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

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

NOME: Luís Carlos Crispim Pereira

N.º DE ESTUDANTE: 2300163

CURSO: LEI – Licenciatura em Engenharia Informática

DATA DE ENTREGA: 20/12/25

TRABALHO / RESOLUÇÃO:

Questão 1 – Distribuição segura de código-fonte para colaboradores remotos

Tendo em conta que o código-fonte constitui o principal ativo da empresa XPTO, a sua distribuição e devolução segura entre a infraestrutura central e os colaboradores remotos deve garantir, de forma consistente, a confidencialidade, a integridade e a autenticidade da informação, ao longo de todo o ciclo de desenvolvimento. Este desafio é particularmente relevante num contexto de trabalho remoto predominante, em que os colaboradores utilizam redes domésticas e equipamentos fora do perímetro físico da organização.

A solução proposta baseia-se numa abordagem integrada, combinando mecanismos técnicos de proteção das comunicações com controlos de acesso rigorosos e processos formais de desenvolvimento, de forma a reduzir o risco de fuga, alteração ou introdução maliciosa de código.

1.1 - Sistema centralizado de controlo de versões

No núcleo da solução encontra-se a utilização de um sistema de controlo de versões distribuído (por exemplo, Git), alojado na infraestrutura central da empresa (on-premise ou em cloud privada). Todo o código-fonte é mantido exclusivamente neste repositório central, sendo o acesso permitido apenas a utilizadores autenticados e autorizados.

As comunicações entre os colaboradores remotos e o repositório devem ser realizadas através de canais cifrados, recorrendo a HTTPS com TLS ou a SSH, garantindo a confidencialidade e a integridade dos dados em trânsito, mesmo quando utilizados em redes não fiáveis.

1.2 - Autenticação forte e controlo de acessos

O acesso ao repositório deve estar integrado com um sistema central de gestão de identidades e acessos (IAM), permitindo autenticação multifator (MFA) e autorização baseada em funções. Desta forma, cada colaborador apenas tem acesso aos repositórios e operações estritamente necessários às suas funções, seguindo o princípio do privilégio mínimo.

Esta abordagem reduz o impacto de credenciais comprometidas e dificulta acessos não autorizados ao código-fonte.

1.3 - Políticas de desenvolvimento e validação do código

Para garantir a integridade do código devolvido pelos colaboradores, devem ser aplicadas políticas rigorosas de desenvolvimento, nomeadamente a utilização de branches dedicadas e a proibição de alterações diretas às branches principais. Todas as alterações devem ser submetidas através de mecanismos de merge request ou pull request, sujeitas a revisão por pares e a validações automáticas.

Este processo reduz o risco de introdução de código malicioso ou defeituoso e cria um registo auditável de todas as alterações efetuadas.

1.4 - Automatização e validação através de CI/CD

A integração de pipelines de Integração Contínua (CI) permite automatizar a validação do código submetido, através de testes, análise estática e verificações de integridade. Apenas código que cumpra os critérios definidos é aceite na infraestrutura central.

Esta automatização assegura que o código devolvido pelos colaboradores remotos mantém um nível consistente de qualidade e segurança, reduzindo a dependência de validações manuais.

1.5 - Garantia de autenticidade e rastreabilidade

Sempre que possível, as submissões de código devem estar associadas a mecanismos de assinatura ou identificação forte do autor, assegurando a rastreabilidade das alterações. Esta medida reforça a responsabilização individual e dificulta ataques internos ou alterações não autorizadas.

Síntese/Justificação da solução

A solução proposta estabelece um modelo integrado para a distribuição e devolução segura do código-fonte, assente na centralização do controlo de versões, na proteção das comunicações e na aplicação de controlos rigorosos de acesso e validação. O uso de canais cifrados (TLS ou SSH) assegura a confidencialidade e a integridade do código durante a sua transferência, mitigando riscos associados à utilização de redes domésticas ou públicas por parte dos colaboradores remotos.

A integração com um sistema de gestão de identidades, aliada à autenticação multifator e à atribuição de permissões baseadas em funções, reduz significativamente a probabilidade de acessos não autorizados e limita o impacto de um eventual comprometimento de credenciais. Em paralelo, as políticas de desenvolvimento, como a utilização de branches dedicadas, revisões de código e validações automáticas em pipelines de integração contínua, garantem que apenas código verificado e validado é integrado na infraestrutura central, protegendo a integridade do software desenvolvido.

