Devoteam Cyber Trust Apresenta as Tendências de Cibersegurança para 2025

Lisboa, 26 de novembro de 2024 - Em 2024 o panorama da cibersegurança revelou desafios significativos, impulsionados pela sofisticação de ameaças baseadas em inteligência artificial (IA), pela evolução dos ataques de ransomware e pela necessidade de fortalecer as cadeias de confiança de identidade. **Métodos convencionais, como a autenticação multifator, mostraram-se insuficientes para mitigar ataques avançados** que exploram tokens de sessão e chaves de API. O episódio **CrowdStrike**, apagão cibernético ocorrido em julho que afetou milhões de dispositivos e paralisou vários serviços em todo o mundo, evidenciou a **necessidade urgente de implementar estratégias de segurança mais robustas** e uma abordagem baseada em Zero Trust, **capaz de reduzir a superfície de ataque e reforçar a resiliência.**

À medida que 2025 se aproxima, esperam-se ameaças mais sofisticadas e ataques mais complexos e direcionados, imprevisíveis e difíceis de mitigar. Para enfrentar este cenário, **a Devoteam Cyber Trust apresenta nove tendências de cibersegurança para 2025**.

1. O Realismo da Inteligência Artificial (AI)

Em 2025, a AI deverá ultrapassar a fase de expectativas inflacionadas e entrar numa etapa de maturidade, com as organizações a focarem-se em aplicações de valor concreto. **A expansão dos agentes de AI autónomos será uma tendência chave**, **automatizando operações em áreas como segurança e logística**, reduzindo tarefas manuais e melhorando a capacidade de resposta em atividades rotineiras. No entanto, **este avanço trará novos desafios, exigindo estruturas rigorosas de governança** para assegurar que as ações destes agentes respeitam as políticas e normas da organização, mitigando riscos éticos e de segurança. **As Plataformas de Governança de AI irão assumir um papel essencial** para garantir transparência e conformidade num cenário onde as exigências regulatórias variam.

2. A Cibersegurança como Serviço (CaaS)

Espera-se que a cibersegurança como serviço (CaaS) cresça em popularidade à medida que as empresas procuram formas mais económicas de proteger os seus ativos digitais. A cibersegurança como serviço, oferece às empresas soluções de cibersegurança externalizadas, que vão desde a monitorização contínua de ameaças até à resposta a incidentes. Ao utilizar estes serviços, até as empresas mais

pequenas podem aceder a ferramentas de segurança avançadas sem necessidade de criar equipas internas. **As soluções de CaaS irão evoluir para incluir deteção de ameaças com IA, resposta a incidentes automatizada e análises em tempo real**, que ajudam as empresas a detetar e mitigar ameaças de forma mais rápida. À medida que os ciberataques se tornam mais sofisticados, a parceria com fornecedores especializados em cibersegurança oferecerá uma opção escalável e flexível para muitas organizações.

3. A Expansão da Arquitetura Zero Trust

O conceito de Arquitetura Zero Trust (ZTA), que opera com o princípio de "nunca confiar, sempre verificar", verá uma adoção generalizada. À medida que as ameaças cibernéticas se tornam mais avançadas, as organizações já não podem confiar na segurança baseada em perímetro. Em vez disso, a ZTA exige uma verificação contínua de utilizadores, dispositivos e aplicações — independentemente de estarem dentro ou fora da rede. A expansão da ZTA ajudará a mitigar riscos como ameaças internas, movimento lateral numa rede comprometida e acesso não autorizado. Com mais organizações a mudarem para ambientes de cloud e trabalho remoto, a implementação da ZTA será crítica para manter uma segurança robusta e limitar potenciais brechas.

4. O Aumento do Roubo de Identidade Reverso

Em 2025**, prevê-se um aumento significativo do roubo de identidade reverso**, um fenómeno em que dados roubados são combinados de forma incorreta, resultando em "sósias digitais". Este problema pode surgir devido a falhas em bases de dados, onde a combinação de nomes comuns ou informações incorretas leva a reivindicações erradas ou até à troca de identidade, criando oportunidades para fraudes ou acusações injustas. **Com o crescente volume de dados pessoais expostos em múltiplas violações, a fusão incorreta de dados irá tornar-se uma preocupação crescente**. Este tipo de roubo de identidade reverso poderá gerar impactos graves, desde problemas de crédito e disputas legais, até à criação de perfis digitais falsos usados para fins maliciosos. **A prevenção exigirá uma vigilância maior sobre a integridade dos dados** e a implementação de medidas rigorosas para verificar a identidade real de indivíduos.

5. A Cibersegurança Centrada no Ser Humano

O **erro humano continua a ser um dos maiores riscos de cibersegurança**, com ataques de phishing e palavras-passe fracas a representar uma parte significativa dos riscos. As organizações deverão ir além das formações tradicionais e adotar

abordagens mais integrativas e contextuais, onde a conscientização sobre segurança seja constantemente reforçada através de simulações realistas, micro formações e conteúdos adaptados ao comportamento e às funções específicas de cada colaborador. Esta abordagem utiliza tecnologias como IA e análise comportamental para identificar potenciais riscos, direcionando o conteúdo certo, no momento certo. Além disso, práticas como a gamificação incentiva os colaboradores a adotarem práticas seguras de forma ativa e voluntária. Outra tendência será o **desenvolvimento de uma cultura de cibersegurança, onde a segurança se torne um valor organizacional partilhado e uma responsabilidade de todos os colaboradores, através da adoção de mecanismos simples, como o Alert Readiness Framework**, no qual as organizações definem e qualificam os seus próprios níveis de alerta.

