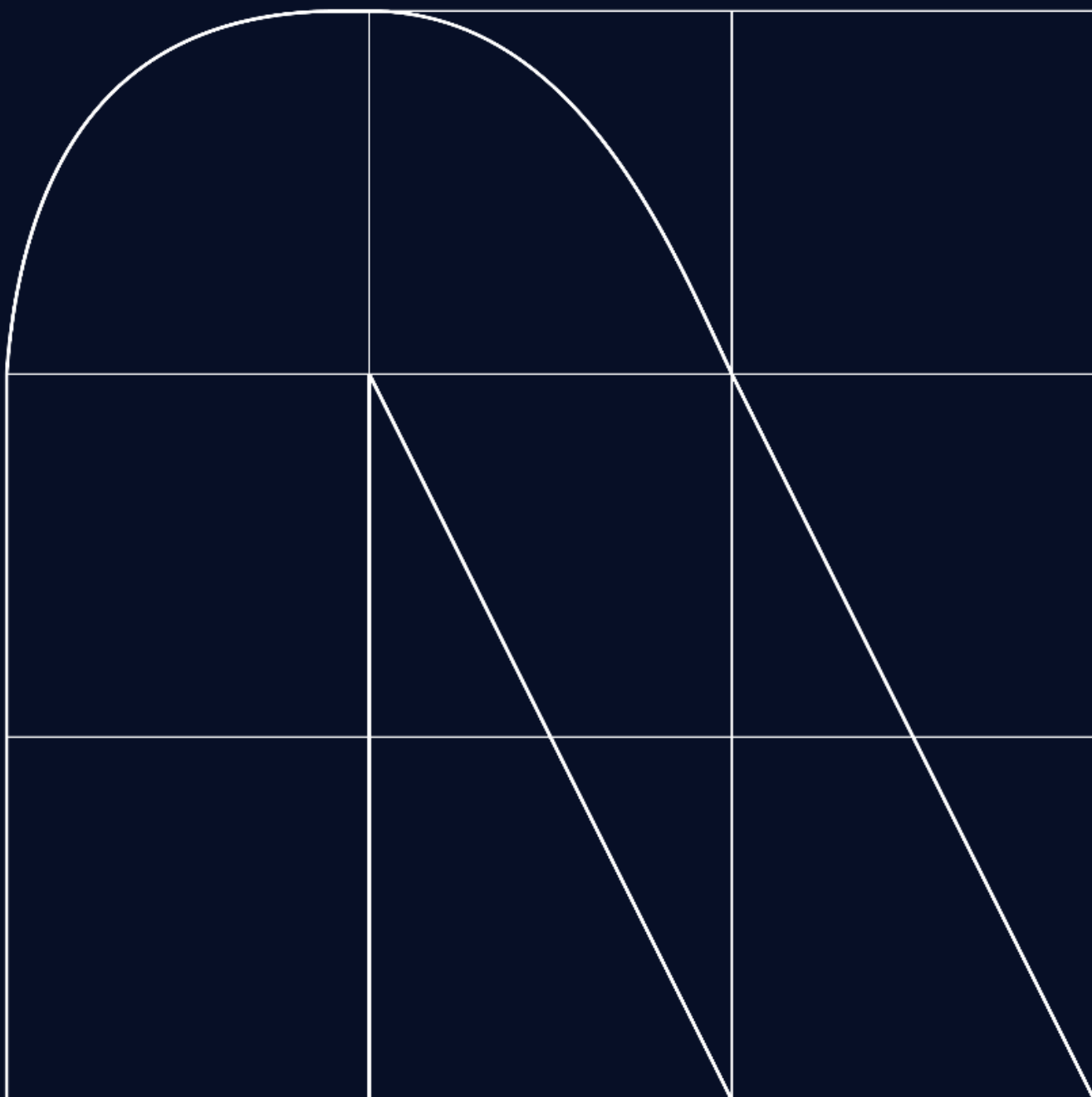
Número 87 | Fevereiro 2024

NTT DATA

Radar

A magazine de cibersegurança



A importância de saber quem é o inimigo (quem está por trás)

EDITORIAL por Jose Manuel Moreno

Empresas e organizações enfrentam a cada ano um número crescente de ataques, com um aumento no nível de sofisticação, causando danos significativos tanto econômicos quanto operacionais, assim como na reputação. As pessoas ou grupos que realizam esses tipos de ataques geralmente têm objetivos claros ao executá-los, bem como sabem quais serão as suas vítimas ou grupos de vítimas (setores ou indústrias).

No relatório sobre Ciberameaças e Tendências de 2023 publicado pelo CCN-CERT no último mês de novembro, destacou-se o aumento da sofisticação dos invasores e grupos de ameaças, a utilização de novas famílias de *malware* e a evolução dos artefatos usados para realizar tais ataques.

