Fique um passo à frente: receba o Radar todo dia útil, de graça. Inscreva-se → hubterritory.com/radar/inscricao

UMA PUBLICAÇÃO HUB TERRITORY · INTELIGÊNCIA DE AMEAÇAS EDIÇÃO Nº 12

Radar de Ciberataques

Incidentes no Brasil, o resumo do mundo e as falhas que estão sendo exploradas

Sexta-feira, 27 de novembro de 2026 Janela: qui 26/11, 07h08 a sex 27/11, 06h57 Edição nº 12

0	0	0
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

MUNDO · TRANSPORTE MARÍTIMO

Invasão por firewalls FortiGate chegou a sistemas de controle de navios, segundo o WSJ

Os navios levavam petróleo, GLP e químicos; não houve relato de interrupção ou dano, e a inteligência dos EUA estima até 50 embarcações atingidas (estimativa). No Brasil, sem incidente novo na janela: o portal do Governo de Alagoas voltou ao ar e o Pix do Banpará foi normalizado. Lição para portos e operadores: separar a rede administrativa da operacional e manter firewalls atualizados.

Como ler: CONFIRMADO a vítima ou uma autoridade confirmou · EM ANDAMENTO caso ainda aberto · "Nota oficial" marca a fonte publicada pelo próprio afetado ou por autoridade.

Nenhum incidente novo no Brasil na janela.

BRASIL · TCU · GOVERNO FEDERAL

TCU vê avanço, mas nenhum de 239 órgãos federais cumpre todas as 56 medidas básicas de cibersegurança

No monitoramento da auditoria de 2024 (Acórdão 2829/2026), o TCU apontou que nenhuma das 239 organizações que responderam à autoavaliação implementou todas as 56 medidas básicas de cibersegurança (grupo IG1).

Houve avanço: as que cumprem mais de 90% passaram de 2 para 12, e as abaixo de 40% caíram de 166 para 123. Ainda assim, 15 órgãos não tinham gestor de segurança da informação designado e 45 de 743 diagnósticos e planos de ação não foram entregues; o tribunal citou falta e rotatividade de profissionais de TI.

Segundo a imprensa, a SGD/MGI deve passar a exigir evidências documentais a partir do ciclo de 2027. Para os órgãos, o caminho é priorizar as medidas básicas, designar o gestor de segurança e guardar a comprovação do que foi implementado.

Fontes: Nota oficial: TCU — notícia oficial, 14/10 · Paraíba Business, 16/11

BRASIL · GSI · LEI GERAL DE CIBERSEGURANÇA

GSI quer levar Lei Geral de Cibersegurança com urgência à Presidência

O ministro do GSI anunciou no Brasil Ciberseguro 2026, em Brasília, que quer levar com urgência ao presidente uma Lei Geral de Cibersegurança que junta a proposta do CNCiber ao texto em discussão no Senado; a Creden terá reunião extraordinária em 2/12, segundo a Convergência Digital (25/11).

A meta é votar a lei ainda em 2026: se a urgência for reconhecida, o governo envia projeto à Câmara, e a Comissão de Ciência e Tecnologia do Senado tem votação marcada para 2 e 3 de dezembro. Pelo texto atual, municípios com menos de 100 mil habitantes podem aderir de forma voluntária, mas passam a cumprir as regras se aderirem; a criação de uma agência ainda depende de definições sobre fiscalização e recursos.

Fonte: Convergência Digital, 25/11

PROVEDORES · CACTI · SEM CORREÇÃO AINDA

Cacti tem falha sem correção que permite executar comandos via conta guest

Um pesquisador divulgou uma falha no Cacti, ferramenta de monitoramento de rede muito usada por provedores e equipes de TI, que permite executar comandos no servidor com poucas requisições HTTP quando a conta guest está habilitada; a watchTowr publicou aviso sobre o caso, segundo o The Hacker News (27/11). A versão afetada citada é a 1.2.31.

Ainda não há correção nem CVE, e não há relato de exploração em ataques até agora. O que fazer enquanto o patch não sai: desativar a conta guest, restringir o acesso à interface web do Cacti (só rede de gestão ou VPN) e revisar as configurações do poller em busca de comandos inesperados.

