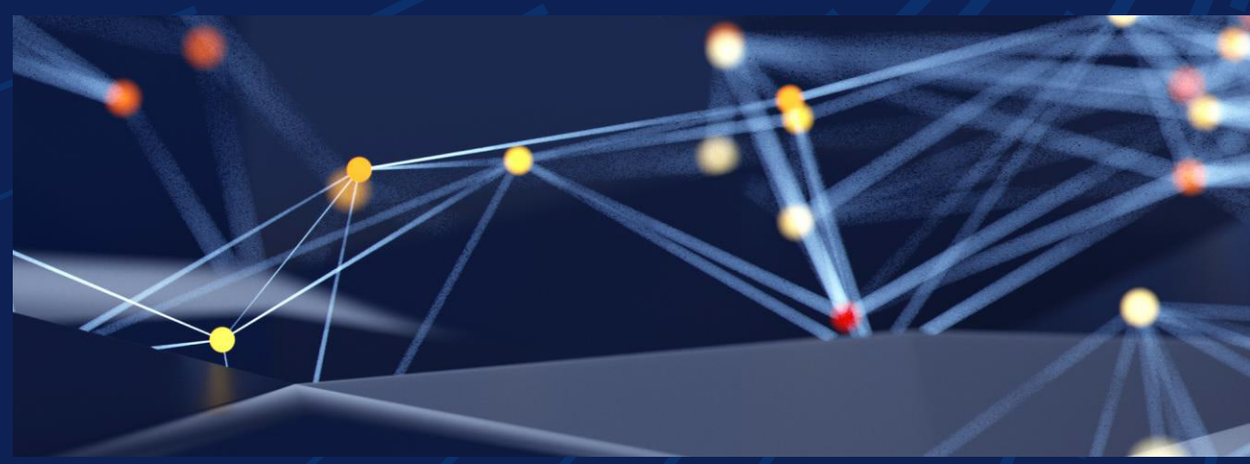
DELL Technologies

O futuro da segurança cibernética:

Adaptação a uma nova era digital



Embora os profissionais de segurança cibernética frequentemente estejam focados na prevenção de ataques e na criação de planos de recuperação, o ambiente de segurança geral está em constante evolução. Portanto, planejar o futuro é essencial.

À medida que olhamos para o futuro, três áreas se destacam: a criptografia pós-quântica, o cenário regulatório em constante mudança e as ameaças emergentes. As organizações devem agir agora planejando e implementando soluções à medida que elas estiverem disponíveis.

O surgimento da criptografia pós-quântica

A computação quântica promete transformar indústrias, oferecendo uma potência computacional surpreendente, capaz de resolver problemas muito além do alcance dos computadores clássicos. No entanto, essa mesma potência pode tornar os métodos criptográficos atuais obsoletos. Algoritmos como RSA e ECC, que sustentam grande parte das comunicações seguras atuais, poderiam ser quebrados em segundos por um computador quântico suficientemente avançado. Essa ameaça iminente aumentou a urgência da criptografia pós-quântica.

A criptografia pós-quântica (PQC) concentra-se no desenvolvimento de algoritmos criptográficos que permaneçam seguros na era da computação quântica. O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) reconheceu esse risco iminente e lidera o processo de padronização de algoritmos resistentes à computação quântica.

Para as empresas, preparar-se para essa transição não é opcional. A adoção antecipada de soluções PQC garantirá que os dados permaneçam seguros quando os adversários tiverem acesso a recursos de computação quântica.

Como destaca Bobbie Stempfley, vice-presidente e diretor de segurança da unidade de negócios na Dell, as organizações devem começar o processo concentrando-se em duas áreas principais:

Identificar e catalogar todos os modelos criptográficos atualmente em uso.

Considere os dados em trânsito, não apenas os dados em repouso.

Pense no gerenciamento de chaves, assinatura de código, identificações de dispositivos, acesso seguro e telemetria. Crie um inventário abrangente e, em seguida, crie um roteiro.

Entendendo a situação dos fornecedores.

Considerando que as empresas modernas podem ter milhares de fornecedores, é preciso estar atento aos riscos que podem vir deles. Trabalhe para garantir que eles também estejam planejando a mudança.

Além desses primeiros passos, realize avaliações de risco para identificar sistemas vulneráveis, observe a implementação de modelos criptográficos híbridos para permanecer operacional durante a transição e colabore com fornecedores que já estão explorando soluções quânticas seguras, mas lembre-se de que não haverá um fornecedor ou tecnologia capaz de oferecer uma solução pronta para uso.

Mudanças regulatórias em um mundo globalizado

Outro fator crítico que molda o futuro da segurança cibernética é o ambiente regulatório em constante mudança. As regulamentações agora vão muito além da conformidade – elas estão se tornando uma estrutura essencial para instigar a responsabilidade, impulsionar as atualizações tecnológicas e proteger os cidadãos em um mundo interconectado e orientado por dados. No entanto, elas estão evoluindo rapidamente e variam significativamente entre diferentes regiões, aumentando a complexidade da conformidade.

