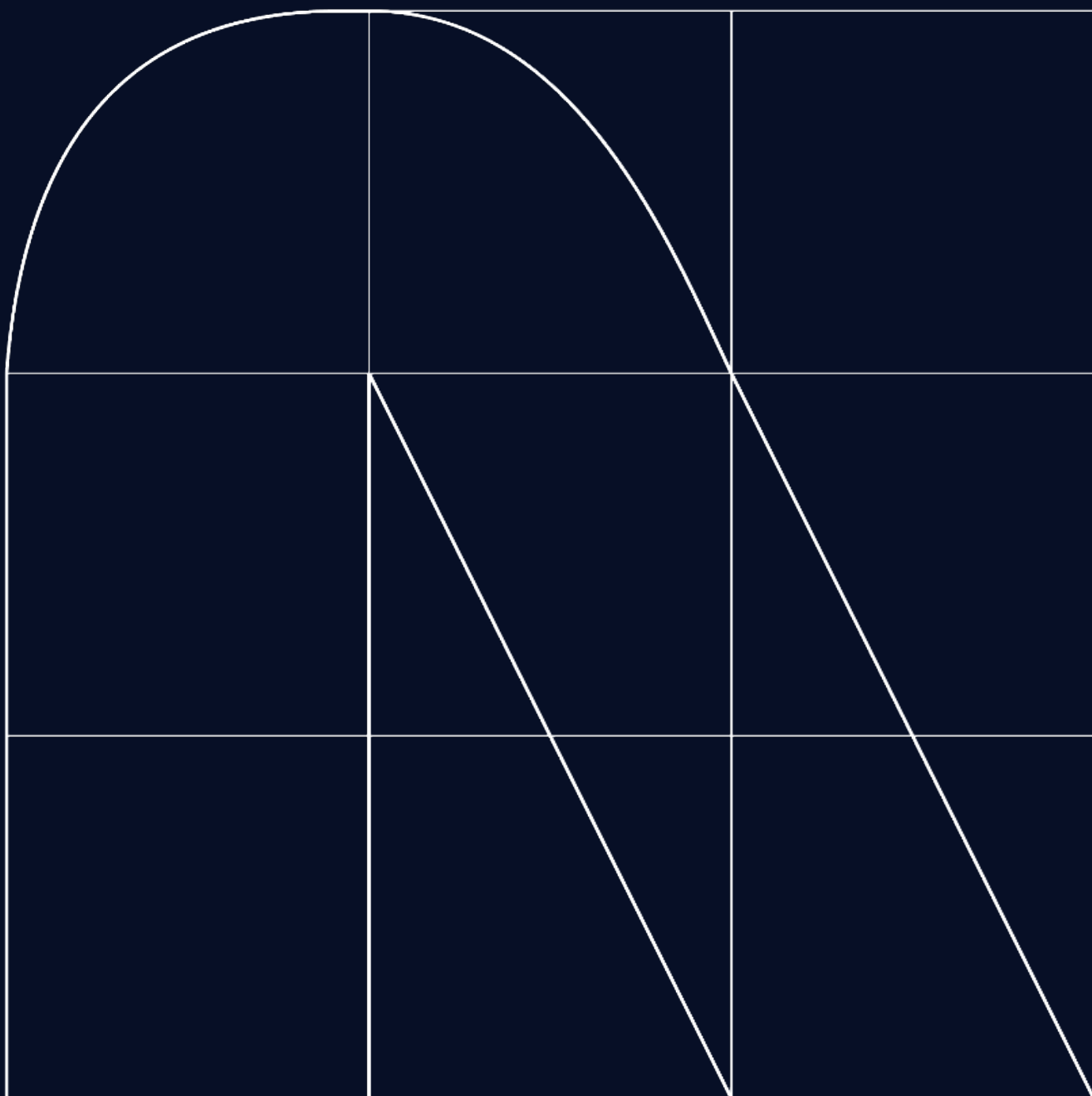
Número 85 | Dezembro de 2023

NTT DATA

Radar

A revista de cibersegurança



O longo caminho rumo à cibersegurança evolutiva

Por: Conrado López

A política de segurança da informação de uma organização determina, em grande medida, quais são os seus objetivos nessa área, associados à missão, visão e valores dessa organização. A estratégia de cibersegurança é o instrumento que permite à gestão da organização estabelecer o caminho a seguir para atingir estes objetivos ao longo do tempo, adaptando-se às mudanças que a própria evolução da empresa atravessa em resposta às necessidades e requisitos determinados pelo ambiente mutável em que se desenvolve.

