OPINIÃO

2026 será o ano da cibersegurança inteligente e mais madura

Sylvio Herbst (*)

À medida que nos aproximamos de 2026, o setor de cibersegurança avança para um momento com menos euforia e mais maturidade tecnológica, já que este foi um ano em que algumas promessas grandiosas não se cumpriram, e isso, longe de ser um fracasso, abriu espaço para uma compreensão mais realista sobre o que de fato protege uma organização em um cenário onde ameaças crescem mais rápido que modismos.

Um dos maiores equívocos de 2025 foi a crença de que a simples adoção massiva de automações e soluções "autônomas" resolveria, por si só, os grandes problemas de segurança. Muitas empresas apostaram que ferramentas com IA conseguiriam detectar e responder a ataques sem esforço humano. Mas a realidade foi outra, já que o aumento de ataques sofisticados mostrou que modelos de IA exigem ajustes constantes, dados de qualidade e supervisão humana experiente. O que vimos foram automações que sem governança, geraram ruídos, alertas falsos e pontos cegos perigosos. A ausência de equipes preparadas para interpretar e calibrar essas tecnologias impediu que boa parte das expectativas se concretizasse.

Também houve a expectativa que focar apenas na migração para infraestruturas híbridas e distribuídas seria suficiente para entregar resiliência. As organizações, de fato, tiveram sucesso, mas a complexidade cresceu mais rápido que a capacidade de administrá-la. Houve um aumento significativo de ataques explorando configurações incoerentes entre ambientes, zonas mal definidas e identidades replicadas sem governança adequada. Ou seja, o movimento para a nuvem não falhou, o que falhou foi a suposição de que o simples fato de "estar na nuvem" seria igual a "estar seguro".

Já a surpresa de 2025 foi o fator humano voltando ao centro do debate, em um cenário onde todo mundo falava em IA, foi justamente o comportamento dos colaboradores, parceiros e usuários, que determinou grande parte dos riscos.

2026 exigirá inteligência, integração e identidade

Para o próximo ano, o setor deve caminhar com foco em três eixos fundamentais:

- **Uma segurança mais inteligente, não apenas mais automatizada:** A IA deixará de ser tratada como "ferramenta mágica" e passará a ocupar seu lugar como força multiplicadora da capacidade humana. O próximo ano será marcado por modelos mais contextualizados, que entendem não apenas o comportamento da rede, mas o propósito do negócio. Empresas maduras irão combinar automação com processos de avaliação contínua, revisões periódicas de risco e profissionais capazes de interpretar sinais fracos antes que se transformem em incidentes críticos.
- **Aproximação real entre redes, aplicações, identidades e governança:** Para 2026, a tendência inevitável é a consolidação de políticas unificadas, plataformas integradas e visibilidade ponta a ponta. Não basta monitorar acessos, será necessário correlacionar identidades com contexto, postura de dispositivos, criticidade dos ativos e comportamento histórico. A segurança deixará de ser apenas reativa e se tornará preditiva.
- **Menos foco em perímetro, mais foco em confiança adaptativa:** A identidade será o elemento central, analisando quem acessa, de onde, com que intenção e com que risco naquele momento específico. A validação contínua deixará de ser vista como burocracia e passará a ser percebida como ferramenta para proteger operações em tempo real.

2026 será o ano da maturidade e da honestidade técnica

Se este ano foi marcado por grandes expectativas, 2026 será lembrado como o ano em que o setor entendeu que segurança não é um produto, é uma prática contínua. Não existe solução única, modelo universal ou proteção instantânea. Há, sim, combinações inteligentes entre tecnologia, processos bem definidos e pessoas que entendem o impacto real de cada decisão.

A cibersegurança do próximo ano será mais humana, técnica e consciente de suas próprias limitações, exatamente o que precisamos para enfrentar um ambiente de ameaças que não perdoa improviso.

Se 2026 trouxer menos promessas milagrosas e mais responsabilidade compartilhada, teremos dado um passo significativo rumo a organizações realmente resilientes.

(*) Formado em engenharia de telecomunicações e pós-graduado em marketing, co-fundador e diretor comercial de marketing na 5F Soluções em TI.

Startup aposta em ondas sonoras contra incêndios

A Sonic Fire Tech, startup fundada pelo engenheiro aeroespacial Geoff Bruder, desenvolveu um sistema capaz de apagar incêndios usando infrassom, ondas sonoras de baixa frequência inaudíveis pelo ouvido humano.

Vivaldo José Breternitz (*)

digitalhallway_CANVA

Bruder diz que o sistema atua sobre as moléculas de oxigênio que alimentam as chamas; sensores detectam calor ou chamas e acionam automaticamente o sistema, que cria um campo de infrassom que afasta o oxigênio, extinguindo as chamas. A ideia interessa especialmente para a proteção de construções que possam ser afetadas por incêndios florestais.

O conceito não é totalmente novo. A agência DARPA, ligada ao Departamento de Defesa dos EUA, estudou o uso de som para controlar fogo entre 2008 e 2011, e universidades chegaram a criar protótipos experimentais. O diferencial da Sonic Fire Tech está na frequência utilizada: abaixo de 20 hertz, capaz de percorrer maiores distâncias sem distorção e sem afetar pessoas ou estruturas.

Numa primeira fase, a ideia é que o sistema seja instalado nas edificações que se deseja proteger; tão logo sensores detectem calor ou chamas, ondas sonoras passam a ser emitidas por dutos metálicos instalados sob o telhado e beirais dos edifícios. Testes já mostraram eficácia a até 7,5 metros de distância.

