CIBERSEGURANÇA EM FOCO

As Principais Notícias das Últimas Duas Semanas

Período: 20 de fevereiro a 13 de março de 2026 · Edição especial de acompanhamento

A quinzena de 20 de fevereiro a 13 de março de 2026 foi marcada por uma explosão de ataques cibernéticos a setores críticos, a maior aquisição da história da indústria de segurança digital, e uma nova doutrina cibernética do governo americano que redefine o papel do Estado na proteção do ciberespaço. O mundo da cibersegurança nunca esteve tão acelerado — nem tão estratégico.

94	US$ 32 bi	45.000	129	78	4,8 mi
presos na Op. Synergia III	aquisição Google/Wiz	IPs maliciosos derrubados	vulns. Android corrigidas	vulns. Microsoft Patch Tuesday	profissionais em falta global

CONCLUSÃO ANALÍTICA

Esta quinzena confirmou uma inflexão histórica: a cibersegurança deixou de ser um departamento de TI e tornou-se infraestrutura estratégica — de estados, empresas e agora de conflitos geopolíticos. O ataque iraniano à Stryker não é apenas um incidente corporativo; é a primeira vez que wiper malware estatal destrói dados de uma empresa de saúde global em tempo de paz. A aquisição da Wiz pelo Google por US$ 32 bilhões sinaliza que a consolidação do mercado de segurança em cloud chegou ao topo. Para profissionais e organizações, a pergunta não é mais 'se preciso de cibersegurança' — é 'como vou sobreviver ao próximo ataque antes que a janela de resposta se feche'.

SUMÁRIO

01	Corrida de Vulnerabilidades: Velocidade Sem Precedentes	3
02	O Ataque à Stryker: Estado, Wiper Malware e Infraestrutura Crítica	4
03	Google Adquire Wiz por US$ 32 Bi: A Grande Consolidação	5
04	Nova Doutrina Cibernética dos EUA: Estratégia e Ofensiva	6
05	Empregos, Economia e o Futuro da Força de Trabalho em Cyber	7
06	Brasil: LGPD, ANPD e a Regulação Avança	8
07	Outros Destaques da Quinzena	9

01 Corrida de Vulnerabilidades: Velocidade Sem Precedentes

Fevereiro e início de março de 2026 registraram um volume sem precedentes de patches críticos e zero-days explorados ativamente — um ritmo que colocou equipes de segurança sob pressão constante. A disputa não é mais apenas entre atacantes e defensores: é uma corrida contra o relógio.

- **Microsoft Patch Tuesday – março (10/mar) —** 78 vulnerabilidades corrigidas em Windows, Office, Azure, SQL Server e .NET. Destaque para CVE-2026-21262, único zero-day do pacote, com exploração ativa confirmada. Também presentes: falhas críticas de RCE no SharePoint (CVE-2026-26114) e elevação de privilégio no Kernel (CVE-2026-26132).
- **Google Chrome – dois zero-days explorados (10/mar) —** CVE-2026-3909 (escrita fora dos limites na biblioteca gráfica Skia, CVSS 8.8) e CVE-2026-3910 (implementação inadequada no motor V8, CVSS 8.8). Ambos corrigidos em atualização de emergência.
- **Android Security Bulletin – março (3/mar) —** 129 vulnerabilidades corrigidas no ecossistema Android, incluindo 10 falhas críticas. A CVE-2026-21385, overflow de inteiro no componente gráfico da Qualcomm, foi confirmada explorada ativamente no campo — afeta 234 chipsets distintos.
- **Cisco Catalyst SD-WAN (CVSS 10.0) —** CVE-2026-20127, bypass de autenticação explorado pelo grupo UAT-8616 desde 2023. A CISA emitiu Diretiva de Emergência 26-03 exigindo correção por agências federais até 5/mar.
- **VMware Aria Operations (Broadcom) —** CVE-2026-22719 adicionada ao catálogo KEV da CISA — injeção de comando não autenticada com execução remota de código durante workflows de migração.

Tendência-chave: a exploração de ferramentas de gerenciamento (vCenter, SIEM, backup managers) virou estratégia deliberada dos atacantes — não mais oportunista. Quem protege a infraestrutura de segurança em si?

Fonte: The Hacker News · DIESEC · BleepingComputer · Cyber Security Review · SecurityWeek

02 O Ataque à Stryker: Estado, Wiper Malware e Infraestrutura Crítica

O episódio mais perturbador da quinzena foi o ataque cibernético à Stryker — gigante global de tecnologia médica — por hackers ligados ao regime iraniano, em uma das mais graves ações destrutivas contra uma empresa privada de saúde de que se tem registro.

