Número 95 | outubro de 2024

NTT DATA

Radar

A revista de cibersegurança

Da cibersegurança à resiliência cibernética

Por María Pilar Torres Bruna

Os profissionais que atuam na área da cibersegurança podem testemunhar como a frequência e a sofisticação dos ataques cibernéticos estão aumentando, levando muitas organizações a aceitar a possibilidade de serem alvos de invasores cibernéticos, que poderão ter êxito em seus ataques. Por isso, é essencial que as empresas não só atuem na prevenção desses incidentes, mas também desenvolvam estratégias eficazes para gerenciá-los, visando minimizar seu impacto na operação e nos clientes finais.

Manter a execução dos processos críticos de uma organização durante um ataque cibernético é o principal objetivo da resiliência cibernética; para alcançá-lo, é necessário pôr em prática uma série de processos, procedimentos e tecnologias concebidos para defender as operações críticas enquanto um ataque ocorre — o que pode durar várias semanas — e continuar a fornecer o serviço durante a regularização das atividades.

Não raro, a resiliência cibernética e a cibersegurança são confundidas e, embora sejam abordagens diferentes, são domínios complementares. A cibersegurança se dedica à proteção e detecção, ou seja, seu foco principal precede os ataques; já a resiliência cibernética prepara as organizações para enfrentar e se recuperar de um ataque através da criação de planos de contingência eficazes, e de uma cultura organizacional que capacite os funcionários a realizar seus trabalhos sem depender de determinados sistemas ou ferramentas habituais.

A preparação da equipe é essencial em qualquer plano de resiliência cibernética. Enquanto o treinamento em cibersegurança visa habilitar os funcionários a identificar potenciais ameaças e adotar comportamentos preventivos, a capacitação em resiliência cibernética gira em torno da resposta aos incidentes, permitindo a continuidade do trabalho sem o uso dos sistemas comprometidos. Como faço para atender os clientes de um banco durante um ataque? Como posso continuar a vender os meus produtos? Como posso continuar a emitir cartões de embarque?

E as organizações precisam estar atentas à sua postura de resiliência cibernética, que precisa melhorar a cada ano. Diante de ataques cibernéticos cada vez mais sofisticados e comuns, apenas uma empresa com resiliência cibernética é capaz de mitigar os prejuízos econômicos, reduzir o investimento necessário para a recuperação, bem como os custos relacionados a punições e litígios. Além disso, se torna capaz de minimizar danos a terceiros, preservar sua reputação e manter a capacidade competitiva, o que a habilita para a liderança no futuro.

Dada a importância da resiliência cibernética no futuro, decidimos dedicar o RADAR deste mês a este tópico.

María Pilar Torres Bruna
Diretora de Cibersegurança

A segurança digital sob ataque

Cibercrónica por Yeiber Basilio Caso Ramirez

Recentemente, o mundo da cibersegurança testemunhou vários incidentes substanciais. De ataques cibernéticos a grandes bancos e empresas de e-commerce a vulnerabilidades críticas em sistemas ferroviários e de dispositivos móveis, a segurança digital continua sendo um desafio constante. A seguir, retrataremos as notícias de maior destaque do mês.

Em especial, temos o caso do ataque cibernético sofrido pelo JPMorgan Chase, que explorou uma vulnerabilidade de dia zero, e permitiu aos invasores desviar grandes somas de dinheiro e comprometer os dados dos clientes, causando danos significativos à reputação do banco.

Nesse meio tempo, a Amazon passou por uma violação massiva de dados. Os cibercriminosos roubaram as informações pessoais e os dados de cartão de crédito de milhões de clientes para vazá-los na dark web. Isso resultou em inúmeros casos de roubo de identidade e transações não autorizadas.

Um grupo de investigadores demonstrou como explorar vulnerabilidades no sistema ferroviário da Renfe, permitindo que atores mal-intencionados enviem ordens aos trens, e até interromper suas atividades. Esta descoberta sublinha a necessidade premente de reforçar a segurança em infraestruturas críticas.

No campo dos dispositivos móveis, foi descoberta uma vulnerabilidade nas bandas base dos dispositivos móveis 5G fabricados pela Samsung, MediaTek e Qualcomm. Tal falha abriria margem para a espionagem dos usuários da rede por eventuais invasores. Tendo isso em vista, no entanto, os fabricantes implementaram as correções necessárias para mitigar a ameaça. Uma vulnerabilidade de dia zero também foi descoberta no aplicativo de mensagens Telegram para Android, apelidado de "EvilVideo", que permitiria a eventuais invasores enviar arquivos APK maliciosos disfarçados de vídeos, comprometendo os dispositivos dos usuários.

Um dos episódios mais alarmantes envolveu a exploração de vulnerabilidades de dia zero da “Versa Director”, posta em prática pelo grupo chinês APT Volt Typhoon. O ataque foi direcionado à infraestrutura crítica da internet nos Estados Unidos, na qual várias organizações deixaram de implementar medidas de segurança adequadas, o que levou à exposição de portas de gerenciamento cruciais. Esse incidente sublinha a urgência em aprimorar práticas de cibersegurança, em especial no caso de infraestruturas que servem de base para serviços essenciais.

Paralelamente, foi relatada uma das maiores violações de dados da história recente, que afetou 3 bilhões de pessoas. O evento destacou a vulnerabilidade das empresas dedicadas à agregação de dados, que, quando comprometidas, expõem as informações de milhões de usuários. A multinacional Toyota foi outra vítima de uma violação de dados, com o vazamento de 240 GB de informações de funcionários e clientes, embora o ataque tenha se originado em um provedor externo.

