Devoteam Cyber Trust IDENTIFICA

14 TENDÊNCIAS EM CIBERSEGURANÇA PARA 2024

Lisboa, 12 de dezembro de 2023

Cibersegurança em 2024

Os ataques cibernéticos aumentaram globalmente 125% até 2021, e volumes crescentes de ataques cibernéticos continuam a ameaçar empresas e indivíduos desde então. A invasão da Ucrânia pela Rússia teve um impacto enorme no cenário das ameaças cibernéticas, sendo o phishing a forma mais comum de crime cometido online. Na Europa, o ransomware foi o principal tipo de ataque, representando 26% dos ataques no continente. Ataques de acesso a servidores (12%) e roubo de dados (10%) foram os tipos de ataque mais comuns.

A Devoteam Cyber Trust tem consciência de que a área da cibersegurança está em constante evolução e que os ciberatacantes estão cada vez mais audazes e perfeccionistas. Desta forma, existe uma maior necessidade por parte das organizações de estarem atentos aos avanços cibernéticos. Para 2024, destacamos algumas tendências do ecossistema de cibersegurança:

1- Adoção de Inteligência Artificial para a defesa e o ataque: A Inteligência Artificial (IA) tem vindo a desenvolver o seu grau de complexidade e os ciberatacantes aproveitam essa evolução para aperfeiçoar os ataques cibernéticos. Estes ataques podem ser ataques de deepfake ou de malware, uma vez que a IA desenvolve recursos para que os atacantes consigam criar vídeos ou áudios falsos com maior precisão e transmitir o malware em sistemas mais desatualizados. Por outro lado, a IA é uma ferramenta para ajudar a detetar, evitar e diminuir ciberameaças devido à autenticação inteligente e à resposta automatizada a possíveis ciberataques.

2- Evolução dos ataques de phishing: Este tipo de ataque de engenharia social, que requer enganar os utilizadores de modo a darem acesso aos atacantes, vai continuar a ser uma preocupação em 2024, sendo definido como a maior ameaça em cibersegurança. Para desenvolverem ataques de phishing, os ciberatacantes

também vão recorrer à IA, uma vez que esta permite uma abordagem mais inteligente e personalizada, como por exemplo o ChatGPT.

3- Cibersegurança como uma prioridade nas organizações: Com o avanço dos ataques cibernéticos, a cibersegurança deve ser uma prioridade estratégica numa organização e não apenas uma parte integrante do departamento de IT em 2024. O relatório da Gartner mostrou as previsões para 2024 e afirma que, até 2026, 70% dos conselhos de administração vão incluir pelo menos um membro com experiência em cibersegurança.

4- Ciberataques com recurso à IoT: A IoT (Internet of Things) consiste no maior número de dispositivos a comunicar entre si através da Internet, o que significa um maior número de potenciais sistemas que os ciberatacantes podem atacar. Com a continuação da integração do trabalho a partir de casa, os possíveis riscos que podem existir através dos trabalhadores que se ligam ou partilham dados através de dispositivos indevidamente protegidos poderão ser cada vez mais uma ameaça. No entanto, a IoT tem benefícios positivos e em 2024 terá uma evolução significativa nomeadamente nos protocolos e nas medidas de segurança.

5- Ciber-resiliência e cibersegurança: Em 2024, tornar-se-á mais visível a distinção entre ciber-resiliência e cibersegurança, no sentido em que a cibersegurança se refere à dita prevenção contra possíveis ataques cibernéticos, enquanto a ciber-resiliência implica assumir que não é possível uma proteção 100% segura. Assim, o desenvolvimento de capacidade de recuperação de dados de forma rápida e eficaz será uma das medidas e práticas de ciber-resiliência, de modo a garantir a continuidade das operações e minimizar a perda de dados.

6- *'Zero-Trust'*: O modelo de *Zero-Trust* assume que tudo é uma ameaça, ou seja, tudo o que está envolvido numa rede empresarial deve ser registado e analisado, incluindo a verificação do acesso dos colaboradores. Uma vez que não é possível definir-se um "perímetro" de segurança numa rede e que as ameaças estão a direcionar-se para além da rede corporativa e a estenderem-se para trabalhadores remotos e dispositivos IoT, é necessário integrar a cibersegurança em contextos organizacionais. Em 2024, o *Zero-Trust* vai deixar de ser um modelo técnico e tornar-se-á num modelo holístico e de fácil adaptação, através da autenticação contínua pela IA e pela monitorização de atividades.

7- A ciberguerra e os ataques cibernéticos patrocinados por Estados: Com a guerra na Ucrânia, a guerra cibernética tornou-se mais popular e é evidente a evolução de

ataques cibernéticos. Os ataques de ciberguerra têm vindo a aumentar mundialmente e uma das tendências para 2024 será mesmo ter em atenção às operações militares que podem estar acompanhadas de operações de ciberguerra, como por exemplo ataques de phishing que têm como objetivo obter acesso a sistemas de informação para desativar comunicações, serviços públicos, transportes ou infraestruturas de segurança. Ainda em 2024 a cibersegurança terá um papel fundamental no mundo da política, uma vez que haverá eleições nos EUA, no Reino Unido e na Índia e será provável que exista um aumento de ataques cibernéticos para desestabilizar e perturbar os processos democráticos.

