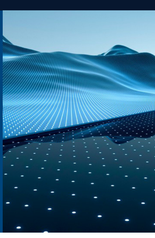
Dez recomendações de segurança cibernética

A tecnologia está avançando em um ritmo muito rápido e, à medida que nós vamos adotando novos sistemas e novas ferramentas que aumentam nossas capacidades, ao mesmo tempo, criamos novas oportunidades para ameaças cibernéticas que visam a explorar vulnerabilidades. Nesse cenário, é crucial implementar sólidas medidas de segurança cibernética para oferecer proteção contra essas ameaças emergentes, garantindo que a inovação possa prosperar em um ambiente seguro. Conforme as organizações se adaptam aos novos riscos, os especialistas em segurança cibernética da Dell Technologies recomendam dez ações fundamentais para aumentar sua maturidade nessa área.

1 Entenda seu ambiente de riscos de ameaças.



Parceiros experientes de segurança cibernética podem contribuir com conhecimentos especializados e recursos valiosos para ajudar você a lidar com o ambiente de ameaças em rápida evolução.

- Realize avaliações completas das vulnerabilidades e testes de penetração para identificar possíveis pontos fracos que precisam ser resolvidos e quaisquer lacunas que você possa ter em sua estratégia.
- Beneficie-se de habilidades e conhecimentos especializados que podem não estar disponíveis internamente, como informações sobre riscos emergentes, técnicas avançadas de ataque e as mais recentes práticas recomendadas e estratégias de segurança.
- Defina lógicas e privilégios de acesso, permitindo o estabelecimento da estrutura adequada de segurança para implementar sua governança e seus controles de negócios.

2 Crie uma estratégia abrangente de segurança cibernética.

A garantia de resiliência cibernética requer um esforço coordenado que envolve equipes de TI, profissionais de segurança cibernética, gerenciamento e, às vezes, especialistas externos.

- Promova a capacitação de toda a empresa — a segurança é responsabilidade de todos.
- Aproveite a automação sempre que possível.
- Certifique-se de ter um plano de IRR bem ensaiado que permita que todas as pessoas certas saibam o que fazer quando ocorrer um ataque cibernético.

3 Trabalhe com fornecedores que têm uma cadeia de suprimentos segura.

A segurança começa antes do que você pode imaginar. Garanta uma base confiável formando parcerias com fornecedores que priorizam a segurança do projeto, da fabricação e da entrega de dispositivos e infraestrutura. Os fornecedores que oferecem uma cadeia de suprimentos segura, um ciclo de vida seguro de desenvolvimento e uma rigorosa modelagem de ameaças podem ajudar você a se antecipar aos agentes de ameaças.

- Proporcione a confidencialidade, a integridade e a disponibilidade das informações que descrevem a cadeia de suprimentos de TI ou a atravessam, bem como informações sobre as partes que participam da cadeia de suprimentos de TI.
- Garanta que os produtos ou os serviços de TI da cadeia de suprimentos sejam autênticos e inalterados e atendam às especificações do adquirente sem funcionalidades adicionais indesejadas.
- Reduza as vulnerabilidades que podem limitar a função pretendida de um componente, gerar falha de componentes ou oferecer oportunidades de exploração.

4 Adote os princípios de Zero Trust.

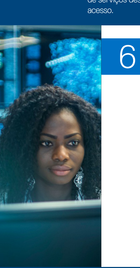
Zero Trust é um conceito de segurança centrado na crença de que as organizações não devem confiar automaticamente em nada dentro ou fora de seus perímetros e, em vez disso, devem verificar tudo o que está tentando se conectar a seus sistemas antes de conceder acesso.

- Abandone os modelos de segurança baseados em perímetro e adote princípios de Zero Trust.
- Implemente o princípio de privilégio mínimo, que restringe as contas de usuários e sistemas para que tenham apenas os direitos mínimos de acesso necessários para suas tarefas. Essa abordagem reduz a superfície de ataque e o possível impacto do acesso não autorizado por invasores.
- Incorpore soluções como microssegmentação, gerenciamento de acesso e identidade (IAM), autenticação baseada em vários fatores (MFA) e lógica analítica de segurança, entre outras.

5 Reduza a superfície de ataque.

A superfície de ataque representa possíveis vulnerabilidades e pontos de entrada que podem ser explorados por agentes mal-intencionados. Para aprimorar sua postura de segurança, as organizações devem minimizar a superfície de ataque, reduzindo os riscos e ampliando as defesas cibernéticas gerais contra ameaças novas e emergentes.

- Treine funcionários e usuários para reconhecer e relatar possíveis ameaças à segurança, tentativas de phishing e táticas de engenharia social para ajudar a minimizar os riscos de ataques bem-sucedidos que exploram as vulnerabilidades humanas.
- Implemente medidas preventivas, como segmentação abrangente de rede, isolamento de dados essenciais, imposição de controles rigorosos de acesso e atualização e aplicação de patches regularmente em sistemas e aplicativos.
- Certifique-se de que os sistemas, as redes e os dispositivos estejam configurados corretamente com as práticas recomendadas de segurança, como a desativação de serviços desnecessários, o uso de senhas fortes e a imposição de controles de acesso.