Especialistas reconhecem o potencial do sistema, mas alertam para os desafios. "A influência acústica sobre chamas é bem conhecida", afirma Albert Simeoni, do Worcester Polytechnic Institute. Ele ressalta, porém, que ampliar a escala da tecnologia exige controle preciso para evitar efeitos vibracionais indesejados. Outros pesquisadores lembram que o método é eficiente em pequenos fogos, enquanto incêndios florestais geram fluxos de calor complexos.

Mesmo assim, a possibilidade de proteger estruturas contra incêndios, atrai a atenção. A Sonic Fire Tech já firmou parceria com duas empresas da Califórnia e prevê cerca de 50 instalações-piloto até o início de 2026.

Se os testes forem bem-sucedidos, o infrassom poderá se juntar a drones, sistemas de detecção por inteligência artificial e outras ferramentas emergentes no arsenal tecnológico usado contra incêndios florestais.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

USP inaugura Espaço Meteorológico em fevereiro e transforma mais de um século de dados em experiência aberta ao público

A Estação Meteorológica Professor Paulo Marques do Santos do Instituto de Astronomia, Geofísica e Ciências Atmosféricas (EM-IAG) e o Parque de Ciência e Tecnologia da Universidade de São Paulo (CienTec-USP) inauguram no sábado, dia 7 de fevereiro de 2026, às 10h, no Hall de entrada de seu prédio principal, o Espaço Meteorológico, uma área expositiva permanente que apresentará mais de um século de observações do tempo e do clima em São Paulo. Idealizado pela equipe da EM-IAG, o espaço combina uma linha do tempo histórica com séries científicas de temperatura e precipitação, instrumentos meteorológicos e observações meteorológicas exibidas em tempo real para explicar, de forma acessível, como a Meteorologia observa o tempo, constrói previsões e ajuda a compreender as mudanças climáticas.

O coração do Espaço Meteorológico é um grande painel que combina história e ciência. Na parte superior, uma série temporal da temperatura média anual mostra, por meio de cores, quando os valores ficaram acima ou abaixo da média histórica. Tons de azul indicam anos mais frios; tons de vermelho, anos mais quentes. "Ao longo dos últimos 20 ou 30 anos, foi possível observar um aquecimento, ou seja, a temperatura na nossa região aumentou", afirma Prof. Morales. Segundo ele, o painel permite visualizar esse padrão de forma direta, sem necessidade de conhecimentos técnicos prévios.

divulgacao_IAG/USP

Abaixo, um segundo gráfico apresenta a chuva anual em mm e as cores representam a porcentagem em relação à média histórica. A opção por percentuais, explica o professor, torna a informação mais intuitiva para o público geral. "Chuva em milímetros é mais difícil de entender. Em porcentagem, a pessoa consegue ver se choveu 10% a mais ou a menos, por exemplo", diz.

Os dados indicam que, nas últimas 9 décadas, a precipitação anual na região aumentou cerca de 400 milímetros, o que representa aproximadamente 60% acima da média em determinados períodos. "O aumento da temperatura e o aumento da chuva aparecem quase em fase", observa Morales. "As leis da física mostram que quanto mais quente a atmosfera, maior a capacidade de reter vapor de água, o que pode se converter em mais chuva".

Ao entrar no CienTec-USP, o visitante passará a ter contato direto com uma narrativa que começa no final do século XIX e atravessa a formação da meteorologia acadêmica no Brasil até chegar às discussões mais atuais sobre clima e aquecimento observado nas últimas décadas. O Espaço Meteorológico nasce com a vocação educativa e científica de mostrar que a previsão do tempo consultada diariamente no celular depende de uma infraestrutura de medições, padronização e continuidade que atravessa gerações.

News @ TI

ricardosouza@netjen.com.br

Solução completa de cibersegurança como serviço

@A TechEnabler amplia os recursos de segurança para mercados corporativo e de telecomunicações por meio da parceria com a empresa norte-americana Planisys. Com foco em soluções e segurança baseadas em DNS (Domain Name System), a tecnologia da Planisys proporciona uma camada essencial para gerenciar, de maneira simples, o DNS como serviço crítico de defesa ao filtrar, monitorar e bloquear requisições maliciosas de DNS antes de concretizadas as ameaças. Principal linha de defesa da Planisys, o RPZ (Response Policy Zone) funciona como um firewall do DNS controlando os domínios aos quais o servidor deve responder e bloqueando acesso a destinos e domínios perigosos ou indesejáveis. Assim, impede o acesso aos usados para phishing, malware e ransomware, reduzindo riscos de invasão, sequestro de dados e movimentação lateral dentro de ambientes corporativos ou de ISPs, que muitas vezes têm dispositivos de usuários infectados (https://techenabler.com.br/).

FIAP e MetaIndústria celebram dois anos de parceria com ampliação de aulas práticas

@Lançado no segundo semestre de 2023 pela Agência Brasileira de Desenvolvimento Industrial (ABDI) em parceria com a SPI Integração de Sistemas, o MetaIndústria e o Centro Universitário FIAP, de São Paulo (SP), celebram os dois anos do projeto e de colaboração mútua com a ampliação de suas ações conjuntas. Agora, a cooperação entre a iniciativa da ABDI e a instituição de ensino inclui estudos em robótica, solução que também integra o Edital MetaIndústria, anunciado em 7/11, e cujas inscrições, prorrogadas, encerram-se nesta sexta-feira (19). As atividades do MetaIndústria com o centro universitário, que consistem na conexão de planos de cursos a demandas reais da indústria, com mentoria e acesso ao MetaIndústria Lab, em São Caetano do Sul (SP), tiveram seu portfólio de desafios atualizado com estudos que vão da robotização convencional a tópicos emergentes, como aplicações com humanoides (https://prosas.com.br/editais/16210).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.