Além desses casos, houve um ataque de ransomware que afetou 200 empresas nos Estados Unidos, incluindo a Kaseya. Os sistemas foram hackeados por cibercriminosos, que exigiram um resgate para desbloqueá-los, causando interrupções significativas nas operações das empresas afetadas.

Na Europa, a Espanha não ficou de fora dessa onda de ataques cibernéticos. Várias empresas espanholas do setor financeiro e de energia relataram incidentes importantes, em especial, ataques de ransomware que paralisaram temporariamente suas operações.

Os invasores usaram variantes avançadas de ransomware que criptografavam dados críticos e exigiam pagamentos com criptomoedas, o que dificultou a recuperação dos sistemas afetados.

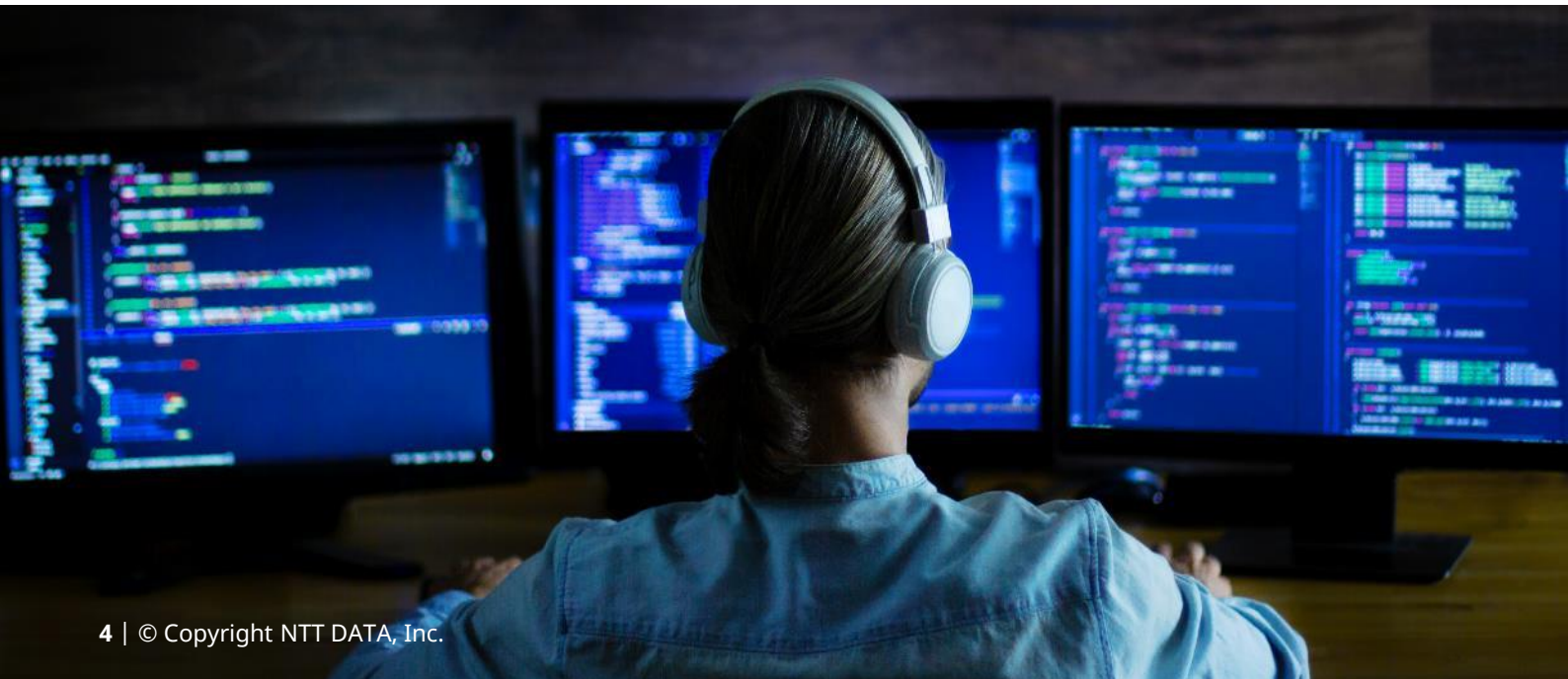
Na América Latina, o Chile sofreu um ataque significativo à sua infraestrutura energética. Um grupo de ransomware, que recentemente adotou o novo nome de APT INC, lançou um ataque que comprometeu os servidores VMware ESXi, amplamente utilizados em sistemas críticos. Esse grupo é conhecido por sua sofisticação e por usar ferramentas avançadas de criptografia, o que complicou as respostas das vítimas.

Na área de infraestrutura crítica, o Aeroporto SeaTac e vários portos marítimos em Seattle sofreram interrupções operacionais devido a ciberataques que forçaram a utilização de processos manuais, afetando gravemente a logística e o transporte. Esses ataques ressaltam a vulnerabilidade de setores que dependem de sistemas digitais interconectados.

Em todo o mundo, houve um aumento substancial nas vulnerabilidades relacionadas ao escalonamento de privilégios. Em um relatório de segurança recente, 36 dessas vulnerabilidades foram identificadas, destacando a crescente tendência dos invasores de explorar tais falhas para obter controle total sobre os sistemas comprometidos. Nesse sentido, os incidentes destacam a importância crítica de manter os sistemas atualizados e aplicar patches de segurança com a maior agilidade possível.