Adicionalmente, a associação das alterações de código a identidades bem definidas reforça a rastreabilidade e a responsabilização, dificultando ataques internos e facilitando auditorias futuras. Esta abordagem não só reduz a superfície de ataque associada ao desenvolvimento distribuído, como também cria um processo consistente e controlado, alinhado com as boas práticas de segurança da informação.

De forma global, a solução equilibra eficazmente os requisitos de segurança com as necessidades operacionais da empresa, permitindo a colaboração eficiente entre equipas distribuídas sem comprometer a proteção do principal ativo da organização. Ao conjugar mecanismos técnicos, controlos organizacionais e processos bem definidos, estabelece-se uma base sólida para o desenvolvimento seguro de software num contexto de crescimento e trabalho remoto.

Questão 2 – Implementação de um perímetro de rede seguro numa infraestrutura híbrida

A empresa XPTO possui atualmente cerca de 120 colaboradores, dos quais aproximadamente 35 trabalham de forma permanente no escritório central, enquanto os restantes desempenham as suas funções remotamente. Este modelo de trabalho híbrido, aliado à coexistência de infraestrutura on-premise e serviços em cloud, exige a implementação de um perímetro de rede seguro que permita acessos remotos frequentes, sem comprometer a confidencialidade, a integridade e a disponibilidade dos sistemas e da informação.

Neste contexto, a proteção do perímetro não pode assentar apenas em mecanismos tradicionais, devendo antes basear-se numa abordagem em camadas, alinhada com os princípios de defesa em profundidade e Zero Trust, assumindo que nenhuma ligação é fiável por defeito, independentemente da sua origem.

2.1 - Gestão centralizada de identidades e acessos

O elemento central do perímetro de segurança deve ser um sistema de gestão de identidades e acessos (IAM), responsável por autenticar e autorizar todos os utilizadores, quer se encontrem no escritório, quer estejam a aceder remotamente. Este sistema deve suportar autenticação multifator (MFA) e autorização baseada em funções, garantindo que cada colaborador apenas acede aos recursos necessários ao desempenho das suas funções.

A centralização do controlo de acessos permite reduzir significativamente o risco associado a credenciais comprometidas e facilita a revogação imediata de acessos em caso de incidente ou cessação de funções.

2.2 - Acesso remoto seguro através de VPN

O acesso dos colaboradores remotos à infraestrutura central deve ser realizado através de uma Rede Privada Virtual (VPN), estabelecendo túneis cifrados entre os dispositivos dos utilizadores e a rede da empresa. A utilização de cifragem forte e a integração da VPN com o sistema IAM e MFA garantem que o tráfego remoto não pode ser intercetado ou alterado por terceiros.

Esta solução permite que os colaboradores acedam aos serviços internos de forma transparente, como se estivessem ligados à rede local, mantendo simultaneamente o isolamento face a redes domésticas ou públicas.

2.3 - Firewalls e controlo rigoroso do tráfego

O perímetro da infraestrutura híbrida deve ser protegido por firewalls configuradas com políticas restritivas, tanto na componente on-premise como nos ambientes em cloud. As regras devem seguir o princípio de deny by default, permitindo apenas o tráfego estritamente necessário ao funcionamento dos serviços.

Por exemplo, o acesso aos repositórios de código pode ser limitado a ligações cifradas em portas específicas, enquanto todo o restante tráfego não essencial é bloqueado. Este controlo reduz a superfície de ataque e dificulta a exploração de serviços indevidamente expostos.

2.4 - Segmentação da rede e isolamento de ambientes

A segmentação lógica da rede, através de mecanismos como Virtual Local Area Networks (VLANs), permite separar diferentes tipos de tráfego e ambientes, como desenvolvimento, testes e produção, bem como distinguir acessos provenientes do escritório central e de utilizadores remotos.

Este isolamento limita o movimento lateral em caso de comprometimento de um sistema ou de uma conta, reduzindo o impacto de um eventual ataque e facilitando a aplicação de políticas de segurança específicas a cada segmento da rede.

2.5 - Monitorização e deteção de intrusões

A implementação de mecanismos de monitorização contínua, como sistemas de deteção e prevenção de intrusões (IDS/IPS), permite identificar tentativas de acesso indevido ou padrões de tráfego anómalos no perímetro da rede. A recolha e análise centralizada de registos facilita a deteção precoce de incidentes e a resposta atempada a potenciais intrusões.

Esta capacidade de visibilidade é particularmente importante num ambiente híbrido, onde o tráfego circula entre múltiplas localizações e infraestruturas distintas.

