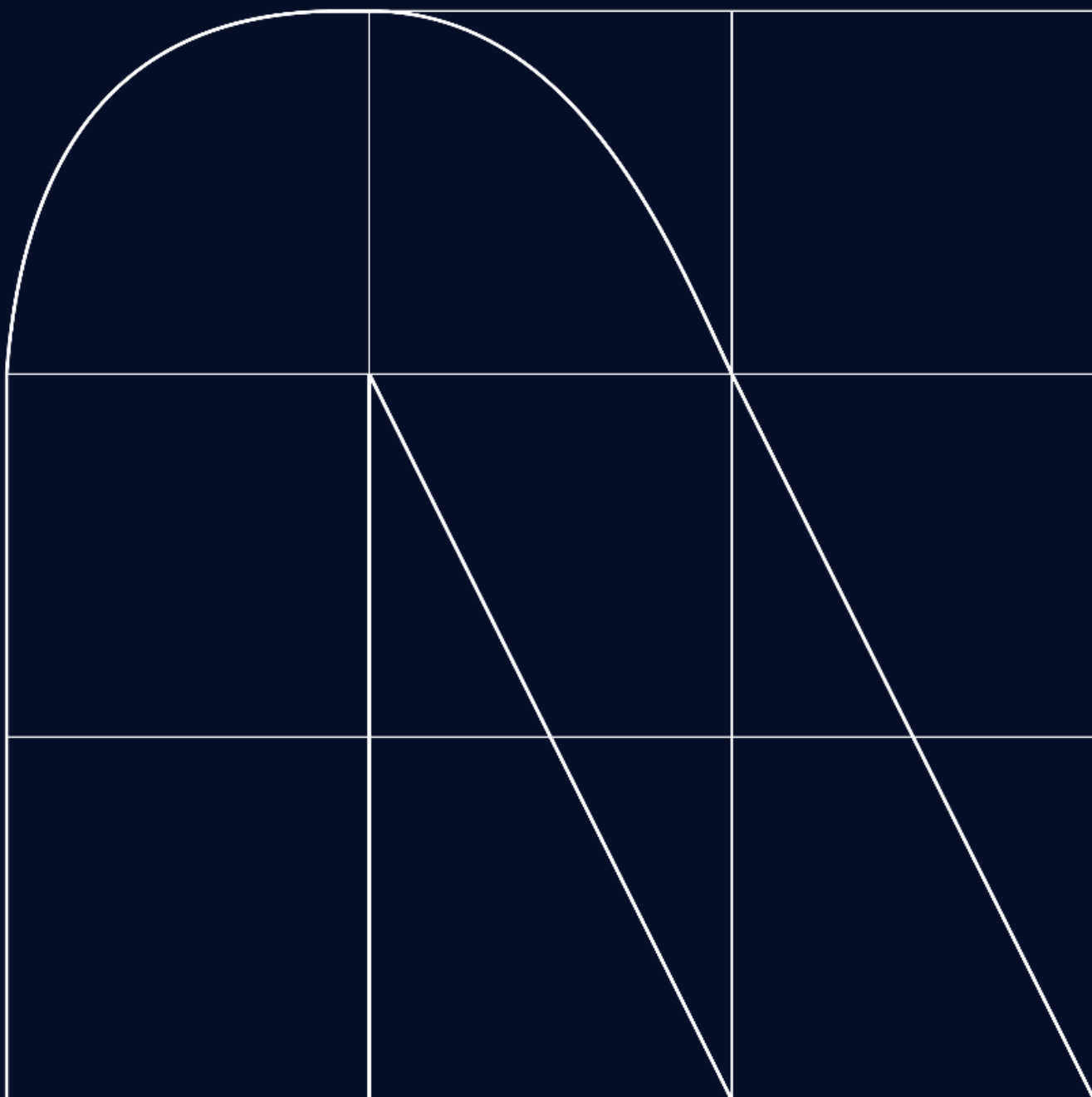
Número 89 | Abril 2024

NTT DATA

Radar

A revista de cibersegurança



Segurança em aplicativos e inteligência artificial

Por Roberto Junior Ruiz Neyra

Mais de 50% dos malwares chegam aos usuários por meio de aplicativos na nuvem. Muitos deles têm origem geopolítica, enquanto outros são provenientes de cibercriminosos, como o grupo russo Wizard Spider, TA505 e FIN7. Entre as principais vítimas desses ataques estão os serviços financeiros e saúde. A maioria dessas situações ocorre devido às brechas de segurança apresentadas pelos aplicativos, onde os cibercriminosos aproveitam as vulnerabilidades para injetar malwares e alcançar seus objetivos.

Por que isso acontece? Tudo começa desde a segurança no design dessas aplicações até o próprio desenvolvimento. Os últimos estudos demonstraram que mais de 70% das aplicações desenvolvidas contêm brechas de segurança, representando um risco importante para as organizações. Esse risco é exponencial quando as aplicações têm um grande alcance comercial, tornando várias empresas e países vítimas potenciais. Um ponto importante a se notar é que, à medida que a IA generativa vem ganhando protagonismo no desenvolvimento de software, o risco de vulnerabilidades aumenta se essa prática não for controlada. Isso ocorre porque o código é escrito por grandes modelos de linguagem treinados em fontes de dados não depuradas, como repositórios públicos do GitHub. Por isso, é de suma importância que a segurança da nova aplicação seja verificada por meio de ferramentas de análise estática de código (SAST) e ferramentas de análise de composição de software (SCA) gerenciadas por especialistas em Cibersegurança com o objetivo de maximizar a identificação de falhas ou vulnerabilidades e corrigi-las, permitindo que os desenvolvedores aproveitem ao máximo as vantagens da IA sem comprometer a segurança das aplicações.

Felizmente, a era da IA não vem apenas para ganhar terreno no âmbito do desenvolvimento de software, mas também na segurança de aplicações. Por exemplo, dentro da prática de DevSecOps e Cloud Security, estão surgindo novas soluções que abrangem casos de uso como interpretação da vulnerabilidade e proposta de scripts de remediação dessas vulnerabilidades em tempo real. Outro caso de uso interessante é o treinamento da IA para realizar testes de segurança por meio da simulação de ataques. Assim como estes exemplos, existem outros nos quais poderemos ter a IA como aliada para assegurar o desenvolvimento e criação das aplicações.
Na NTT DATA, estamos convencidos de que a IA será essencial para evoluir e inovar a segurança nas aplicações onde contribuímos com a agilidade no "time to market", não afetar a experiência do usuário no momento de tornar a segurança mais robusta e nos mantermos firmes com o princípio de "Zero Confiança".

Roberto Junior Ruiz Neyra
Cybersecurity Manager

Cibercrônica

Por Christian Agreda

Iniciamos a cibercrônica deste mês falando sobre a Vulnerabilidade de dia zero do SmartScreen do Windows Defender (CVE-2024-21412) descoberta.

