

A woman with dark hair and glasses is looking at a tablet. The background is a blurred digital environment with blue and white light effects, suggesting a high-tech or cybersecurity setting. The text is overlaid on a white curved shape on the left side of the image.

DOCUMENTO TÉCNICO

11 controles de segurança para reduzir o risco cibernético

Formas práticas de fortalecer suas defesas, melhorar sua resiliência cibernética e diminuir o risco organizacional.

Sumário executivo

Para a liderança de uma organização, é importante entender que a otimização de seus controles de segurança é muito mais do que simplesmente proteger dados e sistemas: significa reduzir riscos organizacionais vinculados à reputação da marca, à confiança do cliente e à continuidade dos negócios. Os ataques cibernéticos, como ransomware e comprometimento de e-mail corporativo (BEC), podem resultar em graves consequências financeiras e operacionais. A previsão é de que o crime cibernético custe ao mercado mundial US\$ 1,2 trilhão em 2025,¹ de acordo com a Cyber Defense Magazine. Mesmo quando mitigados, os ataques podem causar grandes interrupções caso sistemas precisem ser colocados offline para redefinir e recompilar. Algumas organizações conseguem sobreviver a essa situação. Outras enfrentam questões existenciais que nunca previram.

O papel dos controles de segurança na maximização das defesas cibernéticas

Controles de segurança são alavancas que as equipes de segurança podem acionar para reduzir riscos e proteger a organização contra ameaças. Existem vários tipos de controles, mas todos compartilham um objetivo comum: prevenir incidentes e violações ou minimizar danos quando ocorrem eventos de segurança. Alguns tendem mais à prevenção, outros oferecem diferentes níveis de mitigação no processo de prevenção, detecção e resposta. A combinação adequada de controles de segurança em todas as áreas é chave no estabelecimento de uma defesa profunda.

Controles de segurança fortes também são um componente crítico no gerenciamento de risco através do seguro de proteção digital. As seguradoras consideram os controles das organizações ao estabelecer prêmios e limites de cobertura.

Normalmente, isso cobre:

Responsabilidades do primeiro beneficiário incluem danos diretos infringidos à sua organização por um ataque cibernético ou violação, que pode envolver a paralisação dos negócios, custos de restauração de dados, roubo ou pagamentos de ransomware.

Responsabilidades de terceiros partem de clientes, parceiros, órgãos reguladores ou outras entidades e podem incluir processos legais, pedidos de compensação ou multas regulamentares impostas por agências governamentais e/ou associações comerciais.

US\$ 1,2 trilhão

Em 2025, a previsão é de que o crime cibernético custe ao mercado mundial US\$ 1,2 trilhão.¹

Por que importa

Melhores controles não apenas protegem as suas operações — eles podem reduzir prêmios do seguro de proteção digital e melhorar o resultado dos sinistros.

Reduza riscos cibernéticos com estes 11 controles de segurança

Investir em controles fortes ajuda a reduzir o risco cibernético e pode ajudar a melhorar a sua elegibilidade ao seguro digital e os termos e condições de uma futura apólice. Relacionamos a seguir 11 controles fundamentais que fortalecem as defesas em uma gama de categorias de prevenção e redução de impacto.

Implemente-os de forma adequada e sua postura de segurança cibernética será impulsionada por esses controles de segurança, preparando-o para as ameaças atuais e futuras.

1 Gerenciamento de acesso e identidade

2 Segurança de endpoint

3 Autenticação multifator

4 Gerenciamento de vulnerabilidades

5 Segurança de e-mail

6 Gerenciamento de sessão privilegiada

7 Gerenciamento de ativos

8 Segmentação e arquitetura

9 Detecção e resposta estendidas (XDR)

10 Backup e continuidade dos negócios

11 Segurança de rede e controle de tráfego

1. Gerenciamento de acesso e identidade

Gerenciamento de acesso e identidade (IAM) assegura que apenas pessoas autorizadas possam acessar dados e sistemas. Gerenciamento de acesso privilegiado (PAM) limita o acesso dos usuários ao estritamente necessário às suas funções. Pode parecer simples, mas também pode se transformar rapidamente em um campo minado, especialmente para as grandes organizações. Todas as empresas deveriam manter processos rigorosos de admissão e demissão de funcionários, aplicar procedimentos de senha forte e fazer auditorias rotineiras de acesso.

