Número 117 | Agosto 2026

NTT DATA

Radar

A revista de cibersegurança

O que criptografamos hoje será descriptografado amanhã

Por Lluis Quiles Ardila

De tempos em tempos, a mesma notícia reaparece: a computação quântica está prestes a quebrar algum código de segurança digital. A afirmação se espalha rapidamente e deixa no ar uma pergunta incômoda: estamos criando uma tecnologia que destruirá nossa segurança? Atualmente, os computadores quânticos mais avançados operam com pouco mais de cem qubits físicos — ruidosos, instáveis e altamente suscetíveis a erros. Quebrar uma chave RSA como as que usamos habitualmente exigiria milhares de qubits lógicos estáveis, com mecanismos de correção de erros altamente eficientes. Esse nível de maturidade ainda não foi alcançado. As previsões mais otimistas apontam para aproximadamente 2035.

O risco, porém, não está no futuro. É retroativo. A lógica do "colher agora, decifrar depois" (harvest now, decrypt later) consiste em interceptar e armazenar hoje o tráfego criptografado para descriptografá-lo amanhã. Isso significa que todas as informações cuja vida útil ultrapasse a próxima década já estão expostas, de prontuários médicos a segredos industriais. As organizações terão de migrar para a criptografia pós-quântica antes que a ameaça se concretize.

E essa criptografia não é uma promessa. É um padrão. ML-KEM e ML-DSA estão se tornando normas internacionais, com implementações híbridas em VPNs, TLS e certificados. Os Estados Unidos estabeleceram 2035 como prazo para sua consolidação em âmbito federal. Na Europa, o foco está nas infraestruturas críticas até o fim da década. A indústria também já está se movimentando. A NTT Research apresentou uma suíte de segurança Zero Trust adaptada a ambientes pós-quânticos e desenvolveu o primeiro sistema de transporte pós-quântico capaz de alternar o método criptográfico sem interromper as comunicações.

No entanto, limitar o universo quântico à criptografia seria considerar apenas uma face do problema. Por isso, na NTT DATA, desenvolvemos uma oferta de valor que abrange os quatro domínios das tecnologias quânticas. A computação, com otimização, simulação e machine learning. O sensoriamento e a metrologia. As comunicações quânticas, com QKD. E a criptografia pós-quântica, desde a descoberta de ativos até a migração.

Em segurança, também é preciso considerar que esses algoritmos protegerão os agentes mal-intencionados. A criptografia resistente à computação quântica é uma tecnologia de uso duplo e protegerá igualmente comunicações legítimas, redes criminosas e mercados ilícitos.

O Fórum Econômico Mundial, por meio de seus Quantum Computing Governance Principles, e a UNESCO, por meio da COMEST, já trabalham com princípios como transparência, responsabilização e prevenção de usos maliciosos.

Além disso, estamos em plena convergência entre IA e tecnologias quânticas. Cada modelo treinado com dados confidenciais amplia a superfície que precisa ser protegida. O mesmo ocorre com cada agente que opera de forma autônoma em sistemas corporativos. A confiança digital passa a ser uma questão relacionada ao ciclo de vida dos dados.

Nesta edição da Radar, buscamos abordar o que já é realidade: a criptografia pós-quântica, a gestão de chaves e a proteção de dados. E também as tendências que estão redefinindo o ecossistema quântico e as capacidades que deveríamos começar a desenvolver hoje. O desafio é duplo e urgente: preparar-se e experimentar.

É necessário migrar antes que a ameaça se concretize e, ao mesmo tempo, desenvolver aplicações quânticas com impacto real. Os exemplos já existem: a NTT DOCOMO reorganizou as estações-base de sua rede móvel em 40 segundos, em comparação com as 27 horas exigidas pelos métodos clássicos.

Na NTT DATA, também ajudamos a otimizar a gestão logística de um cliente e a aprimorar o modelo de manutenção preditiva de outro. Novos medicamentos, materiais mais eficientes e redes com menor consumo de energia completam a outra metade dessa história — que também começa hoje.