Essa vulnerabilidade se deve a uma falha na aplicação da "Marca da Web" (MotW), uma característica de segurança utilizada pelo Windows para identificar arquivos provenientes de fontes potencialmente não confiáveis, como downloads da Internet, WebDAV e recursos compartilhados do SMB. Em circunstâncias normais, arquivos baixados da web são marcados com MotW, o que faz com que o Windows Defender SmartScreen emita alertas quando tais arquivos tentam ser executados ou quando um usuário tenta executá-los diretamente. Esse mecanismo atua como uma defesa crítica, prevenindo a execução de código malicioso ou não autorizado sem o conhecimento ou consentimento do usuário.

No entanto, a CVE-2024-21412 permitiu que os invasores contornassem essas proteções explorando uma falha no gerenciamento de acessos diretos à Internet (arquivos .URL) e outros mecanismos [8]. Por meio de campanhas de *phishing* elaboradas e o uso de sites comprometidos, os invasores distribuíram esses arquivos .URL maliciosos. Quando executados, esses arquivos não continham a marcação MotW, o que efetivamente cegou o SmartScreen para suas intenções maliciosas. Esse descuido permitiu a execução do malware DarkMe sem ativar os avisos de segurança habituais que alertariam os usuários sobre o perigo potencial.

Ao evitar as defesas do SmartScreen, o Water Hydra conseguiu executar sua cadeia de ataque de forma discreta, infectando as máquinas das vítimas sem ser detectado. O ataque aproveitou a confiança que o Windows deposita nos arquivos que não possuem a designação MotW, assumindo que são seguros e provenientes de uma fonte confiável dentro do ambiente do usuário. Esta exploração representa uma importante violação de confiança nos mecanismos de segurança elaborados para proteger os usuários do mesmo tipo de ataque orquestrado pelo Water Hydra.

A Connectwise abordou duas vulnerabilidades críticas recentemente (CVE-2024-1709 e CVE-2024-1708) em todas as versões locais do ScreenConnect anteriores à 23.9.7 com um patch de segurança urgente lançado em 19 de fevereiro de 2024 [9]. A CVE-2024-1709, uma vulnerabilidade de omissão de autenticação com uma classificação de gravidade crítica de 10/10, compromete o ScreenConnect ao permitir que usuários não autorizados manipulem o acesso URL (exp. /SetupWizard.aspx/anygivenstring) no assistente de configuração, obtendo, potencialmente, privilégios administrativos completos e executando código arbitrário.

Foi descoberta uma vulnerabilidade crítica, identificada como CVE-2023-22527, no Atlassian Confluence, que apresenta um risco de segurança grave com uma pontuação CVSS de 10[10]. Esta vulnerabilidade deve-se a uma falha de injeção de template dentro da linguagem de navegação de gráficos de objetos (OGNL), um componente amplamente utilizado em aplicações web para criar templates do lado do servidor. O método de exploração envolve invasores direcionando arquivos de template .vm específicos dentro do Confluence, que tratam de maneira inadequada a entrada fornecida pelo usuário. Por exemplo, a vulnerabilidade foi identificada no arquivo /confluence/template/aui/text-inline.vm, onde os invasores poderiam injetar códigos maliciosos através de parâmetros destinados a funções legítimas da página. Este arquivo, entre outros, não conseguiu desinfectar adequadamente a entrada, permitindo que os invasores executassem comandos de forma remota no sistema afetado.

Para abordar essa vulnerabilidade, a Atlassian lançou atualizações para o Confluence Data Center e Server, particularmente a versão 8.5.4 e posteriores, que incluem patches para mitigar o risco de exploração. Essas atualizações corrigem a vulnerabilidade garantindo que a entrada do usuário seja adequadamente desinfectada e removendo ou protegendo os arquivos de template afetados.

Concluímos nossa cibercrônica do mês abordando uma vulnerabilidade do Exchange. É possível que seus administradores tenham desfrutado de uma rara pausa de dois meses na aplicação de patches, mas este mês foi publicada a CVE-2024-21410, uma vulnerabilidade crítica de elevação de privilégios no Exchange. A Microsoft explica que um invasor poderia usar credenciais NTLM adquiridas previamente por outros meios para agir como vítima no servidor Exchange por meio de um ataque de retransmissão NTLM. Uma possível forma de aquisição dessas credenciais: uma vulnerabilidade de vazamento de credenciais NTLM no Outlook, como a CVE-2023-36761, sobre a qual a Rapid7 escreveu em setembro de 2023.

Para aumentar a preocupação dos defensores: o Exchange 2016 consta como afetado, mas ainda não há nenhum patch no aviso de CVE-2024-21410. Os patches do Exchange 2019 estão disponíveis para CU13 e a nova série CU14. De acordo com a Microsoft, as instalações do Exchange onde a Proteção Estendida para Autenticação (EPA) já está habilitada estão protegidas, embora a Microsoft recomende fortemente a instalação da última atualização acumulativa. Mais recursos são fornecidos no aviso, incluindo o guia genérico da Microsoft sobre como mitigar ataques do tipo "*Pass the Hash*", bem como o script Exchange Server Health Checker da Microsoft, que oferece uma descrição geral do estado da EPA. A série de atualizações do Exchange 2019 CU14 habilita a EPA de forma pré-determinada.

Um dia após a publicação inicial, a Microsoft atualizou o aviso da CVE-2024-21410 para indicar que, de fato, já tinham conhecimento da exploração.

Christian Agreda Romero
Cybersecurity Lead Analyst

Integração da segurança da informação nas operações diárias da Organização - O caso do DevSecOps

Por Notis Iliopoulos

A transição para a nova realidade digital, liderada por grandes programas de transformação, juntamente com a rápida mudança e adoção da tecnologia que a apoia, destaca a necessidade de implementar um dos princípios fundamentais da segurança da informação: integrar as responsabilidades de segurança em cada função de trabalho. Este artigo concentra-se em incorporar os requisitos de segurança da informação no desenvolvimento de software/sistemas e nas operações de sistemas de informação, explorando como isso pode ser alcançado por meio da adoção e implementação prática da abordagem DevSecOps.

O DevOps já foi adotado como um processo padrão com o objetivo de fechar a lacuna de colaboração entre os departamentos de desenvolvimento de software e de operações de infraestrutura de TI, visando melhorar a confiabilidade do software, otimizar o ciclo de implementação de novas versões (CI/CD) e reduzir o tempo de implementação. O processo de DevOps, servindo como precursor do DevSecOps, foi rapidamente adotado por empresas de desenvolvimento de software e organizações que dependem fortemente de sistemas e aplicativos de TI. No entanto, ficou evidente que os requisitos de segurança da informação, conformidade regulatória, proteção de dados pessoais e robustez do software (coletivamente denominados segurança da informação) devem fazer parte do processo de DevOps. Como resultado, surgiu a filosofia de DevSecOps, abrangendo todos esses aspectos críticos.

