DELL Technologies

Melhore sua segurança cibernética e maturidade Zero Trust

Não deixe que os riscos de segurança impeçam as inovações

Entenda a situação atual de sua segurança cibernética

Saiba aonde ela precisa chegar

No atual cenário de ameaças complexas e em constante evolução, as organizações geralmente enfrentam limitações de recursos e conhecimentos para manter práticas sólidas de segurança cibernética. O aumento da maturidade em segurança cibernética e Zero Trust é essencial para combater as ameaças cibernéticas em evolução, a fim de manter seu ambiente seguro sem impedir as inovações.

Use estas checklists para avaliar o estado atual de sua maturidade em segurança cibernética. Veja como é possível aumentá-la conhecendo os pontos fortes e as vulnerabilidades de sua organização para tomar as medidas certas.

Conteúdo

Saiba mais

Saiba mais sobre como aumentar sua maturidade em segurança cibernética e Zero Trust

Checklist:

Reduza a superfície de ataque

Superfície de ataque se refere a todos os possíveis pontos ou áreas de um ambiente que podem ser visados ou explorados por um invasor cibernético. Esses pontos podem incluir vulnerabilidades de software, configurações incorretas, mecanismos fracos de autenticação, sistemas sem patch, privilégios excessivos de usuário, portas de rede abertas, segurança física insuficiente e muito mais. Estas perguntas podem ajudar a determinar como é possível minimizar as vulnerabilidades e os pontos de entrada que um agente mal-intencionado pode comprometer.

Sim	Não	
☐	☐	Sua organização realiza avaliações, testes de penetração ou simulações de ataques de violação regularmente para identificar vulnerabilidades e pontos fracos em sistemas e redes, permitindo a correção e a melhoria em tempo hábil?
☐	☐	Sua organização realiza treinamentos regulares de segurança para os funcionários?
☐	☐	Sua organização utiliza Autenticação baseada em vários fatores (MFA) e Controles de acesso baseados em funções (RBAC)?
☐	☐	Sua organização implementou segmentação de rede para isolar ativos essenciais e limitar o acesso entre diferentes partes da rede?
☐	☐	Sua organização está implementando práticas seguras de codificação, realizando revisões de código e testes de segurança regulares e usando Firewalls de aplicativos da Web (WAFs) para se proteger contra ataques comuns em nível de aplicativo e reduzir a superfície de ataque dos aplicativos da Web?
☐	☐	Sua organização escolhe fornecedores de TI que possam comprovar os processos e os procedimentos para proteger a própria cadeia de suprimentos?
☐	☐	Sua organização está implementando princípios de Zero Trust para substituir a segurança tradicional baseada em perímetro?
☐	☐	Sua organização utiliza o princípio do privilégio mínimo para limitar os usuários e as contas do sistema a ter apenas os direitos mínimos de acesso necessários para realizar suas tarefas?
☐	☐	Sua organização aplica patches regularmente nos sistemas e nos programas de software?
☐	☐	As ferramentas de segurança de sua organização utilizam recursos de IA/ML para identificar vulnerabilidades proativamente?

Checklist:

Detecte ameaças e reaja a elas

A detecção e a reação a ameaças cibernéticas são componentes essenciais de qualquer estratégia de segurança. Elas envolvem o monitoramento e a análise do tráfego de rede, dos logs do sistema e de outras áreas, além de dados de segurança, para identificar sinais de acesso não autorizado, invasões, infecções por malware, violações de dados ou outras ameaças cibernéticas. Estas perguntas podem ajudar a determinar como sua organização identifica proativamente e aborda ativamente os possíveis incidentes de segurança e as atividades mal-intencionadas em uma rede de computadores, um sistema ou um departamento.