Os ataques de ransomware continuam sendo os mais numerosos, principalmente devido ao retorno, especialmente financeiro, que os grupos de ameaças obtêm com eles. De acordo com o relatório "Cost of a Data Breach" da IBM, o prejuízo financeiro médio no último ano desses ataques aumentou 144% em relação a 2022. Os grupos de ameaças que mais executaram ataques desse tipo foram LockBit 3.0, BlackCat (ALPHV), Hive, Conti e REvil.

Quando temos que enfrentar o desafio de proteger nossas organizações, é crucial saber quem é o inimigo, quem está por trás desses ataques. A realidade é que nem todos os grupos de ameaças têm os mesmos objetivos, nem usam as mesmas técnicas e táticas, e é aqui que a inteligência ou *Threat Intelligence* ganha maior relevância.

O que a *Threat Intelligence* nos oferece e como tirar vantagem sobre o oponente?
Os serviços de *Threat Intelligence* têm como objetivo permitir que uma organização obtenha a maior quantidade de informações possível sobre a situação de cibersegurança, identificar os grupos de ameaças que possam atacar a organização, conhecer as táticas, técnicas e procedimentos (TTP) utilizados por esses invasores e, na medida do possível, rastrear iterativamente os ataques realizados por esses grupos contra qualquer organização no mundo.

No entanto, uma vez obtida toda essa informação, o que fazemos com ela? Os dados por si só não permitem melhorar ou aumentar a resiliência de nossa organização. É por isso que existem outros serviços preventivos que têm como ponto de partida a *Threat Intelligence*.

- ***Threat Hunting*** é um serviço preventivo que visa analisar de maneira ativa os registros das principais linhas de defesa de uma organização buscando qualquer indício de atividade suspeita. Para isso, utiliza informações de inteligência, identificando os principais invasores e seus rastros, a fim de procurar essas evidências em nossos registros de segurança (principalmente no SIEM). Esse serviço proativo pode, portanto, identificar precocemente a presença desses grupos em nossos sistemas e ativar níveis específicos de proteção para nos proteger deles.

- ***Detection Rules*** é outro serviço preventivo que permite aumentar a resiliência de nossa organização criando ou implementando regras de detecção adicionais que permitam identificar a presença ou tentativa dela por parte de grupos de ameaças contra nossa organização. Para isso, a equipe de *Threat Intelligence* deve fornecer o máximo de informações possível sobre qual *malware*, *exploit* ou vulnerabilidades nossos inimigos estão usando, para que este serviço seja capaz de criar sistemas de detecção precisos.

- ***Adversary Simulation*** é um serviço que visa simular o comportamento desses grupos de ameaças contra nossa organização. Trata-se de um exercício essencialmente equivalente a um Red Team, mas surge com o objetivo de imitar a atuação de um grupo de ameaças contra nossa própria organização. Terá como meta utilizar, na medida do possível, as mesmas TTP que os grupos de ameaças e utilizar as ferramentas e *exploits* mais usados pelos grupos "imitados". Este serviço possui um valor significativo para proteger nossa organização e avaliar o nível de resiliência dela contra esses invasores.

Como podemos observar, a evolução e o grau de sofisticação dos nossos inimigos nos obrigam a conhecê-los com o maior detalhe possível e utilizar essa informação para aumentar o nível de resiliência da nossa organização.

José Manuel Moreno
Cybersecurity Director

Especialistas alertam para o perigo iminente de *phishing* gerado por IA

Cibercrônica por Adrián Álvarez Sánchez e Pablo García Díaz

Por isso, empresas como a Trend Micro constantemente alertam sobre os perigos dos grandes modelos de linguagem. Isso porque eles não apenas são capazes de realizar golpes em larga escala de forma simultânea, mas também de gerar empatia e confiança entre as possíveis vítimas. Essa capacidade de automatizar e personalizar ataques os torna ainda mais perigosos e difíceis de detectar.

A Orange sofreu um ataque cibernético, a senha em questão era "ripeadmin" e era tão simples que qualquer pessoa poderia adivinhá-la. O invasor conseguiu acessar a conta como administrador e realizar alterações na tabela de roteamento global, impedindo que os clientes da Orange se conectassem à Internet.

Sancho Lerena, CEO da empresa de gestão de TI e segurança Pandora FMS, considera que "o nível de cibersegurança na Espanha continua sendo inferior ao necessário" e ataques cibernéticos, como o ocorrido na Orange e o sofrido pela Vodafone no ano passado, demonstram isso.

Como era de se esperar, o ataque teve um impacto significativo nos usuários da Orange, pois muitos deles enfrentaram problemas de conectividade, incluindo dificuldades para acessar sites, aplicativos e serviços de voz e dados.

Por outro lado, a empresa de telefonia Tigo relatou um incidente de cibersegurança que afeta o fornecimento normal de alguns serviços específicos a um grupo limitado de clientes no segmento corporativo, mas não afeta nenhum outro serviço em massa ou corporativo de telefonia, internet ou carteira digital.
Um ataque cibernético conseguiu penetrar nos sistemas de informação do Carrefour Soluções Financeiras e extrair informações pessoais de seus clientes. Conforme comunicado pela empresa, as informações roubadas incluem "dados pessoais básicos, de contato, número de identidade, entre outros dados".