A velocidade e frequência com que novas versões de software são desenvolvidas e disponibilizadas demonstram que os métodos tradicionais de gestão de segurança da informação, proteção da privacidade e conformidade regulatória são ineficazes e obsoletos. A adoção da abordagem DevSecOps visa introduzir um novo processo que integre os requisitos de segurança da informação em todo o ciclo de vida do desenvolvimento de software, considerando também as metodologias de desenvolvimento de software Agile mais flexíveis. Este processo representa uma evolução natural do processo DevOps e tem como objetivo incorporar os requisitos de segurança da informação em cada etapa das novas metodologias ágeis de desenvolvimento de software. Portanto, os requisitos de segurança da informação fazem parte de cada ciclo de desenvolvimento (sprint) e não são abordados apenas no final deste processo, como ocorre nos métodos tradicionais.

Um princípio fundamental do processo de DevSecOps é promover uma cultura, seguida por uma metodologia de implementação relevante, onde os requisitos de segurança da informação são integrados de forma fluida nos processos de desenvolvimento, implantação e suporte de software. Por isso, as práticas atuais e antigas precisam de ajustes ou substituição para uma abordagem que se adapte facilmente para garantir a inclusão de todos os requisitos de segurança da informação em um processo repetível que se ajuste facilmente ao cenário tecnológico dinâmico atual. Levando isso em consideração, a segurança da informação deve ser considerada como um serviço fornecido em cada fase do ciclo de vida de desenvolvimento de novos produtos de software ou durante o processo de CI/CD de aplicações de software existentes. Portanto, a adaptação constante do processo, sua operação fluida e repetível e sua automação tornam-se um requisito essencial.

A seguir são apresentados os requisitos principais sobre segurança da informação para cada fase do desenvolvimento de software que devem ser incluídos no processo de DevSecOps:

Concepção e Análise: Durante a fase de concepção, a equipe de implementação identifica as necessidades de segurança da informação para cada etapa do projeto e atribui as responsabilidades pertinentes a engenheiros com as habilidades adequadas. Ao mesmo tempo é realizada uma avaliação inicial de ameaças e riscos de segurança da informação relacionados (perfil de ameaças), com o objetivo de definir os requisitos e especificações de segurança da informação para o produto final entregável (novo produto ou nova versão). Uma maneira eficaz de alcançar isso é por meio da redação e documentação do "Plano de Segurança" do produto em desenvolvimento, que inclui as ameaças de segurança da informação, possíveis vulnerabilidades e medidas de proteção propostas. Além disso, o plano deve abordar os requisitos tanto para a proteção de dados pessoais quanto para conformidade regulatória.

Concepção de Arquitetura do Produto: Adoção da filosofia "Segurança desde a Concepção", na qual cada produto ou cada nova versão do produto é projetada desde o início, levando em consideração as melhores práticas de segurança da informação, que envolvem cada componente do produto, desde o código fonte até a infraestrutura na qual será instalado e operado. Durante a concepção de arquitetura, o citado "Plano de Segurança“ serve como ferramenta principal para projetar as medidas de segurança necessárias e considerar os requisitos de conformidade regulatória relevantes.
Desenvolvimento e Revisão do Código Fonte: A preocupação principal é a melhoria contínua da qualidade, segurança e robustez do produto final através do código fonte. Para isso, é necessário capacitar continuamente os desenvolvedores em práticas de programação segura e robusta. Além da capacitação, é necessário dispor de pautas documentadas sobre segurança do código fonte, às quais os desenvolvedores devem aderir rigorosamente. Ao longo da fase de desenvolvimento do código fonte, os princípios mencionados devem ser conhecidos e implementados pelos engenheiros de software.

Revisão de Segurança de Software: A revisão periódica do código fonte gerado para identificar possíveis vulnerabilidades de segurança da informação e problemas de robustez deve ser considerada como parte das responsabilidades das equipes de desenvolvimento de software. Isso pode ser alcançado por meio de uma combinação de ferramentas automatizadas e verificações manuais, que devem fazer parte das práticas regulares de inspeção de software.

Ao contrário dos métodos tradicionais, nos quais a revisão de segurança de software é realizada no final da fase de desenvolvimento por uma equipe específica, o processo DevSecOps integra revisões de segurança ao longo da fase de desenvolvimento. Isso permite identificar e corrigir precocemente as vulnerabilidades de segurança da informação. Além disso, as organizações que adotam o processo DevSecOps devem desenvolver e aprimorar ainda mais os controles de segurança da informação relacionados ao desenvolvimento de software, devido à adoção de métodos ágeis de desenvolvimento de software que permitem a integração e implementação contínuas de novas versões de software.
Em um ambiente como esse, é necessário incluir todos os controles necessários para avaliar a segurança do novo software ou lançamento o quanto antes. As avaliações devem detectar possíveis vulnerabilidades de segurança tanto no fluxo lógico do software quanto na comunicação entre seus diferentes componentes, incluindo as interações por meio das interfaces de programação (APIs). Tais avaliações podem ser realizadas por meio do uso de ferramentas automatizadas (análise dinâmica do código fonte) e exercícios de testes de penetração. Além disso, essas avaliações devem ser incorporadas nos cenários de teste pré-definidos do produto final, garantindo uma gestão integral das avaliações e testes realizados em cada etapa.

Instalação: A implementação da nova versão de um produto de software no ambiente de produção é realizada por processos automatizados, garantindo uma implementação segura e confiável da última versão. Além disso, é fundamental reforçar o nível de segurança do ambiente de produção onde o produto é instalado, de acordo com a importância dos dados hospedados e as melhores práticas aplicáveis.
Operação: Durante a fase de operação do novo software são utilizados processos automatizados para detectar vulnerabilidades técnicas de segurança. Isso implica o uso de sistemas de monitoramento para detectar ataques maliciosos, sistemas de detecção de invasões e sistemas de varredura de vulnerabilidades de segurança. Dessa forma, aumenta-se a eficácia dos controles contra possíveis fraquezas técnicas que os invasores poderiam explorar. Ao mesmo tempo são coletadas informações em tempo real para identificar possíveis violações de segurança no ambiente de produção, incluindo aquelas relacionadas ao software. Qualquer defeito ou vulnerabilidade identificada por meio do monitoramento é comunicada aos engenheiros de operações do ambiente de produção para que seja resolvida, garantindo uma melhoria contínua, maior confiabilidade e segurança do produto.

Armadilhas que precisamos evitar
Adotar a filosofia do DevSecOps é um processo que, por si só, requer um planejamento cuidadoso e uma implementação fluida. Para melhorar sua eficácia a integração no ambiente operacional existente, recomendamos evitar alguns obstáculos importantes:

Focar exclusivamente em como automatizar partes do processo de DevSecOps: Para aproveitar plenamente as vantagens do DevSecOps, os requisitos de segurança da informação devem fazer parte de cada etapa do ciclo de vida do desenvolvimento de software. Como primeiro passo para adotar o DevSecOps, recomenda-se formar uma equipe interdepartamental de especialistas que participem ativamente e contribuam em todas as fases do ciclo de vida do desenvolvimento de software, ao mesmo tempo em que otimizam o processo adicionando a automação necessária para sustentá-lo.

