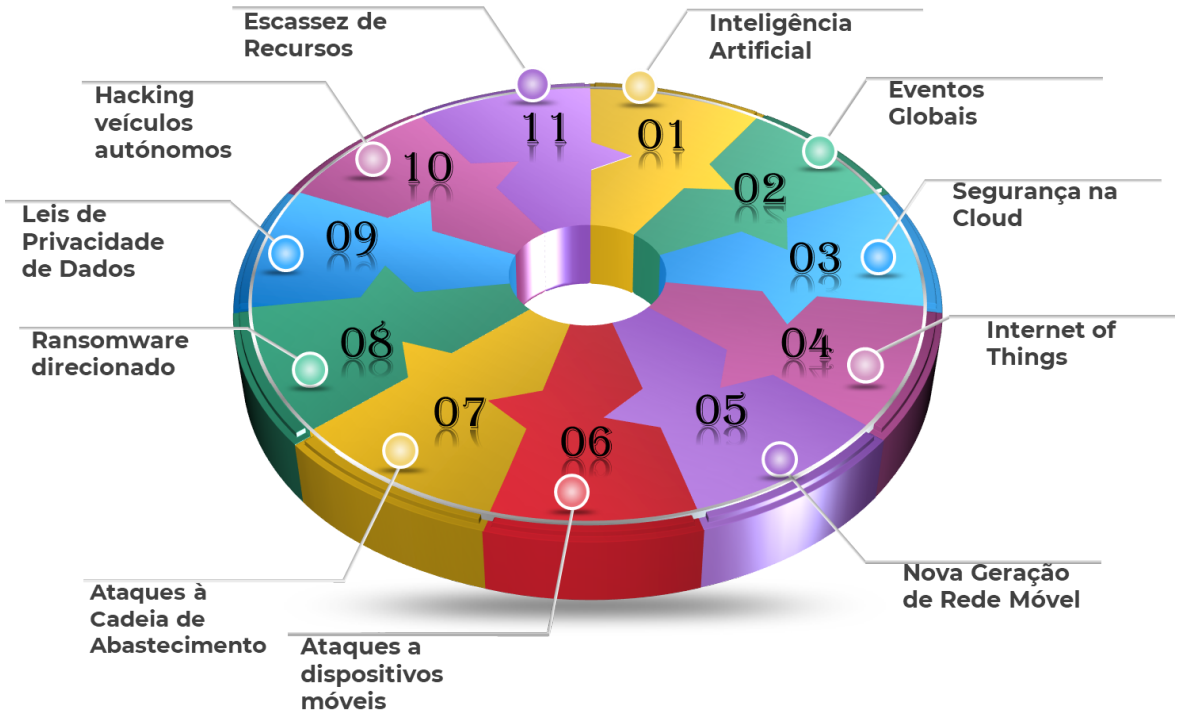
INTEGRITY
Part of Devoteam

11 tendências em cibersegurança para 2023

Securing your business

devoteam
Cyber Trust

11 tendências em cibersegurança para 2023



A cada ano, a tecnologia evolui e molda a forma como conduzimos os negócios, gerimos tarefas e armazenamos dados. O ambiente digital e as oportunidades de ataques estão a mudar constantemente. Desta forma, é importante estar atentos às tendências tecnológicas, principalmente em relação à cibersegurança, que atualmente têm uma importância significativa na gestão e continuidade do negócio. A prevenção e defesa da cibersegurança está intrinsecamente relacionado com identificar tendências, tecnologias e fatores de potenciais ameaças. Com base nestas premissas destacamos aqui aquelas que consideramos serem as tendências para 2023.

1 O impacto da Inteligência Artificial (IA)

A Inteligência Artificial continuará a ter um impacto significativo no ambiente da cibersegurança. Esta, está a assumir um papel importante nos processos de negócios, criando soluções em tempo real mais rapidamente do que um humano. A IA pode executar várias tarefas relacionadas com a segurança, incluindo análise de dados e *machine learning*.

A IA também pode ser utilizada por cibercriminosos. Na cibersegurança, incorporar soluções automatizadas baseadas em IA é uma necessidade, neste momento, para economizar recursos e por ser mais confiável contra ataques automatizados.

Os vídeos deepfake são populares nas redes sociais, e os cibercriminosos sabendo disso, 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.

Como um excelente exemplo, a pandemia do COVID-19 criou um terreno fértil para cibercriminosos e grupos de malware desenvolveram campanhas de ameaças com base no vírus e desinformação em volta do tratamento, como as vacinas. Sempre que surgem assuntos importantes, estes fornecem munição para liderar ataques de phishing, malware e outros ciberataques.