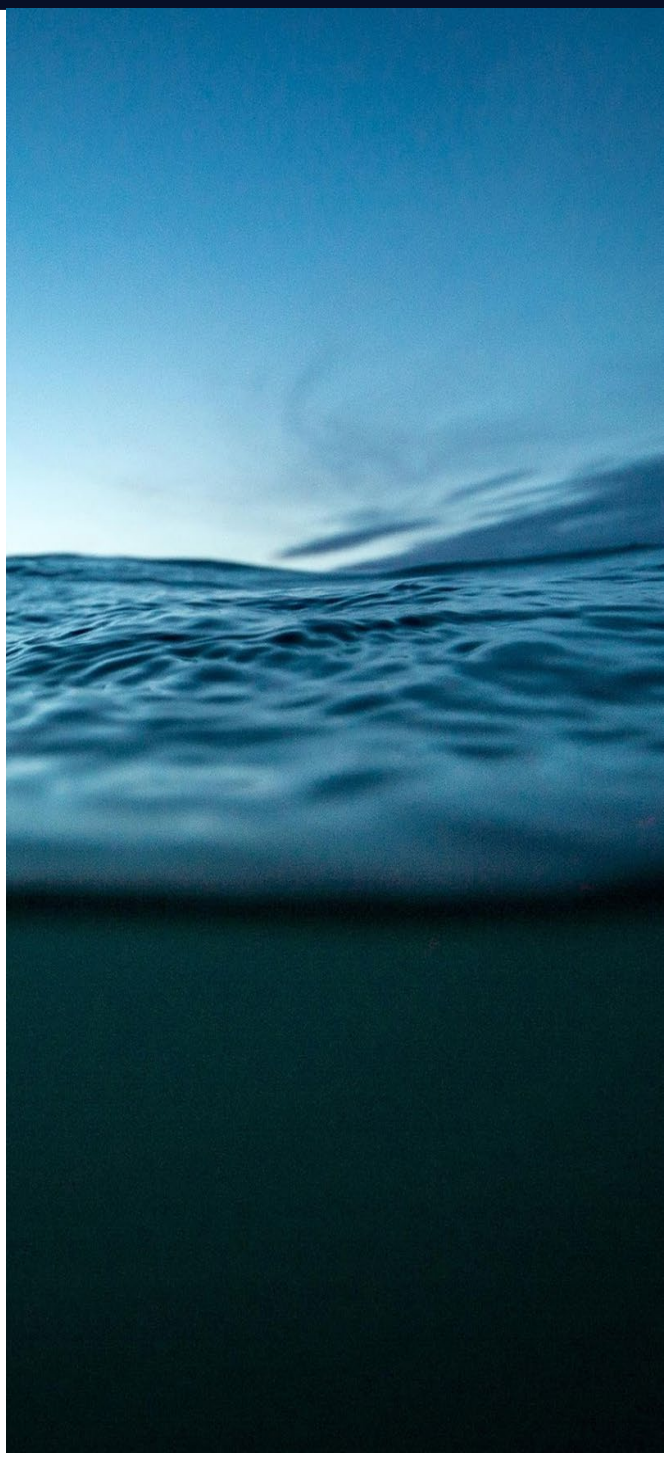
O alinhamento da estratégia de cibersegurança com a estratégia de negócio é um processo contínuo que requer uma estreita colaboração entre a função de cibersegurança e a gestão da organização. Quando este alinhamento é alcançado, a cibersegurança torna-se um facilitador dos objetivos comerciais ao proteger os ativos e a reputação da organização. Mas como conseguir esse alinhamento estratégico? Alguns fatores principais são:

Compreensão e envolvimento da gestão: é essencial que os líderes da empresa compreendam a importância da cibersegurança e como ela está intrinsecamente relacionada com o sucesso da organização. Isto pode ser alcançado por meio de sessões de conscientização e capacitação específicas para os líderes. Definitivamente, a função de cibersegurança deve estar envolvida no planeamento estratégico para garantir que os riscos e oportunidades de segurança sejam levados em conta.

Integração nos processos de negócio: a cibersegurança deve ser "incorporada" naturalmente nos processos de negócio para que seja um componente essencial das operações diárias. Isto inclui a identificação de ativos críticos, a gestão de riscos, a gestão segura da cadeia de suprimentos, a gestão de projetos e a tomada de decisões.

Avaliação de riscos tecnológicos e empresariais: não se trata apenas de avaliar riscos tecnológicos, mas também riscos comerciais. É necessária uma compreensão adequada de como os riscos cibernéticos podem afetar a continuidade do negócio, a reputação da empresa e a conformidade regulatória. De qualquer forma, o risco tecnológico é um componente essencial do risco operacional das organizações na sua transformação digital.

Comunicação eficaz: é crucial estabelecer uma comunicação constante entre a função de cibersegurança e a gestão da organização, mantendo os responsáveis informados sobre as ameaças cibernéticas, vulnerabilidades e conquistas na mitigação de riscos.



Objetivos de cibersegurança alinhados: os objetivos de cibersegurança devem estar alinhados com os objetivos de desenvolvimento do negócio e de evolução tecnológica da empresa. Para isso, é necessário compreender e internalizar diversos aspectos como:

Identificação do cenário de risco a que a organização está sujeita, desenvolvendo uma estratégia adequada de inteligência contra ameaças e uma resposta necessária, tanto de forma proativa como reativa.

Implicações regulatórias e requisitos tecnológicos impostos pela presença da organização em diferentes áreas geográficas.

Necessidade de conformidade com as regulamentações existentes no segmento em que a organização atua

Novos desafios de segurança impostos pela evolução tecnológica planejada para a organização apoiar a sua estratégia de negócio.

Melhoria da cultura de cibersegurança da organização, mantendo uma conscientização adequada de colaboradores e gestão.

Correta medição da eficácia dos processos de gestão da cibersegurança definidos no modelo de governança de segurança da organização, facilitando a tomada de decisões que permitam garantir o alinhamento com os objetivos estabelecidos e facilitando, na medida do possível, a avaliação do retorno do investimento em cibersegurança.

Alocação de recursos: os recursos de cibersegurança precisam estar alinhados com as prioridades do negócio. Isto pode envolver a atribuição de orçamento e pessoal com base nas necessidades de cibersegurança identificadas e, em particular, facilitar a independência e capacidade do responsável da área de cibersegurança (CISO) no desenvolvimento da sua função.

Além disso, a constante evolução do ambiente tecnológico, social, comercial, político e empresarial exige a capacidade de avaliar a situação de segurança da organização (consciência situacional), adaptando de forma flexível a estratégia de cibersegurança na medida em que as ameaças e os objetivos de negócio mudem. Isto requer avaliações periódicas (auditorias regulamentares, auditorias técnicas, análise de maturidade da função de cibersegurança, reavaliações do marco de controle existente, etc.) e ajustar a estratégia conforme necessário.