Incapacidade de obter o apoio da direção: Para garantir o apoio da direção, é necessário destacar as vantagens da adoção do processo de DevSecOps. Isso inclui enfatizar a maior eficácia do processo geral de desenvolvimento e implementação de software, assim como o nível aprimorado de segurança e confiabilidade do produto ou versão.

Aplicar as práticas do DevSecOps apenas ao desenvolvimento de novos produtos: A adoção do processo de DevSecOps é facilitada durante o desenvolvimento de novos softwares. No entanto, o valor imediato para a organização pode ser obtido ao aplicá-lo a produtos de software existentes, mostrando resultados imediatos, como maximizar a flexibilidade, segurança e confiabilidade no lançamento de novos produtos. Portanto, é fundamental entender o valor agregado do novo processo e aplicá-lo como uma prioridade nas áreas que demonstrem diretamente sua utilidade.
Incapacidade ou falha em criar a cultura necessária e as habilidades relevantes: A falta ou a falha em estabelecer a cultura adequada e desenvolver as habilidades pertinentes: A implementação do processo de DevSecOps implica uma mudança cultural, onde todos os envolvidos no desenvolvimento assumem a responsabilidade pela segurança da informação, confiabilidade e robustez, em vez de delegá-la a uma equipe específica. Além disso, a formação e o desenvolvimento das habilidades necessárias são cruciais para o sucesso global da adoção do DevSecOps.

Adoção efetiva e evolução do processo de DevSecOps
A principal mudança que impacta a maneira atual de trabalhar é estabelecer uma equipe de trabalho interdepartamental horizontal. Esta equipe será composta por profissionais com diferentes habilidades que geralmente trabalham em unidades organizacionais distintas, focados verticalmente em áreas específicas de experiência. Isso implica a necessidade de eliminar os silos organizacionais. Além disso, requer o desmantelamento dos silos organizacionais que, tradicionalmente, separam diferentes equipes e departamentos dentro de uma organização. É necessário criar uma unidade organizacional permanente ou uma equipe virtual multifuncional de DevSecOps composta por profissionais com habilidades específicas de diferentes departamentos.

Claramente, a mudança mais significativa que uma organização deve experimentar é a cultural. Isso abrange a operação, o nível de agilidade e os serviços que o processo DevSecOps pretende oferecer. Portanto, a organização precisa identificar aqueles que podem contribuir e promover essa mudança em termos de mentalidade e forma de trabalhar, e designá-los como membros-chave do processo DevSecOps. Isso levará à formação e operação de uma equipe multifuncional, seja como uma entidade completamente autônoma ou uma força-tarefa virtual. O objetivo principal é transferir todo o conhecimento adquirido em toda a organização, garantindo que a segurança da informação se torne uma parte integral da concepção e desenvolvimento de novos produtos de software e novas versões.

As equipes DevSecOps, sejam autônomas ou virtuais, devem ser compostas por engenheiros com habilidades diversas, capazes não apenas em suas áreas de experiência, mas também de enriquecer continuamente suas capacidades. Isso lhes permite executar de maneira eficaz uma variedade de tarefas interconectadas dentro do desenvolvimento de um novo produto ou uma nova versão de software. Tais tarefas incluem o desenvolvimento de software, a implementação e otimização de controles de segurança da informação, e a manutenção e suporte da infraestrutura de TI. Cada membro da equipe é responsável pela segurança e confiabilidade do produto, seja para clientes externos ou uso interno.

O processo DevSecOps, desde sua fase inicial, deve servir como um marco robusto, oferecendo serviços e criando metodologias, procedimentos e ferramentas que possam ser utilizados com ou sem a participação dos membros da equipe DevSecOps. Ao mesmo tempo, os membros da equipe DevSecOps devem aprimorar a eficácia dos serviços e ferramentas que utilizam, além de capacitar e orientar outros engenheiros sobre segurança da informação, robustez e confiabilidade do software.

Conclusão

O DevSecOps é regido por uma nova filosofia que leva a uma nova abordagem no desenvolvimento de novos produtos e novas versões de software. Na maioria dos casos, não é necessário criar uma unidade organizacional específica dedicada às atividades de DevSecOps. A eficácia da nova filosofia/processo é maximizada quando se torna uma maneira convencional de trabalhar e é integrada como parte padrão da cultura em relação ao desenvolvimento de novos produtos e lançamentos de software.

De acordo com previsões e tendências recentes, há uma adoção mais ampla da filosofia que transformará o DevSecOps em BizDevSecOps. Esta é uma nova abordagem para o desenvolvimento de produtos de software que elimina as fronteiras entre o mundo empresarial e as equipes técnicas, com o objetivo de capacitar as empresas para construir produtos de software mais rápidos e confiáveis, adaptados às necessidades do usuário final.

Notis Iliopoulos
Senior Manager
Cybersecurity EMEAL

Aplicações seguras em um sistema de gerenciamento (IAM)

Por Mijail Muñoz

Na segurança de aplicações, uma linha-chave é o Gerenciamento de Identidade e Acesso. Um dos focos dos invasores é o roubo da identidade do usuário, para realizar operações fraudulentas. Contra isso, a conscientização de todos os funcionários deve ser uma das principais estratégias de cibersegurança em uma organização.

Atualmente, existem vários fatores de ataque ao usuário de uma organização. Constam a seguir alguns dos mais conhecidos:

• Phishing: Ataque ao usuário por meio de um e-mail.
• Ransomware: Software malicioso que torna o dispositivo inutilizável e criptografa as informações.
• Spyware: Programa que se instala no computador e coleta informações do usuário.
• Trojan: Malware que pode ser veículo de transmissão de um vírus usado para espionagem, roubo de dados ou tomada de controle do dispositivo.
• Injeção SQL: Tipo de ciberataque que afeta os servidores das empresas, infectando-os e extraindo informações relevantes, como dados de clientes, contas bancárias e senhas.
• Negação de Serviço (DoS): Seu objetivo é sobrecarregar o servidor de um site para torná-lo inutilizável.

A implementação de aplicações seguras em um sistema IAM contribui para fortalecer a segurança, garantir conformidade com regulamentações e melhorar a eficiência na gestão de identidades e acessos.
É importante manter-se atualizado com as melhores práticas de segurança e ajustar as políticas conforme os riscos e as necessidades organizacionais evoluem.
Para garantir a segurança em um sistema de gestão IAM (Identity and Access Management), é importante utilizar aplicações que atendam às melhores práticas de segurança. Especialmente, deve-se garantir que os aplicativos possuam:

1. Provisionamento e Desprovisionamento Automatizado
Automatizar a criação, modificação e remoção de contas de usuário ajuda a evitar erros humanos e garante consistência na aplicação de políticas de segurança.

