NUMERO 75 | FEVEREIRO 2023

NTT DATA
Trusted Global Innovator

Radar

A revista da cibersegurança

GERENCIAMENTO DO RISCO À PRIVACIDADE, UM ELEMENTO CENTRAL PARA A CONFIANÇA E A CONFIANÇA ORGANIZACIONAL

No dia 28 de janeiro é comemorado o **Dia Internacional da Proteção de Dados Pessoais**, referente à Convenção 108, que protege as pessoas em relação ao tratamento automatizado de dados pessoais. Este fato não é relevante apenas devido à importância do uso de dados pessoais em vários setores, mas também em virtude das recentes notícias internacionais sobre violações de segurança em que podem estar envolvidas informações de clientes ou colaboradores e, portanto, os danos reputacionais enfrentados pelas organizações.

Um desafio constante das organizações é alcançar o equilíbrio entre a proteção das informações de seus clientes e colaboradores juntamente com a maximização de seu uso, em prol de oferecer maior valor a essas informações. Não é uma tarefa fácil, considerando o processo de atualização de vários marcos regulatórios na América Latina, aumentando os requisitos que as organizações devem cumprir em termos de proteção de dados pessoais, juntamente com possíveis sanções monetárias em caso de descumprimento.

É por isso que um dos elementos provavelmente mais interessantes estabelecidos pelo regulamento europeu (GDPR) é a abordagem baseada nos riscos em relação ao uso de dados pessoais. Nesse sentido, as organizações que usam esses dados (responsáveis) devem comprovar que identificaram o risco aos direitos dos titulares e que adotaram uma série de medidas para reduzir os riscos que possam ocorrer, como resultado do uso que fazem da organização. Isso é conhecido como "responsabilidade proativa", que, em nenhum caso, inibe o uso de dados pessoais, mas destaca a importância de gerenciar corretamente os riscos a eles associados.

Sem dúvida, um dos aspectos problemáticos para as organizações é demonstrar que medidas estão sendo adotadas para proteger os dados pessoais e que os próprios regulamentos indicam a criptografia ou anonimização como referência, portanto, é relevante que as ações que decidam adotar estejam de acordo com a realidade da empresa. Neste sentido, o trabalho coordenado entre as áreas de compliance e a cibersegurança ou a segurança da informação, torna-se um assunto obrigatório para dar uma resposta adequada às expectativas dos diversos regulamentos, mas atingindo os objetivos do negócio.

Finalmente, as estratégias de privacidade de uma organização devem andar de mãos dadas com planos de conscientização, como treinamento sobre essas questões. A segurança dos dados pessoais é um assunto fundamental que cada membro da organização constrói, não apenas as áreas técnicas, de riscos ou jurídicas. As organizações devem ter uma abordagem comum e trabalhar em conjunto para demonstrar a aclamada proatividade exigida pelos regulamentos sobre o assunto.

Juan Pablo Gonzales Gutierrez
Gerente Sênior de Segurança Cibernética da NTT DATA Chile

CIBERCRÓNICA

Como estamos no início do ano, começamos a cibercrônica mencionando o estudo realizado pela NetScope no qual são mostradas as Tendências e previsões em matéria de cibersegurança na EMEA para 2023.

Um dos aspectos mais importantes deste estudo é que, devido à incerteza econômica global, como resultado da situação atual, as empresas estarão mais orientadas para os modelos de Segurança como Serviço, em comparação com os modelos de construção tradicionais. Isso, por sua vez, afetará o resto da infraestrutura e serviços, os adaptando aos modelos "as-a-service" (SaaS, IaaS etc.), passando de um modelo Capex para um modelo Opex, o que permitirá às empresas conservar uma maior quantia de dinheiro em face de possíveis recessões em nível empresarial.

"O número médio de novos arquivos maliciosos por dia foi de 400.000 (122 milhões em 2022), estimando-se 500.000 para o ano de 2023".

Em relação ao restante das tendências, continuarão ocorrendo tanto ataques baseados em Ransom-as-a-Service (RaaS), em que se procura tanto a exfiltração quanto a criptografia de dados, bem como ataques provenientes apenas dos chamados grupos de extorsão, nos quais apenas o roubo de dados confidenciais é procurado.

Tais ataques serão ainda mais agravados pelo uso de múltiplas táticas simultâneas (por exemplo, exfiltração em conjunto com DDoS), além do uso de novas ferramentas e cargas úteis em conjunto com a colaboração direta de pessoas internas mal-intencionadas.

Outro ponto interessante serão as operações de phishing baseadas em proxies reversos com o objetivo de abusar do OAuth para contornar a Autenticação Multifator (MFA), bem como novos ataques de força bruta, como roubo de tokens e ataques SSO, visando tirar proveito de aplicativos em nuvem de terceiros, em que os controles implantados pelos provedores ainda ficam aquém das técnicas dos invasores.