6. As Mudanças Regulatórias e Conformidade

Com a rápida evolução das ameaças de cibersegurança, **espera-se que os quadros regulatórios se tornem mais rigorosos até 2025.** Os governos em todo o mundo estão a introduzir novas regulamentações que exigem que as organizações melhorem as suas práticas de segurança. Na União Europeia, a NIS 2 e o DORA são as normas que darão mais que fazer às instituições e empresas, exigindo uma adaptação robusta para garantir a resiliência digital, a proteção contra ciberameaças e a continuidade operacional. Enquanto **a NIS 2 está a impor requisitos rigorosos de segurança cibernética e gestão de riscos**, incluindo a proteção da cadeia de fornecimento e a resposta a incidentes, **o DORA foca-se na resiliência operacional digital**, cobrindo a segurança de TI, a recuperação de incidentes e monitorização contínua dos riscos, incluindo os de terceiros. **Juntas, estas diretrizes forçam as organizações a fortalecerem as defesas cibernéticas, a implementarem práticas de governança mais rigorosas** e prepararem-se para a recuperação rápida em caso de ataques, tudo isto com o objetivo de mitigar os riscos e assegurar a continuidade dos serviços críticos num ambiente digital cada vez mais complexo e dinâmico.

7. Third Party Risk Management proativa e colaborativa

A tendência dominante em 2025 para a gestão de riscos de terceiros (TPRM) no contexto da NIS 2 será a monitorização contínua e a avaliação automatizada de riscos ao longo de toda a cadeia de fornecimento. Com as exigências da NIS 2 a ampliar a responsabilidade das organizações sobre a segurança de terceiros, existirá uma maior adoção de ferramentas de inteligência artificial e machine learning para monitorizar, em tempo real, a postura de segurança de fornecedores e parceiros. O que permitirá identificar rapidamente vulnerabilidades ou comportamentos irregulares que possam indicar riscos. **O mercado deve migrar para plataformas integradas de TPRM, que centralizam dados de riscos e facilitam auditorias e conformidade com a NIS 2**, permitindo às empresas demonstrar de maneira mais eficiente o compromisso com a segurança cibernética ao longo de toda a cadeia. A

exigência de resposta rápida a incidentes incentivará as organizações a manter canais de comunicação ágeis e transparentes com os fornecedores, além de estabelecer protocolos de resposta conjunta em caso de incidentes. Dessa forma, **a TPRM em 2025 será cada vez mais proativa e colaborativa**, fundamentada na automação e na transparência para lidar com os desafios impostos pela NIS 2.

8. Desafio na retenção e captação de talento

Este é um tema que se irá manter em 2025. **A captação e retenção de talento em cibersegurança enfrenta desafios significativos**, impulsionados pela crescente procura por profissionais qualificados e pela rápida evolução das ameaças digitais. A velocidade com que as novas tecnologias e tipos de ataques surgem exige que estes profissionais estejam sempre atualizados, o que torna o mercado altamente competitivo e torna a retenção um desafio para as empresas. Além disso, a escassez de talentos em cibersegurança faz com que os profissionais mais qualificados sejam frequentemente disputados. Outro desafio é o desgaste psicológico da área, já que os especialistas em cibersegurança lidam com alta pressão para proteger dados sensíveis e responder rapidamente a ameaças. A carga emocional pode levar ao esgotamento e à rotatividade de pessoal. Para lidar com esses desafios, **muitas organizações irão continuar a investir em formação contínua,** benefícios que promovem o bem-estar e ambientes de trabalho flexíveis, além de **criar uma cultura de suporte e colaboração, essenciais para manter esses talentos no longo prazo.**

9. Melhoria das Estratégias de Defesa e Recuperação Contra Ransomware

Os ataques de ransomware continuam a evoluir, tornando-se mais sofisticados e difíceis de defender. As empresas devem concentrar-se tanto na prevenção destes ataques, como na criação de estratégias robustas de recuperação. **Cópias de segurança regulares, redes segmentadas e o uso de soluções de Deteção e Resposta a Endpoints (EDR) serão componentes-chave de uma defesa forte contra ransomware**. À medida que as táticas de ransomware se tornam mais agressivas, como a dupla extorsão, as empresas também terão de investir em seguros de cibersegurança e planos de resposta para minimizar interrupções operacionais.

Com tanto por acontecer, **é essencial que as organizações se mantenham atentas às novas tendências** e ajustem as suas estratégias de segurança para enfrentar os desafios emergentes. **Desta forma, torna-se essencial encontrar soluções com abordagens simples** e acessíveis a todos os colaboradores das organizações, **que permitam passar de uma postura reativa de cibersegurança para uma postura proativa.**

Aceda à informação completa [aqui.](https://www.integrity.pt/pdf/TendenciasCiberseguranca_2025_PT.pdf)

https://www.integrity.pt/pdf/TendenciasCiberseguranca_2025_PT.pdf

Sobre a Devoteam Cyber Trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e do CIS - Centro de Segurança na Internet. Também somos acreditados pela Iniciativa Europeia de Pagamentos (EPI) para realizar avaliações de segurança do Wero, a carteira digital móvel. Com uma base considerável de clientes, operamos em mais de 20 países.

Contactos

BE Ideas | Boutique PR Agency
Sofia Alcobia
sofia.alcobia@beideas.pt
T: + 351 962 615 717

Magda Carvalho
magda.carvalho@beideas.pt
T: + 351 966 015 450