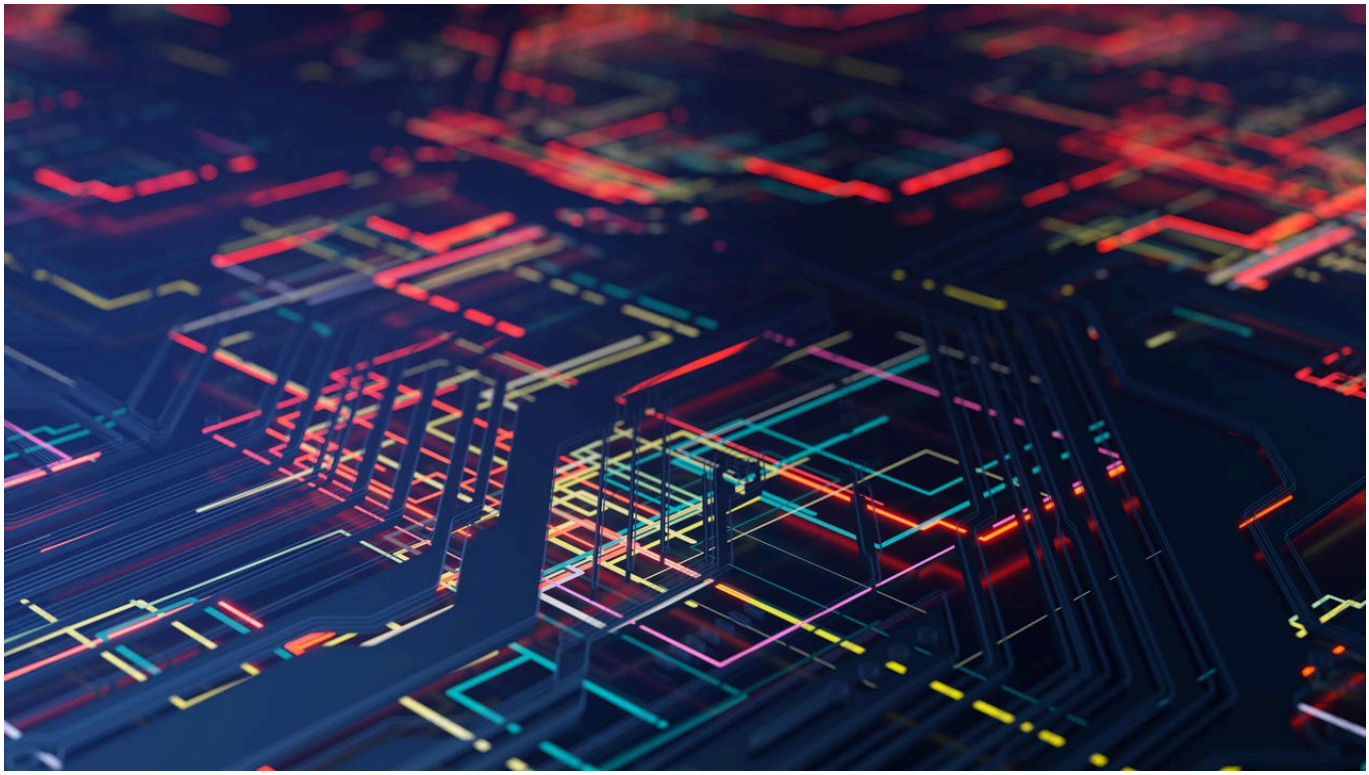
memória virtual



sankai/Getty Images

O cenário da cibersegurança de 2024 foi marcado por ataques devastadores de ransomware, engenharia social alimentada pela inteligência artificial (IA) e operações cibernéticas patrocinadas pelo Estado que causaram milhares de milhões em danos. No início de 2025, a convergência da IA, a instabilidade geopolítica e as superfícies de ataque em evolução apresentam um ambiente de ameaças ainda mais complexo.

Os profissionais de segurança estão se preparando para o que poderá ser o ano mais desafiador até agora na defesa cibernética, à medida que os agentes de ameaças utilizam ferramentas e táticas cada vez mais sofisticadas. Com base na inteligência atual sobre ameaças e nos padrões de ataques emergentes, aqui estão cinco previsões significativas de segurança cibernética que provavelmente moldarão 2025.

O que você vai ler:

# 1. Ransomware se tornará destruição e manipulação de dados

O ransomware não se trata mais apenas de extorsão – está se tornando uma ferramenta para perturbação sistêmica.