Lluis Quiles Ardila
Managing Director

Ransomware, terceiros e patches pendentes: a cadeia invisível do risco

Cibercrônica por Marta Gonzalez Martino

Entre junho e os primeiros dias de julho, vários incidentes relevantes confirmaram uma tendência que atravessa setores e países: a exposição já não depende apenas dos sistemas próprios de cada organização. A dependência de terceiros, o uso de infraestruturas compartilhadas, a falta de aplicação de patches, o uso indevido de credenciais e a automação de etapas do ataque ampliaram o impacto de violações que, em muitos casos, começaram em um único ponto vulnerável.

O segundo maior produtor de açúcar da Austrália, a Mackay Sugar, iniciou o dia 10 de junho com seus sistemas paralisados. A empresa admitiu ter sofrido um ciberataque que afetou duas de suas três principais usinas e precisou acionar processos manuais para processar a cana já colhida. No dia 15 do mesmo mês, o grupo The Gentlemen, identificado pela Microsoft como Storm-2697, assumiu a autoria do ataque. O agente opera sob um modelo de RaaS parcialmente herdado do LockBit e utiliza um mecanismo de criptografia desenvolvido em Go, com capacidade de movimentação lateral do tipo worm, além de técnicas de evasão de EDR por meio do framework GentleKiller. A Mackay Sugar demonstrou que a fronteira entre TI e TO está se tornando cada vez mais tênue.

Quase ao mesmo tempo, o Google Threat Intelligence e a Mandiant divulgaram uma campanha contra o Oracle PeopleSoft atribuída ao ShinyHunters. Entre 27 de maio e 9 de junho, antes que a Oracle publicasse seu aviso de segurança no dia 10, os atacantes exploraram uma vulnerabilidade zero-day no PeopleSoft, software utilizado para gerenciar funções críticas como RH, finanças e cadeia de suprimentos. Segundo o Google, os atacantes implantaram agentes MeshCentral disfarçados de endpoints legítimos na nuvem para executar comandos administrativos.

Em 22 de junho, a Tata Electronics confirmou um incidente de cibersegurança em alguns de seus sistemas corporativos, depois que o World Leaks publicou na dark web mais de 200 mil arquivos, totalizando mais de 630 GB. A Reuters informou que os documentos incluíam supostos projetos, especificações, documentos de fabricação, e-mails, logs e cópias de passaportes, além de materiais relacionados a clientes como Apple e Tesla. Uma informação divulgada posteriormente agravou o caso: o vazamento incluía listas de componentes e fornecedores, além de materiais sobre testes do iPhone 18 Pro, modelo ainda não lançado no mercado.

Após o incidente, a empresa reforçou os controles internos, restringiu o acesso remoto a ferramentas sensíveis, contratou uma auditoria forense e notificou as autoridades e os clientes.

Em 23 de junho, o foco mudou para o Japão. A KDDI Corporation, uma das maiores empresas de telecomunicações do país, confirmou que havia detectado acesso não autorizado a um sistema de e-mail que atendia seis provedores de serviços de Internet, entre eles STNet, KDDI Web Communications, JCOM, Chubu Telecommunications, Nifty e BIGLOBE. O acesso foi detectado em 17 de junho e, segundo a KDDI, ocorreu por meio da exploração de uma vulnerabilidade em um software de terceiros integrado a esse sistema compartilhado. A possível exposição poderia envolver até 14,22 milhões de endereços de e-mail e senhas, incluindo contas ativas, antigas e inativas. A KDDI afirmou que seu sistema de e-mail móvel não foi afetado, mas o incidente deixou uma lição clara: o efeito dominó. Uma vulnerabilidade em uma infraestrutura compartilhada pode se tornar um ponto único de falha para vários provedores ao mesmo tempo.

A partir do fim de junho, o foco se deslocou para uma área mais incômoda: credenciais, patches pendentes e automação dos ataques. BlueHammer, uma vulnerabilidade do Windows Defender classificada pela CISA como ativamente explorada em campanhas de malware e ransomware, já havia sido corrigida pela Microsoft em abril. A vulnerabilidade permitia a elevação de privilégios para SYSTEM explorando uma race condition (condição de corrida).