Podemos dizer, em síntese, que o período foi marcado por uma série de ciberataques que afetaram não apenas empresas tomadas individualmente, mas também colocaram em risco infraestruturas críticas e a segurança nacional de diversos países. A evolução dessas ameaças exige uma resposta coordenada e eficaz, tanto em nível governamental como corporativo, para mitigar os riscos e proteger as informações e os ativos mais valiosos da sociedade global.

Yeiber Basilio Caso Ramirez
Gerente Técnico



Caminho para a resiliência cibernética

Por Alberto Faus Avila

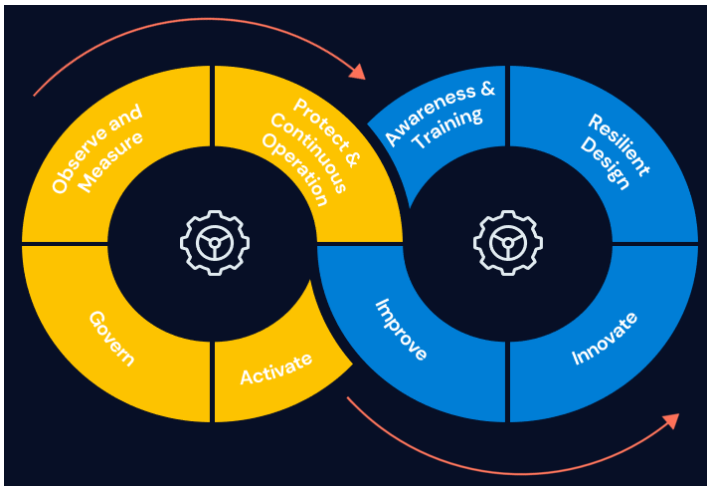
Se a interrupção da CrowdStrike em julho passado nos ensinou alguma coisa, é que estamos muito mais vulneráveis do que pensávamos a incidentes relacionados à tecnologia. A necessidade que se impõe é de uma melhor preparação para eventualidades desse tipo, para evitar seu impacto, ou seja, precisamos desenvolver mais nossa resiliência cibernética.

A resiliência cibernética deve ser definida nos termos acima e não como um mero *Plano de Recuperação de Desastres*, nem confundida com a cibersegurança. Ela não se trata de um produto que pode ser adquirido e que faça nossa empresa ter resiliência cibernética em um passe de mágica.

A resiliência cibernética é a capacidade de uma organização de continuar produzindo os resultados esperados, apesar de qualquer situação adversa relacionada à tecnologia. Ela nos prepara para responder, recuperar e nos adaptar a esses eventos, garantindo a proteção e a recuperação de nossos sistemas de informação, bem como o planejamento e preparação anterior às ocorrências.

Por esse motivo, é importante incorporar a resiliência cibernética em nossas organizações e, para isso, devemos ter um roteiro claro que inclua as seguintes etapas:

- **Nível de maturidade atual:** o caminho para a resiliência cibernética começa por saber em que ponto todas as áreas de TI estão, não apenas em nível de cibersegurança; é assim que poderemos analisar elementos como a governança de TI, processos de segurança, redes e sistemas, nível de treinamento e *conscientização* do nosso pessoal, identificar o nível de preparação para a resiliência cibernética dos líderes das nossas empresas, identificar *ativos* críticos, documentação, gerenciamento de riscos, capacidade de operação contínua, observabilidade etc. Todos esses elementos, entre outros, devem ser objeto de uma atenta *análise* para saber qual é o nosso ponto de partida, o que nos possibilitará entender qual o caminho que devemos seguir para alcançar nosso objetivo.
- **Estratégia:** tendo em mãos os resultados desta *análise*, uma estratégia coletiva e de longo prazo deve ser o próximo passo, essencial para o sucesso. É fundamental ter uma visão holística da resiliência cibernética e um forte compromisso das organizações, mas não apenas delas. Hoje, a colaboração com terceiros é fundamental em nossos ecossistemas e devemos levá-la em consideração. Devemos dar um passo à frente e passar dos benefícios de curto prazo da segurança individual para a visão de longo prazo da Resiliência Coletiva, que precisa de uma abordagem estratégica passo a passo. Devemos conhecer bem e mapear nossos ecossistemas de TI e suas relações de dependência. Essa compreensão e o discernimento sobre os riscos nos dará uma visão clara dos objetivos que devemos priorizar.
- **Dar o primeiro passo:** assim que estivermos a par do nosso estado atual, do objetivo e estratégia a ser seguida, devemos começar a solucionar nossas deficiências por meio de projetos direcionados aos pontos mais críticos em qualquer uma das áreas analisadas. O que é importante entender é que definir, desenvolver e melhorar nosso ecossistema de TI, com o desenvolvimento da resiliência cibernética, não é uma estratégia de curto prazo, pois requer uma liderança forte com uma visão de longo prazo e a capacidade de colaborar com indivíduos e grupos dentro de nossa organização.
- **Ciclo contínuo:** a resiliência cibernética não é uma atividade delimitada no tempo, ela requer uma mudança cultural e uma série de atividades cíclicas que não podem ser negligenciadas, e que exigem constante revisão, melhoria, evolução e inovação.