**Além disso: Os prêmios Best of CES 2025 já chegaram, selecionados pela ZDNET e pelo resto do Grupo CNET**

Os ataques de ransomware tornaram-se uma presença constante no cenário de ameaças à segurança cibernética, com organizações pagando milhões para recuperar dados criptografados. Contudo, a natureza destes ataques está a mudar. Este ano, os grupos de ransomware irão além da criptografia e do roubo de dados, visando a própria integridade dos dados críticos.

Esta evolução poderá incluir ataques que corrompem bases de dados sensíveis, modifiquem registos financeiros ou interrompam as operações de indústrias inteiras. Imagine as implicações de registos médicos alterados num hospital ou de dados financeiros adulterados num banco multinacional. Os riscos vão além das perdas monetárias, ameaçando vidas e desestabilizando a confiança nas instituições.

“As cargas de ransomware em si não mudaram muito. Vimos alguns pequenos ajustes e melhorias”, observa Dick O’Brien, principal analista de inteligência da Symantec Threat Hunter Team da Broadcom. “No entanto, inovações genuínas ocorreram na cadeia de ataque de ransomware. Seu ataque de ransomware médio e bem-sucedido é um processo complexo e de vários estágios que envolve uma ampla gama de ferramentas e uma boa quantidade de atividade prática de teclado por parte dos invasores .”

**Além disso: a engenharia imediata é uma ‘moda passageira’ que impede o progresso da IA?**

O’Brien credita a mudança à evolução de ferramentas e táticas. “A principal tendência tem sido o afastamento do malware. A maioria das ferramentas usadas pelos invasores atualmente são softwares legítimos”, explica ele. “Em muitos ataques, o único malware que vemos é o ransomware, que é introduzido e executado no último minuto.”

Estudos recentes, incluindo insights da Agência de Segurança Cibernética e de Infraestrutura (CISA), enfatizam a crescente sofisticação dos operadores de ransomware que aproveitam a IA e a automação para lançar ataques mais rápidos e mais direcionados.

### O que as organizações podem fazer

- Implemente estratégias avançadas de backup e recuperação de desastres.
- Priorize as verificações de integridade dos dados para garantir que dados adulterados sejam detectados.
- Invista em ferramentas de detecção e resposta de endpoint (EDR) para identificar e isolar ameaças rapidamente.

## 2. Os ataques alimentados por IA ultrapassarão as defesas humanas

A IA está revolucionando as indústrias, e isso inclui o crime cibernético. Em 2025, os adversários aproveitarão a IA para criar campanhas de phishing altamente direcionadas, desenvolver malware avançado e identificar vulnerabilidades do sistema a velocidades sem precedentes. Estes ataques impulsionados pela IA desafiarão até mesmo as equipas de segurança cibernética mais avançadas, uma vez que o grande volume e sofisticação das ameaças ultrapassarão as defesas manuais.

**Além disso: Como se proteger contra ataques de phishing no Chrome e Firefox**

Um exemplo desta ameaça emergente é o uso de IA generativa para criar áudio e vídeo deepfake, que podem ser usados para contornar sistemas de verificação de identidade ou espalhar informações erradas. Em 2024, vários incidentes de grande repercussão demonstraram o quão convincente a tecnologia deepfake se tornou, e o seu potencial para abuso em ataques cibernéticos só está a crescer.

“A comunidade adversária do crime cibernético é oportunista e empreendedora, e tem sido rápida em adotar e implantar novas tecnologias (…) o uso de deepfakes, inteligência artificial e LLMs é o próximo passo nesta evolução, à medida que os invasores buscam estabelecer confiança com a vítima nos estágios iniciais do ataque por meio de engenharia social”, diz Alex Cox, diretor de segurança da informação do LastPass. “Eles geralmente conseguem isso fingindo ser o tomador de decisões da empresa visada, colocando assim autoridade conhecida por trás das solicitações do invasor”.

Os ataques alimentados por IA são perigosos porque são escalonados sem esforço. Um invasor pode programar um sistema de IA para identificar senhas fracas em milhares de contas em minutos ou para verificar vulnerabilidades em uma rede corporativa inteira com muito mais rapidez do que um ser humano conseguiria.

### O que as organizações podem fazer

- Implante ferramentas defensivas baseadas em IA que monitoram redes em tempo real.
- Treine os funcionários para reconhecer tentativas sofisticadas de phishing, mesmo criadas por IA.
- Colabore com parceiros do setor para compartilhar informações sobre ameaças emergentes baseadas em IA.