No início de julho, surgiu o JadePuffer, um caso especialmente relevante para compreender a automação dos ataques. A Sysdig Threat Research Team o descreveu como o primeiro caso conhecido de ransomware agêntico: uma operação de extorsão automatizada por meio de um agente baseado em um modelo de linguagem. O acesso inicial ocorreu por meio da exploração da CVE-2025-3248, uma vulnerabilidade crítica no Langflow que permite a execução de código arbitrário sem autenticação em instâncias expostas.

A partir daí, o agente automatizou o reconhecimento, a busca por credenciais, a extração de dados e a movimentação lateral para serviços internos. Segundo a Sysdig, o ataque acabou afetando uma plataforma Nacos, na qual mais de 1.300 itens de configuração foram criptografados e foi deixada uma exigência de resgate.

Em 1º de julho, a Espanha entrou nessa sequência com a Indra, que confirmou a detecção de ransomware em uma de suas subsidiárias. Seu CSIRT acionou protocolos de análise, contenção, erradicação e recuperação. Segundo a empresa, o incidente ficou restrito a um ambiente não crítico, não se propagou para o restante do grupo e não interrompeu a prestação de serviços. O ataque foi reivindicado pelo The Gentlemen, que incluiu a Indra em seu site de vazamentos com uma contagem regressiva para a publicação de supostos dados roubados, embora a exfiltração e o tipo de informação comprometida ainda não tivessem sido confirmados publicamente.

Nos dias 5 e 6 de julho, surgiu outro caso distinto, mas com o mesmo pano de fundo: o FortiBleed. Segundo informações publicadas pelo The Times e pelo The Sun, atacantes ligados à Rússia teriam utilizado vulnerabilidades em firewalls Fortinet, combinadas com ataques de força bruta e credenciais previamente vazadas, para acessar contas de órgãos públicos britânicos. Entre as vítimas mencionadas estavam colaboradores do Foreign Office, profissionais de administrações locais e equipes técnicas de embaixadas britânicas na Tailândia e nas Ilhas Maurício. O NCSC confirmou uma campanha de força bruta e solicitou que as organizações revisassem suas credenciais e configurações.

Em conjunto, esses incidentes permitem chegar a uma conclusão clara: a superfície de ataque já não termina nos sistemas internos de uma organização. Alcança fornecedores, plataformas compartilhadas, integrações SaaS, credenciais reutilizadas, firewalls expostos, patches pendentes e ferramentas que, se não forem controladas, podem se tornar o primeiro elo de uma invasão de maior alcance.

A Mackay Sugar mostrou como um ataque digital pode afetar uma operação física; a KDDI evidenciou o risco das infraestruturas compartilhadas; o PeopleSoft e a Tata Electronics confirmaram o peso da cadeia de suprimentos; BlueHammer e FortiBleed demonstraram que vulnerabilidades conhecidas e não corrigidas continuam sendo exploráveis; o JadePuffer acrescentou a automação dos ataques como uma nova camada de pressão; e a Indra mostrou que até mesmo um incidente contido pode ser relevante quando a vítima faz parte de setores estratégicos.

Marta González Martino
Cybersecurity Consultant

Segurança pós-quântica: a era da criptoagilidade e da criptoresiliência

Artigo por Kim Bossemans

A computação quântica está saindo dos laboratórios de pesquisa e começa a se consolidar como uma força estratégica com impacto real, incluindo a transformação do panorama da cibersegurança, especialmente devido à sua capacidade potencial de desafiar os fundamentos criptográficos que sustentam a economia digital.

O modelo criptográfico atual se baseia na premissa de que determinados problemas matemáticos são praticamente impossíveis de resolver com os recursos computacionais disponíveis atualmente. Essa premissa está sendo colocada em xeque pela computação quântica, que pode tornar obsoletos algoritmos amplamente utilizados, como RSA e ECC, reduzindo drasticamente o tempo necessário para quebrá-los. O desafio já chegou. O conceito de "colher agora, decifrar depois" parte da premissa de que os dados capturados hoje poderão ser comprometidos quando a tecnologia quântica atingir a maturidade.

As organizações precisam agir com antecedência para obter visibilidade completa sobre onde e como a criptografia é implementada em seus ecossistemas digitais. Isso inclui avaliar sistemas legados, arquiteturas distribuídas e dados que, devido a requisitos regulatórios, precisam permanecer protegidos por anos ou até mesmo décadas.