Informações como as que foram roubadas da financeira do Carrefour são consideradas muito sensíveis para a cibersegurança pessoal.

Possuir essa informação não habilita um invasor a retirar dinheiro diretamente da conta bancária da vítima ou fazer compras em seu nome sem consentimento, mas facilita enormemente o roubo de identidade e golpes. Atualmente, existem várias campanhas de ataques desse tipo em andamento na Espanha.

Descobriu-se que certas versões do org.apache.struts:struts2-core são vulneráveis à execução remota de código (RCE) através da manipulação dos parâmetros de carregamento de arquivos, que possibilitam a realização de um "path traversal" (CVE-2023-50164). Sob condições específicas, é possível fazer o *upload* de um arquivo malicioso que pode ser executado no servidor. Diante de situações como essa, enfatizamos que se deve testar e sanitizar todas as entradas no servidor antes de adicioná-las às aplicações em produção.

O Discord-Recon é um bot criado para reconhecimento de *bug bounty*, varreduras automáticas e coleta de informações por meio de um servidor do Discord. Um invasor poderia executar comandos de Shell no servidor sem ser o administrador. Os desenvolvedores já tomaram medidas e conseguiram mitigar essa vulnerabilidade na versão 0.0.8 do bot.
Isso destaca a importância de não usar ferramentas ou programas de fontes não seguras e que não tenham passado por determinados testes de segurança em servidores públicos (CVE-2024-21663).

Também foram identificados novos CVEs, como o CVE-2023-51448, que trata de uma vulnerabilidade na função de receptores de notificações SNMP do Cacti-s, que poderia permitir que um invasor revele todo o conteúdo do banco de dados do Cacti ou, dependendo da configuração do banco de dados, até mesmo ative a execução de código remoto (RCE).

Cibersegurança OT: Como gerenciar uma auditoria industrial

Por Alejandro Alonso Rodríguez

Na atual era digital, a cibersegurança tornou-se um pilar fundamental para todas as indústrias. No entanto, no âmbito industrial, sua importância é ainda maior. A cibersegurança industrial concentra-se em proteger os sistemas de controle industrial (ICS) que são essenciais para o funcionamento de nossas infraestruturas críticas. Esses sistemas, que incluem uma variedade de dispositivos e redes, são responsáveis por supervisionar e controlar os processos industriais em setores como energia, fabricação, transporte e serviços.

À medida que esses setores se tornam cada vez mais digitalizados e conectados, também se tornam mais vulneráveis a uma variedade de ameaças cibernéticas. Desde ataques direcionados por invasores estatais até incidentes causados por erros humanos, as ameaças à cibersegurança industrial são diversas e estão em constante evolução. Este artigo explorará com profundidade a importância da cibersegurança industrial, as ameaças atuais e como as organizações podem se proteger de forma eficaz neste cenário digital em constante mudança.

No último relatório da empresa Claroty, “The Global State of Industrial Cybersecurity 2023: New Technologies, Persistent Threats and Maturing Defenses.” (https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity-2023), concluiu-se que 75% das empresas industriais foram alvo de *ransomware*. Do total de organizações afetadas por *ransomware*, aproximadamente 69% teve que pagar o resgate.
Isso destaca vários fatos:
- Apesar de 47% das empresas pesquisadas expressarem preocupação com a segurança, o OT está longe da maturidade de segurança existente no âmbito da TI. Dado que o ciclo de vida dos sistemas industriais é de 20 anos, frequentemente são encontrados sistemas *legacy* ou protocolos não seguros que, em suas origens, não estavam preparados para a integração com o mundo da TI e, muito menos, com as novas ameaças.

- Apesar dos novos padrões de cibersegurança industriais e dos esforços por um marco normativo comum para a integridade dos processos de OT, muitas empresas ainda carecem de uma governança clara que as prepare para incidentes cibernéticos em ambientes produtivos.

Um dos objetivos da área de cibersegurança OT da NTT DATA é, precisamente, estabelecer a trajetória das empresas do setor industrial para que alcancem um nível de maturidade ideal ao enfrentar essas ameaças. Para isso, uma das principais ferramentas são os marcos normativos, destacando-se principalmente dois: o NIST 800-82 e o ISA 62443.

As normas NIST 800-82 e ISA 62443 são dois marcos de referência cruciais no campo da cibersegurança, especialmente elaborados para garantir a segurança dos sistemas de controle industrial (SCI) e dos sistemas de automação. Ambas as normativas abordam a necessidade crítica de proteger infraestruturas críticas e processos industriais contra ameaças cibernéticas, que poderiam ter consequências devastadoras.

O NIST 800-82, desenvolvido pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, foca em fornecer pautas e recomendações para a segurança de sistemas de controle industrial. Este documento abrange desde a avaliação de riscos até a implementação de medidas de segurança eficazes, garantindo a integridade, confidencialidade e disponibilidade dos sistemas em ambientes industriais.