2. Controle de Acesso Baseado em Funções (RBAC)
O uso de modelos de RBAC garante que os usuários tenham acesso apenas aos recursos e dados necessários para realizar suas funções específicas. Isso minimiza os riscos associados ao acesso desnecessário.

3. Monitoramento das Atividades do Usuário
Registrar e monitorar as atividades dos usuários ajuda a detectar comportamentos incomuns ou atividades maliciosas. Isso é crucial para estar em conformidade com regulamentações de segurança e responder rapidamente a ameaças.

4. Autenticação Multifatorial (MFA)
Implementar uma MFA adiciona uma camada adicional de segurança ao exigir mais de uma forma de autenticação. Isso reduz significativamente o risco de acesso não autorizado, mesmo se as credenciais do usuário forem comprometidas.

5. Gestão de Senhas
Implementar políticas de senha fortes e utilizar ferramentas de gestão de senhas pode melhorar a segurança sem sacrificar a usabilidade.

6. Federação de Identidade
Permite que os usuários acessem vários sistemas e aplicativos com uma única identidade, reduzindo a necessidade de gerenciar múltiplas credenciais. Isso também pode melhorar a segurança ao centralizar a autenticação.

7. Auditorias e Relatórios
Realizar auditorias periódicas e gerar relatórios detalhados sobre as atividades dos usuários e as alterações nos privilégios ajuda a cumprir os requisitos de conformidade e a identificar possíveis problemas de segurança.

8. Gestão de Sessões
Monitorar e gerenciar as sessões de usuário pode prevenir o acesso não autorizado, especialmente em ambientes sensíveis. A implementação de encerramento automático de sessão após períodos de inatividade também é recomendável.

9. Automatização de Políticas de Acesso
Automatizar a aplicação e atualização de políticas de acesso ajuda a garantir que as mudanças sejam feitas de forma consistente e oportuna, reduzindo o risco de configurações incorretas.

10. Criptografia de Dados:
Implementar a criptografia para proteger dados confidenciais, tanto em repouso quanto em trânsito, garantindo que apenas os usuários autorizados possam acessar a informação sensível.

11. Gestão de Identidade na Nuvem
Caso serviços em nuvem sejam utilizados, é essencial gerenciar de forma segura as identidades e acessos, adaptando-se aos modelos de segurança específicos da nuvem.

A cibersegurança é um campo em constante evolução, por isso é fundamental estar atualizado sobre as últimas tendências, ameaças e soluções em IAM. Por essa razão, é recomendável que as empresas realizem um Assessment IAM das Unidades Organizacionais ou das aplicações de forma periódica, com o propósito de encontrar pontos de melhoria nos 6 domínios (Gestão de contas, Gestão de Autenticação, Gestão de Políticas e Procedimentos, Gestão de funções e permissões, Gestão do sistema IAM e Gestão de contas privilegiadas) e adaptar seu sistema de controle de acessos e de identidade tanto para novas ameaças quanto para a evolução que a organização teve desde o último assessment.

Mijail Muñoz
Cybersecurity IAM Leader

IA: Além da industrialização das tarefas de segurança no ciclo de vida do desenvolvimento de software.

A integração da Inteligência Artificial na indústria do desenvolvimento de software é uma realidade que veio para ficar. Atualmente, são muitos os fornecedores que competem para serem os primeiros a introduzir a IA na detecção e correção automática de vulnerabilidades nos ciclos de vida do desenvolvimento de software de seus clientes.

A disrupção da Inteligência Artificial no mercado de desenvolvimento de software está causando uma mudança na maneira como as organizações tendem a industrializar seus testes de qualidade e segurança durante o ciclo de vida de desenvolvimento de software (doravante SDLC).

São muitos os usos que estão sendo dados à IA, com propósitos mais ou menos lícitos, o que abriu o debate sobre a necessidade de regulamentação dessa muito recente tecnologia. De qualquer forma, a ampla variedade de opções fornecidas pelas diferentes aplicações de IA se traduz em alternativas interessantes para a criação de ferramentas sob o ponto de vista da cibersegurança.

Embora atualmente a cibersegurança dependa amplamente das contribuições humanas, gradualmente vemos que a tecnologia está se tornando melhor do que nós em tarefas específicas, por isso está começando a integrar a IA com diferentes propósitos:

• Detecção e alerta automático de ataques em tempo real.
• Proteção de dados em ambientes híbridos (Legacy e/ou Cloud)
• Classificação automática de vulnerabilidades e atribuição de risco por meio de aprendizado de máquina (*machine learning*).
• Identificação de práticas de segurança inadequadas durante o desenvolvimento.
• Fornecimento de recomendações de segurança para a correção de vulnerabilidades ou defeitos.
• Identificação de requisitos de segurança.
• E tantos outros propósitos que se possam imaginar.

No que diz respeito ao SDLC, as organizações estão explorando diferentes maneiras de automatizar as tarefas nas diferentes fases:
1) Requisitos.
2) Concepção.
3) Implementação/desenvolvimento.
4) Teste e verificação.
5) Implantação.
6) Operação.

As alternativas proporcionadas pela IA em termos de ferramentas automáticas estão impulsionando um grande avanço também nos ambientes SecDevOps, levando à evolução do que hoje conhecemos como ferramentas AST (*Application Security Testing*). Essas ferramentas estão começando a substituir seus motores de busca pela IA, dotando-as de melhor desempenho cognitivo, com o objetivo de detectar defeitos e vulnerabilidades nas diferentes fases do SSDLC. Cada vez mais fornecedores de ferramentas AST estão desenvolvendo módulos de integração com o ChatGPT ou desenvolvendo sua própria IA, aproveitando o poder que essa tecnologia oferece. Graças à IA, não é necessário desenvolver motores de regras e/ou políticas para detectar padrões ou fluxos no código, pois a própria base de dados da IA responderá aos defeitos que possam ser encontrados no código, na aplicação em execução ou nos ambientes.
Portanto, a direção que a indústria de automação parece estar seguindo é o desenvolvimento de módulos simples que consultem a IA, deixando para ela as tarefas complexas de decisão e potência cognitiva. Esses módulos funcionarão como APIs, traduzindo as diferentes consultas para uma linguagem reconhecida pela IA que estejamos utilizando. Dessa forma, seremos capazes de abranger os testes de segurança em todas as fases do SDLC, utilizando:

• Módulos que consultem a IA para estabelecer os requisitos de segurança do software a ser concebido com base em uma série de parâmetros determinados pelas necessidades a serem cumpridas (tecnologias a serem usadas, linguagens, bibliotecas, componentes, ambientes, plataformas, integrações etc.)
• Integrações com o IDE para detectar defeitos durante o desenvolvimento, marcando-os em tempo real e fornecendo aos desenvolvedores alternativas para resolvê-los.
• Módulos de Identificação de melhorias a serem implementadas no próprio SDLC com base nos erros, vulnerabilidades, descobertas ou defeitos mais recorrentes.