Rumo a um roteiro estratégio para a segurança quântica

A transição para a segurança pós-quântica exige uma estratégia consistente que combine tecnologia, processos e capacidades organizacionais. Não existe um "interruptor" nem uma solução mágica capaz de resolver o problema de forma imediata.

Ao longo desse percurso, duas capacidades essenciais precisam ser desenvolvidas. A primeira é a criptoagilidade: a capacidade de se adaptar dinamicamente a novos padrões sem interromper as operações e de priorizar as ações de forma eficaz.

As primeiras etapas essenciais incluem identificar os ativos criptográficos, mapear dependências e compreender quais dados estão em risco. A partir daí, as organizações podem definir um roadmap que viabilize a transição para algoritmos resistentes à computação quântica, juntamente com modelos de gestão mais eficientes e escaláveis.

A segunda capacidade é a criptoresiliência, a capacidade de responder rapidamente a vulnerabilidades emergentes, manter a conformidade regulatória e preservar a confiança em um ambiente em constante evolução.

Convergência com tecnologias emergentes

A convergência com outras tecnologias emergentes, como inteligência artificial, digital twins e blockchain, amplia tanto as oportunidades quanto as exigências de segurança. Os dados utilizados para treinar modelos, otimizar operações ou simular cenários precisam permanecer protegidos, inclusive durante o processamento, elevando o padrão de proteção necessário.

Como resultado, estão surgindo abordagens mais abrangentes que combinam consultoria estratégica, experimentação aplicada e modelos de implementação em etapas. Avaliar tecnologias, desenvolver protótipos e validar casos de uso específicos ajuda a reduzir a incerteza e a acelerar a adoção com menos riscos.

Ao mesmo tempo, a evolução para modelos de criptografia como serviço está transformando a dinâmica operacional ao centralizar capacidades, automatizar a gestão de chaves e adaptar continuamente os algoritmos sem interromper as operações.

Essa abordagem reforça a segurança, simplifica as operações, reduz custos e permite respostas mais ágeis. A computação quântica abre caminho para novos níveis de otimização e eficiência em diversos setores. No entanto, aproveitar esse potencial exige construir hoje uma base sólida de confiança digital. O processo começa com uma pergunta simples: quais algoritmos criptográficos protegem nossos dados mais valiosos e qual é o nível de exposição deles em um futuro quântico?

Kim Boernmans
Head of Cybersecurity NTT DATA Benelux & France

Sete tendências que estão redefinindo o ecossistema das ciências e tecnologias quânticas

Tendências por María Gutierrez

Durante anos, o debate sobre as tecnologias quânticas se concentrou quase exclusivamente na computação quântica. No entanto, a verdadeira transformação é muito mais ampla. A chamada segunda revolução quântica está impulsionando um ecossistema que integra computação, comunicações, criptografia, algoritmos, sensoriamento e metrologia, com implicações estratégicas para a indústria, a segurança e a competitividade. Estas são as principais tendências que, em nossa avaliação, definirão sua evolução nos próximos anos:

1. Do número de qubits ao desempenho útil. O setor deixou para trás a corrida pelo aumento do número de qubits como principal indicador de progresso. A atenção agora se volta para métricas como a confiabilidade das operações, a correção de erros, a escalabilidade das arquiteturas e a capacidade de executar algoritmos com valor prático. Paralelamente, o setor avança para a chamada era Noisy Intermediate-Scale Quantum (NISQ), caracterizada por dispositivos com um número limitado de qubits e ainda suscetíveis a ruídos. O desafio já não é construir processadores maiores, mas sistemas confiáveis e fáceis de usar.

2. O sensoriamento quântico surge como a primeira grande aplicação comercial. Enquanto a computação quântica continua amadurecendo, os sensores quânticos despontam como a tecnologia com maior potencial de impacto no curto prazo. Sua extraordinária sensibilidade permitirá aprimorar a navegação sem dependência de GPS, o monitoramento de infraestruturas críticas, a exploração geológica, o diagnóstico biomédico e a observação da Terra com uma precisão sem precedentes.