Por outro lado, a norma ISA 62443, criada pela Sociedade Internacional de Automação (ISA), é um padrão global que se concentra na segurança cibernética de sistemas de automação e controle. Este marco oferece uma estrutura abrangente para a identificação, avaliação e mitigação de riscos cibernéticos em sistemas de controle, levando em consideração aspectos específicos da segurança em processos industriais.

Ambas as normativas são essenciais para estabelecer práticas robustas de cibersegurança em ambientes industriais, contribuindo para a proteção de ativos críticos, a continuidade operacional e a preservação da integridade dos processos industriais diante das crescentes ameaças.

No entanto, é necessário evitar a "consultoria de papel" e não limitar a cibersegurança a um "checklist" de controles. É preciso agregar valor e garantir que tanto o âmbito estratégico quanto o técnico avancem juntos durante um projeto de cibersegurança OT.
Por isso, na NTT DATA, durante um projeto de governança OT, seguimos várias etapas, cada uma delas mais técnica, detalhada e aprofundada do que a anterior.

São 8 níveis fundamentais que precisam ser revisados e seguidos ao executar um projeto de cibersegurança industrial:

1. **Políticas, procedimentos e conscientização**: A base da cibersegurança em ambientes operacionais reside no estabelecimento de políticas e procedimentos robustos. Essas diretrizes fornecem a estrutura necessária para enfrentar ameaças em sistemas de controle industrial. A conscientização da equipe, por outro lado, é igualmente essencial, cultivando uma compreensão profunda dos riscos e promovendo práticas seguras. Uma equipe bem informada é uma linha de defesa crucial contra possíveis ataques, e a clareza das políticas garante uma implementação efetiva.

Deve existir, pelo menos, uma política de segurança geral que inclua o ambiente de OT e procedimentos operacionais claros (gestão de atualizações, gestão de permissões, gestão de backups...etc.).

Em muitas ocasiões, observa-se que o conhecimento operacional está concentrado em algumas poucas pessoas, o que torna os processos extremamente dependentes, sem responsabilidades claramente definidas e com uma transmissão interna de conhecimento pouco eficaz ou inexistente.

2. **Segmentação de rede**: A segmentação de rede desempenha um papel vital na proteção de sistemas críticos. Ao dividir a infraestrutura em segmentos, limita-se a propagação de ameaças e assegura-se que os sistemas cruciais operem em um ambiente controlado. Essa abordagem estratégica minimiza os riscos e resguarda a continuidade operacional, assegurando que, mesmo em caso de invasão, o impacto permaneça sob controle.
Graças à ISA 62443, temos as ferramentas para definir as zonas de segurança, os condutos de comunicação e adequar as medidas de segurança aos requisitos de cada zona. Nem todas as zonas de rede em um ambiente OT requerem o mesmo grau de proteção, tampouco a mesma atenção.

3. Defesa de protocolos e transporte: A segurança nas camadas de transporte e protocolos é essencial para manter a integridade das comunicações em ambientes industriais. Resistir a ataques nessas camadas significa garantir a autenticidade e confidencialidade dos dados transmitidos. A implementação de medidas de segurança robustas nesse contexto é crucial para proteger a comunicação entre dispositivos e sistemas de controle.

Muitos dos protocolos de OT utilizados atualmente, por sua natureza, são pouco seguros (Modbus, Profinet-DCP, etc.). No entanto, isso não significa que não possamos implementar medidas de segurança perimetrais ou medidas mitigadoras para conter ataques no caso de que uma de suas vulnerabilidades seja explorada.

4. Segurança de rede: A configuração e gestão eficazes de dispositivos de rede são os pilares de uma rede segura. Firewalls, sistemas de prevenção de invasões e detecção e resposta em tempo real são elementos-chave para defender contra ameaças cibernéticas. Uma rede bem protegida fornece a base necessária para a operação segura e confiável de sistemas de controle industrial. Um dos pontos-chave, tratando-se de ambientes operacionais, é a visibilidade. Não podemos proteger o que não podemos ver. Portanto, é importante implantar sistemas de monitoramento e vigilância de ativos.

Muitos dos sistemas atuais, como Nozomi, Claroty, Armis, etc., estão perfeitamente adaptados para realizar essa descoberta de ativos de maneira passiva. Controlar nossos ativos de OT nos torna conscientes de nossa superfície de ataque e nos permite priorizar a resolução de vulnerabilidades, a segmentação e a contenção de ataques.

Da mesma forma, é importante analisar as políticas de rede implementadas em elementos como os *firewalls*.
Muitas vezes, políticas temporárias ou pouco robustas são estabelecidas, confiando que serão breves e controladas; no entanto, em muitas ocasiões, é precisamente uma proteção inadequada ou uma implementação deficiente dos elementos de segurança de rede que servem como porta de entrada para os invasores: Um firewall mal implementado é pior do que não instalar um *firewall*.