O jogo de gato e rato da cibersegurança está a entrar numa fase nova e mais rápida, onde a IA é a principal tecnologia implementada pelas equipas vermelha e azul.

## 3. As infraestruturas críticas serão um alvo precoce

Em 2024, os ataques a infraestruturas críticas chegaram às manchetes, desde as redes energéticas europeias aos sistemas de água nos Estados Unidos. Esta tendência irá acelerar em 2025, à medida que os Estados-nação e os grupos cibercriminosos se concentrarem em perturbar os sistemas dos quais as sociedades mais dependem. Estes ataques visam frequentemente causar o caos máximo com o mínimo de esforço e são cada vez mais utilizados como arma em conflitos geopolíticos.

**Além disso: o tecnólogo Bruce Schneier sobre segurança, sociedade e por que precisamos de modelos de 'IA pública'**

Sistemas antigos e protocolos de segurança fragmentados agravam os riscos para infraestruturas críticas. Por exemplo, muitas redes energéticas dependem de tecnologias legadas nunca concebidas para resistir aos ataques cibernéticos modernos. Entretanto, a crescente interconectividade da tecnologia operacional (TO) e da tecnologia da informação (TI) cria novas vulnerabilidades.

"Ao falar com empresas de água e serviços públicos, descobri que muitos carecem do básico nos seus programas cibernéticos industriais", alerta Ian Bramson, vice-presidente de cibersegurança industrial global da Black & Veatch. "Eles não estabeleceram visibilidade em suas redes de TO ou controle sobre seus ambientes para prevenir, detectar ou responder a ataques".

Bramson exorta os líderes a encararem a cibernética industrial – o que ele chama de "as redes, equipamentos e dispositivos que impactam a segurança e o tempo de atividade (ou seja, a continuidade operacional)" – como uma questão de segurança. "Os ataques virtuais a estes podem ter impactos físicos significativos no mundo real. Tornar o ciberespaço uma preocupação de segurança exige ação e prioriza recursos. Todas as empresas de serviços públicos levam a segurança a sério. Estender isso ao ciberespaço dá-lhe a prioridade de que necessita. Em última análise, é o bem-estar público e a segurança dos funcionários que tornam a TO uma missão crítica para as concessionárias de água."

### O que as organizações podem fazer

- Faça parceria com agências governamentais como a CISA para identificar e mitigar vulnerabilidades.
- Segmente redes de TO e TI para limitar o impacto de violações.
- Invista no monitoramento contínuo e na detecção de ameaças em tempo real para sistemas críticos.

Proteger infraestruturas críticas não é apenas uma prioridade de segurança cibernética – é uma questão de segurança nacional.

## 4. Os ataques à cadeia de abastecimento aumentarão

A natureza interligada dos negócios globais criou uma tempestade perfeita para ataques à cadeia de abastecimento. Essas violações exploram vulnerabilidades em fornecedores terceirizados, permitindo que invasores se infiltrem em diversas organizações por meio de um único ponto de entrada. Em 2025, os especialistas esperam que estes ataques cresçam em frequência e sofisticação.

Um exemplo notável é o ataque cibernético à SolarWinds, que comprometeu milhares de organizações ao atingir um fornecedor de software amplamente utilizado. Da mesma forma, o ataque de ransomware Kaseya destacou como os pequenos fornecedores podem servir como portas de entrada para empresas maiores. Os ataques à cadeia de abastecimento são insidiosos porque exploram relações de confiança entre empresas e seus fornecedores, muitas vezes passando despercebidos durante meses.

**Além disso: Anthropic sinaliza o potencial da IA para 'automatizar ataques cibernéticos destrutivos sofisticados'**

Os governos e os órgãos reguladores estão atentos. Em 2024, foram introduzidas novas directrizes para a segurança da cadeia de abastecimento tanto nos EUA como na União Europeia, enfatizando a necessidade de transparência e responsabilização. No entanto, a conformidade por si só não será suficiente para impedir os invasores que estão em constante evolução nos seus métodos.

Como explica Matti Pearce, vice-presidente de segurança da informação, risco e conformidade da Absolute Security: "Os CISOs precisarão de técnicas inovadoras de detecção e monitoramento para descobrir aplicativos de IA não autorizados que podem não ser diretamente observáveis no tráfego de rede. ferramentas de IA seguras e aprovadas serão estratégias centrais para mitigar esses riscos (…) como o aumento no uso de IA está ultrapassando a segurança da IA, você verá a IA atacando a IA para criar uma tempestade de ameaças perfeita para usuários corporativos."

