# Cenário de segurança cibernética 2025 em meio a vulnerabilidades record

Data: 2025-09-06 06:06:02

Autor: Inteligência Against Invaders

O ano de 2025 se desenrolou em um ambiente marcado pela corroagem de trust em bancos de

dados de vulnerabilidades, um crescimento explosivo em ataques cibernéticos e sobrecarga digital

para as empresas.

As violações de dados se tornaram rotina, o número de CVEs continua a quebrar registros e as abordagens tradicionais de defesa não funcionam mais.

A especialista em segurança cibernética Ilia Dubov, chefe de segurança da informação e conformidade na Kaspersky publicado Uma visão geral do setor e uma estratégia de gerenciamento de vulnerabilidades na revista Top Voices.

Aqui estão os fatos e tendências mais importantes que definem o cenário da indústria este ano.

## 1. Crescimento de CVEs

2024 Defina um recorde para CVEs. De acordo com **O fórum de equipes de resposta a incidentes e segurança (PRIMEIRO)**mais de 45.000 vulnerabilidades foram registradas em doze meses e, em 2025, esse número deve aumentar em outros 11%.

Para os profissionais de segurança, isso significa não apenas uma carga de trabalho cada vez maior, mas também diminuindo o tempo de resposta. O mais preocupante é que a lacuna entre divulgação e exploração diminuiu para apenas algumas horas.

Os invasores estão alavancando a automação e o aprendizado de máquina para armar a CVEs para explorações de trabalho mais rapidamente do que as organizações podem preparar e implantar patches.

## 2. Desafios de infraestrutura

Em meio ao rápido crescimento de novas vulnerabilidades, a comunidade enfrenta desafios de infraestrutura sem precedentes. O exemplo mais revelador é a crise no **Banco de Dados Nacional de Vulnerabilidades (Nvd)**.

Durante anos, desenvolvedores e equipes de segurança em todo o mundo se basearam em NVD, mas em 2024, ficou sobrecarregado e incapaz de acompanhar os dados recebidos.

Em novembro, o banco de dados havia acumulado mais de 20.000 vulnerabilidades não processadas. Destes, 93% eram novos e quase metade já estava sendo explorada ativamente.

Em outras palavras, as próprias ameaças que a comunidade mais necessária para a visibilidade permaneceu não analisada e não categorizada.

Conforme destacado por Dubov, essa situação minou a confiança em fontes centralizadas e abriu oportunidades adicionais para os atacantes.

A quebra do NVD desencadeou um efeito dominó: algumas empresas foram forçadas a recorrer a plataformas comerciais, outras para iniciativas locais, fragmentando ainda mais o cenário de dados e crescendo riscos de duplicação ou perda de informações críticas.

A crise também não passou despercebida no nível político: a União Europeia oficialmente encarregada **ENISA** Com o desenvolvimento de um banco de dados europeu de vulnerabilidade – a primeira vez que um regulador regional questionou publicamente a eficácia da fonte global.

## 3. A transformação digital acelera

Enquanto isso, os negócios não estão desacelerando. Os serviços de nuvem, IoT, SaaS e AI estão sendo adotados em um ritmo cada vez mais rápido, adicionando novos pontos de risco.

Em infraestruturas grandes e distribuídas, as vulnerabilidades estão emergindo mais rápido do que podem ser corrigidas. Dubov enfatiza que as organizações carecem de uma única fonte confiável de dados de ameaças, as atualizações são atrasadas e as recomendações geralmente são inconsistentes.

Sob essas condições, as estratégias clássicas parecem cada vez mais rígidas. Vedificações programadas e ciclos de patch não permitem mais que as organizações permaneçam à frente dos atacantes.

As empresas estão reagindo após o fato, enquanto a superfície de ataque continua a se expandir. Em vez de reduzir constantemente as ameaças, as organizações estão acumulando uma “dívida de segurança” – um número crescente de vulnerabilidades não tratadas que os invasores podem explorar facilmente.