Definitivamente, uma lista de aspectos complexos que exigem conhecimento e dedicação que, levando em conta os resultados fornecidos por diversos estudos de analistas sobre a situação da cibersegurança na Espanha, torna-se cada dia mais necessário para a maioria das organizações contar com o apoio de colaboradores especialistas na área que facilitem a garantia da concretização dos objetivos e a própria estratégia de cibersegurança. Dados como o de que o número de organizações com 5 ou menos colaboradores dedicados à função de cibersegurança na Espanha, independentemente do volume de faturamento da empresa, ultrapassa os 50% (e, entre eles, 30% com faturamento superior a 100M€ (Fórum ISMS, III Indicador de Maturidade da cibersegurança) pareciam corroborar esta afirmação.

Conrad López
Gerente Técnico de Cibersegurança

Cibercrônica: A complexidade do gerenciamento de dados sensíveis na tempestade cibernética

Por: NTT DATA Europe & Latam

Na era da informação digital, a segurança no tratamento de dados é um desafio crucial. Estamos imersos em um cenário onde a integridade e a confidencialidade de nossas informações pessoais estão por um fio, constantemente ameaçadas por cibercriminosos.

Nas últimas semanas, uma conhecida companhia aérea ficou no epicentro das notícias relacionadas à cibersegurança após ter deixado dados sensíveis de milhares de seus clientes nas mãos de cibercriminosos. O ataque, descoberto em 10 de outubro deste ano, levou a companhia aérea a emitir um alerta urgente aos seus clientes, pedindo-lhes que cancelassem os seus cartões de crédito como medida preventiva dada a gravidade da situação.

A organização ainda não divulgou o número oficial de pessoas afetadas mas, segundo diversos meios de comunicação que divulgaram a notícia, são mais de 100.000 clientes. Esta não foi a primeira vez que isto ocorreu, pois há alguns anos a AEPD (Agência Espanhola de Protecção de Dados) a impôs uma multa de 600.000€ por não ter aplicado as medidas de segurança exigidas por lei. A empresa não forneceu mais dados mas, segundo especialistas em cibersegurança, especula-se que o roubo de dados, que inclui alguns dos dados mais sensíveis, como o CVV dos cartões, tenha sido realizado através de outros meios.

> A rápida evolução das táticas dos cibercriminosos exige uma atitude vigilante das organizações

Esta empresa possui certificação PCI-DSS desde 2020, o que significa que passou por diversas auditorias independentes que certificaram que os dados sensíveis dos clientes estavam sendo utilizados de forma adequada e segura. Portanto, os primeiros indícios apontam para uma possível injeção de código chamada web skimming, onde os hackers aproveitaram essa modificação no código-fonte da companhia aérea para enviar tais dados sensíveis para um servidor externo.

O ataque cibernético destaca não só a importância da adoção de práticas de segurança robustas, como através de certificações, como também é essencial que as empresas invistam na capacitação contínua de seus colaboradores, garantindo que estejam atualizados sobre as mais recentes ameaças e técnicas de segurança.

Da mesma forma, é essencial a implementação de tecnologias avançadas como sistemas de detecção de invasões, ferramentas cruciais que permitem identificar e responder rapidamente a possíveis ameaças. Contudo, a tecnologia por si só não é suficiente; a conscientização constante e a vigilância proativa são fundamentais.

A rápida evolução das táticas dos cibercriminosos exige uma atitude vigilante por parte das organizações, que devem estar conscientes das ameaças emergentes e, consequentemente, um desenvolvimento contínuo para adaptar as suas estratégias de segurança.

Portanto, este incidente ressalta a importância de combinar certificações, capacitação contínua, tecnologias avançadas e uma mentalidade proativa para manter a integridade e a confiança das informações dos clientes.

Do DevOps ao SecDevOps: Unindo segurança e agilidade

ANÁLISE

DevOps: Development + Operations. Unir os próprios processos de desenvolvimento de software com aqueles pertencentes à integração e implantação dos referidos desenvolvimentos. Parece difícil e, de fato, é. Se adicionarmos a cibersegurança à equação, ela se tornará complicada. A partir desse momento passamos a falar de DevSecOps, ou inclusive SecDevOps, dependendo do quão presente a segurança está em todo o processo.

As sinergias entre cibersegurança e DevOps

DevOps. O DevOps surge inicialmente da necessidade de construir e entregar software de forma contínua e automática o mais rápido possível. Uma equipe de desenvolvedores implementa uma nova funcionalidade em uma aplicação web, sendo importante que esta funcionalidade seja testada, integrada e implantada o mais rápido possível em ambientes de produção com o objetivo de disponibilizá-la o quanto antes ao usuário final.

Os conceitos-chave aqui são “colaboração” e “acelerar”. Precisamos colaborar para ter agilidade na entrega do software que aspiramos. Isto representa uma série de desafios, principalmente a mudança de mentalidade e a necessidade de comunicação entre departamentos que por vezes não é fácil. Uma função do setor de operação não pode ser colocada na mente de um desenvolvedor e vice-versa. Porém, a mudança não precisa ser imediata e os processos/tecnologias podem ser incorporados aos poucos.

A preocupação das empresas com a cibersegurança tem aumentado nos últimos anos, na medida em que foram crescendo tanto o número de ataques como a gravidade das consequências. Tornou-se clara a necessidade de desenvolver software com atenção especial à sua segurança.