3. A metrologia será um habilitador silencioso da economia digital. Os avanços em relógios atômicos ópticos e interferometria quântica estão redefinindo os padrões de medição e sincronização. Essa capacidade é essencial para redes elétricas inteligentes, telecomunicações avançadas, sistemas financeiros, navegação de precisão e futuras infraestruturas 6G, nas quais a precisão temporal será um ativo estratégico.

4. As comunicações quânticas avançam rumo a infraestruturas seguras. A distribuição quântica de chaves (QKD), as redes quânticas metropolitanas e os primeiros experimentos com repetidores quânticos estão estabelecendo as bases para uma futura Internet quântica. Embora ainda existam desafios tecnológicos relevantes, diversos países já consideram essas capacidades infraestruturas críticas para proteger comunicações governamentais, financeiras e de defesa. Sem dúvida, essa também é uma das grandes apostas da Europa para os próximos anos.

5. A criptografia pós-quântica passa da fase de pesquisa para a de planejamento. A padronização de novos algoritmos resistentes a ataques quânticos marca o início de uma transição que afetará todas as organizações. O desafio não é apenas tecnológico, mas também organizacional: identificar ativos críticos, planejar a migração e garantir a proteção de informações cujo ciclo de vida se estenda por décadas. Este é um dos pontos mais iminentes; na verdade, poderíamos dizer que deixa de ser uma “tendência” para começar a se tornar uma “moda”.

6. A inteligência artificial acelera o desenvolvimento quântico. A convergência entre IA e tecnologias quânticas constitui uma das tendências mais promissoras. A inteligência artificial já otimiza o design de materiais, o controle experimental de dispositivos quânticos e a calibração de sensores, enquanto, no médio prazo, a computação quântica poderá potencializar determinados algoritmos de otimização e machine learning.

7. A vantagem competitiva dependerá do ecossistema, não apenas da tecnologia. A competição internacional já não se limita ao desenvolvimento de hardware. Europa, Estados Unidos e China estão implementando estratégias que combinam investimento público, colaboração industrial, formação de talentos, padronização e infraestruturas de pesquisa. Para as empresas, o desafio consiste em identificar casos de uso, desenvolver capacidades internas e participar desses ecossistemas antes que a tecnologia atinja sua plena maturidade.

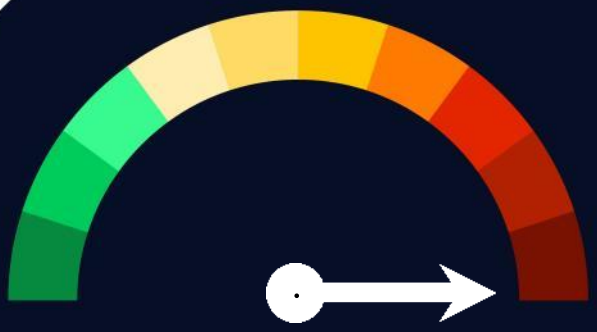
A ciência e as tecnologias quânticas deixaram de ser uma promessa distante para se tornar um elemento estratégico das políticas industriais e de inovação. Sua adoção será gradual e desigual, mas as organizações que começarem hoje a desenvolver conhecimento, alianças e capacidades estarão mais bem posicionadas para aproveitar o valor de uma revolução tecnológica que já começou.

María Gutierrez
Cybersecurity Expert

Vulnerabilidades

Google Chrome Sandbox Escape

Data: 30 de junho de 2026
CVE: CVE-2026-13782



CVSS: 10

CRÍTICA

Descrição

A CVE-2026-13782 é uma vulnerabilidade crítica causada por um erro do tipo *Use-After-Free* (CWE-416) no navegador Chrome, que permite reutilizar ou referenciar uma área da memória depois que já foi liberada.

Nesse contexto, um atacante que tenha comprometido previamente o processo de renderização pode explorar essa vulnerabilidade para escapar da *sandbox* do Chrome por meio de uma página HTML especialmente desenvolvida.

Esse tipo de vulnerabilidade é especialmente crítico, pois a *sandbox* constitui uma das principais barreiras de segurança do navegador, razão pela qual recebeu uma pontuação CVSS 10.

Solução

Recomenda-se:

- Atualizar para o Chrome 150.0.7871.47 ou posterior.
- Manter as atualizações automáticas ativadas.

Produtos afetados

- Google Chrome para Windows, Linux ou macOS anteriores à versão 150.0.7871.47.