Nossas organizações devem migrar da cibersegurança para a resiliência cibernética como o próximo passo na evolução para obter um impacto zero no próximo desafio que o mundo tecnológico nos reserva no futuro. Hoje, a questão não é se esse cenário irá se instalar, mas sim quando.

Alberto Faus Avila
Gerente

Resiliência cibernética regulatória: um pilar fundamental para a segurança digital

Por Melanie Brenis Valencia

Hoje, o crescente avanço tecnológico transformou a maneira como as organizações operam, pois seus processos estão cada vez mais digitalizados. No entanto, é inegável que essa transformação também gerou um aumento significativo nos riscos cibernéticos a que estão expostas. E é aí que entra um conceito-chave: a resiliência cibernética.

Garantir a resiliência cibernética não significa apenas que as organizações estejam preparadas para prevenir ataques cibernéticos, mas, acima de tudo, que estejam capacitadas para uma recuperação rápida de eventuais ataques, com a manutenção da continuidade operacional.

Para que seja possível, a regulamentação torna-se essencial, pois permite o estabelecimento de padrões comuns que fortalecem a segurança das organizações. Sem regulamentos claros, a resiliência cibernética pode ser comprometida, afetando tanto as empresas quanto os clientes finais.

Nesse sentido, a União Europeia (UE) tomou a frente no desenvolvimento de marcos regulatórios para a resiliência cibernética, com destaque para o Regulamento da UE 2022/2554, a Lei de Resiliência Operacional Digital (ou DORA, sua sigla original em inglês), e o projeto de Leia da Resiliência Cibernética (ou CRA, sua sigla original em inglês). Ambas as estruturas visam estabelecer diretrizes claras para reforçar a capacidade de resiliência cibernética das organizações, cada uma focada em diferentes áreas.

- **Regulamento da UE 2022/2254, Lei de Resiliência Operacional Digital**

A Lei de Resiliência Operacional Digital (DORA) foi publicada oficialmente no Jornal Oficial da UE em 27 de dezembro de 2022 e entrará em vigor em 17 de janeiro de 2025. Este regulamento destina-se especificamente a entidades do setor financeiro, incluindo bancos, seguradoras, prestadores de serviços de pagamento e outros atores-chave no ecossistema financeiro. Seu principal objetivo é garantir que essas entidades possam resistir, se recuperar e continuar operando com segurança diante de qualquer tipo de incidente e/ou ataque cibernético.

As principais disposições que a DORA estabelece para as instituições financeiras giram em torno de:

✓ **Gestão de riscos de TIC:** as organizações devem contar com um órgão de governança na vanguarda da gestão de riscos de TIC e implementar estruturas robustas para proteger de forma adequada e eficaz suas infraestruturas físicas e garantir a resiliência digital.

- ✓ **Teste de resiliência operacional digital:** as organizações devem realizar testes periódicos para verificar sua preparação e garantir a detecção de deficiências ou brechas.

- ✓ **Incidentes relacionados às TIC:** as organizações devem acompanhar e registrar os incidentes aos quais foram expostas, além de relatar incidentes graves relacionados às TIC às autoridades competentes.

- ✓ **Gerenciar riscos de terceiros relacionados às TIC:** as organizações devem garantir que seus provedores de serviços de TIC também cumpram os padrões de segurança estabelecidos, legal e tecnicamente.

- ✓ **Acordos de Compartilhamento de Informações:** as organizações podem estabelecer acordos para o intercâmbio de inteligência sobre ameaças cibernéticas com colegas, parceiros estratégicos etc.