5. Segurança física e lógica: A segurança física é a primeira linha de defesa contra acessos não autorizados, enquanto os controles de acesso e a vigilância adicionam camadas de proteção. A segurança lógica, por meio da gestão de identidades e acessos, complementa essas medidas, garantindo que apenas pessoal autorizado tenha acesso a sistemas e dados críticos. A combinação de abordagens físicas e lógicas cria uma barreira robusta contra ameaças internas e externas.

6. *Hardening* de aplicações: A segurança das aplicações é essencial para prevenir vulnerabilidades. O *hardening* de aplicações envolve a configuração adequada e a gestão proativa de *patches*. Esta medida visa evitar a exploração de possíveis vulnerabilidades, assegurando que as aplicações utilizadas em sistemas de controle sejam robustas e seguras. Além disso, é de vital importância ter sistemas de controle para as aplicações que podem ou não ser instaladas em nossas estações de engenharia ou computadores na área de OT.

Felizmente, muitos fabricantes desenvolveram soluções *whitelisting* e *blacklisting* de software adaptadas a esses sistemas, nas quais até mesmo podemos integrar alertas em nosso SIEM para agir rapidamente contra um programa malicioso ou não permitido em nossa rede.

Da mesma forma, muitas dessas soluções nos auxiliam a monitorar e proteger nossos sistemas contra um dos vetores de entrada de *malware* mais comuns em OT: os USB's.

7. *Hardening* de ativos: A configuração segura de ativos, como servidores, estações de trabalho, PLC, SCADA, etc., é crucial para a proteção contra ameaças. Uma gestão eficaz de contas e senhas, juntamente com controles de acesso, reforça a segurança desses ativos. Essas medidas garantem que sistemas e dados críticos estejam protegidos contra acessos não autorizados e manipulações indesejadas.
É importante contar com diretrizes de boas práticas após a instalação de novos equipamentos.
Muitas vezes, os valores padrão e os serviços implementados diretamente pelo fabricante deixam portas abertas para ataques externos.

8. *Hardening* de dispositivos embarcados: Os dispositivos embarcados, como PLCs e sistemas SCADA, requerem medidas específicas para prevenir manipulações não autorizadas. O *hardening* desses dispositivos envolve a aplicação de atualizações de *firmware*, *patches* de segurança e proteção contra manipulações não autorizadas. Essas ações são cruciais para manter a integridade e segurança dos processos em ambientes industriais. Da mesma forma, é importante controlar o software e a programação desses dispositivos. Ter um sistema que nos alerte caso a integridade desses dispositivos seja comprometida ou alterada também é crucial.

Proporcionar essa visão de 360 graus, tanto estratégica quanto técnica, agrega mais valor à consultoria especializada em OT e ajuda a visualizar resultados desde o primeiro minuto do projeto, especialmente em ambientes como o de OT, onde a disponibilidade é crucial e é exatamente nosso objetivo.
A chegada de dispositivos conectados e inteligentes ao mundo industrial fez com que precisássemos adaptar não apenas as tecnologias, mas também a consultoria e a compreensão da segurança em um contexto com ampla obsolescência, onde as mudanças são triviais.

Alejandro Alonso Rodríguez
OT Cybersecurity Manager

Desinformação em ano eleitoral

TENDÊNCIAS por Miguel Tuimil

A desinformação eleitoral é uma preocupação global crescente que envolve a disseminação intencional de informações falsas ou enganosas para influenciar a opinião pública e afetar os resultados eleitorais. Este fenômeno tem se intensificado com o aumento das plataformas de redes sociais e serviços de mensagens instantâneas, onde notícias falsas e teorias da conspiração podem se espalhar rapidamente. Os indivíduos mal-intencionados frequentemente exploram as emoções e polarizações existentes para semear a discórdia e manipular a percepção dos eleitores, representando uma grande ameaça para a democracia e a confiança dos cidadãos nas instituições.

Em **2024**, os processos eleitorais nos Estados Unidos, na Índia, em Taiwan e em outras 40 nações serão um terreno fértil para a engenharia social e as campanhas de desinformação.

De acordo com a UNESCO, as desinformações eleitorais podem ser agrupadas em 4 tipos gerais:

1. As acusações de fraude são frequentemente as mais difundidas durante as eleições. Elas buscam demonstrar uma fraude organizada e coordenada pelas autoridades nacionais, locais e/ou eleitorais, como por exemplo fotos de supostas urnas com selos rompidos ou capturas de atas de apuração com erros que pretendem confirmar um fraude. Tipicamente, as irregularidades involuntárias não beneficiam sistematicamente nenhuma das partes, enquanto as intencionais costumam distorcer os resultados a favor de algum grupo.