6 Detecte ameaças cibernéticas e reaja a elas.

Diante de ameaças sofisticadas, as medidas tradicionais de segurança não são mais suficientes. As organizações devem aprovetiar as metodologias e as tecnologias avançadas de detecção de ameaças para identificar as ameaças conhecidas e desconhecidas e reagir a elas efetivamente.

- Monitore e analise o tráfego de rede, os logs de sistema e outras áreas, bem como dados de segurança, para identificar proativamente sinais de acesso não autorizado, invasões, infecções por malware, violações de dados ou outras ameaças cibernéticas.
- Implemente um plano de resposta para investigar e reduzir imediatamente os incidentes de segurança confirmados. Isso inclui conter o impacto, identificar a causa raiz e implementar as ações necessárias para restaurar sistemas e evitar mais danos.
- Utilize IA/ML para detectar rapidamente ameaças cibernéticas por meio da análise em tempo real de padrões ou comportamentos incomuns dos dados. Essas tecnologias também promovem uma resposta rápida ao avaliar a severidade das ameaças, prever impactos, automatizar determinadas ações defensivas e dimensionar as práticas de segurança, o que minimiza possíveis danos.

7 Recupere-se de um ataque cibernético.

Mesmo com medidas proativas essenciais em vigor, as organizações devem sempre supor que foram violadas e devem ter recursos resilientes implementados e testados com frequência para garantir a recuperação eficaz de um ataque cibernético bem-sucedido.

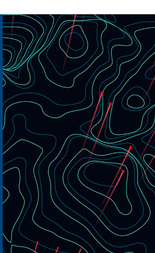
- Adote medidas imediatas para reduzir os danos causados por um ataque cibernético, isolando e contendo o impacto.
- Desconecte os sistemas afetados da rede, desative as contas comprometidas e implemente medidas para evitar maior disseminação ou mais danos.
- O uso de IA/ML pode acelerar a recuperação, identificando rapidamente os sistemas e os dados afetados e automatizando o processo de restauração de backups.

8 Tenha parceiros experientes.

Nenhum fornecedor tem todos os recursos necessários para oferecer segurança completa, seja em termos de pessoas, processos ou tecnologias; é preciso um esforço coletivo. Por isso, é essencial colaborar com uma rede de parceiros experientes.

- Envolva-se com parceiros experientes em segurança cibernética que podem contribuir com conhecimentos especializados e recursos valiosos para ajudar você a lidar com o ambiente de ameaças em rápida evolução.
- Beneficie-se de habilidades e conhecimentos especializados que podem não estar disponíveis internamente, inclusive informações sobre riscos emergentes, técnicas avançadas de ataque e as mais recentes práticas recomendadas e estratégias de segurança.
- Conte com o conhecimento especializado de serviços profissionais experientes e estabeleça relacionamentos colaborativos com parceiros comerciais confiáveis para estabelecer uma postura de segurança abrangente que ofereça proteção eficaz contra as ameaças cibernéticas em evolução.

9 Amplie a segurança cibernética para a borda e ambientes de nuvem.



À medida que as redes vão se espalhando do núcleo à borda e até a nuvem, todas elas se tornaram um ponto crucial de vulnerabilidade. Independentemente de como ocorra a implementação dos aplicativos, eles exigem o mesmo nível de segurança e alinhamento às políticas de negócios para garantir a consistência para o gerenciamento e os usuários de aplicativos.

- Certifique-se de ampliar os princípios de Zero Trust para cobrir ambientes de borda e nuvem, oferecendo sólidos controles de acesso, autenticação contínua e visibilidade e controle abrangentes sobre o tráfego de rede.
- Implemente medidas de segurança, como segmentação de rede, criptografia e monitoramento contínuo, tanto na rede principal quanto nos ambientes de nuvem para protegê-los contra possíveis ameaças.
- Colabore com serviços profissionais especializados em segurança de bora, núcleo e nuvem para aproveitar os conhecimentos especializados deles na implementação de medidas eficazes que protegem sua organização por todos os ângulos.

10 Gerencie proativamente e aumente a resiliência de ponta a ponta.

O gerenciamento de operações de segurança, resposta a incidentes e inteligência contra ameaças pode aprimorar a capacidade de uma organização de detectar ameaças cibernéticas e reagir a elas.

- Estabeleça protocolos proativos de resposta a incidentes e recuperação que definam claramente as funções e as responsabilidades, garantindo a comunicação e a coordenação ininterruptas entre os membros de equipe.
- Aumente a visibilidade sobre o ambiente para permitir que as organizações monitorem as ameaças em suas redes, reajam a elas proativamente e, ao mesmo tempo, apresentam alertas para recuperação quando necessário.
- Fortaleça sua capacidade de detectar ameaças cibernéticas e reagir a elas proativamente aproveitando a inteligência contra ameaças avançada, o Gerenciamento de eventos e informações de segurança (SIEM), as soluções de proteção de endpoints e a lógica analítica comportamental.

Não deixe a segurança impedir as inovações.
Veja como é possível aumentar sua maturidade em segurança cibernética e Zero Trust, em dell.com/SecuritySolutions

DELL Technologies