❑ Projeto da Lei de Resiliência Cibernética

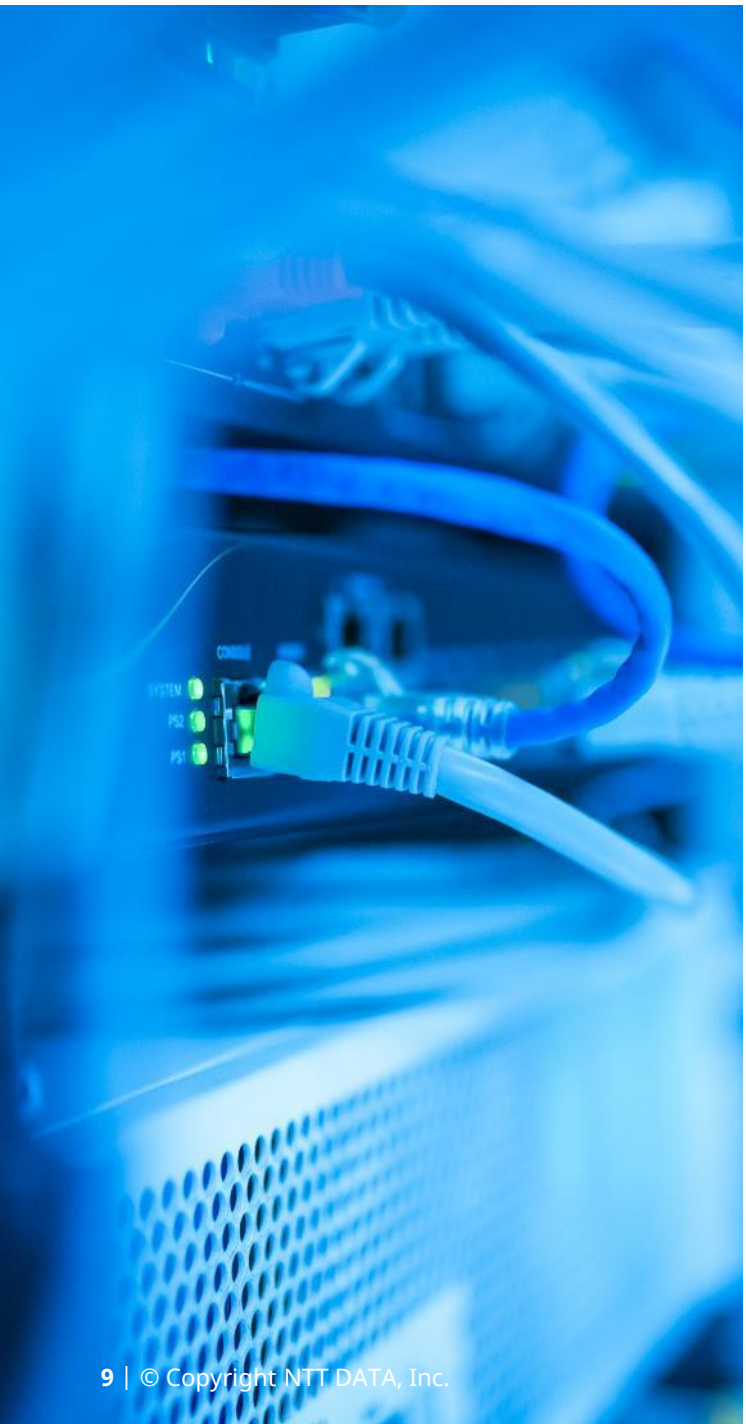
A Lei de resiliência cibernética (CRA) é um projeto regulatório da União Europeia que foi apresentado em setembro de 2022. Embora ainda não tenha sido adotado oficialmente, sua entrada em vigor está prevista para ocorrer até o final de 2024. Ao contrário da DORA, a CRA adota uma abordagem mais ampla, que inclui a segurança de produtos digitais, como dispositivos inteligentes, softwares e aplicativos, a fim de reduzir as vulnerabilidades desde sua concepção.

As principais disposições que a CRA estabelece são:

- ✓ **Security by Design:** as organizações devem garantir que seus produtos tenham uma configuração padrão segura, reduzindo as vulnerabilidades exploráveis.

- ✓ **Atualizações de segurança:** as organizações devem garantir que as vulnerabilidades em seus produtos possam ser resolvidas por meio de atualizações de segurança (incluindo atualizações automáticas).

- ✓ **Dados pessoais:** as organizações devem garantir que seus produtos protejam a confidencialidade e a integridade dos dados pessoais processados, por exemplo, criptografando dados em repouso ou em trânsito.



- ✓ **Disponibilidade de recursos:** as organizações devem garantir que seus produtos protejam a disponibilidade de recursos críticos, incluindo a resiliência e mitigação dos efeitos de ataques de negação de serviço.

Como podemos ver, a resiliência cibernética regulatória representa um passo fundamental para a criação de um ambiente digital mais seguro e resiliente às ameaças cibernéticas. Regulamentos como a DORA e o projeto de CRA não apenas estabelecem obrigações claras para setores-chave, mas marcam uma mudança em direção a uma maior responsabilidade pela segurança digital.

À medida que as organizações se preparam para atender a essas estruturas, o foco na resiliência cibernética vem se tornando um elemento essencial para a estabilidade econômica e operacional em um mundo cada vez mais interconectado.

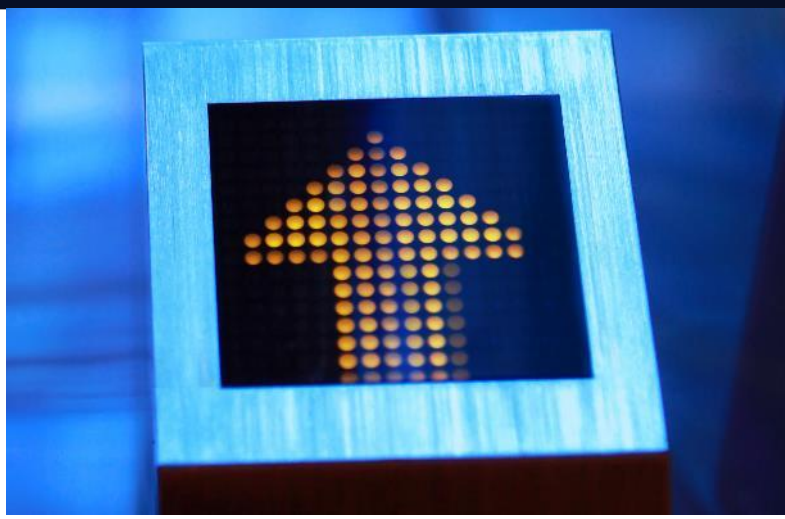
Melanie Brenis Valencia
Consultora Sênior de Cibersegurança

Auto Coding Agent

Tendências por Alberto Faus Avila

Auto Coding Agent (Agente de Codificação Automática)

Nas equipes de desenvolvimento, estima-se que pelo menos um quarto das equipes passe o dia dedicada ao aprimoramento de códigos. Isso significa que todo esse esforço é voltado para corrigir, não agregar valor ao negócio.



Quando há um incidente, muito tempo é gasto recuperando aplicativos quando, em muitos casos, as ações necessárias são conhecidas e tudo o que é necessário é que as próximas etapas sejam avaliadas e executadas.