Independentemente do tamanho, toda organização deve ter regras claras para remover identidades obsoletas — do contrário, os golpistas poderão explorar contas esquecidas para escalonar privilégios e mover-se lateralmente pelo seu ambiente sem ser detectados.

2. Segurança de endpoint

Todo dispositivo conectado ao seu ambiente é um alvo em potencial. O trabalho híbrido aumentou a exposição, fazendo da proteção de endpoint algo ainda mais crítico. Muitos ataques começam com ameaças de “baixo nível” que ferramentas de endpoint fortes podem detectar e neutralizar. Contudo, os endpoints esquecidos e sem suporte se transformam rapidamente em fraquezas e passam a ser um ponto de entrada comum aos [ataques de ransomware remoto](#). Assegure-se de que todos os dispositivos estejam cobertos.

3. Autenticação multifator

A autenticação multifator (MFA) valida a identidade de um usuário usando diferentes fatores: algo que o usuário conhece (por exemplo, senha), algo que o usuário tem (por exemplo, um token) ou algo que ao usuário pertence (por exemplo, sua impressão digital). As credenciais comprometidas continuam sendo uma das causas mais frequentes de ataque,² e a MFA representa um controle vital para as organizações modernas. Considere formas mais avançadas, como a geolocalização e a correspondência numérica, para melhorar a resiliência contra as táticas evasivas dos golpistas e encontrar um equilíbrio entre experiência e privacidade do usuário.

Conclusões

Contas dormentes e privilégios não utilizados são pontos de entrada fáceis para os golpistas. Uma vez dentro do sistema, elas podem ser usadas para obter acesso elevado e silenciosamente expandir o alcance de um ataque.

O ponto de entrada mais comum é, geralmente, o menos visível. Não deixe que endpoints desatualizados se transformem em backdoors.

Implemente uma MFA adaptável para aumentar a verificação em cenários de alto risco sem criar atrito desnecessário.

4. Gerenciamento de vulnerabilidades

Gerenciamento de vulnerabilidades é o processo corrente de identificação, avaliação e remediação das fraquezas na segurança do seu ambiente. Isso inclui práticas comuns, como aplicação de patches em softwares e sistemas, configuração de atualizações e monitoramento de vulnerabilidades recém-descobertas. Uma inteligência de ameaça forte é um fator crítico para ajudar a se manter à frente dos riscos emergentes.

Saber onde os ativos residem na sua rede é essencial para uma varredura completa. Com essa visibilidade, as organizações podem seguir uma abordagem baseada em risco para [priorizar quais vulnerabilidades resolver primeiro](#) — com base na exposição, probabilidade de exploração e impacto comercial.

5. Segurança de e-mail

Apesar de ser uma tecnologia antiga, o e-mail continua a ser um dos principais pontos de entrada dos invasores. Phishing, em particular, é um vetor comum de ransomware e roubo de credenciais. O comprometimento de e-mail corporativo (BEC) também se encontra entre os sinistros de seguro de proteção digital mais frequentes.³ Uma segurança de e-mail forte pode impedir que o conteúdo malicioso se aproxime da sua caixa de entrada, fazendo dela uma linha crítica de defesa. Como a IA generativa melhora as táticas de phishing com mensagens mais bem escritas, as proteções precisam evoluir para diminuir a taxa de sucesso desses ataques antes que atinjam os usuários.