Síntese/Justificação da solução

A solução proposta define um perímetro de rede seguro adequado a uma infraestrutura híbrida e a um modelo de trabalho maioritariamente remoto. A centralização da gestão de identidades, aliada à autenticação multifator, garante que apenas utilizadores devidamente autenticados e autorizados conseguem aceder à infraestrutura da empresa, reduzindo o risco associado a credenciais comprometidas.

O acesso remoto através de VPN assegura a confidencialidade e a integridade das comunicações entre os colaboradores e a infraestrutura central, protegendo o tráfego que circula em redes domésticas ou públicas. Em complemento, a aplicação de políticas restritivas nas firewalls e a segmentação lógica da rede permitem limitar a superfície de ataque e dificultar o movimento lateral em caso de comprometimento de um sistema ou de uma conta.

A monitorização contínua do perímetro, suportada por mecanismos de deteção e prevenção de intrusões, fornece visibilidade sobre o tráfego e os acessos, permitindo identificar atempadamente comportamentos anómalos. De forma global, a abordagem em camadas adotada permite equilibrar a necessidade de acessos remotos frequentes com a proteção dos sistemas internos, garantindo um perímetro de rede coerente, controlado e alinhado com as boas práticas de segurança.

Questão 3 – Medidas adicionais de segurança no interior da rede

Mesmo com a implementação de um perímetro de rede seguro, é necessário assumir que nenhum mecanismo de proteção é infalível e que um atacante pode, eventualmente, conseguir ultrapassar as defesas externas. Assim, a segurança no interior da rede deve ser concebida segundo o princípio da defesa em profundidade, aplicando controlos adicionais que permitam reduzir a superfície de ataque interna, limitar o impacto de incidentes e detetar comportamentos anómalos de forma atempada.

3.1 - Endurecimento e configuração segura dos sistemas

A segurança interna deve começar pela aplicação consistente de práticas de endurecimento (hardening) em todos os sistemas, incluindo servidores e estações de trabalho. Para garantir uniformidade e reduzir erros de configuração, é recomendada a utilização de imagens base padronizadas (golden images), previamente configuradas de acordo com boas práticas de segurança. Estas imagens devem incluir apenas os serviços estritamente necessários, com funcionalidades obsoletas ou inseguras desativadas por defeito.

Deve ainda existir um processo centralizado de gestão de atualizações, assegurando que correções de segurança e patches críticos são aplicados de forma regular e atempada. A redução da janela de exposição a vulnerabilidades conhecidas diminui significativamente a probabilidade de exploração bem-sucedida por parte de atacantes com acesso à rede interna.

No que respeita à autenticação, devem ser aplicadas políticas de palavras-passe robustas, incluindo requisitos de complexidade e rotação periódica, por exemplo a cada 90 dias, sobretudo para contas privilegiadas ou associadas a sistemas críticos. Estas medidas reduzem o risco de reutilização de credenciais e dificultam ataques prolongados baseados em acessos indevidos.

3.2 - Controlo de acessos internos e separação de privilégios

No interior da rede, o controlo de acessos deve continuar a seguir o princípio do privilégio mínimo, assegurando que utilizadores e serviços apenas dispõem das permissões estritamente necessárias ao desempenho das suas funções. A separação de privilégios entre diferentes perfis de utilizador e entre ambientes distintos, como desenvolvimento, testes e produção, reduz o impacto de acessos indevidos e limita a escalada de privilégios em caso de comprometimento.

A aplicação consistente destas políticas contribui para a proteção de ativos sensíveis, como repositórios de código-fonte e servidores críticos, mesmo quando um atacante consegue obter acesso inicial à rede.

3.3 - Segmentação interna e limitação do movimento lateral

A segmentação interna da rede deve ser reforçada através da separação lógica de diferentes áreas funcionais e tipos de sistemas. Esta segmentação permite isolar serviços críticos e restringir a comunicação entre segmentos apenas ao estritamente necessário ao funcionamento normal da infraestrutura.

Ao limitar o movimento lateral, reduz-se significativamente o alcance de um incidente de segurança, dificultando a progressão de um atacante para sistemas de maior valor ou sensibilidade e contribuindo para a contenção de danos.

3.4 - Monitorização interna, auditoria e deteção de comportamentos anómalos

A monitorização contínua da atividade interna da rede é essencial para a deteção precoce de incidentes de segurança. A recolha e análise de registos de acesso, eventos de sistema e padrões de tráfego permitem identificar comportamentos anómalos, como tentativas repetidas de acesso a recursos sensíveis ou atividades incompatíveis com o perfil normal de um utilizador.