- **11/mar — O ataque —** Hackers associados ao grupo Handala (pró-palestino, vinculado ao Irã) implantaram wiper malware na rede da Stryker, apagando permanentemente dados em sua sede em Cork, Irlanda, e comprometendo dispositivos em escala global. Diferente do ransomware, o objetivo era destruição — não extorsão.
- **Impacto operacional —** Milhares de funcionários ficaram sem acesso a sistemas críticos. Times de cibersegurança internos e engenheiros da Microsoft foram mobilizados para contenção e investigação. Operações mundiais severamente afetadas.
- **Contexto geopolítico —** O ataque ocorre em meio a tensões crescentes entre operações cibernéticas estatais e alvos privados do setor de saúde. Empresas de medtech e pharma — antes consideradas fora do radar de ataques estatais — tornaram-se alvos estratégicos.
- **Resposta do setor —** O caso intensificou o debate sobre a responsabilidade de governos em proteger infraestrutura crítica privada contra ataques de Estados-nação. Nenhum dado foi exfiltrado — somente destruído, tornando a recuperação especialmente complexa.

O caso Stryker estabelece um precedente sombrio: wiper malware estatal agora mira hospitais e empresas de saúde. A linha entre guerra cibernética e crime organizado contra civis continua a se dissolver.

Fonte: CybersecurityNews · SecurityWeek · BleepingComputer · Malwarebytes

03 Google Adquire Wiz por US$ 32 Bi: A Grande Consolidação

Em paralelo às ameaças, o maior movimento de consolidação da história da cibersegurança foi concluído nesta quinzena: o Google finalizou a aquisição da Wiz por US$ 32 bilhões em dinheiro — superando qualquer outra transação já registrada no setor.

- **11/mar — Fechamento do negócio —** A Wiz, plataforma líder de segurança em cloud fundada por ex-engenheiros da Microsoft, passa a integrar o Google Cloud mantendo sua marca e compromisso com ambientes multi-cloud, incluindo AWS, Azure e Oracle Cloud.
- **Por que é histórico —** O negócio supera a compra da CyberArk pela Palo Alto Networks (US$ 25 bi) e a aquisição do Splunk pela Cisco (US$ 28 bi). A Wiz cruzou US$ 1 bilhão de ARR em 2025 e havia recusado oferta anterior do Google.
- **O que muda na prática —** A combinação une o Google Threat Intelligence e Google Security Operations com a plataforma cloud-native da Wiz — criando uma camada de proteção unificada com IA (Gemini) para multicloud. Agentes de IA de segurança serão lançados em breve.
- **Regulação —** A aquisição recebeu aprovação antitruste do DOJ americano (novembro/2025) e da Comissão Europeia (fevereiro/2026) sem condições — sinal de que reguladores ainda não veem a consolidação em cibersegurança como risco anticompetitivo.
- **Impacto de mercado —** Index Ventures (~US$ 3,8 bi), Sequoia (~US$ 3,2 bi) e Insight Partners (~US$ 2,9 bi) embolsam retornos expressivos. A aquisição aquece o mercado de M&A em cyber: 42 negócios anunciados só em fevereiro de 2026.

Tendência-chave: a segurança em cloud deixou de ser produto complementar — é o próximo campo de batalha estratégico das big techs. Quem controla a segurança da nuvem controla a infraestrutura digital global.

Fonte: TechCrunch · SecurityWeek · Cybersecurity Dive · Google Cloud Blog

04 Nova Doutrina Cibernética dos EUA: Estratégia e Ofensiva

Em 6 de março de 2026, o governo Trump lançou sua Estratégia Cibernética Nacional e um Decreto Executivo contra crimes cibernéticos — os documentos mais importantes de política de cibersegurança do país desde 2023, mas com abordagem radicalmente diferente.

- **A nova doutrina —** A estratégia de sete páginas — contra 39 páginas do governo Biden — prioriza imposição de custos aos adversários, postura ativa de caça a ameaças e uma visão do ciberespaço como domínio estratégico a ser dominado, não apenas defendido.
- **Os seis pilares —** Defesa de infraestrutura crítica, proteção de dados americanos de adversários estrangeiros, modernização das redes federais com zero-trust e criptografia pós-quântica, uso de IA para defender sistemas federais, cooperação com setor privado e resposta a crimes cibernéticos transnacionais.
- **Decreto contra cibercrime —** Complementa a estratégia com foco em fraude digital habilitada por tecnologia. O DOJ havia implementado regras de segurança de dados em fevereiro/2026, restringindo acesso de estrangeiros a dados sensíveis de americanos.
- **Críticas e lacunas —** Especialistas apontam falta de detalhes de implementação — o documento não designa responsáveis nem prazos concretos. Espera-se que decretos executivos subsequentes definam como cada pilar será operacionalizado.
- **CISA sem liderança confirmada —** A indicação de Sean Plankey para diretor da CISA segue travada no Senado, deixando a principal agência de defesa cibernética dos EUA sem liderança confirmada em meio ao lançamento da nova estratégia.

Fonte: Federal News Network · Data Matters (Sidley Austin) · CyberScoop

05 Empregos, Economia e o Futuro da Força de Trabalho em Cyber

Os debates sobre o impacto da cibersegurança no mercado de trabalho ganharam novos dados e tensões nesta quinzena — entre a escassez histórica de profissionais e a transformação acelerada das funções pelo avanço da IA.