Mas a proteção não deve parar na entrega: as URLs e anexos que, inicialmente, parecem seguros, podem se tornar maliciosos após a mensagem chegar à caixa de entrada. Agora, as [soluções avançadas de segurança de e-mail](#) oferecem detecção e remediação pós-entrega, que faz uma nova varredura automática do conteúdo, separa as mensagens maliciosas e neutraliza os links caso o perfil de risco mude. Esses controles ajudam a capturar ameaças que burlam as defesas iniciais e a minimizar o tempo que as mensagens mal-intencionadas permanecem na caixa de entrada dos usuários.

Conclusões

Procure vulnerabilidades nos seus serviços de nuvem e aplicativos de terceiros, não apenas em seus sistemas principais.

Um clique é tudo de que se precisa. A melhor forma de acabar com o phishing é garantir que os usuários nunca mordam a isca, inclusive depois da entrega.

6. Gerenciamento de sessão privilegiada

Contas administrativas dão aos agentes de ameaças um imenso poder, especialmente quando esses privilégios incluem acesso a sistemas de identidade, controles de configuração e ferramentas de segurança. Se um invasor conseguir acesso no nível de administrador, ele poderá desabilitar defesas e lançar ransomwares em grande escala.

Para diminuir o risco, as organizações deveriam implementar um modelo em camadas para o acesso privilegiado e monitorar ativamente como essas contas são usadas. O Gerenciamento de sessão privilegiada (PSM) proporciona supervisão através de log, gravação e, em alguns casos, controle de sessões admin em tempo real, ajudando a detectar atividades suspeitas, prevenir o uso indevido e dar suporte à conformidade.

7. Gerenciamento de ativos

Você não pode proteger aquilo que não sabe que tem. As organizações devem manter atualizados os seus inventários de ativos físicos e de dados. Durante um incidente, é crítico saber onde estão armazenados os dados mais sensíveis para fazer uma investigação eficiente, gerar relatórios precisos e realizar uma contenção rápida. O gerenciamento adequado de ativos auxilia na investigação detalhada, ajuda a estabelecer as responsabilidades e diminui o impacto da violação.

8. Segmentação e arquitetura

Quando um agente de ameaça consegue obter acesso ao seu ambiente, o próximo passo esperado é o movimento lateral, utilizado para tentar escalonar privilégios, acessar sistemas sensíveis ou implantar um ransomware; mas a segmentação de rede forte e o design arquitetônico podem dificultar essa movimentação interna. Ao criar atrito e forçar os golpistas a criar ruído, a segmentação aumenta as suas chances de detectá-los antecipadamente na cadeia de ataque.

A arquitetura do seu sistema deve ser edificada sobre os princípios da confidencialidade, integridade, disponibilidade e resiliência. Isso inclui limitar o acesso sistema a sistema e usuário a sistema por meio de um modelo Zero Trust, em que cada transação é verificada com base na identidade, dispositivo e permissões do usuário.

Conclusões

Você pode ver quem acessou a sua camada admin na última terça-feira e o que fizeram, exatamente? Se não puder, é hora de acirrar a supervisão.

Manter registros desnecessários pode inflar os custos do seguro de proteção digital e multiplicar o danos de reputação durante uma violação.

Use a segmentação de rede para isolar sistemas críticos dos pontos de acesso de rotina.

9. Detecção e resposta estendidas (XDR)

Trabalhar com dezenas de ferramentas distintas pode fragmentar os alertas, retardar a triagem e ocultar a atividade das ameaças. A [Detecção e resposta estendidas \(XDR\)](#) corrige isso ao oferecer uma exibição unificada das atividades de endpoints, firewall, rede, e-mail, identidade, backup e sistemas de segurança de nuvem, reduzindo o ruído de alertas e possibilitando uma tomada de decisão mais rápida e confiante. Isso elimina o cenário de “cadeira giratória”, em que os analistas precisam trocar entre ferramentas independentes para investigar e responder a ameaças.