2. Aquelas que se referem a pessoas não autorizadas que supostamente votam. Durante as eleições, circulam muitos conteúdos que buscam atacar as minorias, garantindo que imigrantes votarão em países onde não é permitido ou não cumpram as condições legais quando o voto de estrangeiros é permitido. Também circulam desinformações que afirmam que pessoas falecidas estão incluídas no censo eleitoral ou que documentos de identidade de pessoas falecidas são usados para votar. No entanto, em muitos casos, trata-se de erros no registro que são corrigidos pelas autoridades.

3. Aquelas que se referem ao próprio processo de votação. Durante as eleições, é comum a circulação de conteúdos falsos que buscam desorientar ou gerar medo nos cidadãos em relação ao momento da votação. Cada país possui normas diferentes que estabelecem quando um voto deve ser anulado ou impugnado (ou seja, não contabilizado como válido).

4. Declarações ou propagandas falsas dos candidatos. Utiliza-se a edição e manipulação de fotos, assim como imagens retiradas de contexto. Para as declarações falsas, são usados quadros ou logotipos de algum meio de comunicação com a imagem de um candidato e uma suposta frase. Também circulam vídeos manipulados ou retirados de contexto, além de áudios paródicos ou falsamente atribuídos aos candidatos.

Combater a desinformação nas eleições requer esforços coordenados entre governos, plataformas tecnológicas e cidadãos. As estratégias incluem a verificação de fatos, promoção da alfabetização midiática, transparência na propaganda política on-line e colaboração internacional para lidar com campanhas de desinformação transfronteiriças. É fundamental fortalecer a resiliência da sociedade diante da desinformação, promovendo uma cidadania informada e crítica capaz de discernir entre informações verdadeiras e enganosas no contexto eleitoral.

Vulnerabilidades

Múltiplas vulnerabilidades no Juniper Secure Analytics

Data: 28 de dezembro de 2023
CVEs: CVE-2023-40787 e mais 17

CVSS: 9.8
CRÍTICA

Descrição

Recentemente foram relatadas dezoito vulnerabilidades no Juniper Secure Analytics. Dessas dezoito vulnerabilidades, duas são de gravidade crítica, sete são de gravidade alta, outras sete são de gravidade média e duas são de gravidade baixa.

A seguir são apresentadas as vulnerabilidades de gravidade crítica:

- CVE-2023-40787: vulnerabilidade com relação à execução de consultas SQL no SpringBlade V3.6.0. Especificamente, ocorre quando os parâmetros enviados pelo usuário não estão entre aspas, o que provoca uma injeção SQL.
- CVE-2023-46604: vulnerabilidade que poderia permitir a um invasor remoto com acesso de rede a um cliente ou a um *broker* OpenWire baseado em Java executar comandos *shell* arbitrários, manipulando tipos de classe serializados no protocolo OpenWire para fazer com que o cliente ou o *broker* (respectivamente) instanciem qualquer classe no *classpath*.

Produtos afetados

A vulnerabilidade afeta a seguinte versão do produto:

- Juniper Secure Analytics, versões até 7.5.0 UP7.

Solução

O fabricante recomenda manter seus produtos sempre atualizados com a última versão, a fim de evitar riscos de segurança relacionados a novas vulnerabilidades. Especificamente, é recomendado atualizar para a versão 7.5.0 UP7 IF03 do Juniper Secure Analytics, pois esta atualização corrige as vulnerabilidades identificadas.

Referências

- www.incibe.es
- supportportal.juniper.net

Vulnerabilidade de injeção SQL no Ivanti EPM

Data: 04 de janeiro de 2024
CVEs: CVE-2023-39336

CVSS: 9.6
CRÍTICA

Descrição

Recentemente foi descoberta uma vulnerabilidade crítica no produto EPM *(Endpoint Manager)* da Ivanti.

A vulnerabilidade descoberta, do tipo injeção SQL, permite que um invasor com acesso à rede interna execute consultas SQL arbitrárias, resultando na obtenção do resultado dessas consultas sem a necessidade de autenticação. Isso pode permitir que um invasor controle os dispositivos executados pelo operador do Ivanti EPM.

Além disso, quando o servidor central está configurado para utilizar o SQL Express, a vulnerabilidade detectada pode levar a uma execução remota de código (RCE) no servidor central.

Produtos afetados

A vulnerabilidade afeta as seguintes versões do produto Ivanti EPM:

- Ivanti EPM 2021.
- Ivanti EPM 2022 prévias ao *Service Update* 5.

Solução

O fabricante recomenda atualizar o produto Ivanti EPM para a versão 2022 SU5.

Referências

- www.incibe.es
- forums.ivanti.com
- www.ivanti.com

Patches

CRÍTICA

Novos *patches* de segurança para produtos da Microsoft

Data: 10 de janeiro de 2024
CVE: CVE-2024-0057 e mais 47

Descrição
No último dia 10 de janeiro, a Microsoft lançou uma série de atualizações para corrigir múltiplas vulnerabilidades de segurança em seus sistemas operacionais Windows e outros *softwares*. No total, foram divulgadas 48 vulnerabilidades, das quais 2 são críticas, 26 são importantes e 20 têm gravidade média.