Também por isso, as organizações tiveram de se adaptar e definir novas políticas de segurança durante a pandemia para os seus funcionários. As precauções básicas incluíam o uso de dispositivos dedicados, acessos reservados e orientação aos funcionários sobre segurança. Atualmente assistimos a uma adoção de trabalho híbrido, quando possível, nas organizações. Agora que a pandemia está a chegar ao fim, 2023 mostrará se alguma das precauções tomadas nestes anos fará a diferença.

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 sua aplicação nos negócios como pela prevenção da continuação do negócio. Atualmente, é líder em proteção contra ransomware, principalmente devido à sua funcionalidade de backup e capacidade de construir infraestrutura rapidamente.

Nos últimos anos, houve grandes desenvolvimentos na segurança na cloud, um dos quais é a arquitetura de segurança na cloud Zero Trust. Zero Trust é uma framework de segurança que exige que todos os utilizadores, dentro ou fora da rede da organização, sejam autenticados, autorizados e continuamente validados antes de receberem ou manterem o acesso a aplicativos e dados.

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.

Computadores ou smartphones têm melhores precauções de segurança em comparação com outros dispositivos IoT. Tendo isto em conta, um dos tópicos críticos de cibersegurança a serem observados em 2023 é a IoT e o aumento da digitalização.

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. Assim como a IoT, o 5G ainda é uma nova arquitetura, então levará algum tempo para se adaptar e proteger. Os early adopters devem ser cautelosos ao integrar tecnologia de ponta e até mesmo limitar o uso de dispositivos baseados em 5G.

6 Ataques a dispositivos móveis

Os ciber criminosos 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.

De acordo com relatórios de open source, o número de ataques à cadeia de abastecimento aumentou 430% em 2021.

Embora os ataques à cadeia de abastecimento já não sejam uma novidade, outros cibercriminosos oportunistas e motivados financeiramente ficarão alerta sobre o potencial existente e impacto que pode desencadear. Os cibercriminosos estão mais dispostos a aplicar uma estratégia que vejam ter sucesso.

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. Com oportunidades crescentes em recursos e alvos, espera-se que os casos de ransomware patrocinados e direcionados, como por exemplo, o incidente do Colonial Pipeline, aumentem proporcionalmente.

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 RGPD), 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 ciber criminosos poderão controlar veículos ou ouvir conversas através de microfones.

Por isso, é fundamental estar atento aos inúmeros riscos associados à aquisição destes novos veículos autónomos.

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.

Muitas organizações carecem de talento, conhecimento e experiência em cibersegurança – e o défice está a crescer. Em geral, a gestão de risco cibernético não acompanhou a proliferação das transformações digitais e analíticas, e muitas empresas não sabem ao certo como identificar e gerir os riscos digitais. Para agravar o desafio, os reguladores estão a aumentar a orientação dos recursos de cibersegurança corporativa, geralmente com o mesmo nível de supervisão e foco aplicado a riscos de crédito e liquidez em serviços financeiros e a riscos operacionais e de segurança física em infraestrutura crítica.

Ao mesmo tempo, as empresas enfrentam requisitos de conformidade mais rígidos, resultado de crescentes preocupações com a privacidade e violações de segurança de alto perfil.

Em 2023 esse desafio mantém-se, prevendo-se que poderá aumentar a procura por talentos e a exigência dos reguladores.

Compreender as tendências, especialmente as ameaças à cibersegurança, significa permanecer ciente do mundo ao nosso redor.

Fontes:

- https://www.insiderintelligence.com
- https://www.techtarget.com/searchsecurity/tip/5-steps-to-help-prevent-supply-chain-cybersecurity-threats
- https://www.computerweekly.com/news/252500508/Colonial-Pipeline-ransomware-attack-has-grave-consequences
- https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html
- https://infosecwriteups.com/car-hacking-cyber-security-in-automotive-industry-e9a7a4ffd6bb
- https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html
- https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Portugal	United Kingdom	España
Edifício Atrium Saldanha Praça Duque de Saldanha, nº 1, 2º andar 1050-094, Lisboa | Portugal T: +351 21 33 03 740 E: info@integrity.pt www.integrity.pt	5th Floor, Cottons Centre Hay's Lane London, SE1 2QG | United Kingdom T: +44 20 7288 2800	Calle Cronos 63, 4ª planta Oficina 2 28037, Madrid | España T: +34 91 376 88 20

Conteúdo produzido pela Integrity part of Devoteam