Também vale ressaltar que são empreendidos grandes esforços para revisar e melhorar a aplicação, como parte da melhoria contínua. Mas, muitas vezes, o foco da revisão de logs e verificação de erros é perdido.

A solução da NTT Data para esse problema é o Auto Coding Agent, uma solução inteligente que é responsável pela autorremediação e autoevolução:

- O agente verifica os logs do aplicativo em tempo real. Com base no conhecimento gerado, ele analisa se há erros ou alertas sobre a plataforma ou o próprio aplicativo.
- Em incidentes da plataforma, ela analisa as soluções que foram bem-sucedidas anteriormente e toma a melhor decisão possível, executando comandos para restaurar a plataforma ao seu estado ideal.
- Em um primeiro estágio, o agente é capaz de analisar os incidentes e inserir o código ideal, para análise por um líder técnico antes de ser executado. Em um futuro próximo, a intervenção humana não será necessária se não for desejada, entrando numa fase totalmente automatizada.

O Auto Coding Agent é o futuro do suporte a aplicativos e será uma alavanca muito importante para a eficiência operacional e o aumento da qualidade de nossos serviços de desenvolvimento de aplicativos.

Alberto Faus Avila
Gerente

Vulnerabilidades

Vulnerabilidade crítica no FileCatalyst Workflow

Data: 27 de agosto de 2024
CVE: CVE-2024-6633

CVSS: 9,8

CRÍTICA

Descrição

A vulnerabilidade crítica CVE-2024-6633 no software FileCatalyst Workflow da Fortra se origina da publicação das credenciais padrão para o HSQL Configuration Database (HSQLDB) em um artigo do fornecedor.

A empresa de soluções de cibersegurança Fortra observa que o HSQLDB é obsoleto e não se destina ao uso em produção, embora ainda esteja incluído no FileCatalyst Workflow.

A vulnerabilidade permitiria que um invasor com acesso à rede e capacidade de varredura de portas obtivesse acesso remoto ao banco de dados usando as credenciais padrão, sendo capaz de manipular e/ou exfiltrar dados, bem como criar usuários administrativos.

Solução

A Fortra resolveu a vulnerabilidade limitando o acesso ao banco de dados HSQLDB apenas ao localhost.

A empresa recomenda não usar o banco de dados HSQL incluído e ressalta que a vulnerabilidade só pode ser explorada se o invasor tiver acesso à rede, realizar varredura de porta e se a porta HSQLDB estiver exposta à internet.

Os patches são incluídos a partir do build 156 do FileCatalyst Workflow versão 5.1.7, que também resolve uma vulnerabilidade de injeção de SQL de alta gravidade identificada como CVE-2024-6632.

Produtos afetados

Essa vulnerabilidade afeta as seguintes versões:

- FileCatalyst Workflow versões 5.0.4 a 5.1.6.139

Referências

- forttra.com
- cvedetails.com
- securityweek.com
- unaaldia.hispasec.com

TLP:WHITE

Vulnerabilidades

Múltiplas vulnerabilidades em produtos da Cisco

Data: 04 de setembro de 2024
CVE: CVE-2024-20439 e mais 5

CVSS: 9,8

CRÍTICA

Descrição

A Cisco divulgou 6 vulnerabilidades, incluindo 2 críticas, 1 alta e 3 de gravidade média. As vulnerabilidades críticas são:

- CVE-2024-20439: um invasor remoto não autenticado pode aproveitar uma credencial administrativa estática não documentada para obter acesso total ao sistema com privilégios de administrador.
- CVE-2024-20440: o excesso de detalhes nos arquivos de log de depuração permite que um invasor, por meio de uma solicitação HTTP mal-intencionada, acesse informações confidenciais, como credenciais de API.

Solução

Para corrigir essas vulnerabilidades, a Cisco lançou vários patches de segurança, que estão incluídos em uma única versão do software.

Os usuários afetados são aconselhados a atualizar para a seguinte versão o mais rápido possível:

- Cisco Smart License Utility: atualizar para a versão 2.3.0.

Produtos afetados

As vulnerabilidades críticas descritas acima afetam as seguintes versões do Cisco Smart License Utility:

- Cisco Smart License Utility versão 2.0.0
- Cisco Smart License Utility versão 2.1.0
- Cisco Smart License Utility versão 2.2.0

Referências

- sec.cloudapps.cisco.com
- sec.cloudapps.cisco.com
- sec.cloudapps.cisco.com
- sec.cloudapps.cisco.com
- sec.cloudapps.cisco.com
- incibe.es

TLP:WHITE

Atualizações de segurança para vulnerabilidades em produtos Veeam

Data: 04 de setembro de 2024
CVE: CVE-2024-40711 e 17 outros

Crítica

Descrição

A Veeam lançou um novo boletim com atualizações de segurança que abordam 18 vulnerabilidades críticas e altas de seu Veeam Backup & Replication, Service Provider Console e One.

As vulnerabilidades corrigidas incluem a vulnerabilidade crítica CVE-2024-4071 (com uma pontuação de 9,8). Essa vulnerabilidade afeta o Veeam Backup & Replication (VBR) e permite a execução remota de código (RCE) sem autenticação.

Embora o fornecedor não tenha revelado muitos detalhes, a vulnerabilidade permitiria que um invasor assumisse o controle total do sistema, por desserialização.NET Remoting.