Por fim, o novo modelo de trabalho após a pandemia dificulta a identificação proativa de ameaças internas, o que exige o desenvolvimento das organizações em suas práticas de segurança. Assim, em 2023, veremos que as organizações perceberão o pouco controle que têm sobre seus próprios dados.

Outras análises interessantes foram publicadas recentemente pela Kaspersky (análise e previsões anuais e o relatório da Crimeware e ameaças financeiras para 2023).
Segundo estes, o número médio de novos arquivos maliciosos por dia foi de 400.000 (122 milhões em 2022), estimando-se 500.000 para o ano de 2023. Também é importante ressaltar que 85% dos vários arquivos maliciosos detectados visavam o sistema operacional Windows.
Por outro lado, são identificadas novas tendências relacionadas ao software criminoso. Destaca-se o aumento dos ataques contra smart contracts vulneráveis, o aumento no uso de malware loaders para evitar a detecção na indústria do

Malware-as-a-Service (MaaS) e novas técnicas e frameworks de infiltração. Há também uma diminuição dos ataques baseados em bitcoin para a cobrança de resgates devido à regulamentação do mercado, passando a exigir, em vez disso, a tomada de decisões políticas, ou, simplesmente, sem outro objetivo que não seja a destruição de recursos.

No que se refere aos incidentes de cibersegurança que surgiram recentemente, 2022 fechou o ano com uma das violações mais graves e notórias dos últimos tempos que afetou a solução de gestão de segredos LastPass.
Em meados de dezembro, a organização divulgou um comunicado notificando os usuários do aplicativo que, em agosto de 2022, um operador anônimo obteve acesso ao seu ambiente de armazenamento em nuvem.
As informações obtidas durante a violação de segurança levaram à exfiltração de informações pertencentes aos clientes da organização, como nomes, dados de contato ou endereços de IP utilizados para acessar o serviço.
Dos dados roubados, o mais relevante seria uma cópia dos bancos de dados secretos dos clientes, que são criptografados usando o algoritmo AES-256 com uma chave, como regra, derivada da chave mestra de desbloqueio do banco de dados secretos definido pelo próprio usuário.
A própria empresa esclarece que a arquitetura de criptografia aplicada aos bancos de dados armazenados em seus sistemas dificulta muito o acesso de invasores às informações desde que sejam seguidas as recomendações do LastPass ao definir a senha mestra.
No entanto, os usuários que optaram por não seguir essas recomendações, ou que reutilizaram sua senha mestra em outros serviços, só podem estar seguros quando todas as senhas e segredos armazenados em sua conta do LastPass tiverem sido alterados.

Fechando o ano, na véspera de Ano Novo, outro notável, o Slack, publicou uma nota de imprensa que informou aos seus usuários sobre o acesso não autorizado a seus repositórios do Github, públicos e privados.
O Slack garante que os cibercriminosos não fizeram alterações no código ou acessaram os dados do cliente, limitando o impacto à perda da propriedade intelectual da organização.

Já em 2023, o surgimento de informações relacionadas a usuários do Twitter com mais de 200 milhões de registros, disponíveis de forma totalmente gratuita em um conhecido fórum de hacking, criou uma grande confusão sobre sua origem.
Uma vez que os principais meios de comunicação conseguiram analisá-las em profundidade, o consenso geral indica se tratar de uma composição obtida consumindo a API do Twitter com uma lista de endereços de e-mail obtidos em violações anteriores, o que permitiu a coleta de dados pessoais dos usuários como o nome, o identificador do Twitter, ou o número de seguidores.

Por outro lado, de acordo com um estudo publicado pela TransUnion, uma em cada quatro compras originadas na Espanha durante a Black Friday foi potencialmente fraudulenta.