• Iniciativas de conscientização e/ou treinamento para desenvolvedores, com base nas tecnologias usadas e nos defeitos e vulnerabilidades encontrados.
• Desenvolvimento de ferramentas para consulta de vulnerabilidades em código, bibliotecas ou durante a execução.
• Módulos de detecção automática de assinaturas de malware e resposta automática a incidentes.
• Previsão de ataques com base nos comportamentos do software ou sistemas.
• Automatização da categorização de eventos, alertas e/ou vulnerabilidades.
• E uma infinidade de outras necessidades ainda não atendidas pelas organizações, que podem ser abordadas por meio do desenvolvimento de um simples módulo que realize a tradução de uma consulta para a IA.

Estamos convencidos de que essas integrações das ferramentas AST com a IA trarão uma maior eficiência às tarefas de revisão de segurança no software, resultando em uma grande economia de custos. Observando sua trajetória, a IA provavelmente reduzirá os "Falsos Positivos ou Falsos Negativos" nas descobertas, bem como a fadiga de alertas e eventos. Além disso, está permitindo melhorar os processos de categorização e classificação dessas descobertas de forma automática, o que, por sua vez, repercute na agilidade das tarefas de desenvolvimento seguro de software.

No entanto, apesar da potência que a IA moderna está começando a demonstrar, ainda não é capaz de interpretar os resultados com as mesmas habilidades que um ser humano, então não devemos deixar de revisar esses resultados em busca de possíveis "Falsos Positivos ou Falsos Negativos". Nesse sentido, as equipes de segurança não devem temer serem substituídas por uma IA (pelo menos por enquanto), pois as equipes humanas continuarão sendo necessárias para a operação, revisão de resultados e tomada de decisões "criativas". No entanto, como é comum no campo da cibersegurança, o verdadeiro desafio será continuar se inovando, investindo para se manter atualizado nas novas tendências do mercado e no futuro da tecnologia. O setor precisa de mais especialistas em cibersegurança capacitados em IA, capazes de inovar na integração de ambos os mundos e obter o desempenho diferencial esperado dessa tecnologia.

Na NTT DATA estamos convencidos de que a integração da IA nos ambientes SecDevOps é uma realidade que ainda está se formando, pois, embora esteja sendo trabalhada atualmente, a IA ainda não alcançou seu pleno potencial, sendo uma ferramenta muito poderosa, porém que precisa se estabilizar para inspirar confiança.

A IA também está amadurecendo, estabelecendo ambientes de confiança, modelos fechados que não compartilham dados e permitirão uma maior privacidade, o que fará com que a IA amadureça e possamos finalmente incluí-la em ambientes industrializados e de produção.

Estamos trilhando um caminho que parece emocionante e motivador para aqueles que trabalham em empresas de tecnologia. Em um momento em que a evolução para Cloud é prioritária, juntamente com a automação e industrialização, revolucionadas pelo poder cognitivo da IA. Sob esta perspectiva, as equipes de segurança terão que dar o máximo para lidar com o novo paradigma, mas... quem disse que temos medo?

Jose Carlos Moral Cuevas
Chief of Security Architecture
Area & Technical Manager

Aumentando a segurança das aplicações através de Security Chaos Engineering

Tendências

É provável que todas as aplicações existentes no mundo tenham enfrentado algum tipo de falha que tenha causado problemas para mais de uma pessoa. Em 2011, a Netflix introduziu o conceito de caos em seus sistemas para testar sua resiliência; ao desligar aleatoriamente instâncias do EC2 na AWS, conseguiram determinar que seus balanceadores de carga não funcionavam com eficiência. Hoje, essa poderosa ideia foi transferida para a cibersegurança, oferecendo uma perspectiva inovadora para descobrir vulnerabilidades nas aplicações.

A Security Chaos Engineering consiste em introduzir deliberadamente falhas de segurança nas aplicações com o objetivo de analisar o comportamento de seus componentes. Este conceito representa uma mudança na forma como a segurança de um sistema é auditada, permitindo a identificação de cenários de risco que não são facilmente detectáveis.
Atualmente, a produtividade do ciclo de vida do software tem se baseado em práticas DevOps, onde a construção e entrega rápida de funcionalidades são fundamentais para garantir a transformação digital. Além disso, a segurança tem sido aprimorada pela integração de ferramentas de análise estática e dinâmica, que permitem identificar vulnerabilidades rapidamente.

No entanto, uma confiança excessiva nas ferramentas pode ser contraproducente, especialmente quando os motores de varredura não são robustos o suficiente ou quando as equipes de desenvolvimento podem manipular as configurações. É aí que o Hacking Ético continua desempenhando um papel fundamental na descoberta de brechas que não podem ser identificadas por meio da automação.

Então, se existem ferramentas automatizadas de segurança e Hacking Ético para testar as aplicações, qual é a contribuição da Security Chaos Engineering? O poder desse conceito reside em sua metodologia, pois se baseia na descoberta de vulnerabilidades por meio de metodologia científica. Da mesma forma que Pasteur descobriu a penicilina, através da observação de um evento, formulação de uma hipótese e execução de um experimento, é possível descobrir novos cenários de risco nas aplicações.

Imagine o seguinte cenário: a conta de um desenvolvedor de software foi comprometida por um invasor devido a credenciais fracas e à ausência de autenticação de múltiplos fatores; o invasor tem a intenção de infectar os repositórios das aplicações com código malicioso para obter acesso aos servidores da organização. Será que o ecossistema DevOps (processos, ferramentas e pessoas) será capaz de detectar, prevenir e mitigar esse tipo de vetor de ataque?
A SolarWinds presumia que sim, no entanto, sua ferramenta de análise estática não detectou o código malicioso, seus stakeholders não alertaram sobre os desenvolvedores autopromovendo código para os ramos principais, também não foram detectadas variações injustificadas no desempenho de seus servidores, muito menos o tráfego de pacotes não convencionais em sua rede. Isso desencadeou o Supply Chain Attack com o maior impacto das últimas décadas, afetando mais de 20.000 empresas em todo o mundo.

A Security Chaos Engineering oferece a possibilidade de injetar falhas de segurança no código-fonte, em bibliotecas, servidores e até mesmo na própria arquitetura de solução de um sistema, a fim de determinar se a organização está preparada para ataques direcionados. Além disso, a Security Chaos Engineering promove a automação, portanto, idealmente, as hipóteses, a observabilidade e os experimentos podem ser automatizados por meio de scripts para serem testados em diferentes aplicações e cenários.
Com o aumento da transformação digital, os ciberataques estão se tornando cada vez mais sofisticados e exigem novos mecanismos de proteção e prevenção. A Security Chaos Engineering surge como um paradigma inovador que permite desafiar a segurança dos sistemas e, assim, contribuir para manter um ecossistema tecnológico resiliente e seguro.

