Integrity part of Devoteam IDENTIFICA

11 TENDÊNCIAS EM CIBERSEGURANÇA PARA 2023

Lisboa, 10 de janeiro de 2023

A cibersegurança continuará a ser uma grande preocupação em 2023. Os indicadores não deixam margem para dúvidas, e em 2022 **manteve-se a tendência de aumento do volume de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional, segundo o observatório do CNCS (Centro Nacional de Cibersegurança).** Ameaças maliciosas e acidentais, juntamente com regulamentações de dados cada vez mais rígidas e com atacantes mais criativos e sofisticados, serão alguns dos temas para os quais é importante estarmos informados.

O que nos espera em 2023? Estaremos preparados para a criatividade e ousadia dos cibercriminosos? Aqui destacamos algumas das tendências de cibersegurança para 2023 que os especialistas da Integrity part of Devoteam identificaram:

1. O impacto da Inteligência Artificial (IA)

A Inteligência Artificial continuará a ter um impacto significativo no ambiente da cibersegurança. Esta está a começar a assumir um papel importante nos processos de negócios, criando soluções em tempo real mais rapidamente do que um humano.

Os cibercriminosos estão a apostar, por exemplo, em vídeos deepfake. Usam-nos para manipular informações, destruir credibilidade e fazerem-se passar por fontes confiáveis. Segundo especialistas, a tecnologia deepfake é neste momento a mais preocupante no uso de inteligência artificial, visto esta poder ter efeitos significativos no terrorismo e no cibercrime.

Estima-se que mais temáticas de cibersegurança serão disponibilizadas com sistemas de IA ano após ano.

2. Eventos Globais

A turbulência global ou eventos politicamente voláteis podem desencadear sérios riscos de cibersegurança. Além disso, eventos com potencial impacto internacional costumam definir tendências para moldar a ação e a resposta na esfera de tecnologias de informação e cibersegurança.

3. Segurança na Cloud
À medida que as organizações migram para a cloud, é inevitável que a cibersegurança desenvolva soluções específicas. E a tendência é que aumente a migração por parte das entidades. Pode-se dizer que a cloud continuará a ser uma componente chave tanto pela utilidade quanto de defesa do negócio. Atualmente, é líder em proteção contra ransomware, principalmente devido à sua funcionalidade de backup e capacidade de construir infraestrutura rapidamente.

4. Internet of Things
O uso comum da IoT cria uma base de ataque atrativa aos cibercriminosos. De acordo com a *Insider Intelligence*, provavelmente haverá 64 biliões de dispositivos IoT implantados em todo o mundo nos próximos cinco anos. A oportunidade de ataque de uma organização cresce à medida que mais dispositivos são ligados à Internet.

5. Nova Geração de Rede Móvel
Como o 5G é uma tecnologia muito recente, é difícil prever quais os efeitos que terá na cibersegurança.
Novos níveis inéditos de ligação sem fio e velocidade são introduzidos com o 5G. Existem mais oportunidades para iniciar ataques maiores e com velocidade mais rápida.

6. Ataques a dispositivos móveis
Os cibercriminosos atacam dispositivos móveis através de diversos métodos, como phishing e aplicações não autorizadas. Atualmente, estes dispositivos podem armazenar grandes quantidades de dados valiosos e realizar funções remotamente, e muitas das vezes possuem um nível baixo de segurança. A segurança móvel é muitas vezes subvalorizada, e sendo estes mais uma porta potencial para a violação de rede apesar dos esforços dos fabricantes para implementar a segurança, é muito provável que os ataques de phishing e malware a estes dispositivos aumente.

7. Ataques à Cadeia de Abastecimento
Os ataques à cadeia de abastecimento podem usar vulnerabilidades em software de terceiros e causar perdas financeiras substanciais.
As operações de negócio de hoje são suportadas principalmente pela rede mundial de fornecedores, serviços de terceiros e cadeias de abastecimento. Infelizmente, esta dependência aumenta as possibilidades de ataque às empresas e oferece aos cibercriminosos mais pontos de entrada para exploração.

8. Ransomware direcionado
Ransomware, a maior ameaça que mais visibilidade suscita, é um dos grandes problemas com os quais a cibersegurança tem que lidar.
As campanhas de ransomware exigem recursos e, portanto, as de grande impacto podem ser patrocinadas por terroristas que pretendem infligir um ataque massivo a um território ou organização. Com a situação atual de guerra na Ucrânia vimos isso a acontecer com a ciberguerra. Estes ataques de ransomware podem até vir a tornar-se um cenário regular.

9. Leis de Privacidade de Dados
Numa época em que partilhamos as nossas informações pessoais em quase todos os serviços, os governos começaram a tomar medidas rígidas sobre a segurança de dados.
75% da população mundial terá as suas informações pessoais protegidas por legislações modernas de privacidade de dados estabelecidas por várias autoridades de proteção de dados (como GDPR), a partir do final de 2023.
Os consumidores poderão saber que tipo de dados são recolhidos sobre si e qual a finalidade. As organizações começarão a gerir várias leis de proteção de dados e ir-se-ão concentrar em automatizar a abordagem de privacidade de dados.

10. Hacking veículos autónomos
Os veículos autónomos são um tema que nos deixa a todos curiosos e entusiasmados. Mas estará a cibersegurança preparada para esta tecnologia?
Os automóveis frequentemente têm software automatizado, permitindo recursos como *cruise control*, sincronização do motor, airbags, fecho automático de portas e sistemas de suporte à condução.
Atualmente, acredita-se que os cibercriminosos poderão controlar veículos ou ouvir conversas através de microfones.

11. Escassez de Recursos
De forma, a dar resposta às exigências regulatórias e aos desafios dos cibercriminosos com ataques cada vez mais engenhosos e criativos, a procura por especialistas e talentos em cibersegurança aumentou consideravelmente. A carência de talento, com conhecimento e experiência em cibersegurança é um dos principais desafios para 2023.

Para aceder ao whitepaper com a informação completa sobre as 11 Tendências em cibersegurança para 2023 .

Sobre a Integrity part of Devoteam

A INTEGRITY part of Devoteam é uma empresa de Consultoria e Auditoria Tecnológica de Cibersegurança, certificada na ISO 27001, ISO 9001, certificada pelo PCI e membro CREST e do CIS – Center for Internet Security. Conta com uma experiência de mais de 12 anos, e opera em 19 países na EMEA oferecendo serviços de valor acrescentado em Cibersegurança, que combinam a sua experiência e tecnologia proprietária para reduzir, de forma consistente e eficaz, o risco cibernético dos seus clientes. As gamas de serviços abrangentes incluem Testes de Intrusão Persistentes, Consultoria e Soluções de ISO 27001, PCI-DSS, GRC e gestão de risco de terceiros.

Contacts

INTEGRITY, SA

Portugal
Edifício Atrium Saldanha
Praça Duque de Saldanha, nº
1, 2º andar
1050-094 Lisboa
T: +351 21 33 03 740
www.integrity.pt

United Kingdom
5th Floor, Cottons Centre
Hay's Lane
London, SE1 2QG
T: +44 20 7288 2800

España
Calle Cronos 63
4ª planta, Oficina 2
28037 Madrid
T: +34 91 376 88 20

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