Estes mecanismos de monitorização suportam igualmente processos de auditoria interna, permitindo verificar o cumprimento das políticas de segurança, identificar desvios de configuração e facilitar a investigação de incidentes. A deteção atempada de atividades suspeitas contribui para uma resposta mais rápida e eficaz, reduzindo o impacto de ataques internos ou externos.

3.5 - Formação e consciencialização dos utilizadores

Os utilizadores continuam a representar uma das principais superfícies de ataque no interior da rede. A promoção de ações regulares de formação e consciencialização em segurança contribui para reduzir riscos associados a erros humanos, como a execução de software malicioso, a utilização de palavras-passe fracas ou a divulgação inadvertida de credenciais.

Uma maior sensibilização dos colaboradores reforça a eficácia das medidas técnicas implementadas e contribui para uma postura de segurança mais consistente em toda a organização.

Síntese/Justificação da solução

As medidas propostas reforçam a segurança no interior da rede ao assumir explicitamente que o perímetro pode ser comprometido e ao aplicar controlos adicionais orientados para a redução da superfície de ataque, a contenção de danos e a deteção precoce de incidentes. O endurecimento dos sistemas, o controlo rigoroso de acessos, a segmentação interna e a monitorização contínua atuam de forma complementar, criando múltiplas camadas de proteção.

A existência de mecanismos de auditoria e de monitorização facilita a identificação de incidentes e suporta uma resposta mais eficaz, enquanto a implementação de políticas adequadas de autenticação e de recuperação, nomeadamente através de cópias de segurança regulares, contribui para a resiliência da infraestrutura e para a recuperação de serviços em caso de falha ou ataque. De forma global, esta abordagem em profundidade aumenta a robustez da rede interna e contribui para a proteção contínua dos ativos críticos da empresa.

Questão 4 – Ameaças de malware em contexto de trabalho remoto

O modelo de trabalho remoto adotado pela empresa XPTO aumenta significativamente a exposição a ameaças de malware, uma vez que os colaboradores utilizam dispositivos fora do perímetro físico da organização e recorrem frequentemente a redes domésticas ou públicas. Este risco é particularmente elevado quando os utilizadores dispõem de privilégios administrativos nos seus equipamentos, permitindo que código malicioso seja executado com permissões elevadas e comprometa não apenas o sistema local, mas também recursos internos da empresa.

Neste contexto, a mitigação das ameaças de malware deve assentar numa combinação de medidas técnicas e organizacionais, orientadas para a prevenção, deteção e resposta a incidentes.

4.1 Gestão e limitação de privilégios administrativos

A atribuição de privilégios administrativos nos dispositivos dos colaboradores deve ser rigorosamente controlada. Sempre que possível, os utilizadores devem operar com contas sem privilégios elevados, recorrendo a mecanismos de gestão de acessos privilegiados (Privileged Access Management – PAM) para executar tarefas administrativas apenas quando estritamente necessário.

Esta abordagem reduz significativamente o impacto de infeções por malware, dificultando a instalação persistente de software malicioso e a alteração de configurações críticas do sistema.

4.2 Proteção avançada dos endpoints

Os dispositivos utilizados em trabalho remoto devem estar protegidos por soluções avançadas de segurança para endpoints, como plataformas de Endpoint Detection and Response (EDR). Estas soluções permitem não só a deteção de malware conhecido, mas também a identificação de comportamentos anómalos, como tentativas de escalada de privilégios, execução de código suspeito ou comunicações maliciosas.

A deteção baseada em comportamento é particularmente relevante para mitigar ameaças mais avançadas, que possam não ser identificadas por mecanismos tradicionais baseados em assinaturas.

4.3 Atualizações, correções de segurança e controlo de aplicações

A aplicação regular de atualizações e correções de segurança nos sistemas operativos e aplicações instaladas nos dispositivos remotos é essencial para reduzir a exploração de vulnerabilidades conhecidas. Adicionalmente, devem ser aplicadas políticas de controlo de aplicações (application control), permitindo apenas a execução de software autorizado.

Estas medidas reduzem significativamente a superfície de ataque e dificultam a introdução e execução de malware através de aplicações não confiáveis ou vulneráveis.

4.4 Controlo de dispositivos externos e vetores de infeção

A utilização de dispositivos externos, como unidades USB, constitui um vetor frequente de infeção por malware. Devem ser aplicadas políticas que limitem ou controlem a utilização destes dispositivos nos equipamentos corporativos, em particular em dispositivos com acesso a recursos internos sensíveis.

