Número 111 | Fevereiro 2026

NTT DATA

Radar

A revista de cibersegurança

A cibersegurança começa – e termina – nas pessoas

Por Francisco Javier García Lorente

Durante anos, a cibersegurança foi tratada como um problema eminentemente tecnológico. *Firewalls* mais robustos, ferramentas de detecção mais sofisticadas e inteligência artificial aplicada ao monitoramento de ameaças. Tudo isso é necessário. Tudo isso tem valor. Mas não é suficiente. A realidade, respaldada por dados e pela experiência, é contundente: a maioria dos incidentes de segurança ainda decorre de ações humanas. Não por má fé, mas por falta de conhecimento, excesso de confiança ou hábitos mal adquiridos.

É nesse ponto que entra um conceito essencial que muitas organizações ainda subestimam: a cultura de cibersegurança. Mais especificamente, o papel da liderança humana como motor dessa cultura.

Falar em cultura de cibersegurança não significa ter normas publicadas em um portal corporativo nem treinamentos obrigatórios que são esquecidos ao fechar a janela do navegador. Falar em cultura é falar de comportamentos recorrentes, decisões cotidianas e atitudes frente ao risco. E a cultura, queiramos ou não, é construída a partir do exemplo das lideranças.

Liderança pelo exemplo: atitudes falam mais do que palavras

As organizações não mudam apenas porque recebem um e-mail. Elas mudam quando as suas lideranças agem de forma coerente e visível. Na área de cibersegurança, isso é especialmente crítico. Um executivo que compartilha senhas "para agilizar", evita o segundo fator "porque é incômodo" ou minimiza um incidente dizendo que "não aconteceu nada" transmite uma mensagem clara para toda a organização: a segurança é secundária.

Por outro lado, uma liderança que integra a cibersegurança em suas decisões, que questiona, que se interessa, que respeita os processos e que fala abertamente sobre riscos e aprendizados gera um efeito multiplicador. Não é preciso que os líderes sejam especialistas técnicos. É preciso que tenham consciência de sua influência.

Cultura não se impõe. Se cultiva.

Um dos erros mais comuns em programas de cibersegurança é tratar os colaboradores como "o elo frágil". Essa narrativa, além de injusta, acaba sendo ineficaz. As pessoas não são o problema — são parte da solução, desde que recebam o contexto, as ferramentas e o respaldo necessários.

Aqui, novamente, a liderança é determinante. Uma liderança que estimula uma cultura do medo — do erro, da punição, de "pisar na bola" — gera silêncio. E o silêncio, em cibersegurança, é letal. Os incidentes deixam de ser reportados, os e-mails suspeitos são ignorados e os erros ficam ocultos até que seja tarde demais.

Uma liderança humana, por outro lado, normaliza o erro como parte do aprendizado, estimula a notificação antecipada e valoriza as boas práticas. Transforma os colaboradores em sensores ativos de risco — e não em usuários seguidores de normas.

Cibersegurança como valor, não como obstáculo

Outro desafio cultural importante é a percepção da cibersegurança como um obstáculo para os negócios. "Isso atrasa", "isso complica", "isso é pouco prático". Quando esse discurso ganha força, a segurança passa a ser vista como uma imposição externa.

A liderança tem a responsabilidade de reformular essa mensagem: a cibersegurança não trava o negócio — ela o protege e o torna sustentável. Não é custo; é um investimento em confiança, reputação e continuidade. Em um ambiente onde clientes, parceiros e órgãos reguladores exigem cada vez mais garantias, a segurança deixou de ser opcional.
Quando as lideranças incorporam esse posicionamento ao discurso estratégico, a organização passa a entender que trabalhar com segurança é, na verdade, trabalhar da forma certa.

Liderança humana em um ambiente digital complexo

Vivemos em um contexto de hiperconectividade, trabalho híbrido, cadeias de suprimento digitais e ameaças cada vez mais sofisticadas. Tentar controlar esse cenário apenas com tecnologia é uma ilusão perigosa. A variável humana é inevitável — e justamente por isso, precisa ser gerida com inteligência.

A liderança humana em cibersegurança exige empatia, uma comunicação clara e coerência. Isso implica adaptar as mensagens aos diferentes perfis, compreender as pressões reais do dia a dia e desenhar medidas de segurança que apoiem o usuário — em vez de colocá-lo em conflito com o sistema. A tecnologia protege e a liderança alinha.

Formação contínua não é ação pontual

Uma cultura sólida não se constrói com campanhas isoladas. Ela se constrói com continuidade. Mais uma vez, a liderança faz toda a diferença. Quando a capacitação em cibersegurança é percebida como algo estratégico, recorrente e conectado à realidade do negócio, deixa de ser uma obrigação e passa a ser uma ferramenta útil.