Vulnerabilidades

Vulnerabilidade de injeção de código no PostgreSQL.

Data: 6 de março de 2024
CVE: CVE-2024-27304

CVSS: 9.8

CRÍTICA

Descrição
Pgx é uma biblioteca para Go projetada para interagir com bancos de dados PostgreSQL. O risco de segurança identificado consiste na possibilidade de injeção de código SQL quando um invasor consegue fazer com que uma consulta ou mensagem de ligação [*bind message*] exceda 4 GB de tamanho.

Este problema é decorrente de um estouro de inteiros no cálculo do tamanho, permitindo que uma mensagem de grandes dimensões seja dividida em várias mensagens sob o controle do invasor.

O fabricante orientou os usuários a atualizarem para a versão mais recente para corrigir essa vulnerabilidade. Além disso, propõe-se como medida temporária a rejeição de solicitações que excedam um determinado tamanho.

Produtos afetados
A vulnerabilidade afeta o produto PGX, especificamente as seguintes versões:

- Versões anteriores à 4.18.2.
- Versões compreendidas entre a 5.0.0 e a 5.5.3 (ambas inclusive).

Solução
Recomenda-se que os usuários atualizem para as versões 4.18.2 ou 5.5.4 para se protegerem contra possíveis ataques.

Além disso, também é recomendado que rejeitem qualquer entrada do usuário que possa resultar em uma única consulta ou mensagem de ligação que exceda 4 GB de tamanho, mitigando assim o risco de exploração dessa vulnerabilidade.

Referências
- www.incibe.es
- nvd.nist.gov

Vulnerabilidade de escalonamento de privilégios no Microsoft AKS

Data: 12 de março de 2024
CVE: CVE-2024-21400

CVSS: 9

CRÍTICA

Descrição
Microsoft Azure Kubernetes Service (AKS) é um serviço de gerenciamento da Microsoft Azure que permite aos usuários implementar, gerenciar e dimensionar facilmente clusters de contêineres baseados em Kubernetes na nuvem da Azure.

A vulnerabilidade CVE-2024-21400 consiste em uma elevação de privilégios no contêiner oficial do serviço Microsoft Azure Kubernetes. Essa vulnerabilidade permite que os invasores obtenham acesso não autorizado a recursos protegidos dentro de um cluster Kubernetes. Isso poderia levar à manipulação de dados confidenciais, interrupção do serviço ou até comprometimento total do cluster.

Produtos afetados
A vulnerabilidade afeta o produto Microsoft Azure Kubernetes Service, especificamente as seguintes versões:

- Versões anteriores à 0.3.3.
- Desde a versão 1.0.0 está inclusa.

Solução
Recomenda-se atualizar para a versão mais recente para corrigir erros.

Esta atualização será realizada através do uptade da extensão *confcom* usando a seguinte interface de linha de comando:

- `az extension update -n confcom`

Referências
- www.incibe.es
- www.msrc.microsoft.com

Patches

CRÍTICA

Novo patche de segurança para JetBrains TeamCity

Data: 4 de março de 2024
CVE: CVE-2024-27198 e mais 3

Descrição
A JetBrains publicou uma série de atualizações de segurança para resolver vários problemas que afetam o produto TeamCity. A atualização corrige um total de 4 vulnerabilidades, uma delas de gravidade crítica, outra de gravidade alta e duas de gravidade média.

A vulnerabilidade crítica (CVE-2024-27198) permite aos usuários omitir o processo de autenticação, concedendo-lhes acesso não autorizado para realizar ações de administração. Essa brecha de segurança permitia que qualquer pessoa executasse tarefas de administração sem a necessidade de autenticação.

As demais vulnerabilidades corrigidas são:

- CVE-2024-27199 (alta): vulnerabilidade de *path traversal*.
- CVE-2024-28173 (média): vulnerabilidade nos campos do tipo *password*.
- CVE-2024-28174 (média): autorização incorreta de URLs de acesso a S3.

Produtos afetados
Esta vulnerabilidade afeta o produto TeamCity em versões anteriores à 2023.11.4. A JetBrains organiza suas versões com base na data, então será possível observar de forma intuitiva se você tem uma versão anterior à necessária.

Solução
A JetBrains recomenda atualizar para a versão 2023.11.4 do produto, que contém os patches necessários para mitigar as vulnerabilidades descritas.

Referências
- nvd.nist.gov
- www.jetbrains.com

ALTA

Novos patches para os sistemas operacionais da Apple

Data: 5 de março de 2024
CVE: CVE-2024-23225 e mais 1

Descrição
A Apple lançou atualizações de segurança de emergência que corrigem duas vulnerabilidades de dia zero no iOS, identificadas como CVE-2024-23225 e CVE-2024-23296, as quais foram exploradas em ataques direcionados a dispositivos iPhone.

As CVE-2024-23225 e CVE-2024-23296 são duas vulnerabilidades de corrupção de memória que afetam os sistemas operacionais iOS e iPadOS. A exploração dessas vulnerabilidades permitiria a um invasor, com capacidade arbitrária de leitura e escrita no kernel, contornar as proteções de memória do mesmo.

Dessa forma, a CVE-2024-23225 consiste em uma falha de corrupção de memória do kernel, enquanto a CVE-2024-23296 é uma falha de corrupção de memória RTKit.

Produtos afetados
As vulnerabilidades afetam os seguintes dispositivos:

- iPhone XS e posteriores.
- iPad Pro de 12,9 polegadas de 2.ª geração e posteriores.
- iPad Pro de 10,5 polegadas.
- iPad Pro de 11 polegadas de 1.ª geração e posteriores.
- iPad Air de 3.ª geração e posteriores.
- iPad de 6.ª geração e posteriores.
- iPad mini de 5.ª geração e posteriores.

Solução
A Apple recomenda atualizar seus dispositivos para as versões iOS 17.4, iPad 17.4, iOS 16.7.6 e iPad 16.7.6, corrigindo um problema de corrupção de memória por meio da melhoria da validação.