Temos um cenário em que precisamos construir e entregar software de forma ágil (DevOps), mas ao mesmo tempo garantindo sua robustez contra ataques cibernéticos (Sec). Foi assim que nasceu o DevSecOps. Novamente, isto tem os seus desafios, pois agora não se trata apenas de uma colaboração entre Devs e Ops, mas também a integração da equipe de cibersegurança. Além disso, a inclusão de ferramentas e processos de segurança no final pode repercutir na rapidez com que um desenvolvimento é lançado em um ambiente de produção. Isso porque incluir as análises necessárias para verificar a segurança desse desenvolvimento pode retardar o processo global, principalmente se for necessária a inclusão de filtragem de falsos positivos. Porém, devemos decidir o que é importante: que os desenvolvimentos sejam lançados o mais rápido possível em ambientes de produção independentemente das vulnerabilidades que possam conter ou que, apesar da velocidade mais lenta nesta implantação, os nossos desenvolvimentos tenham um grau de segurança suficiente.

Da teoria à prática: ferramentas para tornar o desenvolvimento seguro

Hoje existe uma ampla variedade de ferramentas que nos ajudam a fornecer segurança aos desenvolvimentos incluídos em um ambiente DevSecOps. Dependendo do tipo de tarefa que realizam e do momento em que são executadas, podemos diferenciar os seguintes tipos:

- SAST: Static Application Security Testing. Nesta classificação encontramos aquelas ferramentas que analisam o código-fonte dos desenvolvimentos em busca de possíveis defeitos que possam provocar vulnerabilidades de segurança. Exemplos de tecnologias SAST são: Veracode, Fortify ou Coverity.
- SCA: Software Composition Analysis. Este tipo de software é responsável por detectar se existem vulnerabilidades de segurança conhecidas nas dependências externas utilizadas nos desenvolvimentos. Exemplos de ferramentas SCA são: Snyk, Black Duck ou XRay.
- DAST: Dynamic Application Security Testing. Semelhante ao SAST, mas com a diferença que em vez de analisar o código fonte dos desenvolvimentos, analisa o seu comportamento uma vez implantados. Realiza testes automatizados em busca de comportamentos que possam levar a falhas de segurança, como vazamento de informações ou indisponibilidade de serviços. Exemplos de ferramentas DAST são: Burp Suite, Nessus, Acunetix.
- RASP: Runtime application self-protection. Semelhante à tecnologia dos WAF (Web Application Firewall). É responsável por detectar e bloquear possíveis tentativas de ataque às aplicações implantadas. Diferentemente dos WAFs, que operam em nível de rede, os RASP são executados em nível de aplicação. Eles possuem certas informações sobre a funcionalidade e a infraestrutura interna das aplicações que protegem e, portanto, são mais precisos na detecção de possíveis ataques. Exemplos de RASP são: Imperva, Hdiv e OpenRASP.

DevSecOps x SecDevOps

Atualmente, ambos os termos são usados indistintamente como sinônimos e a diferença é bastante difusa. Porém, existem algumas nuances que os diferenciam.

- DevSecOps é um ambiente de DevOps ao qual foram incluídas adições de segurança: Ferramentas SAST/SCA para analisar o código e as dependências, talvez um RASP para monitorar e proteger os desenvolvimentos já implantados... Em suma, a segurança existe no ambiente DevOps como algo necessário, mas sem afetar todos e cada um dos processos que são executados.
- SecDevOps é um ambiente de DevOps no qual a segurança é priorizada e é ressaltado de forma consciente que cada um dos processos existentes a levem em consideração. Os desenvolvedores têm à sua disposição ferramentas de análise SAST em seus IDEs; há uma bateria de testes de segurança atualizada regularmente que é executada sempre que o código é carregado nos repositórios; são executadas análises completas de SAST, SCA, DAST e/ou IAST com security gates que impedem a implantação de desenvolvimentos vulneráveis, e os desenvolvimentos implantados são monitorados e protegidos usando ferramentas RASP e/ou SIEM.

Enquanto no DevSecOps a segurança é contemplada e levada em consideração, no SecDevOps é priorizado e considerado o elemento que deve abranger o restante.

Como observação final, o nosso objetivo é construir software, não só de forma ágil, mas também com as maiores garantias de segurança possíveis. Portanto, devemos sempre contar com um ambiente SecDevOps. No entanto, tentar passar diretamente de um ambiente DevOps para um ambiente SecDevOps provavelmente será contraproducente, pois todos os usuários envolvidos ficarão sobrecarregados com um volume tão grande de novas ferramentas e processos. A melhor estratégia será implementar gradualmente estas ferramentas e, ao mesmo tempo, treinar os usuários na sua utilização.

Miguel Otero
Cybersecurity Lead Architect
NTT DATA Europe & Latam

Antonio Gallego
Cybersecurity Analyts
NTT DATA Europe & Latam

SBOM em Cibersegurança: A chave para uma defesa eficaz.

TENDÊNCIAS

Com a crescente ameaça de ataques cibernéticos sofisticados, as organizações procuram constantemente formas inovadoras de proteger os seus ativos digitais. Neste contexto, o SBOM (*Software Bill of Materials*) surge como uma ferramenta crucial para fortalecer as defesas cibernéticas.

O SBOM é essencialmente uma lista detalhada de todos os componentes de software utilizados em uma aplicação ou sistema. Esta lista fornece informações vitais sobre as bibliotecas, frameworks e módulos que compõem o software. No contexto da cibersegurança, o SBOM é uma ferramenta inestimável, pois fornece uma visão completa da superfície de ataque potencial.

Ao incorporar o SBOM na estratégia de cibersegurança, as organizações ganham uma transparência sem precedentes na sua cadeia de suprimento de software. Isso significa que cada componente utilizado no desenvolvimento de software é documentado e pode ser facilmente rastreado.

A visibilidade na cadeia de suprimento é crucial para identificar potenciais vulnerabilidades e riscos de segurança. A capacidade de conhecer e compreender cada elemento de software utilizado permite que as organizações tomem medidas proativas para mitigar riscos e fortalecer suas defesas. Um dos maiores benefícios do SBOM no campo da cibersegurança é a sua capacidade de facilitar a gestão de vulnerabilidades e patches. Ao conhecer todos os componentes de software e suas versões, as organizações podem identificar rapidamente vulnerabilidades conhecidas e aplicar os patches correspondentes com eficiência.