As lideranças devem impulsionar uma formação viva, prática e contextualizada, que evolua com as ameaças e com a própria organização. Não se trata de saber tudo — e sim de saber como reagir.

Conclusão: liderar é proteger

Falar de cultura de cibersegurança e de liderança é, acima de tudo, falar de responsabilidade.
A cibersegurança não é apenas uma questão de sistemas; é uma questão de pessoas, decisões e valores. E os valores se praticam com liderança.

As organizações que entendem isso não procuram culpados após um incidente — elas buscam aprendizado. Não confiam cegamente na tecnologia — confiam em suas equipes. Não delegam a segurança exclusivamente a um departamento — elas a integram ao seu DNA. Porque, no mundo digital de hoje, liderar também é proteger. E proteger começa pelas pessoas.

Francisco J. Garcia Lorente
Cybersecurity Project Manager

Shai-Hulud 2.0: o dia em que o malware se expandiu para toda a cadeia

Cibercrônica por Leire Cubo Arce

Encerramos o ano com um dezembro que, mais uma vez, se mostrou um dos períodos mais ativos no cenário da cibersegurança. Enquanto muitas organizações reduzem suas atividades por conta das férias e da menor disponibilidade de pessoal, os cibercriminosos aproveitam esse contexto para intensificar campanhas que exploram tanto vulnerabilidades técnicas quanto a confiança dos usuários.

Um dos acontecimentos mais relevantes do mês foi a divulgação de uma vulnerabilidade crítica no MongoDB, identificada como CVE-2025-14847 e conhecida como MongoBleed. A falha permite que invasores extraiam informações sensíveis de bancos de dados afetados sem necessidade de autenticação, o que representa um risco significativo para organizações que mantêm instâncias expostas ou mal configuradas. Pouco depois da divulgação pública, pesquisadores de segurança confirmaram tentativas de exploração ativa, reforçando a necessidade de aplicação urgente de patches e reforço nos controles de acesso a infraestruturas de dados.

O mês de dezembro também foi marcado pelo último "Patch Tuesday" do ano, com a Microsoft corrigindo mais de cinquenta vulnerabilidades em seu ecossistema. Destacam-se diversas falhas de dia zero que já estavam sendo ativamente exploradas, permitindo a execução remota de código e a elevação de privilégios. Esse cenário evidencia que plataformas empresariais amplamente utilizadas seguem sendo alvos prioritários para atacantes que buscam gerar impacto em larga escala.

Para além dos ambientes tradicionais de TI, a tecnologia operacional (OT) segue ganhando protagonismo. Ao longo do mês, a agência CISA publicou diversos avisos de segurança envolvendo sistemas de controle industrial e dispositivos médicos de fabricantes amplamente utilizados. Esses alertas destacam a crescente convergência entre TI e OT e a maior exposição das infraestruturas críticas a ameaças cibernéticas — especialmente em setores onde os ciclos de atualização são longos ou onde parar as operações representa um desafio significativo.

A atividade de *ransomware* também seguiu intensa conforme 2025 se aproximava do fim.

Os grupos cibercriminosos seguiram mirando as organizações de saúde, os órgãos públicos e os provedores de serviços, muitas vezes explorando credenciais previamente roubadas ou vulnerabilidades em *softwares* de terceiros.
Os analistas observaram que muitos desses ataques têm como base os acessos iniciais obtidos há muito tempo, o que reforça a ideia de que os atacantes operam com paciência e esperam o momento estratégico para lançar suas operações.

Ao mesmo tempo, os relatórios de ameaças publicados neste mês revelaram a magnitude da exposição de credenciais em fóruns clandestinos, com bilhões de nomes de usuário e senhas comprometidas circulando no ecossistema criminal. Essa disponibilidade massiva de credenciais alimenta ataques automatizados, como o *credential stuffing* e a tomada de controle de contas, tornando a proteção de identidades e o uso de autenticação multifator mais críticos do que nunca.

As tensões geopolíticas também se manifestaram no ciberespaço. Os relatórios divulgados no fim do ano indicaram uma atividade cibernética contínua e em larga escala contra infraestruturas críticas na região da Ásia-Pacífico, com foco especial nas instituições financeiras, nos hospitais e nos órgãos governamentais. Essas campanhas estão amplamente associadas a operações de ciberespionagem e estratégias de guerra híbrida, evidenciando como a cibersegurança está cada vez mais vinculada à estabilidade global.
As violações de dados também mantiveram impacto direto sobre os cidadãos.

A divulgação de um incidente de segurança que afetou um importante portal de saúde na Nova Zelândia expôs centenas de milhares de documentos médicos sensíveis. O episódio reacendeu o debate sobre a proteção de dados, a fiscalização regulatória e a responsabilidade dos provedores de serviços digitais na área da saúde.