Sim	Não	
☐	☐	Sua organização monitora continuamente as atividades da rede e do sistema usando ferramentas e tecnologias de segurança como Extended Detection and Response (XDR), sistemas de detecção de invasão (IDS), sistemas de prevenção contra invasão (IPS), SIEM e análise de logs?
☐	☐	Sua organização analisa os dados coletados para identificar padrões, anomalias e indicadores de comprometimento (IoCs) e/ou indicadores de ataque (IOA) que possam indicar uma possível ameaça cibernética?
☐	☐	Sua organização implementou as ferramentas mais recentes de visibilidade e monitoramento para detectar e alertar rapidamente sobre o potencial de ameaças?
☐	☐	Sua organização monitora o tráfego de rede em busca de padrões incomuns ou atividades suspeitas que possam indicar um ataque cibernético em andamento?
☐	☐	Sua organização implementou alguma ferramenta de IA/ML para detectar ameaças cibernéticas por meio de análise em tempo real de padrões ou comportamentos incomuns dos dados?
☐	☐	Sua organização considerou implementar uma solução de SIEM de última geração para gerenciar melhor os alertas de segurança e iniciar a correlação de dados de eventos de segurança de todo o ecossistema de TI?
☐	☐	Sua organização realiza testes e gerenciamento de vulnerabilidades para priorizar e abordar as vulnerabilidades existentes, além de reagir com eficiência às novas vulnerabilidades?
☐	☐	Sua organização tem um plano de resposta a incidentes em vigor para investigar e reduzir os incidentes de segurança confirmados?
☐	☐	Sua organização incorpora ferramentas de Orquestração, automação e resposta de segurança (SOAR) para acelerar as ações de resposta a incidentes que podem ajudar a reduzir a propagação de um ataque cibernético?
☐	☐	O plano de resposta a incidentes de sua organização considera políticas de contenção, planos de comunicação, requisitos de conformidade, análise forense e processo de recuperação?

Checklist:

Recupere-se de um ataque cibernético

Recuperar-se de um ataque cibernético é o processo de restaurar os sistemas, as redes e os dados afetados para um estado seguro e operacional após um incidente de segurança. Ele envolve a realização de ações para reduzir os danos causados pelo ataque, recriar serviços e dispositivos comprometidos ou interrompidos, analisar o incidente para evitar ataques futuros e retornar as operações da organização ao normal. Estas perguntas podem ajudar a determinar se sua organização está se recuperando efetivamente de ataques cibernéticos.

Sim	Não	
☐	☐	Sua organização implementou alguma medida de contenção de incidentes para isolar e conter um ataque cibernético?
☐	☐	Sua organização tem processos em vigor para restauração de sistemas e/ou dispositivos após a contenção de um incidente?
☐	☐	Sua organização utiliza isolamento de dados, imutabilidade ou um cofre cibernético para proteger dados?
☐	☐	Sua organização estabeleceu procedimentos para recuperar dados corretamente em caso de dados comprometidos, criptografados ou excluídos?
☐	☐	Sua organização utiliza tecnologias de IA/ML para automatizar ou acelerar a recuperação de um ataque cibernético?
☐	☐	Sua organização avalia continuamente o incidente e identifica áreas de melhorias após um ataque e uma recuperação?
☐	☐	Sua organização realizou uma análise forense para entender a metodologia do ataque, determinar a extensão da violação, identificar sistemas e dados afetados e coletar evidências para aumentar sua segurança e tomar medidas legais ou disciplinares?
☐	☐	Sua organização sabe como notificar as partes relevantes, como clientes, parceiros e fornecedores, sobre um ataque cibernético e qualquer possível impacto sobre os dados ou as operações delas?
☐	☐	Sua organização pratica as estratégias de recuperação várias vezes por ano para ganhar confiança na restauração dos negócios e cumprir os SLAs?
☐	☐	Sua organização colabora com provedores de serviços para ajudar na recuperação de sua organização?

Aumente a maturidade em segurança cibernética e Zero Trust

Quando se trata de segurança cibernética, é vital que os departamentos de TI se planejem para o pior cenário e tenham várias camadas de defesa. No ambiente de segurança cibernética com ameaças em constante evolução, é essencial promover continuamente práticas de segurança e adotar princípios de Zero Trust. Isso abrange:

Reduza a superfície de ataque

Minimize as vulnerabilidades e os pontos de entrada que podem ser explorados para comprometer o ambiente.

Detecte e responda a ameaças cibernéticas

Identifique e resolva ativamente possíveis incidentes de segurança e atividades maliciosas.

Recuperar-se de ataques cibernéticos

Restaure a organização para um estado seguro e operacional anterior e conhecido após um incidente de segurança.

Ao aproveitar o conhecimento especializado de serviços profissionais e colaborar com parceiros comerciais confiáveis, a Dell pode ajudar as organizações a estabelecer uma postura de segurança abrangente que protege contra as ameaças cibernéticas em evolução. À medida que a tecnologia continua avançando, nossa abordagem de segurança cibernética também deve avançar para proteger nossa infraestrutura digital e manter a confiança no ambiente digital.

DELL Technologies

Sobre a Dell Technologies

A Dell Technologies ajuda organizações e indivíduos a construir o respectivo futuro digital, além de transformar a maneira como trabalham, vivem e se divertem. A empresa oferece aos clientes o mais amplo e inovador portfólio de tecnologias e serviços do setor na era de dados.

Para obter mais informações, acesse www.dell.com/securitysolutions