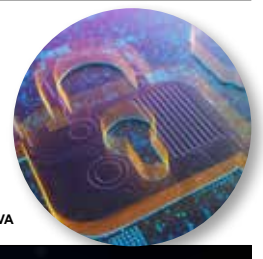
Empresas & Negócios

Matéria de capa



kanawatTH_CANVA

DESAFIOS E OPORTUNIDADES

PREVISÕES DE SEGURANÇA DIGITAL PARA 2025

A DigiCert, empresa provedora líder global de confiança digital, acaba de divulgar seu estudo anual de previsões de segurança cibernética para identidade, tecnologia e confiança digital que devem moldar o cenário em 2025 e além.

Essas previsões fornecem um parecer dos desafios e das oportunidades de segurança cibernética que as empresas encontrarão nos próximos meses.

1 **A criptografia pós-quântica decola** – 2025 marca um ano crucial quando a criptografia pós-quântica (PQC) muda de estruturas teóricas para implantações no mundo real. Com anúncios iminentes da Agência de Segurança Nacional dos EUA (NSA) e crescentes pressões de conformidade, a adoção do PQC aumentará, capacitando as indústrias a adotar soluções resistentes a quantum.

2 **Chief Trust Officers assumem o centro do palco** – A confiança digital se torna uma prioridade da sala de diretoria, levando a um aumento contínuo de Chief Trust Officers (CTrOs) que supervisionarão a IA ética, experiências digitais seguras e conformidade em um ambiente cada vez mais regulamentado.

3 **Automação e criptoagilidade se tornam uma necessidade** – Com as mudanças da indústria em direção a vidas úteis mais curtas de certificados SSL/TLS, a automação e a criptoagilidade surgirão como recursos essenciais para organizações que buscam manter operações seguras em meio a padrões em evolução.

4 **Proveniência de conteúdo se torna popular** – Em uma era de deepfakes e desinformação digital, a Coalition for Content Provenance and Authenticity (C2PA) está pronta para redefinir como verificamos o conteúdo digital. Espere ver o ícone de credencial de conteúdo do C2PA se tornar comum em imagens e vídeos para aumentar a confiança em todas as plataformas de mídia.

peshkov_CANVA

5 **Organizações exigirão resiliência e zero interrupções** – A interrupção do CrowdStrike neste verão ressaltou a necessidade de melhores testes de atualizações automatizadas e maior confiança digital. À medida que a adoção da IoT cresce, preocupações sobre a segurança de atualizações sem fio, especialmente para carros autônomos, estão gerando pedidos por maior transparência nas práticas de segurança.

A Lei de Resiliência Cibernética da UE, em vigor em 2027, impulsionará padrões de segurança cibernética mais rigorosos, promovendo um ecossistema de IoT mais seguro e confiável.

6 **Ataques de phishing impulsionados por IA aumentarão** – A proliferação da IA alimentará um aumento sem precedentes em ataques de phishing sofisticados, tornando-os mais difíceis de detectar. Os invasores aproveitarão a IA para criar campanhas de phishing altamente personalizadas e convincentes, enquanto ferramentas automatizadas permitirão que eles dimensionem ataques a uma taxa alarmante, visando indivíduos e organizações com precisão.

7 **Novos padrões de PKI privada como o ASC X9 ganharão força** – O ASC X9 está pronto para ganhar força, pois setores como finanças e saúde exigem cada vez mais estruturas de segurança personalizadas para atender a rigorosas demandas regulatórias e necessidades operacionais exclusivas.

Ao contrário da PKI pública, o ASC X9 oferece maior flexibilidade ao permitir políticas personalizadas e modelos de confiança, abordando áreas críticas como integridade de dados e autenticação. Essa capacidade de promover estruturas seguras, escaláveis e interoperáveis tornará o ASC X9 um padrão preferencial para organizações que priorizam confiança e colaboração.

8 **A Lista de Materiais de Criptografia (CBOM) ganha força** - Em resposta às crescentes ameaças à segurança cibernética, os CBOMs se tornarão uma ferramenta vital para garantir a confiança digital catalogando ativos e dependências criptográficas, permitindo melhores avaliações de risco.

ismagilov_CANVA

9 **A Era do Gerenciamento Manual de Certificados Termina** – O gerenciamento manual de certificados, ainda comum em quase um quarto das empresas, será eliminado gradualmente, pois a automação se tornará indispensável para lidar com vidas úteis mais curtas de certificados e protocolos de segurança mais rigorosos.

10 **As organizações continuarão a priorizar menos fornecedores** – Apesar das preocupações sobre os riscos de fornecedores únicos e um pico de financiamento de capital de risco para startups de IA, as empresas continuarão a consolidar fornecedores para simplificar o gerenciamento, melhorar a integração e aprimorar as práticas gerais de segurança.

"O ritmo implacável da inovação não está apenas remodelando nossas vidas digitais — está expondo novas vulnerabilidades mais rápido do que podemos protegê-las, exigindo uma reformulação ousada de como abordamos a segurança cibernética", disse Jason Sabin, CTO da DigiCert.

"As previsões para 2025 ressaltam a necessidade urgente de ficar à frente dessas vulnerabilidades, impulsionando a prontidão quântica, aumentando a transparência e reforçando a confiança como a base do nosso ecossistema digital em rápida mudança". Mais detalhes sobre as previsões de segurança em: (https://www.digicert.com/blog/2025-security-predictions).