Por fim, dezembro também foi um mês de reflexão para a comunidade de cibersegurança. Diversas análises publicadas na reta final de 2025 questionaram se os modelos tradicionais de segurança estão realmente preparados para enfrentar as ameaças emergentes associadas ao uso de inteligência artificial. Riscos como *prompt injection*, *model poisoning* e a automação ofensiva com base em IA estão levando as organizações a repensar o desenho e a aplicação de seus controles de segurança em um cenário cada vez mais apoiado nessas tecnologias.

Com o encerramento de 2025, dezembro deixa uma mensagem clara: as ameaças cibernéticas continuam evoluindo nos campos técnico, humano e geopolítico. Para o novo ano, a vigilância constante, a aplicação ágil de correções e a adoção de estratégias de segurança adaptativas seguirão sendo elementos essenciais para lidar com um cenário de ameaças em constante transformação.

Leire Cubo Arce
Cybersecurity Consultant

Liderança e transformação digital: do controle de colaboradores a *firewalls* humanos

Artigo por Isabel Lopez e David Contel

Durante muito tempo, a transformação digital foi compreendida basicamente como uma questão de implementação tecnológica. Alguns protagonistas eram ferramentas, *softwares*, segurança e controle. Para que a transformação digital possa gerar resultados efetivos — e a área de cibersegurança não seja exceção — ela precisa começar pelas pessoas que a executam e pela forma como são lideradas, mais do que pelos próprios sistemas. Ao longo da história, as organizações desenvolveram diferentes estilos de liderança que refletiam não apenas perfis individuais, mas também modelos sociais mais amplos — frequentemente influenciados por formas de governo e por um determinado inconsciente coletivo da sociedade.

Liderança clássica versus liderança moderna

Para comparar as características de diferentes tipos lideranças, podemos analisar dois perfis.

O que se costuma definir como liderança clássica. Historicamente, funcionou nas organizações e suas práticas partiam do princípio de uma cultura corporativa que exigia a supervisão dos colaboradores para garantir o cumprimento de metas. A premissa inicial era a desconfiança implícita, a fiscalização direta e a percepção constante do risco de negligência ou procrastinação.

Quando esse paradigma é transferido para a área de segurança da informação, ele tende a se traduzir em medidas como limitação de acessos, bloqueio de sites, monitoramento dos colaboradores via SIEM e, como consequência, adotar uma postura de blindagem da organização. A segurança é vista como custo, como uma questão puramente técnica ou disciplinar.

Na prática, esse modelo apresenta limitações relevantes. Mesmo com os sistemas protegidos, os usuários — que são os principais agentes da transformação — não desenvolvem, necessariamente, senso de responsabilidade em relação à cibersegurança. Em outras palavras, os usuários deixam de perceber que também são parte essencial da solução para evitar incidentes de segurança e contribuir para a transformação da cultura organizacional — algo indispensável para que a transformação digital seja efetiva.

Na outra ponta, temos a liderança moderna, baseada na premissa de que as pessoas podem e devem ser protagonistas da mudança. Com todas as nuances que poderíamos apontar, uma de suas premissas é que as pessoas podem e devem ser agentes ativos da mudança. Esse paradigma implica, de forma inevitável, que os colaboradores só se tornam verdadeiros protagonistas quando são devidamente capacitados.

As competências que precisam ser adquiridas seriam definidas por cada organização, orientada por suas culturas corporativas, mas de forma mais executável, a partir de suas próprias políticas. Independentemente da característica comportamental de cada organização, é possível partir do clássico binômio entre *hard skills* e *soft skills*.

Por um lado, os usuários da organização devem ser capacitados em boas práticas de segurança da informação, em políticas de segurança ou em competências mais técnicas ou específicas, de acordo com o perfil de cada pessoa.

Mas, ainda mais importantes do que os conhecimentos, são as competências pessoais, e há uma em particular que deve ser promovida pela organização em todos os seus níveis: a autonomia com responsabilidade. É fundamental que os colaboradores não apenas saibam como reagir a uma possível fraude ou incidente de segurança, mas também acreditem que são capazes de fazê-lo, que podem ajudar seus colegas e, o que é ainda mais importante, que podem propor melhorias a partir do conhecimento operacional de suas respectivas áreas para melhorar a segurança da organizaçao. Em síntese, que cada colaborador internalize que faz parte da solução.

Essa abordagem, quando aplicada na prática, conduz a um cenário positivo no qual a segurança técnica é complementada e pode, inclusive, compensar até certo ponto vulnerabilidades de segurança, graças a esse firewall humano que são os usuários capacitados.

O impulso da mudança: por que ocorre?

Embora muitas organizações estejam em processo de transformação, os motivos que levam suas lideranças a impulsionar essas mudanças podem variar consideravelmente. No campo da cibersegurança, as causas que normalmente levam a mudanças estruturais são as exigências regulatórias, os ataques sofridos pela própria organização ou por concorrentes diretos e a decisão estratégica de promover mudanças internas.