Esta capacidade de resposta rápida é essencial para combater ameaças emergentes. Os cibercriminosos muitas vezes exploram vulnerabilidades conhecidas em software desatualizado para realizar ataques. O SBOM permite que as organizações fechem estas brechas de segurança o quanto antes, reduzindo significativamente o risco de exploração.

Em um ambiente regulamentado, o SBOM é um aliado fundamental para garantir a conformidade regulatória. As regulamentações de cibersegurança cada vez mais estritas exigem uma abordagem proativa para gerenciar riscos. O SBOM fornece documentação detalhada que facilita a demonstração da conformidade com as regulamentações vigentes.

Além disso, facilita auditorias de segurança. As equipes de segurança podem revisar minuciosamente a lista de componentes de software, verificar a presença de patches e avaliar a postura geral de segurança da organização. Isto não só atende os requisitos normativos, mas também fortalece a postura de segurança da organização.

A incorporação do SBOM nas práticas de desenvolvimento seguro é essencial para maximizar a sua eficácia. Integrar o SBOM no ciclo de vida de desenvolvimento de software desde o início garante que a transparência e o gerenciamento de riscos sejam parte integrante de todo o processo.
As equipes de desenvolvimento podem utilizar o SBOM para tomar decisões conscientes sobre a seleção de componentes de software, avaliando a segurança de cada elemento antes da implementação.

Esta prática proativa contribui para a criação de software mais seguro desde o início, reduzindo a necessidade de correções dispendiosas em fases posteriores.

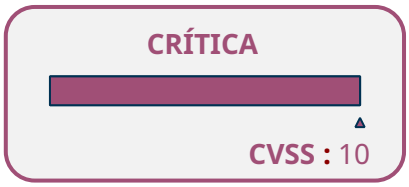
Em suma, o SBOM tornou-se uma ferramenta essencial na cibersegurança moderna. Proporciona transparência, visibilidade e eficiência na gestão de vulnerabilidades, o que é crucial em um ambiente digital cada vez mais ameaçador. Integrar o SBOM na estratégia de cibersegurança não só fortalece as defesas de uma organização, mas também contribui para a conformidade regulamentar e para o desenvolvimento seguro de software.

Por fim, o SBOM não é simplesmente uma lista de componentes de software, mas uma ferramenta estratégica para construir um futuro digital mais seguro.

Vulnerabilidades

Vulnerabilidade no Confluence Data Center and Server

Data: 31 de outubro de 2023
CVE: CVE-2023-22518



Descrição

A Atlassian publicou uma vulnerabilidade de gravidade crítica que afeta seus produtos Confluence Data Center e Confluence Data Server. Esta vulnerabilidade afeta todas as versões de ambos os produtos.

Por meio desta falha de segurança, um hacker não autenticado pode se beneficiar de uma autorização incorreta, que permitiria reiniciar a instância do Confluence e criar uma conta de administrador.

Uma vez obtidos os privilégios de administrador, o hacker pode executar todos os tipos de ações na instância do Confluence, resultando em perda total de confidencialidade, integridade e disponibilidade.

Links:
https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
https://jira.atlassian.com/browse/CONFSERVER-93142
https://nvd.nist.gov/vuln/detail/CVE-2023-22518

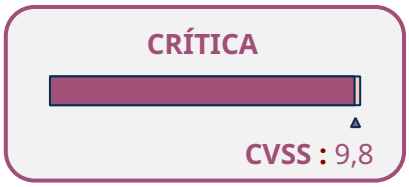
Produtos afetados:
A vulnerabilidade afeta todas as versões dos seguintes produtos:
- Confluence Data Center
- Confluence Data Server

Resolução:
O fabricante recomendou a atualização o mais rápido possível para uma das seguintes versões:
- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

Vulnerabilidades

Múltiplas vulnerabilidades em produtos QNAP

Data: 3 de novembro de 2023
CVE: CVE-2023-23368



Descrição

No dia 4 de novembro, a QNAP publicou uma vulnerabilidade crítica que afeta vários dos seus produtos (QTS, QuTS hero e QuTScloud).

Esta vulnerabilidade de injeção de comandos pode permitir que hackers executem comandos de forma remota.

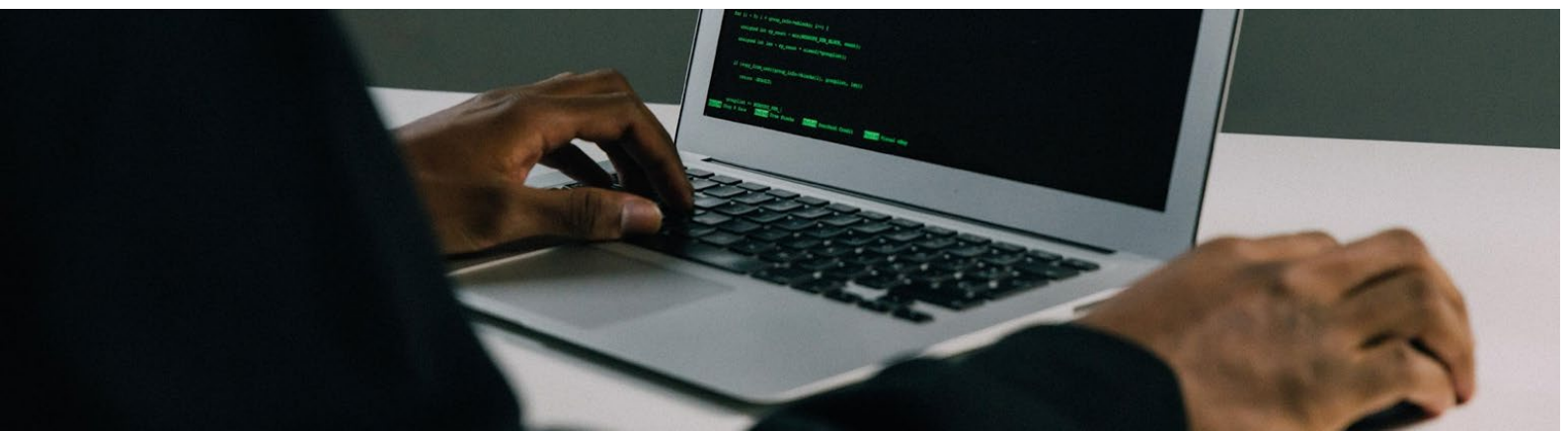
A QNAP informa que o problema foi resolvido e recomenda atualizar os sistemas para a versão mais recente o quanto antes possível para evitar a exploração da referida vulnerabilidade pelos hackers.