Produtos afetados

A vulnerabilidade publicada no boletim afeta os seguintes produtos:

- Veeam Backup & Replication 12.1.2.172 e todas as versões 12.x.
- Veeam Agent para Linux 6.1.2.1781 e todas as versões 6.x.
- Veeam ONE 12.1.0.3208 e todas as versões 12.x.
- Veeam Service Provider Console 8.0.0.19552 e todas as versões 8.x.
- Veeam Backup for Nutanix AHV Plug-In 12.5.1.8 e todas as versões 12.x.
- Veeam Backup for Oracle Linux Virtualization Manager e Red Hat Virtualization Plug-In 12.4.1.45 e todas as versões 12.x.

Solução

Recomenda-se aplicar as atualizações publicadas pelo fabricante em seu boletim de segurança.

Referências

- bleepingcomputer.com
- veeam.com
- watchtowr.com

TLP:WHITE

Atualização de segurança crítica para Ivanti Endpoint Manager

Data: 10 de setembro de 2024
CVE: CVE-2024-29847 e mais 9

Crítica

Descrição

A Ivanti lançou várias atualizações de software para resolver várias vulnerabilidades críticas que afetam o Endpoint Manager (EPM).

A principal vulnerabilidade detectada com uma pontuação de 10,0 é a CVE-2024-29847, uma vulnerabilidade de desserialização de dados que permite a execução de código para um invasor remoto não autenticado.

Outras 9 vulnerabilidades críticas corrigidas com esta atualização são falhas de injeção SQL não especificadas que permitiriam que um invasor autenticado com privilégios de administrador executasse um código remotamente.

A Ivanti confirmou que a identificação dessas vulnerabilidades foi feita por meio de varredura interna, exploração manual e testes. Além disso, confirmou que, na data da publicação desta atualização de segurança, nenhuma exploração ativa dessas vulnerabilidades e nenhum indicador conhecido de comprometimento foi detectado.

Produtos afetados

As versões de EPM afetadas são:

- Endpoint Manager: versão 2024. Ele deve ser atualizado para a versão 2024 SU1.
- Endpoint Manager: Versão 2022 SU5 e anteriores. Ele deve ser atualizado para a versão 2024 SU6.

Solução

A Ivanti recomenda aplicar os patches publicados em sua atualização de segurança, dependendo da versão afetada do Endpoint Manager disponível.

Referências

- bleepingcomputer.com
- thehackernews.com
- ivanti.com

Eventos

Cybersecurity & Cloud Expo (1-2 de outubro)

A Cyber Security & Cloud Expo é um evento importante que será realizado em Amsterdã, de 1 a 2 de outubro de 2024. Ele reunirá mais de 7.000 participantes e 150 especialistas do setor para discutir tópicos fundamentais, como segurança em nuvem, detecção de ameaças, Zero Trust, adoção de nuvem híbrida e integração com DevSecOps. É uma oportunidade fundamental para aprender sobre as mais recentes inovações e estratégias em cibersegurança e tecnologia em nuvem.
Link

PCI SSC Europe Community Meeting (8-10 de outubro)

O PCI Security Standards Council (PCI SSC) Europe Community Meeting 2024 será realizado em Barcelona de 8 a 10 de outubro. Este evento é fundamental para os profissionais de segurança de dados e cumprimento de obrigação regulatória, pois reúne especialistas em PCI DSS para debater atualizações, melhores práticas e padrões de segurança em evolução no setor de pagamentos.
Link

World Summit AI (9-10 de outubro)

A World Summit AI 2024 é um evento global que reúne especialistas em inteligência artificial, líderes empresariais e tecnólogos em Amsterdã para explorar as mais recentes inovações em IA. O evento aborda tópicos como ética em IA, inteligência artificial na nuvem e cibersegurança relacionada a sistemas de IA. É uma plataforma fundamental para aprender sobre avanços, estabelecer conexões e discutir o futuro da inteligência artificial em todo o mundo.
Link

IT-sa Expo & Congress (22-24 de outubro)

A it-sa Expo&Congress 2024 é a principal feira de segurança de TI da Europa, que ocorre de 22 a 24 de outubro em Nuremberg. O evento reúne especialistas e tomadores de decisão de vários setores para discutir as últimas tendências em cibersegurança, incluindo proteção de infraestrutura crítica, segurança em nuvem e defesa contra ameaças. É uma plataforma essencial para explorar inovações de segurança e estabelecer contatos importantes no setor.
Link

Conferência Europeia ISACA 2024 (23-25 de outubro)

A Conferência Europeia ISACA 2024 é um evento emblemático a ser realizado em Dublin de 23 a 25 de outubro de 2024. O encontro inclui uma grande variedade de sessões educativas, oficinas interativas e painéis de discussão. Os tópicos variam de gerenciamento de riscos a cibersegurança e governança, oferecendo aos profissionais uma oportunidade de se aprofundar nos desafios atuais e nas tendências emergentes do setor de tecnologia.
Link

Recursos

Padrões viciantes no tratamento de dados pessoais

A Agência Espanhola de Proteção de Dados (AEPD) publicou o documento intitulado “Patrones adictivos en el tratamiento de datos personales: Implicancias para la protección de datos”. Este recurso bibliográfico analisa como determinados projetos e estratégias digitais podem manipular o comportamento do usuário, incentivando o uso excessivo ou viciante de aplicativos e serviços. Também destaca a importância de garantir que as empresas adotem práticas éticas no projeto de interfaces e no gerenciamento de dados pessoais, e propõe diretrizes para evitar a exploração de vulnerabilidades psicológicas dos usuários.
Link