O controlo destes vetores reduz a probabilidade de infeções acidentais e complementa as restantes medidas de proteção dos endpoints.

4.5 Deteção e resposta a incidentes de malware

Para além da prevenção, é essencial garantir capacidade de deteção e resposta a incidentes de malware. As soluções de EDR, em conjunto com mecanismos de monitorização centralizada, permitem identificar rapidamente sinais de comprometimento e atuar de forma eficaz, por exemplo através do isolamento do dispositivo afetado ou da remoção de software malicioso.

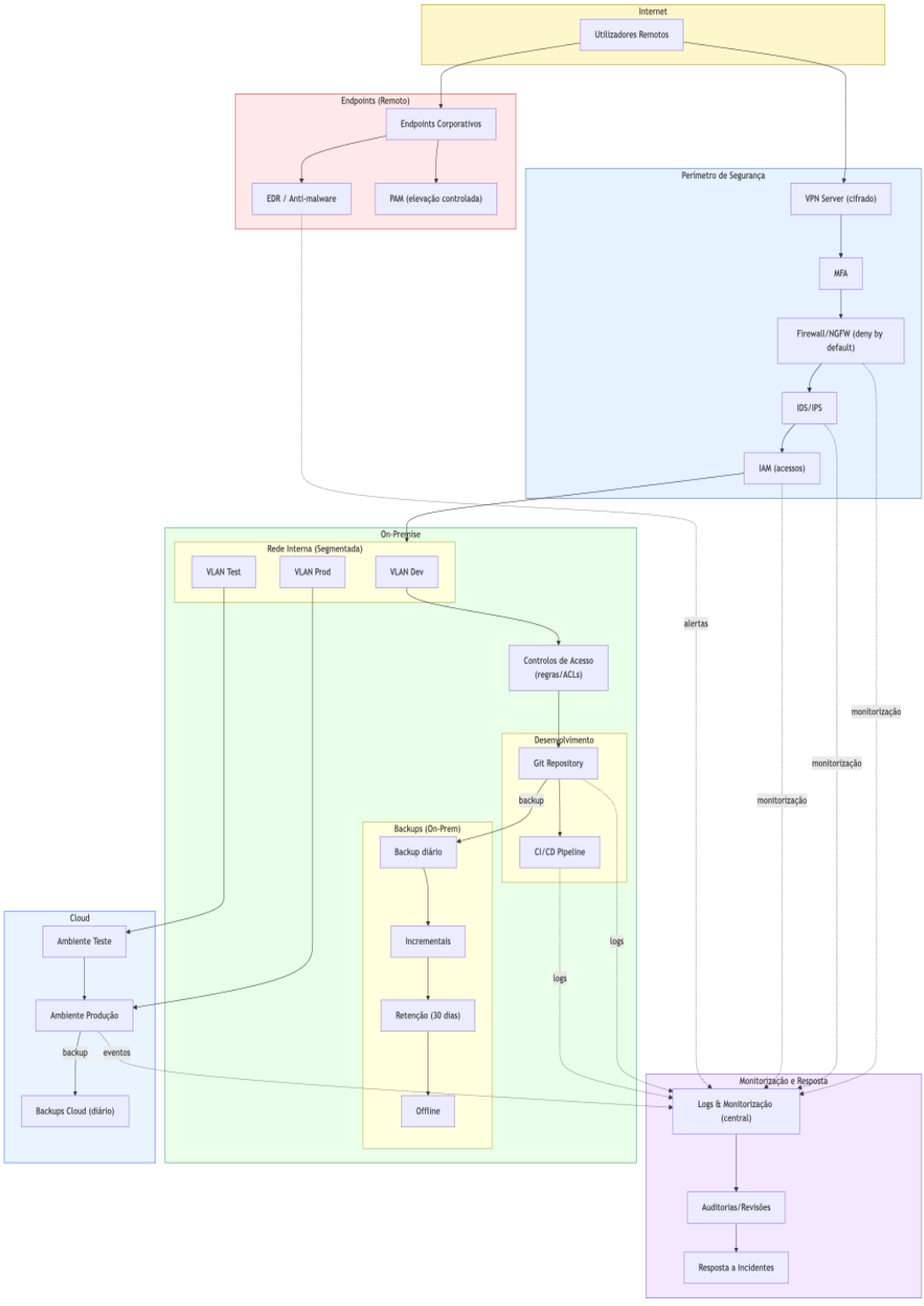
Uma resposta atempada reduz o impacto do incidente e limita a propagação do malware para outros dispositivos ou para a rede interna da empresa.

