Buddy Email

**Microsoft identifica cinco tendências que vão marcar o futuro da segurança digital**

**Lisboa, 19 de agosto de 2025** – A inovação nas empresas está a acelerar, com tecnologias como a inteligência artificial (IA), a computação quântica e agentes inteligentes a transformar a forma como operam. Porém, à medida que estas transformações impulsionam a produtividade e a competitividade, também multiplicam os riscos de segurança, pelo que, para as organizações atuais, a questão já não é se a disrupção vai impactar a sua segurança, mas com que rapidez conseguem adaptar-se.

A segurança deixou de ser apenas uma função técnica, tornando-se um imperativo estratégico para o negócio. Para se manterem competitivas e protegidas, as organizações devem adotar ações imediatas, através da construção de programas de segurança resilientes e orientados para o futuro.

Perante este cenário, a Microsoft identificou **cinco tendências de segurança que irão moldar a próxima década**:

**Agentes de IA impulsionarão a produtividade, mas vão multiplicar o risco**

Um futuro do trabalho onde agentes de IA executam processos empresariais em conjunto com indivíduos e equipas deixou de ser uma utopia. Nos próximos cinco anos, estes agentes estarão totalmente integrados no nosso dia a dia, aumentando a produtividade e interagindo de forma natural por nós.

Esta mudança impactará profundamente as organizações, promovendo maior produtividade no trabalho, com os agentes a assumir tarefas repetitivas, libertando as pessoas para atividades que exigem ideação, criatividade, visão e ligação interpessoal. Estes agentes também terão um papel relevante na gestão e automatização de aspetos da segurança.

No entanto, embora os agentes de IA melhorem a produtividade global das organizações, a sua utilização por agentes maliciosos pode introduzir novos riscos de segurança, sendo [importante proteger implementações do Model Context Protocol (MCP),](https://techcommunity.microsoft.com/blog/microsoft-security-blog/understanding-and-mitigating-security-risks-in-mcp-implementations/4404667) uma vez que esta é uma área cada vez mais ameaçada. Ao reconfigurar a força de trabalho para incluir agentes de IA, as organizações devem construir estruturas de segurança paralelas que utilizem as mesmas competências operacionais dos agentes para se defender contra cenários de ameaça mais amplos e complexos.

**Agentes ciberfísicos vão expandir o perímetro de segurança**

À medida que os sistemas de IA começam a governar ambientes físicos (controlando desde fechaduras de portas a operações de veículos e linhas de produção inteiras), o perímetro de segurança estende-se para além do domínio digital. Esta evolução, com sistemas de IA incorporados em sistemas físicos, introduz novos riscos e potenciais alvos para manipulação ou disrupção.

A convergência entre sistemas digitais e físicos significa que uma violação num domínio pode ter repercussões no outro e, por isso, as estratégias de segurança devem considerar este cenário de ameaça alargado, garantindo que os sistemas físicos estão tão protegidos quanto os digitais. Para tal, é essencial integrar a segurança física na estratégia global de cibersegurança das empresas, através do investimento em sistemas que monitorizem, verifiquem e defendam ambientes físicos com IA, garantindo também a segurança integral da cadeia de abastecimento.

**A computação quântica criará ameaças retroativas e exigirá tecnologia de proteção específica**

A computação quântica deixou de ser uma possibilidade distante, passando a ser uma realidade que se aproxima rapidamente. Quando os sistemas quânticos atingirem 1 milhão de qubits, terão capacidade para quebrar os algoritmos criptográficos mais utilizados atualmente, o que alterará fundamentalmente o panorama da segurança.

Esta não é uma ameaça futura, visto que se podem recolher dados encriptados agora e decifrá-los mais tarde, quando as capacidades quânticas estiverem disponíveis. Este risco retroativo obriga a uma transição imediata para encriptação resistente à computação quântica, sendo necessário priorizar o investimento em [criptografia pós-quântica](https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803), avaliar as dependências criptográficas da organização e desenvolver uma estratégia para atualizar os sistemas antes que as ameaças quânticas se tornem reais.

**Equipas de trabalho potenciadas por IA vão redefinir talento e risco**

A IA está a transformar a forma como trabalhamos. Nos próximos três a cinco anos, os indivíduos liderarão as suas próprias equipas virtuais, potenciadas por agentes de IA com diferentes funções, o que redefinirá a produtividade e os modelos de talento em todos os setores.

Contudo, à medida que a IA amplia as equipas de trabalho, também expande a superfície de ataque, e as equipas de segurança devem preparar-se para um mundo onde tanto elas como os invasores são potenciados por IA e em que as oportunidades residem no seu uso para reforçar as defesas, automatizar a deteção de ameaças e acelerar a resposta.

As implicações para melhorar a segurança são reais. As *blue teams* (responsáveis por defender contra ataques simulados ou reais) dependerão cada vez mais de assistentes virtuais para recolher, analisar e enriquecer dados. Estas equipas potenciadas por IA vão melhorar a análise de *logs,* simplificar a gestão de *patches* e elevar a capacidade de resposta a ameaças. Este nível de assistência poderá estar disponível nos próximos 18 meses, acelerando tanto a velocidade, como a precisão das operações de segurança.

Neste sentido, é importante que as organizações promovam a colaboração entre as equipas de recursos humanos e de tecnologias da informação para apoiar modelos de trabalho amplificados por IA, e que construam programas de segurança que a utilizem para prevenção, deteção e resiliência, garantindo a capacitação e proteção da força de trabalho.