Ao longo dos últimos anos, surgiram **órgãos reguladores** que pressionam as organizações a criar sistemas de gestão da segurança da informação, como o LPIC, a NISD ou diferentes normas ISO. Essas regulações obrigam as empresas a implementar mudanças que, do ponto de vista das camadas executivas, podem ser percebidas como um custo. De qualquer forma, esse fator externo tem sido um motor para essas transformações, embora seja preciso considerar diversos aspectos.

Em espanhol, há uma expressão popular que pode ser aplicada aos cenários de cibersegurança: "quando você vê a barba do seu vizinho sendo cortada, coloque a sua de molho". O livre mercado, por natureza, leva as empresas a monitorar o que sua concorrência imediata está fazendo.

Esse acompanhamento não se limita apenas a produtos, estratégias comerciais ou sinergias de mercado; a **concorrência direta** costuma ser o espelho daquilo de que se pode vir a ser vítima em algum momento. Um ciberataque é uma realidade bastante plausível, não apenas pelas consequências operacionais, mas também por possíveis sanções dos órgãos reguladores. Na prática, isso acaba se tornando um forte elemento motivador para a mudança, ainda que com ressalvas.

No entanto, o verdadeiro fator que conduz a uma transformação é a abordagem estratégica. Em outras palavras, quando executivos e líderes das organizações passam a enxergar a gestão da segurança da informação não apenas como um investimento, mas também como uma oportunidade de gerar diferenciação, proteger a organização e servir de exemplo como marca no mercado. Esse fator motivador interno é o que realmente pode levar a mudança a todos os níveis da organização, uma vez que o comprometimento da liderança é fundamental para a eficácia de qualquer ação que se pretenda implementar.

O papel da liderança na transformação digital

As lideranças intermediárias são um elemento essencial em qualquer transformação digital, pois são elas que, de fato, colocam as mudanças em prática no dia a dia operacional.

As mesmas bases de liderança discutidas anteriormente se aplicam a esse nível hierárquico. Cabe a essas lideranças não apenas garantir o cumprimento dos objetivos operacionais, mas também influenciar diretamente a forma como eles são alcançados. Uma liderança de perfil clássico tende a gerar dependência das instruções do gestor. Já uma abordagem mais atual, na qual não apenas competências, mas também capacidade de decisão e iniciativa são delegadas aos membros da equipe, permite uma implementação mais eficaz, uma vez que esses usuários passam a se responsabilizar diretamente pela execução. Além disso, as lideranças intermediárias funcionam como um canal de amplificação das políticas e das novas iniciativas da organização, sendo muitas vezes mais eficazes do que uma área formal de comunicação.

Conclusão

A liderança evoluiu ao longo do tempo para se adaptar às novas realidades do mundo. No entanto, a forma como é exercida depende de variáveis culturais, pessoais e da experiência profissional de cada líder.

Tudo isso indica que as organizações e as equipes que hoje são conduzidas de determinada maneira tenderão a mudar no futuro. Ainda assim, independentemente do estilo adotado, não há dúvidas de que o envolvimento de todos os usuários de uma organização em um processo de transformação garante resultados mais consistentes.

Isabel Lopez
Cybersecurity Consultant

David Contel
Cybersecurity Expert Consultant

O caminho para cima e para baixo é o mesmo: cibersegurança, navegação e liderança.

Artigo por Jorge Ortí Navarro

Víctor López Barrantes, Country Manager da NTT DATA Espanha, compartilhou em uma comunicação corporativa em abril de 2025 que "uma liderança inspiradora é essencial para o nosso futuro". Nessa mesma direção, Abhijit Dubei, Presidente e CEO da NTT DATA, Inc., destacou que liderança não se resume a cargos ou funções, é sobre "assumir ativamente a responsabilidade pelo futuro que estamos construindo, estando prontos todos os dias para inspirar, apoiar e cuidar". Abhijit Dubei convida a todos a exercer a liderança, independentemente do nosso papel.

Em um mundo como o da cibersegurança, onde o surgimento de novas ameaças é constante e as certezas são poucas, as organizações precisam, mais do que nunca, de líderes capazes de oferecer direção e equilíbrio sem frear o progresso.

Num cenário de dúvidas e incertezas, especialmente no universo da cibersegurança, cabe uma pergunta: como estabelecer um modelo de liderança que impulsione uma cultura de segurança consciente, estável e, sobretudo, capaz de avançar mesmo diante de ameaças em constante evolução?

Os clássicos já nos ensinaram que o caminho para cima e para baixo é o mesmo. E foi inspirados por essa ideia que encontramos uma possível resposta num lugar improvável: a arte da navegação.