## 4. Métodos desatualizados estão perdendo eficácia

O gerenciamento tradicional de vulnerabilidades foi construído na varredura programada, priorização baseada em CVSS e patches de rotina.

Esse modelo funcionou quando o volume de vulnerabilidades foi menor e as façanhas levaram semanas para se desenvolver. Hoje, tornou -se amplamente uma formalidade.

Os scanners não cobrem adequadamente ambientes híbridos, como contêineres, nuvem e SaaS. As pontuações do CVSS não refletem a verdadeira probabilidade de exploração ou a criticidade dos negócios dos ativos.

Como resultado, as organizações recebem relatórios com centenas de vulnerabilidades “vermelhas”, mas não têm clareza sobre quais representam ameaças imediatas. O processo existe no papel, mas não reduz mais os riscos do mundo real.

Ainda mais importante, o modelo antigo tem **grandes pontos cegos**. Ele se concentra

exclusivamente nas vulnerabilidades registradas (CVEs) e ignora amplamente:

- Equívocas (por exemplo, baldes S3 expostos, gateways VPN e errôneos incorretos);
- contas esquecidas ou fracas, incluindo contas de serviço sem MFA;
- tokens e chaves codificadas no código -fonte;
- Shadow TI ativos e serviços SaaS fora da visibilidade da equipe de segurança.

Esses problemas não são rastreados no NVD e não recebem pontuações do CVSS, mas, na prática, são frequentemente os pontos de entrada iniciais para os atacantes.

Em outras palavras, o processo clássico cobre apenas a “ponta do iceberg”, deixando as organizações expostas a um amplo espectro de riscos que os scanners simplesmente não podem ver.

### 5. Mudança para gerenciamento de exposição

O caminho a seguir é uma transição para o gerenciamento de exposição. Esse novo modelo olha além do CVS para abranger todo o espectro de pontos de risco: configurações expostas, contas esquecidas, tokens codificados e links fracos nas cadeias de suprimentos.

Em sua essência, há um inventário de ativos abrangente e atualizado, de sistemas locais a serviços em nuvem, IoT e OT.

A agregação de dados em várias fontes – NVD, CISA KEV, Vulncheck, Feeds de inteligência de ameaças e boletins de fornecedores – fornece uma imagem mais precisa da qual as ameaças realmente importam.

A priorização é impulsionada pelo contexto dos negócios: quão crítico é o ativo, a probabilidade de exploração e o impacto potencial.

A automação e a IA desempenham um papel central, permitindo uma reação mais rápida e mais nítido, concentre -se no que mais importa.

A eficácia é medida com novas métricas que Dubov enfatiza em seu artigo:

- **Tempo médio para detectar/responder (mttd/mttr)** – velocidade de detecção e resposta;
- **Taxa de patch** – conformidade com slas de remendos;
- **Taxa de recorrência de vulnerabilidade** – Com que frequência os problemas reaparecem, por exemplo, em imagens de contêineres ou novos lançamentos;
  **Índice de exposição a ameaças** – Uma visão holística do risco organizacional de liderança executiva.

## O que vem a seguir

2025 está se tornando um ponto de virada. Os métodos desatualizados não podem mais acompanhar o ritmo e a escala dos ataques.

O novo modelo-gerenciamento de exposição-requer automação, dados integrados e colaboração multifuncional entre segurança, DevOps e equipes de negócios. As organizações que se adaptam

serão capazes de manter o controle real de riscos.

Aqueles que continuam confiando em patch-and-sray permanecerão na defensiva e enfrentam ataques mais frequentes pelos quais não estão preparados.

Para o mercado e as organizações individuais, isso se traduz em três ações principais:

- Mudança de patches de vulnerabilidade reativa para sistemática **Gerenciamento de exposição**;
- implantando **Automação e AI** em escala nos processos de detecção e patch;
- adotando novos **métricas de eficácia** Isso reflete não o número de CVEs fechados, mas a redução real de risco.

Para estratégia detalhada e recomendações práticas, consulte Ilia Dubov's artigo – *Estratégia de implementação para gerenciamento de vulnerabilidades na paisagem de segurança cibernética de 2025*.