**Segurança ao nível do hardware vai reduzir ameaças e exigir atualizações de sistemas**

Uma mudança significativa já em curso é a migração para um modelo de segurança ao nível do hardware ou equipamentos. Ao incorporar a segurança diretamente nos componentes físicos, em dispositivos *endpoint* ou equipamentos de rede, as organizações podem reduzir a dependência de *patches* de software e otimizar a segurança.

Isto é especialmente importante à medida que dispositivos de *edge legacy*, como routers, impressoras e equipamentosVPN, se tornam alvos comuns, visto que estes sistemas executam software desatualizado e carecem de proteções modernas. Os equipamentosmodernos, no entanto, estão cada vez mais equipados com funcionalidades de segurança incorporadas, como *secure boot*, validação de *firmware* e isolamento baseado em hardware, oferecendo um caminho para defesas mais sólidas e fiáveis.

Assim, as organizações devem planear atualizações de hardware e firmware, transferindo os dispositivos para uma rede isolada para garantir segurança ao nível do equipamento. Este investimento vai reforçar as capacidades de prevenção e reduzir a carga sobre os sistemas de deteção e resposta, garantindo que a infraestrutura vital está protegida em todas os níveis.

**Estratégias de segurança para as organizações se prepararem para o futuro**

Para enfrentar um cenário de ameaças cada vez mais sofisticadas, as organizações precisam de adotar uma abordagem proativa em relação à segurança. Para tal, devem começar por **assegurar cadeias de abastecimento de software e hardware fiáveis**, tendo em conta que estas são altamente interconectadas e vulneráveis a ataques, para evitar que agentes maliciosos introduzam componentes comprometidos ou enfraqueçam a criptografia das redes. Paralelamente, é essencial **priorizar o investimento em prevenção em detrimento da deteção**, apostando em estratégias como Zero Trust e segurança baseada em hardware, que reduzem a superfície de ataque e impedem incidentes antes que ocorram, libertando as equipas para se concentrarem em ameaças críticas.

Ao mesmo tempo, as organizações devem **apostar na IA agentiva como um aliado estratégico de segurança**, capaz de auditar redes, analisar *logs* e identificar anomalias em tempo real, funcionando como um multiplicador de capacidades para equipas com recursos limitados e possibilitando a defesa perante ataques mais complexos. Além disso, o **investimento em mecanismos que assegurem a integridade e autenticidade de dados, código e comunicações** torna-se indispensável, com a atual proliferação de conteúdos sintéticos e *deepfakes*. Finalmente, a **aposta em protocolos de manutenção e segurança consistentes**, caracterizados pelas atualizações regulares, autenticação sem palavra-passe, rotação de credenciais e monitorização disciplinada, continua a ser a melhor defesa contra muitos ataques comuns. Estas estratégias são fundamentais para construir programas de segurança resilientes e preparados para um futuro marcado por disrupção tecnológica.

Nesta lógica, a Microsoft apoia várias iniciativas concebidas para tornar todos os ambientes digitais que utilizam os seus produtos mais seguros e resilientes a incidentes, nomeadamente:

* [**Secure Future Initiative (SFI):**](https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative) compromisso plurianual da Microsoft para continuar a integrar segurança nos produtos, serviços e operações. O objetivo é melhorar o design, a construção, os testes e a operação da tecnologia para cumprir os mais elevados padrões de segurança.
* [**Windows Resiliency Initiative (WRI**):](https://blogs.windows.com/windowsexperience/2024/11/19/windows-security-and-resiliency-protecting-your-business/) iniciativa da Microsoft que se concentra na prevenção, gestão e recuperação de incidentes de segurança e fiabilidade, mitigando rapidamente problemas caso surjam e facilitando a recuperação contínua em toda a plataforma Windows. A WRI inclui a capacidade de recuperar sistemas remotamente e integra um esforço contínuo para tornar o Windows a plataforma aberta mais resiliente e segura.
* [**Microsoft Virus Initiative (MVI**):](https://learn.microsoft.com/en-us/unified-secops-platform/virus-initiative-criteria) programa de parceria com outros fornecedores independentes de software que disponibilizam soluções *antimalware*. A Microsoft colabora com os parceiros MVI para definir e seguir Safe Deployment Practices (SDP), resposta a incidentes e desenvolvimento de novas capacidades de plataforma no Windows 11.
* [**Zero Trust:**](https://www.microsoft.com/en-us/security/business/zero-trust) estratégia e abordagem de segurança que exige verificação explícita, utilização do princípio de menor privilégio e pressupõe a existência de uma violação. O *framework* foi criado para ajudar as organizações a reduzir vulnerabilidades de segurança com maior visibilidade em todos os seus ambientes digitais, controlos de acesso baseados em risco e políticas automatizadas.

Estamos a entrar numa nova era de disrupção, impulsionada pela IA, pela tecnologia quântica e por outras tecnologias transformadoras. Através de estratégias proativas e segurança integrada, é possível proteger dados, garantir resiliência e preparar as organizações para o futuro.

**CONTACTOS**

|  |  |  |
| --- | --- | --- |
| **Catarina Brito** | **Inês Filipe** |  |
| catarina.brito@lift.com.pt  | ines.filipe@lift.com.pt |  |
| 914 310 661 | 910 283 054 |  |

**SOBRE A MICROSOFT**

Microsoft (Nasdaq "MSFT" @microsoft) cria plataformas e ferramentas robustecidas por Inteligência Artificial para entregar soluções inovadoras que correspondam às necessidades crescentes dos nossos clientes. Enquanto empresa de tecnologia está comprometida com a democratização do acesso a Inteligência Artificial de forma responsável, mantendo a missão de capacitar todas as pessoas e organizações no planeta para atingir mais.