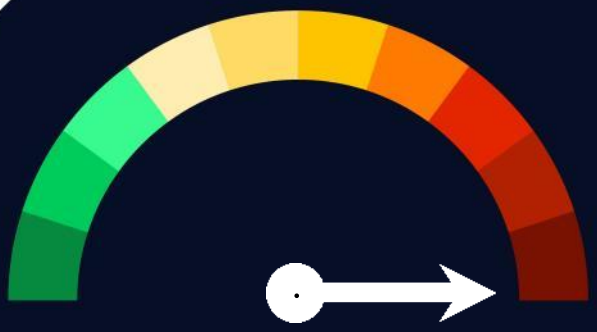
Referências

- nvd.nist.gov
- rapid7.com
- incibe.es
- cvedetails.com

Vulnerabilidades

Adobe ColdFusion Path Traversal

Data: 30 de junho de 2026
CVE: CVE-2026-48282



CVSS: 10

CRÍTICA

Descrição

O Adobe ColdFusion é afetado por uma vulnerabilidade de *path traversal* no componente *Remote Development Services (RDS)*. Essa vulnerabilidade permite que um atacante não autenticado manipule caminhos de arquivos enviados ao servidor por meio de requisições HTTP, saia dos diretórios permitidos e acesse locais arbitrários do sistema ou salve código *ColdFusion Markup Language (CFML)* malicioso em diretórios acessíveis pela aplicação web, obtendo, assim, a execução remota de código.

A causa principal está no fato de o ColdFusion não validar nem restringir adequadamente o caminho de arquivo fornecido pelo usuário em determinadas operações do serviço RDS.

Solução

Recomenda-se:

- Atualizar as versões para ColdFusion 2025 Update 10 e ColdFusion 2023 Update 21.

Produtos afetados

- ColdFusion 2025 Atualização 9 e anteriores.
- ColdFusion 2023 Atualização 20 e anteriores.

Referências

- adobe.com
- nvd.nist.gov
- sentinelone.com
- cvereports.com

Patch de segurança da BMC para vulnerabilidade crítica do Control-M/Server

Data: 01 de julho de 2026
CVE: CVE-2026-10539

Crítica

Descrição

Devido a uma validação insuficiente de comandos, a vulnerabilidade CVE-2026-10539 pode permitir que um atacante remoto não autenticado execute comandos não autorizados no servidor Control-M, possibilitando uma eventual movimentação lateral na infraestrutura.

O Control-M é uma solução de automação de cargas de trabalho *(workload automation)* utilizada por grandes empresas dos setores de telecomunicações, bancos, seguros, administração pública e indústria. Por isso, o impacto potencial dessa vulnerabilidade é elevado, pois ela pode comprometer um sistema do qual dependem diversos processos de negócio e outros sistemas.

Produtos afetados

Produtos afetados:

- Control-M/Server desde a versão 9.0.20.x até a versão 9.0.21.200 incluída.

Solução

Recomenda-se:

- Atualizar Control-M/Server para a versão 9.0.21.300 ou posterior.
- Restringir o acesso ao Control-M/Server apenas a redes confiáveis.

Referências

- incibe.es
- nvd.nist.gov
- bmcapps.my.site.com

 |

BeyondTrust corrige múltiplas vulnerabilidades no Remote Support e Privileged Remote Access.

Data: 6 de julho de 2026
CVE: CVE-2026-40138 e mais 3

Crítica

Descrição

A BeyondTrust corrigiu diversas vulnerabilidades relacionadas às soluções *BeyondTrust Remote Support (RS)* e *Privileged Remote Access (PRA)*, dois produtos utilizados para acesso remoto, suporte remoto e gestão de acessos privilegiados.

Essas vulnerabilidades permitem que um atacante não autenticado contorne controles de acesso, obtenha acesso não autorizado ao sistema ou provoque uma negação de serviço.

Além disso, uma das vulnerabilidades permitia que usuários autenticados com privilégios limitados acessassem recursos ou dados fora do escopo autorizado. O risco é especialmente relevante em ambientes nos quais essas soluções estejam expostas à rede ou à Internet.