Links:
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-23368
https://www.qnap.com/en/security-advisory/qsa-23-31
https://nvd.nist.gov/vuln/detail/CVE-2023-23368

Produtos afetados:
Os diferentes produtos afetados pela vulnerabilidade são os seguintes:

- QTS (versões 5.0.x)
- QTS (versões 4.5.x)
- QuTS hero (versões h5.0.x)
- QuTS hero (versões h4.5.x)
- QuTScloud (versões c5.0.x)

Resolução:
O fabricante publicou uma série de atualizações para resolver esta vulnerabilidade. Recomenda-se a instalação desses patches o quanto antes possível.



Patches

Múltiplos patches para vulnerabilidades na Veeam

Data: 6 de novembro de 2023
CVEs: CVE-2023-38547, CVE-2023-38548, CVE-2023-38549 e CVE-2023-41723

CRÍTICA

CVSS : 9,9

Descrição

A Veeam publicou uma série de patches de segurança que corrigem um total de 4 vulnerabilidades, sendo duas delas de gravidade crítica e duas de gravidade média:

- **CVE-2023-38547:** vulnerabilidade crítica que permite que um hacker não autenticado faça uma execução remota de código em servidores SQL.
- **CVE-2023-38548**: vulnerabilidade de gravidade crítica que permitiria que um usuário sem privilégios com acesso à Veeam ONE Web Client obtivesse *hashes* NTLM de contas usadas pela Veeam.
- **CVE-2023-38549:** vulnerabilidade XSS de gravidade média que permite escalonamento de privilégios de usuário "Power User" para "Administrator".
- **CVE-2023-41723**: vulnerabilidade de gravidade média que permite que um usuário com privilégios de "Read-Only" consulte informações da seção "Dashboard Schedule".

A Veeam recomenda interromper imediatamente os serviços da Veeam ONE, caso esteja usando as versões afetadas, aplicar os patches e reiniciar esses serviços.

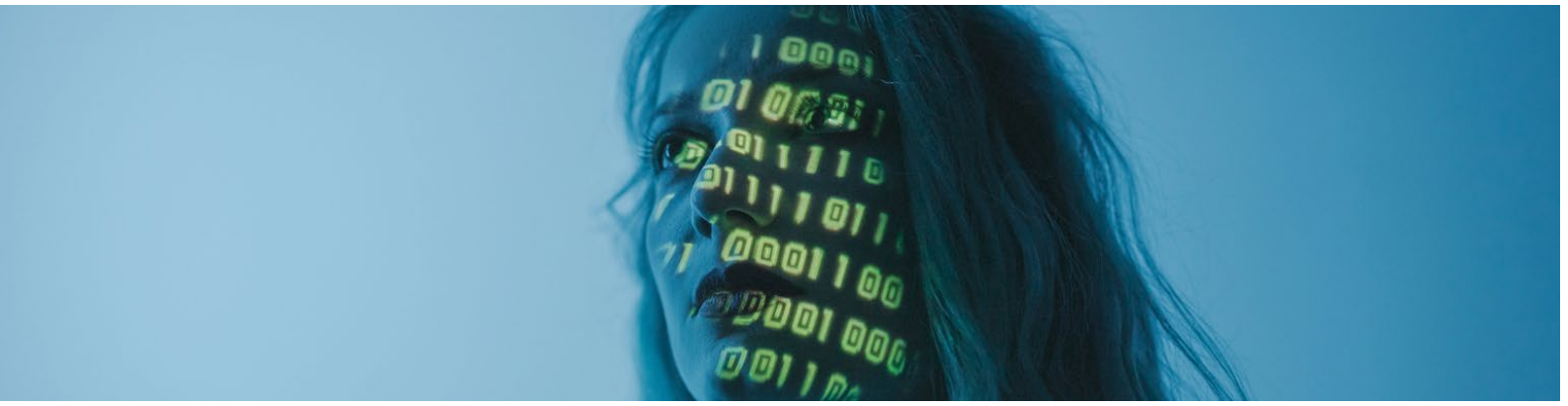
Links:
https://www.veeam.com/kb4508
https://thehackernews.com/2023/11/critical-flaws-discovered-in-veeam-one.html

Produtos afetados:
Essas vulnerabilidades afetam as seguintes versões da Veeam ONE:

- Veeam ONE 11
- Veeam ONE 11a
- Veeam ONE 12

Atualização:
A solução proposta pelo fabricante consiste na atualização para as seguintes versões:

- Veeam ONE 11 (11.0.0.1379)
- Veeam ONE 11a (11.0.1.1880)
- Veeam ONE 12 P20230314 (12.0.1.2591)



Patches

Múltiplos patches de segurança para produtos Microsoft

Data: 14 de novembro de 2023
CVEs: CVE-2023-36025, CVE-2023-36033, CVE-2023-36036, CVE-2023-36038, CVE-2023-36413, CVE-2023-36028, CVE-2023-36397