Sistemas XDR mais robustos também aplicam análises avançadas, detecção priorizada por IA, pesquisa profunda de dados, e correlação e escalonamento automatizados de alertas. Essa convergência de recursos melhora a precisão da detecção, acelera as investigações e ajuda as equipes de segurança a se concentrarem nas ameaças de mais alto risco sem se envolverem no mérito das ferramentas.

10. Backup e continuidade dos negócios

Quando um incidente cibernético interrompe as suas operações ou corrompe os seus sistemas, backups bem preparados e um plano forte de continuidade dos negócios podem ser a diferença entre uma recuperação fácil e um extenso período de inatividade. Contudo, nem todos os backups são criados do mesmo modo. Para serem eficientes, os backups devem ser validados, testados regularmente e capazes de restaurar sistemas e dados na íntegra.

Uma falha comum ocorre na configuração. Muitas organizações descobrem tarde demais que seus backups restauram seus sistemas apenas parcialmente ou que perdem dados críticos, transformando uma interação de curto prazo em uma contenda de semanas.

Da mesma forma, também é importante que os backups estejam protegidos por meio de autenticação fora da banda. Sem ela, um agente de ameaça com amplo acesso pode tentar desabilitar ou remover os dados de backup como uma parte do ataque.

Conclusões

O XDR transforma alertas desconexos em ações decisivas, acelerando as investigações e melhorando o conteúdo das respostas.

Mantenha os backups segmentados e offline sempre que possível. Não trabalhe com apenas um único canal de recuperação, nunca.

11. Segurança de rede e controle de tráfego

A rede é mais do que uma camada de conexão — ela é um ponto de controle estratégico para inspecionar, filtrar e gerenciar o tráfego no seu ambiente. Firewalls, sistemas de prevenção de invasão (IPSs), filtragem de DNS e gateways da Web seguros formam a espinha dorsal da imposição de camadas.

Contudo, nem todos os firewalls são criados do mesmo modo. Soluções legadas, com erros de configuração ou subutilizadas podem deixar lacunas a explorar. Avaliar suas defesas periodicamente, mantê-las em dia com patches e atualizações e alinhá-las ao seu cenário de ameaças corrente é essencial para manter a resiliência.

Controles modernos, como o Zero Trust Network Access (ZTNA), oferecem imposição de acesso mais granular e contextualizada. Juntamente com proteções tradicionais, eles ajudam a reduzir a superfície de ataque, prevenir movimentos laterais e interromper a exfiltração em ambientes de nuvem e híbridos.

Da visão holística à abordagem holística

Segurança cibernética não se trata apenas de implantar as ferramentas certas, mas, sim, trata-se de ter uma estratégia que reúna pessoas, processos e tecnologias. Esses 11 controles, quando implementados com atenção e consistência, podem reduzir significativamente o nível de exposição da sua organização.

Uma resiliência duradoura se conquista com um programa forte de segurança cibernética que seja reproduzível, adaptável e baseado em responsabilidades claras. A tecnologia é poderosa, mas exige equipes especializadas e processos estruturados para garantir que seja utilizada eficientemente.

As ameaças evoluem, as tecnologias mudam e o seu negócio se transforma. Manter-se à frente significa pensar de modo holístico, adaptar-se continuamente e construir uma cultura em que a segurança não seja apenas uma caixa de seleção, mas um promotor que centraliza os seus negócios.

Conclusões

Integre telemetria de rede a seu arsenal de detecção para melhorar a visibilidade, acelerar as investigações e sinalizar atividades anômalas, especialmente o movimento lateral e o tráfego de comando e controle.

¹ Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach \$1.2-\$1.5 Trillion by End of Year 2025

² Relatório de Ameaças Anual da Sophos 2025

³ Dark Reading, "Email-Based Attacks Top Cyber-Insurance Claims", 8 de maio de 2025

Pronto para avaliar seu programa de segurança cibernética?

Fale com um [especialista da Sophos ainda hoje](#).

Vendas na América Latina
+61 2 9409 9100
E-mail: latamsales@sophos.com