Vamos partir do início: os barcos. Segundo a RAE, a "vela" é a peça de lona ou outro material que se prende às vergas para receber o vento e impulsionar a embarcação. A "âncora" é o instrumento de ferro com ganchos, ligado a uma corrente, que se lança ao fundo do mar para manter o barco estático. Já a "quilha" é a peça que aumenta o calado da embarcação e garante mais estabilidade e melhor controle direcional.

Nesse espírito, o escritor Jesús Terrés publicou em 5 de março de 2022 o artigo "*Ser orza y no ancla*" (Seja uma quilha e não uma âncora, em tradução literal), no qual distingue três tipos de pessoas. Primeiro, a "pessoa vela": aquela que não hesita, que é puro ímpeto, que não tem medo da aventura, de passar dos limites ou até mesmo de perder de controle. Essa pessoa não se importa em começar a noite em Valência e terminá-la dançando em Berghain, em Berlim.

Uma “pessoa vela” decide por puro sentimento, sem qualquer raciocínio. É movido pela paixão, pelo inusitado, e por isso nunca impedirá que a embarcação derive — porque estar à deriva é parte da sua natureza.

Deixar-se levar por impulsos e ser incapaz de frear a tempo, acaba levando a destinos indesejados. Deixar-se levar por impulsos, sem conseguir frear a tempo, leva a encalhes inevitáveis.

Já a "pessoa âncora" é o oposto, é quem não permite avançar. Como explica Jesús, quando falamos de "pessoas âncora", falamos de peso morto, de quem está parado e impede os outros de seguir adiante. Âncoras se prendem a rochas ou fundos arenosos que imobilizam o barco. Pode até ser que, se a âncora estiver lançada enquanto sopra um vento forte, sua força acabe danificando o próprio barco, justamente porque a âncora o mantém preso.

Já a "pessoa quilha" é ao contrário. Não freia, como a âncora. Não impede a chegada a Berlim. A quilha apenas oferece estabilidade. E não no sentido de rigidez. O que é estável permite avançar, seguir em frente sem obstáculos e, ao mesmo tempo, previne possíveis danos causados pelas adversidades do tempo.

Talvez seja esse o papel da navegação e do mar possa nos ensinar. Mostrar que estabilidade é uma das maiores virtudes de uma pessoa — e, por extensão, de um líder. Pessoas que buscamos para dividir vitórias e atravessar derrotas. Porque é nessa estabilidade que encontramos calma. Ou, talvez, aquilo que todos buscamos em algum momento: uma referência.

Alguém que nos ajude a navegar em alta velocidade pelos sete mares, contra ventos e marés, sem naufragar. Sem nos perder no caos que por vezes define o mundo da cibersegurança.

A "pessoa quilha" nunca freará o crescimento, a mudança ou a evolução. Simplesmente apoia quem precisa, se importa com as necessidades do outro e, acima de tudo, oferece a segurança de que, mesmo em meio a mudanças, aventuras ou projetos impossíveis, não acabaremos isolados em uma ilha deserta ou naufragados no fundo do mar. Porque mesmo nas piores tempestades, com ventos impiedosos e ondas gigantes, chegaremos em segurança até o próximo porto.

Esse é o líder a que Abhijit Dubei se refere. Aquele capaz de oferecer a estabilidade necessária para pensar, refletir e seguir em frente. A "quilha" não é "vela", mas é o que nos permite navegar com a segurança de não virar. Uma peça discreta, muitas vezes ignorada, mas sem a qual o barco inevitavelmente permanece à deriva ou paralisado. Sustentação. Apoio constante. Discrição que impulsiona. E é esse impulso que nos permite continuar, dia após dia.

Na opinião de Jesús Terrés, como já mencionado anteriormente:

Ser uma quilha e não uma âncora; tentar fazer com que as pessoas que você ama se tornem melhores (e nunca contê-las), ser um fertilizante e não um abrigo, um caminho e não lama. Resistir (juntos) às marés, facilitar as coisas, deixar as coisas acontecerem, deixar as janelas bem abertas, saber que você está protegido, mas nunca prisioneiro, que meu mundo é sua rede, que você pode se deixar levar: esse será meu triunfo [...]. Ser sua quilha e não sua âncora.

O caminho para cima e para baixo é o mesmo. Talvez a navegação e a cibersegurança também compartilhem esse princípio. Talvez ambas precisem dos mesmos líderes. Da mesma estabilidade. Sejamos, então, quilhas que sustentam o ambiente onde trabalhamos todos os dias — e do qual possamos sentir orgulho de fazer parte.