- **Gap de 4,8 milhões de profissionais —** A ISC² estima que o déficit global de profissionais de cibersegurança permanece em 4,8 milhões, com 90% das equipes relatando lacunas de habilidades. Só nos EUA, 750 mil vagas permanecem abertas.
- **IA como multiplicador de força —** Palo Alto Networks prevê que agentes de IA serão o principal mecanismo para fechar o gap em 2026, com SOCs autônomos triando alertas em segundos — reduzindo a fadiga que afeta 55% das equipes.
- **Reestruturação, não substituição —** 52% dos profissionais acreditam que a IA reduzirá demanda por analistas Tier 1 e scanners de vulnerabilidade de rotina. Novas funções como AI Threat Hunter, AI Security Architect e Model Security Engineer crescem 25% ao ano.
- **Custo do crime cresce —** Mais de 52% das organizações reportaram que incidentes cibernéticos custaram mais de US$ 1 milhão em 2024 — contra 38% em 2021. 86% das organizações sofreram ao menos uma violação relevante em 2024.
- **Identidade como novo campo de batalha —** Com agentes de IA proliferando nas empresas em uma proporção de 82 máquinas por humano, ataques de deepfake a executivos e sequestro de agentes autônomos tornaram-se as principais ameaças de 2026.

Fonte: ISC² Workforce Study · Palo Alto Networks · WEF Global Cybersecurity Outlook 2026 · StationX

06 Brasil: LGPD, ANPD e a Regulação Avança

No Brasil, a cibersegurança avança na agenda regulatória com a ANPD acelerando sua pauta para 2025-2026 e empresas respondendo às exigências crescentes de conformidade com a LGPD diante da explosão de aplicações de IA.

- **ANPD — Agenda Regulatória 2025-2026 —** A Autoridade Nacional de Proteção de Dados publicou sua pauta prioritária, que inclui: regulação de direitos dos titulares, avaliações de impacto (DPIAs), dados de menores, dados biométricos, medidas de segurança e inteligência artificial — expressamente na segunda fase.
- **Notificação obrigatória de incidentes —** A Resolução CD/ANPD nº 15 estabelece procedimentos obrigatórios para controladores notificarem a ANPD e titulares sobre incidentes de segurança — passo decisivo para criar cultura de transparência em violações de dados no país.
- **Transferências internacionais regulamentadas —** A Resolução CD/ANPD nº 19 detalhou procedimentos de transferência internacional de dados e disponibilizou as Cláusulas Contratuais Padrão (SCCs) brasileiras — alinhando o Brasil ao padrão europeu do GDPR.
- **Conformidade corporativa em expansão —** 95% das empresas brasileiras expandiram seus programas de conformidade com a LGPD como resposta direta às exigências criadas pelas aplicações de IA, segundo dados do setor.
- **Malware bancário VENON —** Pesquisadores da ZenoX identificaram novo malware bancário escrito em Rust, batizado de VENON, mirando usuários brasileiros com comportamentos típicos de trojans da região (Grandoreiro, Mekotio, Coyote). Marca a adoção de linguagens modernas por cibercriminosos do ecossistema latino-americano.

Fonte: Baker McKenzie · The Hacker News · ANPD · BrightDefense

07 Outros Destaques da Quinzena

- **Operação Synergia III (13/mar) —** A INTERPOL coordenou a maior operação global contra cibercrime de sua história: 72 países, 94 presos, 110 sob investigação, 45.000 IPs maliciosos derrubados e 212 dispositivos apreendidos. Foco em phishing, ransomware, fraude de cartão e romance scams. Parceiros: Group-IB, Trend Micro, S2W.
- **SocksEscort takedown (12/mar) —** Autoridades europeias e americanas desmantelaram a rede proxy SocksEscort. 34 domínios e 23 servidores apreendidos; US$ 3,5 milhões em criptomoedas congelados.
- **Wynn Resorts — brecha em 800 mil registros —** O grupo ShinyHunters reivindicou responsabilidade pela violação de dados do Wynn Resorts, comprometendo 800.000 registros sensíveis. Natureza exata dos dados ainda sob investigação.
- **Starbucks — exposição de dados de funcionários (13/mar) —** Agentes de ameaça obtiveram acesso às contas do Starbucks Partner Central, expondo dados de centenas de funcionários em incidente divulgado pela empresa.
- **Under Armour — 72 milhões de clientes —** O grupo Everest ransomware publicou base de dados com 72,7 milhões de e-mails únicos e 191 milhões de registros totais, após a empresa não responder ao prazo de negociação.
- **Advogados e fabricação de citações por IA —** O Supremo Tribunal de Connecticut foi instado a rejeitar processo após advogados admitirem uso de IA generativa que fabricou citações judiciais inexistentes — alerta sobre riscos do uso não supervisionado em contextos de alta responsabilidade.

Relatório compilado em 13 de março de 2026 · Fontes: The Hacker News, BleepingComputer, SecurityWeek, DIESEC, Infosecurity Magazine, The Register, INTERPOL, TechCrunch, Cybersecurity Dive, Federal News Network, ISC², WEF, Palo Alto Networks, ANPD, Baker McKenzie, Malwarebytes, SharkStriker, BlackFog, CybersecurityNews e demais citadas em cada seção.