A seguir, estão detalhadas as vulnerabilidades classificadas como críticas:

- CVE-2024-0057: vulnerabilidade que afeta o NET, .NET Framework e Visual Studio, através da qual um invasor pode usar um certificado X.509 não confiável por meio de uma API para inserir esse certificado e explorar o erro retornado para inserir código malicioso.
- CVE-2024-20674: esta vulnerabilidade afeta o protocolo de segurança Kerberos do Windows, onde um invasor autenticado, ao realizar uma falsificação de rede local, pode enviar uma mensagem Kerberos maliciosa ao cliente vítima e se passar pelo servidor de autenticação Kerberos.

O restante das vulnerabilidades pertencem a vários tipos: elevação de privilégios, contorno de funções de segurança, execução remota de código, divulgação de informações, negação de serviço e roubo de identidade.

Produtos afetados
Essas vulnerabilidades abrangem uma grande variedade de produtos Microsoft. Esses produtos podem ser consultados em: msrc.microsoft.com

Solução
Aplicar o *patch* de segurança correspondente nos produtos afetados.

Referências
- msrc.microsoft.com
- es-la.tenable.com

CRÍTICA

Patches críticos para GitLab Community e Enterprise Edition

Data : 11 de janeiro de 2024
CVE: CVE-2023-7028

Descrição
O GitLab recomenda fortemente aplicar *patches* para suas versões mais recentes nos produtos GitLab Community Edition (CE) e Enterprise Edition (EE), pois incluem correções de segurança importantes.

Os invasores que explorarem a vulnerabilidade CVE-2023-7028 podem redefinir as senhas das contas de usuários do GitLab. Não estão isentos os usuários com autenticação de dois fatores, tornando também vulneráveis os usuários com 2FA.

O fabricante confirmou que não foi detectado nenhum abuso dessa vulnerabilidade em plataformas administradas pelo GitLab.

Esta vulnerabilidade afeta as instâncias autoadministradas do GitLab que estão executando as versões previamente descritas.

Esta vulnerabilidade possui seu teste de conceito (PoC) e um *exploit* publicado.

Produtos afetados
As diferentes versões afetadas por essa vulnerabilidade são as seguintes:

- 16.1 antes de 16.1.5
- 16.2 antes de 16.2.8
- 16.3 antes de 16.3.6
- 16.4 antes de 16.4.4
- 16.5 antes de 16.5.6
- 16.6 antes de 16.6.4
- 16.7 antes de 16.7.2

Solução
O GitLab recomenda que os administradores de instâncias do GitLab ativem a autenticação de dois fatores (2FA) para todas as contas e atualizem para as versões 16.7.2, 16.6.4, 16.5.6 do GitLab CE e EE.

Referências
- about.gitlab.com
- nvd.nist.gov

Eventos

SANS Offensive Operations London 2024
O SANS Offensive Operations London 2024 será realizado on-line e presencialmente de 05 a 10 de fevereiro. Há vários cursos que oferecem conhecimentos práticos sobre tópicos especializados, como análise forense do Windows, fundamentos de segurança em ambientes de rede, *endpoint*, nuvem, testes de penetração de aplicativos web e *hacking* ético.

Link

HackCon
A conferência nacional norueguesa sobre cibersegurança, HackCon, tem como objetivo a cada ano, dentro dos temas de grande relevância, revisar cerca de 1.200 a 1.400 apresentações e pesquisas para escolher as melhores palestras para a HackCon. De todas as apresentações/pesquisas, seleciona-se aproximadamente um por cento (12 a cada ano) para ter a oportunidade de falar na HackCon. Este ano, o evento será realizado de 12 a 14 de fevereiro na cidade de Oslo, Noruega.
Link

Zero Trust World
O Zero Trust World é um evento que acontece em Orlando, Estados Unidos, de 26 a 28 de fevereiro, no qual os participantes adquirirão conhecimentos e habilidades necessárias para avançar em direção a uma postura de cibersegurança de confiança zero. Haverá palestras principais pela manhã, sessões de trabalho à tarde, laboratórios práticos de *hacking* e uma sala de exposições cheia de fornecedores com soluções para explorar.
Link

SecureWorld Financial Services
A conferência virtual SecureWorld Financial Services é um evento de destaque que procura reunir especialistas da indústria financeira para fornecer orientação sobre temas críticos dos serviços financeiros e seu impacto na cibersegurança. Durante um dia, ela oferece informações essenciais sobre como as instituições financeiras podem se preparar para ataques cibernéticos, disrupção tecnológica e questões relacionadas à privacidade de dados no setor financeiro.
Link