Referências
- support.apple.com
- securityaffairs.com

Eventos

IV JORNADAS STIC & CONGRESSO ROOTED_CON (10 a 12 ABRIL)

Os dois eventos de referência no setor de cibersegurança na Espanha, as Jornadas STIC e o Congresso RootedCON, uniram esforços para organizar em conjunto um novo capítulo internacional de seus encontros, desta vez no Panamá, de 10 a 12 de abril de 2024. Ambos escolheram a cidade panamenha como local estratégico para realizar o maior evento de cibersegurança da América Latina
Link

I JORNADA CIBERLEGAL (23 ABRIL)

A Red Seguridad realizará, no Ilustre Colégio de Advogados de Madri, em 23 de abril, a primeira Jornada Ciberlegal. Um evento bastante inovador, cujo objetivo principal é conhecer em primeira mão os desafios que a cibersegurança impõe tanto à Administração Judiciária (juízes, promotores...) e Autoridades de Segurança quanto aos profissionais da área de Direito (advogados, procuradores etc.) e aos departamentos jurídicos das organizações.
Link

ASLAN 2024 (17-18 ABRIL)

A 31ª edição do Congresso & Expo Aslan 2024 já está em andamento, com o tema "Um grande avanço na digitalização". Organizado pela associação @aslan, o congresso explorará a inteligência artificial (IA) nos processos de transformação digital das organizações. E acontecerá nos dias 17 e 18 de abril de 2024 no Palácio Municipal de Congressos Ifema, em Madri.
Link

MUNDO HACKER 2024 (22 – ABRIL)

No Mundo Hacker Day, mais de 30 especialistas abordarão alguns dos diversos temas relevantes no mundo da cibersegurança. Além disso, os participantes terão a oportunidade não apenas de compartilhar conhecimento e experiências, mas também de promover o networking.
Link

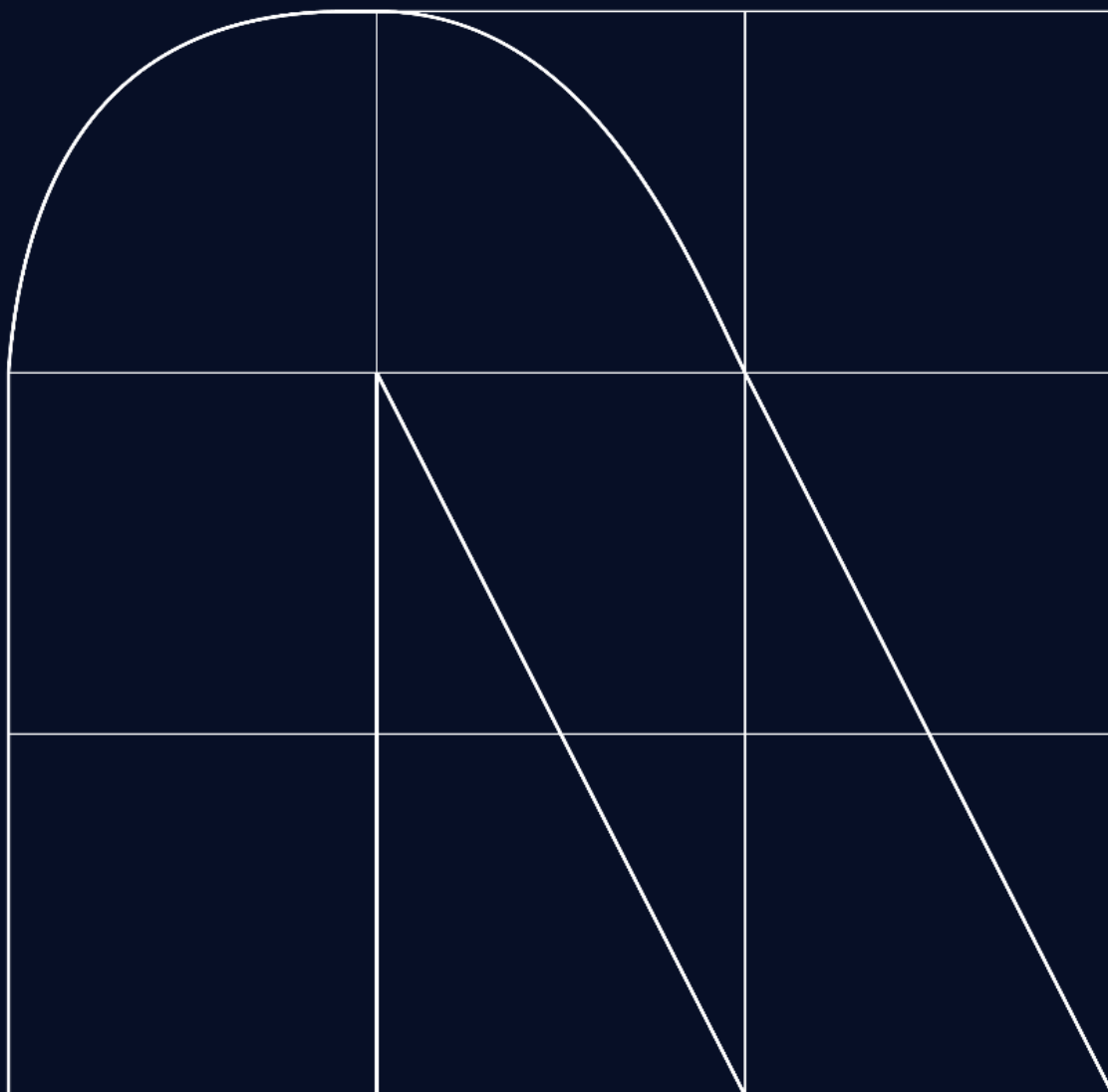
Recursos

Kali Linux 2024.1
A novidade de destaque do Kali Linux 2024.1 não está relacionada ao sistema operacional, mas sim à infraestrutura, pois a distribuição apresentou a CDN Micro Mirror, que é "uma rede de espelhos (*mirrors*) dedicados a servir Linux e Software Livre. Ao contrário dos espelhos tradicionais que hospedam cerca de 50 TB de arquivos de projetos, os Micro Mirrors são máquinas com 'apenas' alguns terabytes de armazenamento que se concentram em hospedar apenas os projetos de maior demanda.
Link

SORA
OpenAI, a empresa pioneira em inteligência artificial generativa, apresentou o Sora, um modelo revolucionário que transforma descrições textuais em cenas de vídeo realistas. O Sora é capaz de criar cenas complexas com múltiplos personagens e movimentos específicos, incluindo detalhes tanto do componente principal quanto do cenário. O modelo compreende como os objetos interagem no mundo físico e gera personagens convincentes que expressam emoções vibrantes.
Link

Tendências de cibersegurança 2024
Conheça as Tendências em Cibersegurança de maior impacto para 2024 de vários analistas como Gartner, Google, Forrester, IDC e SealPath. Este artigo reúne previsões futuras e tem como objetivo ajudá-lo a combater as ameaças cibernéticas em 2024 e a ficar atualizado sobre as últimas tendências para melhorar sua capacidade de resposta e adaptação.
Link

Ciber-Cluedo
O Centro Criptológico Nacional (CCN), vinculado ao Centro Nacional de Inteligência, desenvolveu uma nova ferramenta educacional para conscientização sobre phishing. O "Ciber-Cluedo" agora faz parte da seção de gamificação de "Ángeles". Seu objetivo principal é promover o aprendizado sobre ameaças de cibersegurança, identificar os riscos associados a roubo de identidade e implementar medidas de segurança adequadas para uma melhor proteção contra esse tipo de ataques.
Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com