Jorge Ortí Navarro
Cybersecurity Expert Consultant

Tendências-chave de cibersegurança em 2026

Tendências por Diego Turiegano de las Heras

Em 2026, a cibersegurança será marcada por uma mudança clara na forma como os ataques digitais são realizados e defendidos. O avanço da inteligência artificial generativa (GenAI), o uso cada vez mais realista de *deepfakes* e a automação do crime cibernético tornarão o cenário mais complexo e difícil de controlar. As ameaças deixarão de depender tanto de conhecimentos técnicos avançados e passarão a contar com ferramentas cada vez mais acessíveis, que permitem lançar ataques sofisticados com pouco esforço. Isso obrigará empresas e usuários a repensarem como se protegem em um ambiente onde o digital faz parte de quase todas as atividades cotidianas.

A inteligência artificial terá um papel-chave e contraditório. Por um lado, ajudará a aprimorar a cibersegurança, permitindo detectar ameaças com mais rapidez, analisar grandes volumes de dados e apoiar as equipes de segurança na tomada de decisões.

Por outro, será uma ferramenta poderosa nas mãos dos invasores, que a utilizarão para automatizar tarefas, criar mensagens mais convincentes e adaptar os ataques a cada vítima. Esse uso ambíguo da IA reduzirá ainda mais a linha que separa ataque e defesa, ampliando os riscos.

Um dos aspectos mais preocupantes será o uso de *deepfakes* como ferramenta de fraude. Em 2026, esses conteúdos falsos deixarão de ser pontuais e passarão a ser utilizados com frequência para falsificar identidades e enganar tanto pessoas quanto organizações.

As falsificações de voz, em especial, serão cada vez mais realistas e fáceis de criar, o que facilitará golpes direcionados, como chamadas falsas em nome de executivos ou colegas de trabalho. Além disso, a ausência de sistemas confiáveis para identificar conteúdo gerado por inteligência artificial dificultará ainda mais a detecção dessas fraudes.

Também começarão a ganhar relevância os *deepfakes* em tempo real, capazes de alterar imagem ou voz durante uma videochamada. Embora hoje ainda exijam certa complexidade técnica, sua evolução constante permitirá seu uso em ataques mais diretos, especialmente em ambientes profissionais onde há um alto nível de confiança na comunicação por vídeo ou voz.

Isso colocará em xeque os métodos tradicionais de verificação baseados simplesmente em "reconhecer" a pessoa do outro lado da tela. A automação do cibercrime será outra das grandes transformações.

Em 2026, a inteligência artificial será usada em todas as fases de um ataque: desde a criação de *malware* até a busca por vulnerabilidades ou a distribuição de *software* malicioso.

Isso permitirá ataques mais rápidos e em maior escala, reduzindo o tempo de reação das equipes de segurança.

Além disso, o uso de modelos de IA de código aberto, com menos mecanismos de controle, facilitará que essas tecnologias sejam aplicadas tanto para fins legítimos quanto ilícitos, dificultando a análise e a atribuição dos ataques.

Apesar de todos esses avanços tecnológicos, o fator humano continuará sendo um dos principais pontos vulneráveis.

O roubo de credenciais seguirá como uma das formas mais eficazes de acessar sistemas, sobretudo porque muitas pessoas ainda utilizam senhas fracas, repetem senhas em diferentes serviços ou deixam de ativar a autenticação multifator.

Os invasores explorarão esse cenário com técnicas de engenharia social cada vez mais sofisticadas, projetadas para enganar o usuário e levá-lo a executar ações aparentemente legítimas.

O *ransomware* também não desaparecerá. Ao contrário, será mais frequente e mais veloz em 2026. Modelos de ataque como serviço permitirão que pessoas com pouco conhecimento técnico lancem ofensivas complexas utilizando ferramentas prontas para uso.

A inteligência artificial contribuirá para automatizar processos como criptografia de dados, exfiltração de informações e até negociação de resgates, reduzindo o tempo de resposta das vítimas e aumentando o impacto dos ataques.

Por fim, a adoção massiva de inteligência artificial nas empresas trará novos riscos associados à cadeia de suprimentos digital.

Muitas soluções serão implementadas sem a devida análise de segurança, incorporando dependências e possíveis vulnerabilidades. Ao mesmo tempo, o uso malicioso da IA continuará crescendo, com campanhas de *phishing* mais personalizadas, *bots* mais eficazes para fraudes e os primeiros casos de *malware* gerado com apoio dessas tecnologias.

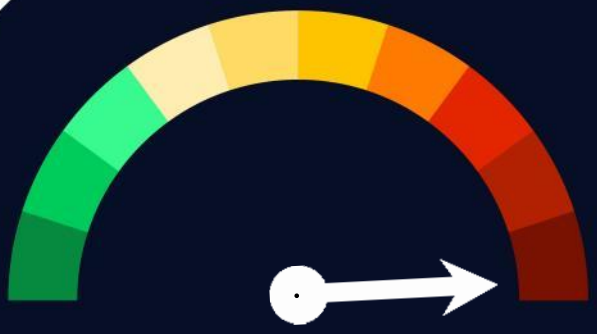
Nesse contexto, o grande desafio de 2026 será encontrar um equilíbrio entre aproveitar os benefícios da inteligência artificial e controlar os riscos inerentes, apostando em prevenção, capacitação e uma gestão de riscos mais consciente.