CRÍTICA

CVSS: 9,8

Descrição

A Microsoft publicou seu boletim de segurança mensal para corrigir um total de 63 vulnerabilidades em seus produtos. Entre elas, há um total de 5 vulnerabilidades 0-day:

- **CVE-2023-36025 (CVSS: 8.8):** vulnerabilidade no Windows SmartScreen Security Feature que permite contornar algumas medidas de segurança.
- **CVE-2023-36033 (CVSS: 7.8):** vulnerabilidade de escalonamento de privilégios na Windows DWM Core Library.
- **CVE-2023-36036 (CVSS: 7.8):** vulnerabilidade de escalonamento de privilégios no Windows Cloud Files Mini Filter Driver.
- **CVE-2023-36038 (CVSS: 8.2):** vulnerabilidade DoS no ASP.NET Core.
- **CVE-2023-36413 (CVSS: 6.5):** vulnerabilidade no Microsoft Office que permite contornar determinados recursos de segurança.

Além disso, duas vulnerabilidades de gravidade crítica foram corrigidas:

- **CVE-2023-36028 (CVSS: 9.8):** vulnerabilidade de execução remota de código no Microsoft Protected Extensible Protocol (PEAP).
- **CVE-2023-36397 (CVSS: 9.8):** vulnerabilidade de execução remota de código no Windows Pragmatic General Multicast (PGM).

A Microsoft recomenda a instalação de todos os patches de segurança nos produtos afetados, pois alguns deles estão sendo explorados ativamente.

Links:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov
https://thehackernews.com/2023/11/alert-microsoft-releases-patch-updates.html

Produtos afetados:
Essas vulnerabilidades abrangem um grande número de produtos Microsoft. Estes produtos podem ser consultados em: https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov

Atualização:
Aplicar o patch de segurança correspondente aos produtos afetados.

Eventos

XV JORNADAS STIC CCN-CERT
30 de novembro – 3 de dezembro

A Jornada STIC CCN-CERT, na sua décima quinta edição, de 30 de novembro a 3 de dezembro, é um evento chave de cibersegurança na Espanha que evoluiu durante quinze anos, reunindo profissionais, entidades públicas, empresas e universidades. Apesar dos desafios da COVID-19, a última edição foi adaptada com sucesso. Este ano, sob o lema "Cibersegurança 360º. Identidade e Controle de Dados", o evento será híbrido, com atividades presenciais e online, oferecendo uma visão abrangente do setor a nível nacional e internacional

Link

A ÚLTIMA CEIA DE OSINT
2 de dezembro

Em resposta à crescente importância do ciberespaço e a cibersegurança na geopolítica global, a QuantiKa14 organiza um evento efêmero único: A Última Ceia OSINT em Sevilha. Este encontro excepcional oferecerá discussões de vanguarda sobre inteligência cibernética, com palestrantes e patrocinadores ilustres. A noite contará com três apresentações, coffee break e networking, seguida de um jantar onde a conversa será tão deliciosa quanto os pratos. Sevilha se tornará o epicentro desta conversa vital em um momento crucial para se manter informado e conectado nesta área chave.

Link

BLACK HAT EUROPE 2023
4 - 7 de dezembro

Black Hat é um evento de destaque em cibersegurança que reúne especialistas do setor para explorar as pesquisas e tendências mais recentes. Durante quatro dias, oferece capacitações técnicas práticas seguidas de dois dias de apresentações sobre vulnerabilidades. A Black Hat Europe ocorrerá presencialmente em Londres de 4 a 7 de dezembro, seguida de uma experiência virtual a partir de 13 de dezembro com gravações de todas as sessões. Este ano será apresentado o programa "Certified Pentester", um exame prático de um dia focado em pentesting

Link

CIBER1C MX
7 de dezembro

Ciberilatam, em colaboração com o Centro Criptológico Nacional da Espanha e a Fundação Borredá, organiza o I Congresso de Cibersegurança em Infraestruturas Críticas e Serviços Essenciais do México (CIBER1C MX) no dia 7 de dezembro no Club de Periodistas. Este evento, também apoiado pela Segurilatam, reunirá profissionais para explorar estratégias de cibersegurança na proteção de infraestruturas críticas e serviços governamentais essenciais, abordando desafios, ameaças em cibersegurança para a governança corporativa e discutindo o futuro do setor, entre outros temas relevantes.

Link

Recursos

Flipper zero desafia a segurança dos iphones

O Flipper Zero, reconhecido como o “tamagotchi” para hackers, ganhou notoriedade por sua versatilidade e capacidade de realizar experimentos de hacking. Foi recentemente revelado que este dispositivo multifuncional pode desafiar a segurança dos iPhones, especialmente aqueles que executam o iOS 17. Custando cerca de 250 euros, o Flipper Zero pode interceptar e reproduzir sinais sem fios, mas a sua capacidade de enviar iPhones para loops de negação de serviço (DoS) por meio de uma enxurrada de mensagens via Bluetooth gerou preocupações significativas. Embora ainda não exista uma solução definitiva para prevenir estes ataques, a situação destaca a importância da regulamentação e da ética no setor da cibersegurança na medida em que as tecnologias avançam e podem ser utilizadas de forma maliciosa.

Link

Microsoft oferece novas ferramentas de IA para combater ataques cibernéticos

A Microsoft anunciou seu compromisso de melhorar na área de cibersegurança, ampliando as capacidades de suas ferramentas e técnicas para detectar ameaças. A empresa pretende disponibilizar estas capacidades diretamente aos seus clientes, concedendo ferramentas de inteligência artificial (IA) com o objetivo de reforçar a defesa contra ataques cibernéticos. Esta abordagem reflete a iniciativa da Microsoft em fortalecer os usuários com soluções avançadas na luta contra ameaças digitais.
Link

O golpe do falso filho (whatsapp, bizum...)