Produtos afetados

Produtos afetados:

- BeyondTrust Remote Support (RS) versão 25.3.2 ou anteriores
- BeyondTrust Privileged Remote Access (PRA) versão 25.3.2 ou anteriores

Solução

Recomenda-se:

- Atualizar os programas para a versão 25.3.3.
- Em ambientes que não possam ser atualizados imediatamente, aplicar o *Security Rollup* de abril de 2026.

Referências

- beyondtrust.com
- thehackernews.com
- nvd.nist.gov
- cybersecuritynews.com
- csirt.telconet.net

Eventos

Black Hat USA 2026
1 - 6 de agosto

O evento de cibersegurança de maior destaque do ano retorna ao Mandalay Bay com uma programação reformulada de seis dias, criado para impulsionar a inovação, romper barreiras e reunir a comunidade global de segurança como nunca visto antes.

A edição deste ano contará com quatro dias de treinamentos imersivos conduzidos por especialistas, de 1º a 4 de agosto, seguidos pelo Summit Day, na terça-feira, 4 de agosto, e por uma conferência principal de dois dias, com briefings inovadores, demonstrações de ferramentas open source no Arsenal, um dinâmico Business Hall e diversas oportunidades de aprendizado e networking.

Link

DEF CON 34
6 – 9 de agosto

A DEF CON é a maior e mais tradicional conferência hacker do mundo, conhecida por seu modelo de “villages”, no qual comunidades de interesse organizam workshops práticos e palestras. O Car Hacking Village da DEF CON é o principal ponto de encontro para pesquisadores de segurança automotiva, com demonstrações ao vivo de hacking de veículos, competições CTF voltadas a sistemas automotivos reais e apresentações sobre as vulnerabilidades mais recentes em veículos conectados. A DEF CON é o evento em que muitas das principais descobertas em segurança automotiva são apresentadas pela primeira vez.

Link

SANS Security Awareness & Culture Summit 2026
19 – 28 de agosto

Esta é a 13ª edição do evento, voltado para profissionais das áreas de conscientização, comportamento humano e cultura de cibersegurança. O encontro busca compartilhar conhecimentos, experiências e ferramentas práticas para promover mudanças reais na cultura de segurança das organizações.

A programação inclui palestras especializadas, casos de uso, sessões práticas e workshops presenciais, com foco em como influenciar não apenas os comportamentos, mas também as atitudes e crenças dos colaboradores em relação à cibersegurança. Além disso, oferece oportunidades de networking com especialistas e outros profissionais do setor.

Como complemento, a SANS oferece cursos relacionados à liderança em cibersegurança e à gestão do risco humano, voltados ao fortalecimento de capacidades em programas de awareness, treinamento e mudança cultural. É um evento especialmente relevante para organizações que buscam evoluir de campanhas pontuais de conscientização para modelos mais maduros de Human Risk Management.

Link

Recursos

➢ Relatório de tendências e ciberameaças

O relatório da equipe de Cyber Threat Intelligence da NTT DATA apresenta uma visão atualizada das principais ameaças observadas durante o primeiro semestre de 2026, incluindo a evolução do ransomware, a atividade de agentes mal-intencionados, a exploração de vulnerabilidades, as tendências na dark web, o impacto da IA no cibercrime e os principais riscos para as organizações. Um recurso essencial para antecipar ameaças, fortalecer as capacidades de defesa e orientar a tomada de decisões em cibersegurança.

Link

➢ Cyber Frontier 2026

Publicação anual da NTT DATA que reúne perspectivas de especialistas, pesquisadores e profissionais de cibersegurança. A edição de 2026 aborda temas como a lacuna de talentos, a defesa contra violações, as ameaças de desinformação impulsionadas por IA e a preparação para as disrupções causadas pela computação quântica.

Link

➢ Verizon 2026 Data Breach

Um dos relatórios mais reconhecidos sobre violações de segurança e incidentes reais. A edição de 2026 apresenta insights para responder a ataques potencializados por IA, pressão financeira, ransomware, vulnerabilidades e riscos específicos de cada setor. Também inclui resumo executivo, infográficos e recursos por setor.

Link

NTT DATA

CLIQUE AQUI E SIGA A RADAR

Powered by the cybersecurity NTT DATA team

br.nttdata.com