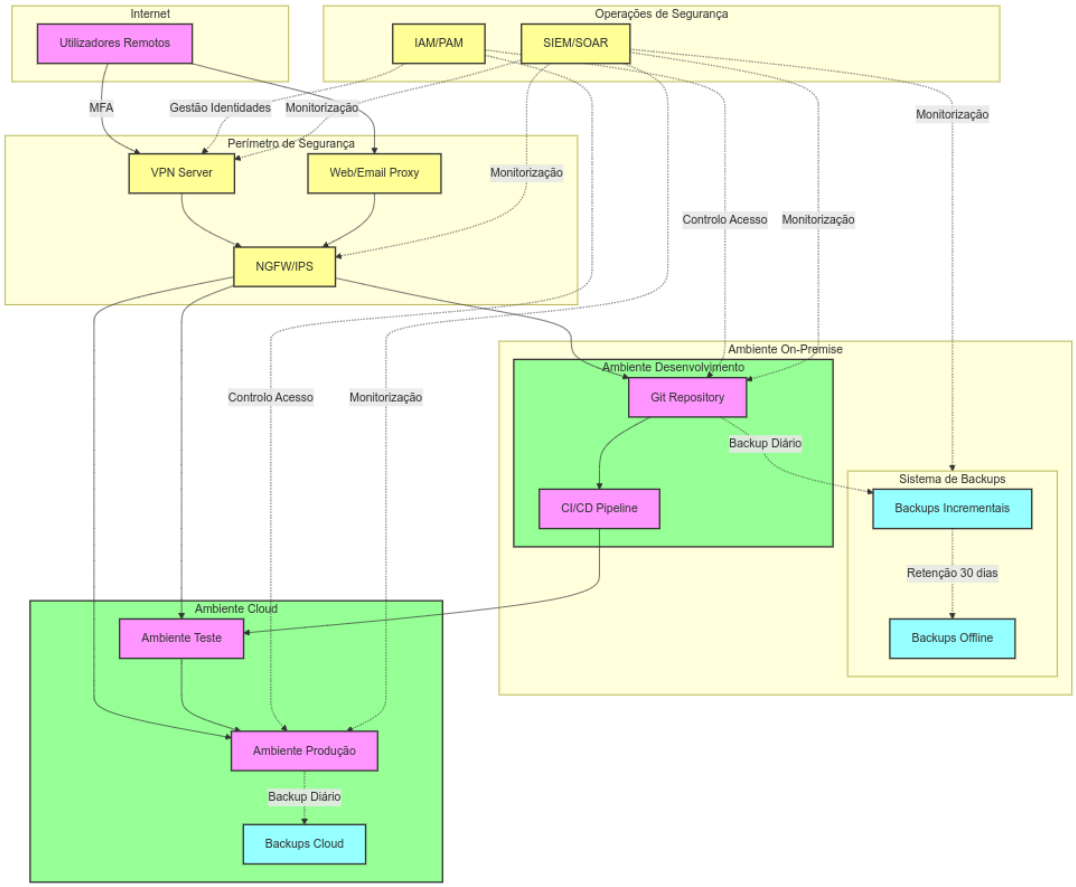
4.5 Recuperação de Incidentes

Procedimentos detalhados de resposta a incidentes de malware são estabelecidos e testados regularmente. Em caso de infecção, o plano inclui isolamento imediato do dispositivo afetado, análise forense para determinar o vetor de ataque, e recuperação através de *backups* validados. Por exemplo, se um dispositivo for infetado com *ransomware*, o sistema EDR isola automaticamente o dispositivo, enquanto a equipa de segurança inicia o protocolo de recuperação utilizando os backups mais recentes.

As soluções propostas trabalham em conjunto para criar uma defesa robusta contra *malware*, especialmente relevante no contexto de trabalho remoto da XPTO. A remoção dos privilégios administrativos locais, combinada com proteção ativa nos *endpoints* e capacidade de resposta a incidentes, reduz significativamente o risco de comprometimento por *malware*. Esta abordagem protege não apenas os dispositivos individuais, mas também salvaguarda o acesso ao código-fonte, o principal ativo da empresa.

Conclusão

As soluções apresentadas formam uma estratégia de segurança integrada e abrangente, desenhada especificamente para atender aos desafios únicos da XPTO. A empresa, que cresceu rapidamente nos últimos três anos, necessitava de uma abordagem que protegesse seu principal ativo - o código-fonte - num ambiente predominantemente remoto.



A proteção começa com a distribuição segura do código-fonte através de um sistema Git protegido e políticas rigorosas de desenvolvimento, continua com um perímetro de rede robusto que permite conexões seguras dos trabalhadores remotos, é reforçada por controlos internos que previnem e detetam ameaças, e culmina com proteção específica contra *malware* nos *endpoints* distribuídos.

Todas estas camadas são integradas através de sistemas centralizados de gestão de identidades e monitorização de segurança, criando uma arquitetura de segurança coesa que equilibra proteção e usabilidade. A solução não apenas resolve as necessidades atuais da XPTO, mas também estabelece uma base sólida para seu crescimento futuro, permitindo a expansão segura tanto da equipa quanto da infraestrutura.

Como ilustrado no diagrama de infraestrutura, cada componente foi posicionado estrategicamente para maximizar a segurança enquanto mantém a eficiência operacional,

resultando numa solução que é tanto robusta quanto prática para o contexto específico da empresa.

Fontes

Anthropic. (2024). Claude AI Assistant (Claude 3.5 Sonnet). https://www.anthropic.com/claude

NIST. (2020). SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology.

OpenAI. (2024). ChatGPT. https://chat.openai.com

Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

Stallings, W., Brown, L. (2024). Computer Security: Principles and Practice. 5th Edition (Global Edition), Pearson.

Nota: Este trabalho foi desenvolvido com o auxílio dos modelos de linguagem Claude e ChatGPT para pesquisa e esclarecimento de conceitos.