Uma mudança significativa foi observada nas táticas aplicadas pelo grupo pró-iraniano de ciberespionagem APT42 para atingir um espectro de alvos mais amplo. Entre estes objetivos podemos identificar desde pesquisadores médicos a agentes imobiliários ou agências de viagens.
Também é interessante uma nova campanha de malware baseada na clonagem de sites e apoiada no Google Ads para sua promoção.
Igualmente inovadoras são as novas ferramentas que começam a aparecer nos fóruns da comunidade hacker, que têm o toque da inteligência artificial favorita da internet, o ChatGPT.
Analistas da Check Point começaram a ver menções de ferramentas geradas ou aprimoradas usando o chatbot, como um malware destinado a roubar informações, ou fragmentos de código para formação de malware.
Embora tenhamos tentado perguntar ao ChatGPT sobre seu envolvimento, o chatbot estava além de sua capacidade no momento da redação desta cibercrônica e, portanto, não pôde comentar.
No entanto, não podemos confiar muito no ChatGPT. Uma pesquisa conjunta da Microsoft e das universidades da Virgínia e da Califórnia levou a um artigo que discute a possibilidade de envenenar os modelos de aprendizado utilizados em ferramentas como o Co-Pilot do Github ou o próprio ChatGPT, fazendo com que o código sugerido contenha backdoors que poderiam ser explorados por agentes mal-intencionados.
Os pesquisadores, que batizaram a técnica como “Trojan Puzzle”, relatam um sucesso moderado: de 30% para os ataques mais simples e fáceis de detectar, e até 4% para os mais complexos.
Não há dúvidas de que a cibersegurança em 2023, seja do ponto de vista defensivo ou ofensivo, será marcada por incríveis avanços no campo da inteligência artificial. Se esses avanços são aliados ou inimigos, só o tempo dirá.
De qualquer forma, sem mais delongas, despedimo-nos e desejamos que você tenha tido felizes e seguras celebrações este ano.

PRIVACY BY DESIGN E SUA APLICAÇÃO METODOLÓGICA

Por: NTT DATA Europa & Latam

Um termo muito utilizado quando falamos de Privacy e proteção de informações pessoais é Privacy by Design (Privacidade desde a Concepção), porém, alguns de seus elementos são pouco conhecidos. Privacy by Design é um framework que tem como objetivo principal a Proteção de Dados Pessoais desde a concepção e projeto de uma solução tecnológica.

Sendo um conceito destinado a proteger os direitos dos titulares de dados pessoais, o Privacy by Design deve ser pensado de forma a abranger não apenas a solução em si, mas toda a estrutura que compõe a execução dos serviços, tratamento, armazenamento e troca segura de dados pessoais, bem como sua respectiva remoção, quando for necessário. Isso significa que o Privacy by Design deve estar presente e integrado por padrão durante todo o ciclo de vida dos dados pessoais.

Este conceito está previsto tanto no regulamento europeu de dados pessoais (GDPR/RGPD), especificamente em seu artigo 25, quanto na Lei Geral de Proteção de Dados do Brasil (LGPD), no artigo 46, parágrafo 2º.

O Privacy by Design é composto por sete princípios metodológicos que buscam orientar sua aplicação e abrangência em projetos tecnológicos, identificados a seguir:

1. Ação Proativa e Não Reativa; Preventiva e Não Corretiva

Baseado no conceito de que riscos devem ser evitados e não reparados, o Privacy by Design apresenta uma condição proativa, antecipando possíveis mitigadores de riscos de dados pessoais, que devem ser adotados desde a concepção de soluções tecnológicas.

A ideia central é a prevenção como forma de mitigação, na tentativa de antecipar e evitar riscos que causem danos aos titulares no tratamento dos seus dados pessoais

A forma de implementar esta condição é por meio do conhecimento aprofundado da solução, com foco na implantação de medidas e procedimentos eficazes em Cibersegurança, procurando eliminar, na medida do possível, todas as vulnerabilidades e ameaças que possam estar presentes na execução da atividade a que se dedica.

2. Privacidade por padrão (Privacy by Default)

De acordo com este critério, a Privacidade deve ser concebida como parte da própria arquitetura da solução, ou seja, deve ser pensada como um elemento essencial e obrigatório desta, embora de forma equilibrada, que não afete a sua funcionalidade.

Alguns pontos relevantes para o cumprimento deste objetivo: I) Finalidade da coleta de dados pessoais; II) Limitação do tratamento apenas destinada à necessidade para a qual os dados pessoais foram coletados; III) Priorização de dados não identificáveis (anônimos ou pseudônimos); IV) Tratamento precisamente vinculado à finalidade, com descarte seguro assim que cumprido.

3. Privacidade integrada no projeto

A privacidade deve abranger tanto as soluções, desde a sua concepção, como a arquitetura tecnológica que suporta o seu funcionamento em operação. Idealmente, a solução deve manter o equilíbrio entre Funcionalidade completa e Privacidade em cada etapa de desenvolvimento/operação.

Para que este propósito seja consolidado, é importante que a solução apresente um amplo campo de atuação, baseado não só no viés de integração de diversas áreas de interesse complementares, mas também que respeite os limites do Privacy by Default .

4. Funcionalidade x Privacidade

Para que a solução seja apresentada de forma completa e competitiva, o ideal é que nenhuma regra de Privacidade afete seu desempenho regular e pleno, quando estiver em produção.