Fonte: The Hacker News, 27/11

MUNDO · EQUIPAMENTOS DE REDE

Relatório InfraTrust: correções atrasadas em componentes embutidos deixam firewalls e roteadores expostos

O relatório mensal InfraTrust Pulse (Eclypsium), citado pelo BleepingComputer em 25/11, analisou 373 avisos de 23 fabricantes de equipamentos de infraestrutura entre 15/10 e 19/11; 38 deles tratam de falhas que estão no catálogo KEV da CISA.

Segundo o relatório, 33 desses 38 avisos corrigem componentes de terceiros embutidos nos aparelhos (PHP, Node.js, OpenSSH), e há atraso até o fabricante redistribuir o firmware; em 20/11, Fortinet, Juniper, Lenovo, HPE, Netgear, HP e Siemens ainda tinham correções parciais ou ausentes para o PHP2Shell.

Prioridades citadas: Cisco Expressway, PHP2Shell (Palo Alto e Check Point), Check Point CVE-2026-123039, Arista VeloCloud Orchestrator (CVE-2026-114625), Cisco ASA/FTD (CVE-2026-76418) e SonicWall SonicOS. Enquanto não houver correção, tirar interfaces de gerência da internet e procurar backdoors em equipamentos já expostos.

Fontes: BleepingComputer, 25/11 · InfraTrust Pulse — novembro/2026, 25/11

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Governo de Alagoas: portal voltou ao ar. O portal institucional voltou em 25/11, numa nova plataforma desenvolvida pela equipe do Itec; o governo informou que nenhuma informação foi perdida e o conteúdo está sendo reinserido. Como o acesso usou uma credencial de administrador válida, a lição para outros órgãos é exigir MFA e revisar periodicamente as contas privilegiadas.

Fonte: CadaMinuto, 26/11

Banpará: Pix normalizado. O Pix, suspenso em 25/11, voltou a funcionar, assim como o aplicativo e os serviços digitais; o banco informou que novas tentativas de invasão foram contidas e que segue monitorando.

Fonte: Diário do Pará, 26/11

Check Point (GT13): campanha atingiu 17 países. A atividade foi confirmada entre 17/10 e 2/11; a partir da gerência, os invasores copiaram a base dos firewalls e arquivos da autoridade certificadora interna. A Check Point diz que foi usada falha já divulgada; vale proteger o material da CA e acompanhar tarefas de política fora de horário.

Fonte: BoletimSec, 26/11

Suíça: quatro de cinco ataques com agentes de IA tiveram sucesso. Segundo o centro nacional de cibersegurança, em entrevista à TV pública SRF, dos três ataques contra operadores de infraestrutura crítica dois foram bem-sucedidos, sem interrupção grave; pequenas e médias empresas também estão entre as vítimas.

Fonte: The Hacker News, 27/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

EUA · NAVIOS COMERCIAIS / FORTIGATE

Hackers usam FortiGate para chegar à rede de controle de navios

Segundo reportagem do Wall Street Journal repercutida pelo BoletimSec em 26/11, invasores entraram por firewalls FortiGate de navios comerciais e passaram da rede administrativa para a rede de tecnologia operacional que controla equipamentos de bordo. Os navios levavam petróleo, GLP, químicos e outras cargas perigosas.

A inteligência dos EUA estima até 50 navios atingidos (estimativa, não confirmada). FBI e Guarda Costeira abordaram dois navios em agosto e emitiram alerta em setembro; não houve relato de interrupção operacional nem dano. Os EUA investigam ligação com o Irã, sem atribuição pública.

Lição para portos e operadores marítimos: manter o firewall de borda atualizado, separar a rede administrativa da operacional e monitorar o tráfego entre elas.