Recursos

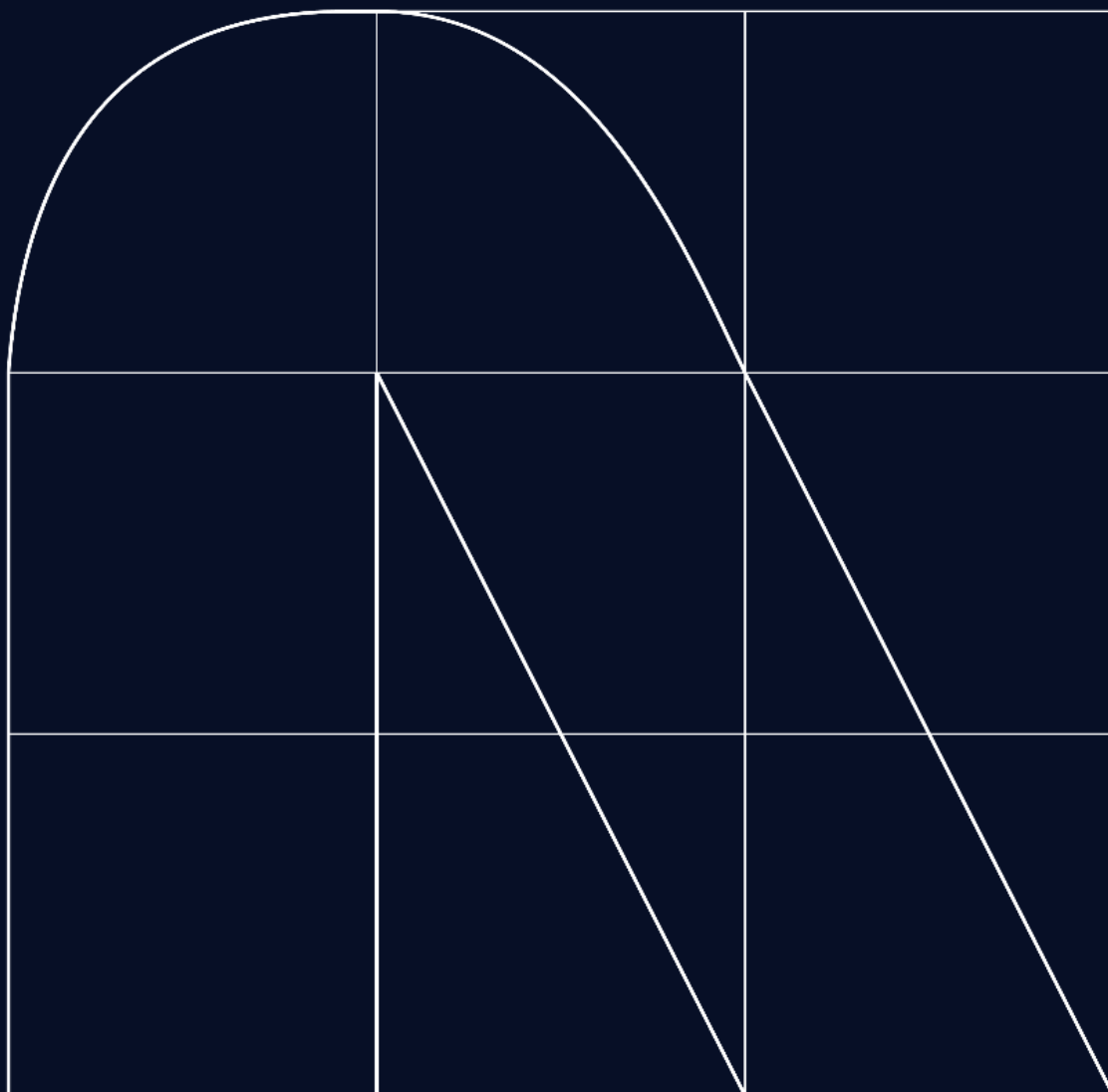
0dAI
0dAI é uma plataforma SaaS (Software as a Service) voltada para cibersegurança impulsionada por inteligência artificial. Oferece uma ampla variedade de serviços, como: Desenvolvimento de *malware*, engenharia social, desenvolvimento de *exploits* e análise de SOC entre uma ampla gama.
Link

WebCheck
WebCheck é uma ferramenta de código aberto que permite realizar uma análise completa de aplicações web, coletando informações relevantes, como: *cookies*, registros DNS, geolocalização do servidor e cabeçalhos.
Link

CUPP
CUPP é uma ferramenta que permite ao usuário desenvolver dicionários personalizados com informações relacionadas ao alvo, como o nome da empresa, familiares ou a data de nascimento, possibilitando assim um ataque mais dinâmico.
Link

CervantesSec
CervantesSec é uma plataforma colaborativa de código aberto para *pentesters* que possibilita economia de tempo na gestão de seus projetos, permitindo o desenvolvimento de modelos personalizados, a administração de vulnaerabilidades e a atribuição de funções e permissões aos membros da equipe.
Link

T-Pot
T-Pot é uma plataforma de *honeypot all-in-one*, que oferece uma visualização clara de um mapa global com ataques ao vivo e uma ampla variedade de ferramentas para facilitar a compreensão dos ataques em andamento.
Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com