Diego Turiegano de las Heras
Cybersecurity Consultant

Vulnerabilidades

Vulnerabilidade crítica no n8n

Data: 26 de dezembro de 2025
CVE: CVE-2025-68668



CVSS: 9.9

CRÍTICA

Descrição

Foi detectada a vulnerabilidade crítica **CVE-2025-68668** no n8n, uma plataforma de automação de fluxos de trabalho de código aberto.

Essa vulnerabilidade permite a usuários autenticados executar comandos arbitrários no sistema subjacente. A falha se deve a um problema nos mecanismos de proteção dentro do *Python Code Node*, o que possibilita sair do ambiente restrito e executar código com os mesmos privilégios que o processo do n8n.

Embora requeira autenticação e permissões para criar ou modificar fluxos, considera-se um risco elevado pela possibilidade de execução de comandos no *host*.

Solução

Recomenda-se atualizar imediatamente para versões com patches oficiais do n8n:

- Versão 2.0.0 ou superior.

Como mitigação temporária, recomenda-se:

- Desabilitar o *Code Node* por meio da variável NODES_EXCLUDE: ["n8n-nodes-base.code"].
- Desativar o suporte a Python no nó com N8N_PYTHON_ENABLED=false.

Produtos afetados

As versões vulneráveis são:

- Da versão 1.0.0 até as anteriores à versão 2.0.0.

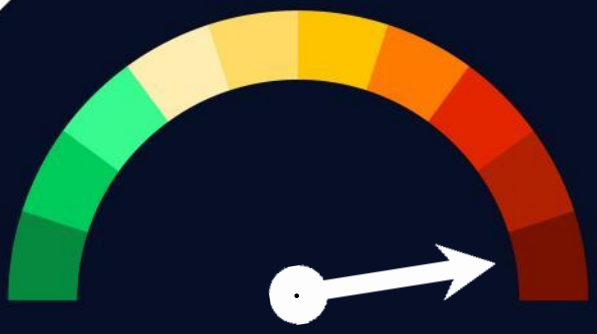
Referências

- nvd.nist.gov
- thehackernews.com

Vulnerabilidades

Vulnerabilidade crítica em roteadores D-Link DSL

Data: 5 de janeiro de 2026
CVE: CVE-2026-0625



CVSS: 9.3

CRÍTICA

Descrição

Foi identificada uma vulnerabilidade crítica (CVE-2026-0625) de execução remota de código que afeta vários roteadores D-Link DSL antigos e já fora de linha (sem suporte).

A falha se deve a uma injeção de comandos no *endpoint* de configuração DNS (dnscfg.cgi), que permite a um invasor remoto e não autenticado executar comandos com privilégios de sistema.

Essa vulnerabilidade está sendo explorada ativamente e pode resultar em controle total do roteador, sequestro de DNS, espionagem de tráfego ou integração a *botnets*.

Solução

Não existe atualização oficial para a maioria dos modelos afetados.

Recomenda-se:

- Substituir os dispositivos vulneráveis.
- Desabilitar a administração remota.
- Restringir acessos via firewall/ACL.

Produtos afetados

Roteadores D-Link DSL (modelos EoL), incluindo:

- DSL-2640B
- DSL-2740R
- DSL-2780B
- DSL-526B

Referências

- incibe.es
- thehackernews.com

IBM corrige vulnerabilidade crítica de omissão de autenticação

Data: 31 de dezembro de 2025
CVE: CVE-2025-13915

Crítica

Descrição

A IBM publicou atualizações de segurança para o API Connect com o objetivo de corrigir a vulnerabilidade crítica de omissão de autenticação identificada como **CVE-2025-13915**, com pontuação CVSS de 9.8.

A falha de segurança pode permitir que um invasor remoto acesse serviços protegidos sem a necessidade de credenciais válidas, comprometendo a confidencialidade e integridade das APIs gerenciadas pela plataforma.

A IBM indicou que a vulnerabilidade pode ser explorada remotamente e sem interação do usuário, o que aumenta significativamente o risco para ambientes empresariais expostos à internet. Por isso, recomenda-se aplicar as atualizações de segurança o quanto antes.