Fontes: BoletimSec, 26/11 · Jerusalem Post (via WSJ) — contexto de setembro, 17/09 · Nota oficial: Guarda Costeira dos EUA + FBI — Maritime Cyber Alert 02-26, 01/09

MUNDO · MICROSOFT 365

Kit EvilTokens volta a roubar contas do Microsoft 365 após derrubada

O kit de phishing EvilTokens, vendido no Telegram, voltou a operar depois da derrubada feita pela Microsoft em 22 de setembro, segundo relatório de 24/11 repercutido pelo BoletimSec. Em vez de imitar a tela de login, ele abusa do fluxo OAuth de código de dispositivo: a vítima digita um código na página real da Microsoft e o atacante recebe os tokens.

O kit foi ligado a mais de 12 mil caixas de e-mail comprometidas em mais de 10 mil organizações, com iscas que imitam Adobe, DocuSign, OneDrive e SharePoint. A Microsoft acompanha o desenvolvedor como Storm-2992.

Recomendação citada: bloquear o fluxo de código de dispositivo por Acesso Condicional no Entra ID (testar antes em modo só relatório) e, em caso suspeito, revogar sessões e tokens de renovação e remover dispositivos registrados.

Fonte: BoletimSec, 25/11

SUÉCIA · CADEIA DE SUPRIMENTOS DE SOFTWARE

Registro de pacotes Hex.pm (Elixir/Erlang) tem servidores invadidos por falha nota 10

Em 23/11, um atacante explorou uma falha de execução remota de comandos (CVE-2026-129514, CVSS 10) e rodou comandos em seis servidores de produção do Hex.pm, registro de pacotes usado por desenvolvedores Elixir e Erlang. A correção foi aplicada em todos os servidores cerca de 15 minutos após o início das requisições maliciosas.

A equipe diz não ter achado pacotes alterados, mas não descarta leitura de dados do banco: e-mails, hashes de senhas, segredos de 2FA, sessões e pacotes privados. O incidente foi comunicado à autoridade sueca de proteção de dados, à CISA e à ENISA.

Recomendação oficial: trocar a senha no hex.pm, refazer o 2FA, autenticar de novo o cliente e baixar pacotes só de repo.hex.pm até sair o cliente com novo sistema de assinatura.

Fontes: Nota oficial: Hex.pm (blog oficial) — Security incident on hex.pm, 24/11 · The Hacker News, 25/11

COREIA DO NORTE · CADEIA DE SOFTWARE

Campanha norte-coreana PolinRider contamina milhares de repositórios no GitHub

Pesquisadores da Apiiro estimam ao menos 7.609 repositórios de 2.330 contas no GitHub com um carregador malicioso em Python escondido em pacotes utilitários ou no conftest.py; a SafeDep achou 375 repositórios. A campanha é atribuída a atores norte-coreanos ligados à Contagious Interview, que usam tokens roubados de desenvolvedores para reescrever commits mantendo autor e data.

O carregador busca comandos em transações de carteiras Ethereum, roda JavaScript via Node.js, adultera ferramentas como VS Code, Cursor e GitHub Desktop e entrega ladrões de credenciais; na onda mais recente, abrir a pasta no VS Code já dispara o código. Entre 27/10 e 6/11 foram 2.040 repositórios atingidos.

O que fazer (orientação geral, não do fabricante): revisar repositórios e dependências de terceiros antes de abrir no editor, desconfiar de 'testes técnicos' de recrutamento e trocar tokens do GitHub expostos.

Fonte: The Hacker News, 26/11

Método: notícias públicas, rastreadores e as notas dos próprios afetados (fabricantes, órgãos, empresas, CVM, ANPD, CTIR Gov), com o link de cada fonte junto do texto; nenhum site de vazamento ou fórum criminoso foi acessado. Os textos são paráfrases. Conteúdo informativo, produzido com apoio de inteligência artificial a partir de fontes públicas. Alegações de grupos criminosos não foram confirmadas pelas vítimas. Correções e atualizações são publicadas nas edições seguintes.

Receba o Radar todo dia útil

Inovação, Ciberataques, Cidades e Governo Digital e Investimentos em TI por e-mail ou no canal do WhatsApp. É grátis, e você cancela quando quiser.

Inscreva-se: hubterritory.com/radar/inscricao