“Hoje, a indústria de segurança ainda não sabe como proteger bem a IA”, continua Pearce. “O erro humano – e não os adversários maliciosos – será a razão deste conflito esperado. Com a crescente adoção da IA, podemos esperar ver o envenenamento da IA na já vulnerável cadeia de abastecimento. Além disso, uma falha crítica da IA será o ponto de entrada para um ataque potencialmente novo e inovador que não será detectado e causará perturbações económicas significativas.”

### O que as organizações podem fazer

- Conduza auditorias de segurança completas de todos os fornecedores terceirizados.
- Implemente princípios de confiança zero para limitar o impacto de parceiros comprometidos.
- Use inteligência contra ameaças para identificar e responder proativamente às vulnerabilidades da cadeia de suprimentos.

A segurança da sua cadeia de abastecimento é tão forte quanto o seu elo mais fraco.

## 5. A lacuna de competências em segurança cibernética no local de trabalho irá aumentar

A indústria de segurança cibernética enfrenta uma escassez significativa de talentos. De acordo com um relatório do ISC², o número de empregos não preenchidos em segurança cibernética – mais de 3,4 milhões a nível mundial em 2024 – deverá crescer em 2025. Esta lacuna na força de trabalho apresenta um desafio significativo à medida que aumenta a procura de profissionais qualificados.

**Além disso: você pode aprimorar suas habilidades em segurança cibernética gratuitamente com esta nova iniciativa**

A escassez não se trata apenas de números – trata-se de experiência. Muitas organizações lutam para encontrar funcionários com habilidades especializadas em inteligência contra ameaças, defesas baseadas em IA e segurança na nuvem. Como resultado, as equipas sobrecarregadas correm maior risco de esgotamento, levando a taxas de rotatividade mais elevadas e agravando ainda mais o problema.

“Está em curso uma mudança no equilíbrio de poder no submundo do crime, exigindo soluções humanas”, diz O’Brien**.** “Historicamente, os operadores de grandes famílias de ransomware estavam no topo da cadeia alimentar do crime cibernético. Eles franqueavam seus negócios usando o modelo de negócios de ransomware como serviço (RaaS), onde invasores “afiliados” alugavam suas ferramentas e infraestrutura em troca por uma redução nos pagamentos do resgate.

“No entanto, a consequência não intencional deste modelo de negócio tem sido colocar mais poder nas mãos dos afiliados, que podem migrar rapidamente para operações rivais se uma delas for encerrada. As operações de ransomware estão agora a competir entre si por afiliados, oferecendo condições cada vez melhores para os seus negócios. .”

**Além disso: os ataques de ‘enganar você mesmo’ aumentaram mais de 600% – aqui está o que procurar**

Para enfrentar esta crise, as organizações estão a recorrer a soluções criativas. Programas de qualificação e iniciativas de treinamento interno estão ajudando os funcionários existentes na transição para funções de segurança cibernética. Além disso, a automação e a IA lidam com tarefas repetitivas, liberando os analistas humanos para se concentrarem na tomada de decisões estratégicas.

### O que as organizações podem fazer

- Invista em programas de treinamento e mentoria para desenvolver talentos internos.
- Faça parceria com universidades e campos de treinamento de codificação para construir um fluxo de trabalhadores qualificados.
- Abrace iniciativas de diversidade para atrair candidatos de grupos sub-representados.

Colmatar a lacuna de talentos em segurança cibernética não é apenas um desafio da indústria – é um imperativo social.

## O que essas previsões significam para 2025

Os desafios da cibersegurança de 2025 são assustadores, mas não são intransponíveis. As organizações podem defender-se contra ameaças cibernéticas inovadoras utilizando uma abordagem multicamadas que combina soluções tecnológicas com experiência humana.

As ferramentas defensivas alimentadas por IA fornecem vigilância de rede em tempo real, enquanto a segmentação rigorosa entre sistemas operacionais e de tecnologia da informação protege a infraestrutura crítica. Os princípios de segurança de confiança zero e auditorias minuciosas dos fornecedores ajudam a mitigar as vulnerabilidades da cadeia de fornecimento. Ao investir em programas de formação em cibersegurança para resolver a escassez de talentos, as organizações podem aproveitar a engenhosidade humana para contornar as vulnerabilidades de forma proativa.