Produtos afetados

As versões vulneráveis do IBM API Connect são:

- Versões de 10.0.8.0 a 10.0.8.5
- Versão 10.0.11.0

Solução

Recomenda-se:

- Aplicar imediatamente os patches e correções disponibilizados pela IBM (baixar e instalar a atualização disponível para o API Connect via Fix Central conforme a versão afetada)

Referências

- thehackernews.com
- incibe.es

OWASP Core Rule Set corrige vulnerabilidade crítica de bypass de segurança

Data: 7 de janeiro de 2026
CVE: CVE-2026-21876

Crítica

Descrição

Foi identificada uma vulnerabilidade crítica no OWASP *Core Rule Set (CRS)*, o conjunto de regras mais utilizado em Web Application Firewalls (WAF), como o ModSecurity.

A falha está no processamento de requisições *multipart*, o que permite que um invasor contorne as regras de segurança por meio de requisições especialmente manipuladas. Essa evasão pode permitir que cargas maliciosas (como injeções SQL, XSS ou outros ataques web) não sejam detectadas nem bloqueadas pelo WAF.

Embora não provoque diretamente a execução de código, a vulnerabilidade reduz significativamente a capacidade defensiva do WAF, facilitando ataques de alto impacto contra aplicações web protegidas.

Produtos afetados

Os produtos afetados por esta vulnerabilidade incluem:

- OWASP Core Rule Set (CRS)
- Versões anteriores à 4.22.0 (ramo 4.x)
- Versões anteriores à 3.3.8 (ramo 3.x)

Qualquer WAF que integre essas versões do CRS.

Solução

Recomenda-se:

- Atualizar para o OWASP CRS versão 4.22.0 ou superior (ramo 4.x)
- Atualizar para o OWASP CRS versão 3.3.8 ou superior (ramo 3.x)

Referências

- cvedetails.com
- secalerts.co

TLP:WHITE

Eventos

Cyber Security & Cloud Expo Global 2026
4 e 5 de fevereiro

Evento internacional de referência que reúne líderes tecnológicos, CISOs, arquitetos de cloud e responsáveis por inovação para analisar as grandes tendências em cibersegurança e cloud computing. O congresso tem foco em ameaças emergentes, segurança em ambientes híbridos e *multicloud*, Zero Trust, IA aplicada à defesa, conformidade regulatória e resiliência digital, com palestras estratégicas, casos reais e uma ampla área de exposição com os principais fornecedores do setor.

Link

h-c0n : Hackplayers' Hacking Conference
6 e 7 de fevereiro

h-c0n é uma conferência técnica de cibersegurança com ADN *hacker*, centrada em investigação avançada, *hacking* ético, *reverse engineering*, *red teaming*, *blue teaming* e segurança ofensiva e defensiva. Destaque para a abordagem prática, palestras profundas sem marketing, *workshops* técnicos e uma comunidade altamente especializada, voltada para profissionais da área de cibersegurança – com mentalidade *hands-on* e espírito de aprendizado contínuo.

Link

EspañaSec Cyber Summit 2026
10 e 11 de fevereiro

O EspañaSec Cyber Summit é um congresso de alto nível orientado à visão estratégica da cibersegurança, dirigido a executivos, CISOs e responsáveis por risco, tecnologia e conformidade. A abordagem posiciona a segurança como habilitadora do negócio, com temas como governança, gestão de risco, regulação, ciberresiliência, impacto da IA e tomada de decisões em ambientes complexos, com palestrantes de alto nível e ênfase em liderança e estratégia.

Link

Ondata Congress – Informática Forense e Ciberinteligência
18 de fevereiro

O Ondata é um congresso consolidado na área de forense computacional e inteligência cibernética, destinado a profissionais técnicos, forças de segurança, analistas e especialistas em investigação digital. O evento explora a análise forense, a resposta a incidentes, a investigação de crimes cibernéticos, a OSINT e a inteligência contra ameaças, combinando exigência técnica, casos reais e uma abordagem muito prática que o torna uma referência nacional nessas disciplinas.

Link

Recursos

➢ *Checklist* de melhores práticas

Lista atualizada de ações de cibersegurança com foco operacional: controles de identidade, atualizações críticas, *backups* verificados, *vendor controls*... ideal como *checklist* para inspeções rápidas ou auditorias internas.

Link

➢ Global Cybersecurity Outlook 2025 – Fórum Econômico Mundial (WEF)

Relatório estratégico e global que examina como a cibersegurança está evoluindo frente a tecnologias emergentes, tensões geopolíticas e desafios de resiliência. Fornece dados-chave sobre riscos relacionados à dependência de cadeias de suprimentos, sofisticação de ataques e disparidades entre organizações, com recomendações para líderes que enfrentam esse cenário em constante evolução.

Link

➢ GCA Cybersecurity Toolkit (Global Cyber Alliance)

Kit de ferramentas e guias práticos para avaliar a postura de segurança, reforçar controles comuns e acessar soluções gratuitas com foco em defesas básicas amplamente recomendadas.

Link

Inscreva-se na RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

br.nttdata.com