A Polícia Federal da Espanha alertou os cidadãos sobre o golpe do falso filho, que levou à prisão de 17 pessoas na Catalunha pelo roubo de 60.000 euros com este método. O golpe trata-se de golpistas se passando por filhos ou filhas por meio de mensagens do WhatsApp, solicitando dinheiro para emergências fictícias. As vítimas, geralmente mães preocupadas, transferem dinheiro para contas bancárias ou identificadores Bizum fornecidas pelos golpistas. A polícia aconselha desconfiar de mensagens inesperadas, verificar a autenticidade dos pedidos de dinheiro urgente, contatar diretamente os familiares supostamente afetados e abster-se de fazer transferências para contas desconhecidas para evitar cair neste tipo de golpe.

Link

Responsáveis Ciber

María Pilar Torres Bruna

Diretora de Cibersegurança na NTT DATA Latam e Peru
maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schawarzer

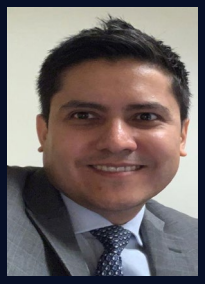
Diretora de Cibersegurança na NTT DATA Brasil
carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzón Ramírez

Manager de Cibersegurança na NTT DATA Colômbia
miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis Rivero

Diretor de Cibersegurança na NTT DATA México
fernando.vilchisrivero@emeal.nttdata.com

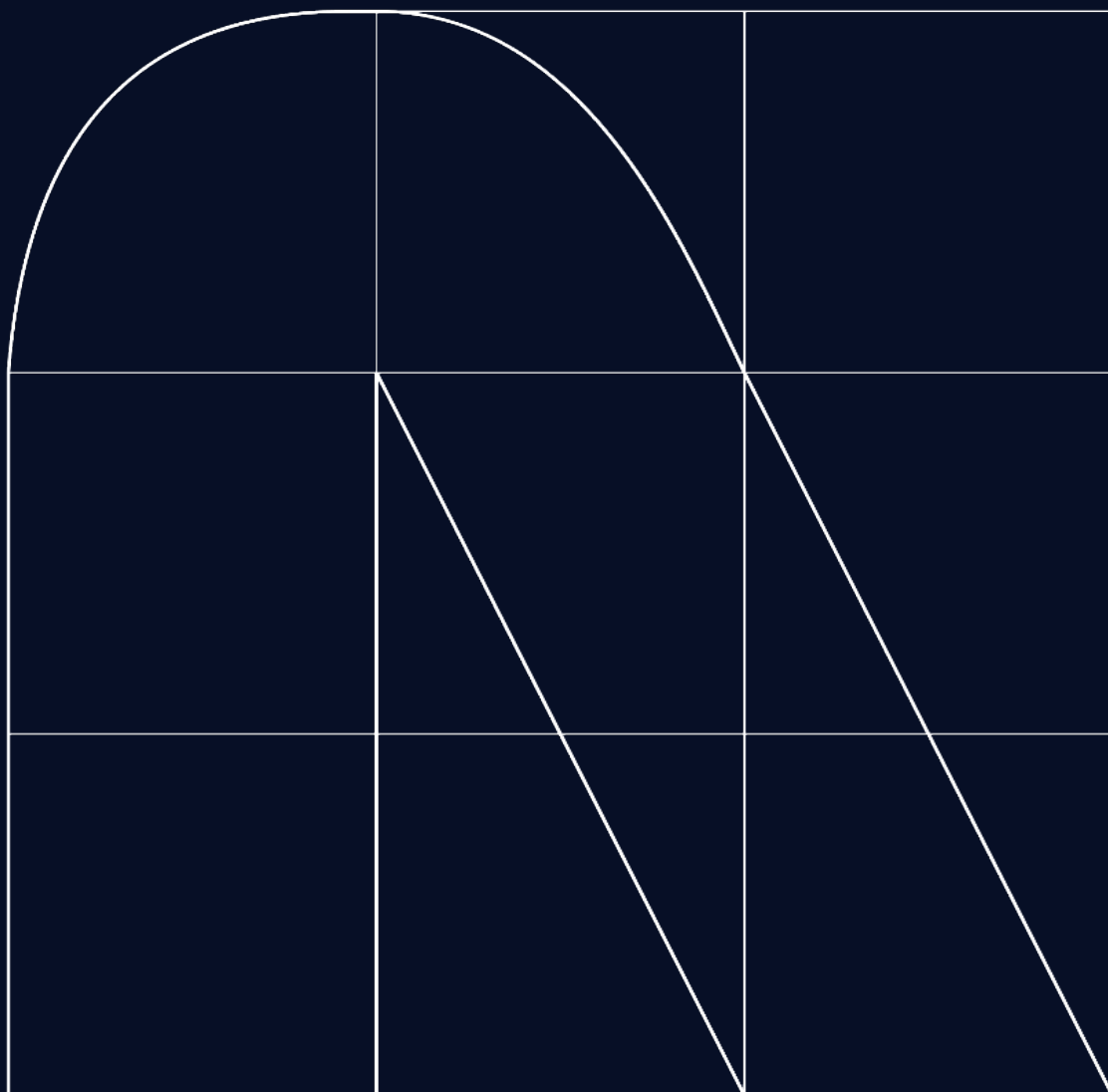


Nestor Gerardo Ordoñez

Manager de Cibersegurança na NTT DATA USA
nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Manager de Cibersegurança na NTT DATA Chile
jose.uzcategui@emeal.nttdata.com



Com o apoio da segurança cibernética Equipe da NTT DATA

es.nttdata.com