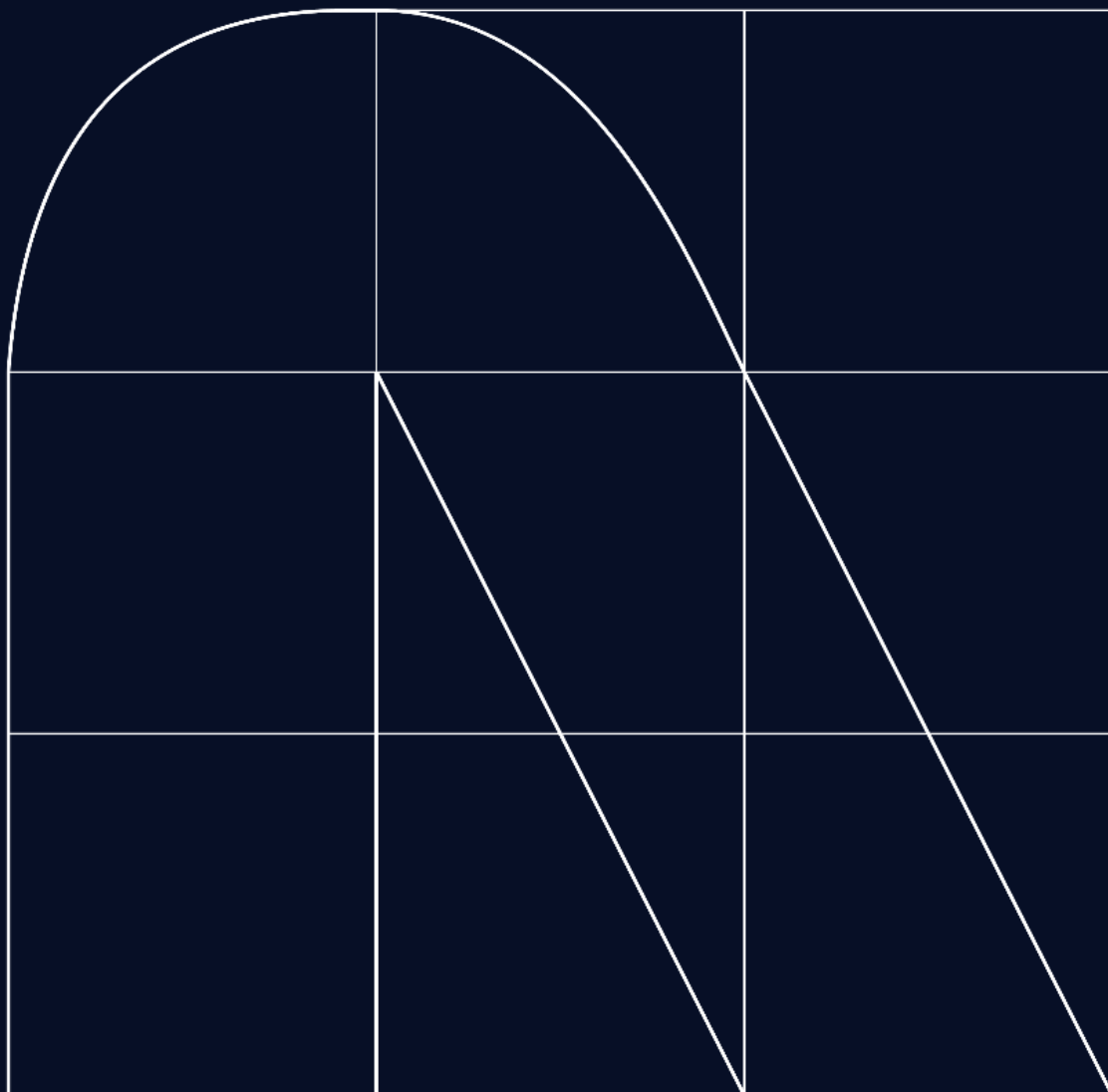
2º conjunto de políticas no âmbito da Lei de Resiliência Operacional Digital

As Autoridades Europeias de Supervisão (ESAs) publicaram o 2º conjunto de políticas no âmbito da Lei de Resiliência Operacional Digital ("DORA"). O documento inclui diretrizes e especificações técnicas para a implementação do DORA, abordando aspectos-chave, como o gerenciamento de riscos tecnológicos, supervisão de fornecedores terceirizados e requisitos de relatórios de incidentes, a fim de reforçar a estabilidade do sistema financeiro europeu contra ameaças digitais. Atualmente, o 2º conjunto de políticas está em revisão pela Comissão Europeia, e deve ser emitido em sua versão mais recente nos próximos meses; no entanto, de antemão, devem ser considerados como um ótimo recurso bibliográfico a ser consultado.
Link

Padrões de criptografia pós-quântica

O NIST finalizou os três primeiros padrões de criptografia pós-quântica, projetados para proteger as informações eletrônicas contra futuras ameaças de computadores quânticos. Esses padrões, desenvolvidos ao longo de oito anos, incluem algoritmos para criptografia geral e assinaturas digitais, garantindo segurança em um mundo pós-quântico. O NIST pede a adoção imediata desses padrões para a preparação para possíveis ataques cibernéticos baseados em tecnologia quântica.
Link

Inscreva-se na RADAR



Desenvolvida pela equipe de cibersegurança da NTT DATA

es.nttdata.com