Dito isso, essas regulamentações vão além de simples penalidades por não conformidade, elas funcionam como catalisadores para melhores práticas de segurança cibernética. As empresas que alinham ativamente suas políticas com os requisitos regulatórios podem desbloquear novos níveis de confiança e eficiência operacional. Para isso, as organizações devem estabelecer estruturas de governança que permaneçam flexíveis para se adaptarem às mudanças legais, realizar auditorias regulares de conformidade e investir em treinamentos para que os funcionários lidem com informações confidenciais de acordo com os padrões mais recentes.

Enquanto os executivos de segurança se preparam para atender às regulamentações, é importante garantir que as políticas sejam claras e compreensíveis. Muitas vezes, os profissionais de segurança falam em termos técnicos que não fazem sentido para clientes, reguladores e outras partes interessadas. A responsabilidade recai sobre os profissionais de segurança para garantir que sejam compreendidos, e não sobre os ouvintes para interpretá-los.

DELL Technologies

> Pense na mudança para a criptografia pós-quântica, como mover todos os itens de uma casa totalmente mobiliada. É uma tarefa complexa, e o grande desafio seria não quebrar nenhum objeto no processo.
>
> ***Bobbie Stempfley***
> *Vice-presidente, diretor de segurança cibernética e segurança de unidade de negócios, Dell Technologies*

A evolução do cenário de ameaças (e defesas)

A IA está revolucionando os negócios, aumentando a produtividade e desvendando novas oportunidades do potencial humano. Quando se trata de segurança cibernética, a IA está beneficiando tanto os agentes mal-intencionados quanto os defensores:

Uso adversário: a IA está possibilitando ataques mais sofisticados, como spear phishing e deepfakes altamente convincentes.

Uso defensivo: A IA ajuda os defensores a:

- Processar rapidamente grandes volumes de dados de segurança.
- Priorizar ameaças de forma mais eficaz.
- Aprimorar os recursos de detecção e resposta.

No entanto, as ferramentas de segurança só continuarão a melhorar com o processamento de linguagem natural, que permite aos profissionais de segurança interagir mais diretamente com seus sistemas e capacitar os sistemas para que realizem ações corretivas de segurança cibernética de forma proativa.

As organizações devem trabalhar simultaneamente para aproveitar as vantagens dos recursos e, ao mesmo tempo, garantir que seus mecanismos de treinamento e outros mecanismos defensivos permaneçam atualizados. O treinamento é a melhor maneira de evitar que os funcionários sejam vítimas de ataques cada vez mais sofisticados.

Diminuindo o uso de senhas

As senhas já não são os métodos mais seguros para o gerenciamento de identidade e acesso.

Os sistemas tradicionais baseados em senhas apresentam vulnerabilidades significativas, tornando-os uma solução cada vez mais inadequada para as necessidades modernas de segurança cibernética. As senhas são suscetíveis a ataques, como preenchimento de credenciais, phishing e tentativas de força bruta, geralmente expondo as organizações a riscos desnecessários. Além disso, comportamentos indevidos dos usuários, como a reutilização de senhas ou a criação de senhas fracas, aumentam ainda mais essas vulnerabilidades.

Os métodos de autenticação sem senha, como biometria, certificados e tokens de hardware, oferecem uma alternativa mais segura eliminando classes inteiras de ameaças que se aproveitam de senhas. A migração para sistemas sem senha representa uma evolução crítica no gerenciamento de identidade e acesso, alinhando as medidas de segurança com a crescente sofisticação das ameaças cibernéticas.

A adoção de tecnologias sem senha também oferece inúmeros benefícios, incluindo a redução da superfície de ataques, o aprimoramento da experiência do usuário por meio de logins mais rápidos e contínuos e a redução dos custos de TI por meio da redução de incidentes relacionados a senhas. O uso de métodos avançados garante uma postura de segurança mais robusta e ajuda as organizações a atender aos padrões regulatórios. A transição para sistemas sem senha não é apenas uma tendência, é uma etapa necessária para criar um ecossistema digital mais seguro e eficiente, tanto para indivíduos quanto para organizações.

Conclusão

A segurança cibernética está entrando em uma era de transformação, moldada pela computação quântica, mudanças regulatórias e ameaças cada vez mais sofisticadas. Para se manter à frente, as organizações devem adotar inovações como criptografia pós-quântica, defesas orientadas por IA e autenticação sem senha. Ao priorizar a preparação, a colaboração e o investimento estratégico, as empresas podem construir um ambiente digital mais seguro e resiliente. O momento para agir é agora.

Produtos e soluções da Dell que podem ajudar

Solução Dell em destaque	Descrição
Cybersecurity Advisory Services	Orientação especializada que pode ajudá-lo a planejar o cenário de ameaças em evolução, incluindo ameaças atuais e emergentes.
vCISO	Diretor virtual de segurança das informações (vCISO) e especialista em segurança cibernética que pode ajudar a identificar e gerenciar riscos, bem como orientar a tomada de decisões estratégicas.

Saiba como lidar com alguns dos principais desafios de segurança cibernética atuais em **dell.com/cybersecuritymonth**