Síntese/Justificação da solução

A mitigação das ameaças de malware em contexto de trabalho remoto exige uma abordagem integrada, combinando a gestão rigorosa de privilégios administrativos, a proteção avançada dos endpoints através de soluções EDR, a aplicação consistente de atualizações de segurança e o controlo da execução de software e de dispositivos externos. Estas medidas reduzem significativamente a probabilidade de infeção e o impacto de ataques bem-sucedidos.

Adicionalmente, a capacidade de deteção e resposta a incidentes permite identificar rapidamente compromissos de segurança e atuar de forma eficaz para conter danos e restaurar os sistemas afetados. De forma global, a solução proposta reforça a postura de segurança da empresa face a malware, mesmo num cenário de trabalho remoto com dispositivos distribuídos e potenciais privilégios administrativos.

Representação esquemática da arquitetura de segurança



Conclusão

O presente trabalho abordou a segurança de uma infraestrutura híbrida num contexto de trabalho maioritariamente remoto, partindo do princípio de que o código-fonte constitui o principal ativo da empresa XPTO e, como tal, deve ser protegido ao longo de todo o seu ciclo de vida. Ao longo das quatro questões foram analisados e propostos mecanismos de segurança complementares, cobrindo a distribuição segura do código, a proteção do perímetro de rede, a segurança no interior da infraestrutura e a mitigação de ameaças de malware associadas ao trabalho remoto.

A centralização do controlo de versões, aliada ao uso de comunicações cifradas, autenticação multifator e políticas rigorosas de desenvolvimento, permite garantir a confidencialidade, a integridade e a rastreabilidade do código-fonte, mesmo quando os colaboradores operam a partir de redes externas à organização. A automatização de validações através de pipelines de integração contínua reforça este processo, reduzindo o risco de introdução de código malicioso ou defeituoso na infraestrutura central.

A implementação de um perímetro de rede seguro, suportado por mecanismos como VPN, firewalls configuradas de forma restritiva, sistemas de deteção e prevenção de intrusões e gestão centralizada de identidades, assegura que os acessos à infraestrutura são controlados e monitorizados de forma consistente. A segmentação lógica da rede, através de VLANs e controlos de acesso internos, contribui adicionalmente para limitar o movimento lateral e reduzir o impacto de eventuais compromissos de segurança.

No interior da rede, a adoção de uma estratégia de defesa em profundidade, assente no endurecimento dos sistemas, no controlo rigoroso de privilégios, na monitorização contínua e na existência de mecanismos de auditoria e cópias de segurança, permite assumir de forma realista que nenhuma camada isolada é infalível. Estas medidas aumentam a resiliência da infraestrutura e facilitam a deteção precoce e a resposta eficaz a incidentes.

Relativamente às ameaças de malware em contexto de trabalho remoto, a limitação de privilégios administrativos, a utilização de soluções de proteção avançada dos endpoints e a integração com mecanismos de monitorização e resposta a incidentes revelam-se fundamentais para reduzir o impacto de infeções e conter rapidamente potenciais compromissos de segurança, protegendo tanto os dispositivos dos colaboradores como os recursos internos da empresa.

O esquema síntese apresentado complementa a análise desenvolvida ao longo do trabalho, oferecendo uma visão integrada da arquitetura de segurança proposta e evidenciando a forma como os diferentes mecanismos e camadas de proteção interagem entre si. Em termos globais, a solução apresentada equilibra de forma adequada os requisitos de segurança com as necessidades operacionais da empresa, permitindo a colaboração eficiente entre equipas distribuídas sem comprometer a proteção dos ativos críticos, constituindo uma base sólida para a segurança da infraestrutura da empresa XPTO num contexto de evolução e crescimento contínuos.

Referências

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

ENISA. (2023). Cybersecurity best practices for remote working. European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu

ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security management systems — Requirements. International Organization for Standardization.

NIST. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). National Institute of Standards and Technology. Disponível em: https://csrc.nist.gov

NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology. Disponível em: https://csrc.nist.gov

OWASP. (2023). OWASP Top 10 – The ten most critical web application security risks. Disponível em: https://owasp.org

Stallings, W. (2018). Network security essentials: Applications and standards (6th ed.). Pearson.

Nota: Houve utilização pontual de ferramentas de IA generativa como apoio à redação do texto. A análise técnica, os conteúdos de segurança e os esquemas apresentados foram integralmente elaborados, estruturados e validados pelo autor.