8- Evolução dos ataques de ransomware (Ransomware as a Service - RaaS): O ransomware, um tipo de ciberataque que consiste no bloqueio do acesso ao sistema informático até que o utilizador pague um resgate, tem sido uma ameaça preocupante, nomeadamente para os prestadores de cuidados de saúde, e continuará a ser um ataque recorrente em 2024. O que tornará ainda mais perigoso este tipo de ciberataque é o crescente avanço dos negócios na dark web que consistem em vender malware, ou seja, é mais difícil de rastrear a origem do ataque. Os vendedores de RaaS funcionam exatamente como outro tipo de negócio, em que os ciberatacantes podem comprar e personalizar o ransomware através de um portal de cliente.

9- Privacidade e Conformidade Regulatória (DORA, NIS2): A NIS2, *Network and Information Security Directive*, constitui um dos esforços mais abrangentes da União Europeia, de modo a melhorar a cibersegurança e proteger as infraestruturas contra as ciberameaças, pretendendo garantir que os prestadores de serviços digitais tenham acesso a medidas de segurança adequadas para se protegerem contra possíveis incidentes cibernéticos e assegurarem a ciber-resiliência das redes e sistemas informáticos. Já o objetivo da DORA, *Digital Operational Resilience Act*, é garantir que a resiliência operacional digital do setor financeiro da UE seja funcional, através de um quadro regulamentar que dê resposta à dependência do setor relativamente à tecnologia, propondo que as organizações tenham de cumprir certos requisitos. Em 2024, os Estados-Membro da UE podem adotar a norma NIS2, no entanto apenas indivíduos ou sistemas, que tenham autorização prévia, podem aceder a uma rede ou um sistema de uma organização, levando a que os fornecedores de serviços digitais desenvolvam práticas de cibersegurança mais rigorosas e eficazes.

10- Extended Detection and Response (XDR): Com o avanço constante tecnológico, as ferramentas tradicionais de cibersegurança deixarão de ser suficientemente

eficazes e darão lugar a soluções mais abrangentes. Por exemplo, as plataformas XDR (Deteção e Resposta Alargadas) têm como função a recolha e a correlação automáticas de dados, integrando vários níveis de segurança como o correio eletrónico, servidores, armazenamento de cloud e redes. Esta análise de segurança permite às organizações correlacionar dados, prever ameaças e responder de forma rápida e eficiente.

11- Intensificação de investimentos em Supply Chain Risk Management (Third Party): O Third-Party Risk Management é o processo de análise e diminuição de riscos associados à subcontratação de fornecedores ou prestadores de serviços a terceiros. Em 2023, houve um aumento dos ataques a dados relacionados com terceiros e as supply chain tornaram-se numa preocupação devido a questões geopolíticas. Assim prevê-se que em 2024 existam várias tendências a nível dos riscos relacionados com supply chain, destacando-se as ameaças de cibersegurança com a potencial exposição à confidencialidade, integridade ou disponibilidade da infraestrutura e dos dados e sistemas tecnológicos.

12- Tecnologias de preservação da privacidade: A privacidade de dados e a sua regulamentação vão servir como forma de desenvolvimento de tecnologias de preservação da privacidade, como por exemplo a encriptação homomórfica. Isto é, uma inovação que permite a computação segura em dados encriptados, salvaguardando a privacidade dos mesmos sem comprometer a sua utilidade.

13- Integração do DevSecOps: O DevSecOps deixará de ser um conceito e tornar-se-á numa parte fundamental no que diz respeito ao desenvolvimento de software. O conceito de DevSecOps significa Desenvolvimento, Segurança, Operações e tem como principal objetivo incorporar a parte da segurança em todas as fases do processo de desenvolvimento e das operações de software. Neste mesmo processo de desenvolvimento, a segurança será integrada através de medidas de segurança proativas.

14- Segurança em ambiente Cloud e Multi-Cloud: A segurança em cloud ou multi-cloud tem sido referida como uma tendência a adotar no ecossistema de IT, e que se vai manter em 2024. No entanto, apesar de ser uma ferramenta que facilita o armazenamento de dados de uma organização, é também uma forma de os atacantes cibernéticos conseguirem aceder aos sistemas informáticos. Assim, prevê-se uma melhoria e um reforço de ambientes Cloud mas, também que exista um aumento de ataques cibernéticos a esses mesmos ambientes.

Para aceder ao whitepaper com a informação completa sobre as 14 tendências para 2024 em cibersegurança (link).

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 CIS - Centro de Segurança na Internet, prestamos serviços a um número considerável de clientes, operando em mais de 20 países.

Contacts

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