A Privacidade deve atuar como aliada da solução e não como obstáculo de suas funções. Ambos os critérios (Funcionalidade e Privacidade) são necessários para que a solução seja efetiva e regular quando for disponibilizada aos usuários.

Nesse sentido, ter regras simples como uma documentação clara e objetiva da solução; o equilíbrio entre a Funcionalidade e Privacidade de uma solução e a preservação dos direitos dos titulares dos dados pessoais, são boas práticas para conduzir a uma solução viável do ponto de vista da Cibersegurança.

5. Segurança total (ponta a ponta)

Não basta que apenas a solução seja segura, é importante que as operações e os ambientes em que a solução está localizada ou por onde transita também estejam protegidos.

É muito importante que regras como transmissão, armazenamento e eliminação segura de dados pessoais sejam observadas ao longo de todo o ciclo de vida dos dados pessoais. Atividades como criptografia, anonimização ou pseudonimização de dados pessoais ajudam a reduzir os riscos derivados delas.

Pontos que cumprem os preceitos de Confidencialidade, Integridade e Disponibilidade e que atendem aos padrões básicos de Segurança da Informação.

6. Transparência

Isto significa que a solução deve "entregar exatamente o que promete" ao usuário, sem dúvidas ou omissões quanto ao tratamento de dados pessoais que serão efetuados para esse fim. Aspectos como o compartilhamento de dados com terceiros, a retenção e exclusão de dados pessoais, a finalidade da coleta e a finalidade do tratamento devem ser claros e evidentes nos Termos de Uso e nas Políticas e regulamentos da solução.

7. Respeito à Privacidade do usuário

Por fim, a solução deve favorecer a privacidade do usuário ao utilizar a ferramenta, adotando medidas essenciais como o uso obrigatório de senhas seguras; possibilidade de autenticação em formato multifatorial; configurações de gestão de acesso apropriadas e seguras; rastreabilidade e backup das informações, quando necessário e aplicável; armazenamento seguro, transmissão e exclusão de dados pessoais.

Estas práticas conduzem a uma solução completa e segura, que favorece a Privacidade do titular dos dados pessoais e conduz a um caminho de sucesso e integridade para todos aqueles que utilizam os serviços oferecidos.

TENDÊNCIAS

Proteção Automatizada de Aplicativos

A combinação da transformação digital e uma pandemia global acelerou a necessidade de criar mais aplicativos, mais rapidamente, para atender às demandas em constante mudança dos clientes, concorrentes ou do mercado.

Esse contexto tem incentivado as metodologias ágeis e o crescimento do DevOps na área de aplicativos. Um dos desafios desses aplicativos é identificar exemplos práticos de como burlar seu perímetro de segurança a fim de evitar o roubo de dados dos clientes, da propriedade intelectual da empresa ou até mesmo de dinheiro, por isso é necessário mantê-los a salvo de ameaças.

Assim, embora seja reconhecido que aumentar a segurança dos aplicativos que são criados é fundamental, dependendo das necessidades imediatas, ou da maturidade de uma organização em relação aos processos automatizados do CICD, os responsáveis pelos aplicativos podem ser vistos nas seguintes situações:

1. Não pensar em segurança como parte do processo DevOps de modo algum
2. Ver a segurança como um impedimento para chegar ao mercado com eficiência (os controles de segurança atrasam a entrega do software, afetam negativamente a experiência do usuário etc.)
3. Querer reforçar a segurança, mas não saber por onde começar.

Por isso, há uma série de soluções focadas na proteção automatizada de aplicativos, entre as quais se destacam o Digital.ai Application Security Solution ou Denuvo, especializados em evitar o tampering e a gestão de direitos digitais (DRM) para celulares e outros aplicativos.

Em que se baseia este tipo de proteção?

Primeiro, o código é ofuscado pelo código desprotegido original e introduzido, juntamente com o nível de proteção especificado (ou recomendado pela própria ferramenta), em um motor que produz o código protegido. O aplicativo protegido contém código de máquina ofuscado que é executado conforme projetado originalmente, mas é praticamente ilegível para as ameaças, mesmo depois de inserido em um desmontador.

Além disso, aplica uma metodologia anti-tampering que fornece a capacidade de detectar duas condições.

- Detectar quando um aplicativo está sendo executado em um ambiente inseguro que possa permitir que ele seja manipulado. Exemplos clássicos desse tipo de ambiente são depuradores, emuladores ou dispositivos rooteados/jailbroken.
- Detectar quando o código de um aplicativo foi modificado.

Também fornece visibilidade em uma plataforma centralizada, SIEM etc. sobre os ataques a aplicativos e tentativas de executá-los em ambientes inseguros. Por exemplo, se uma ameaça tentar modificar o código, será dado um alerta, além de muitos detalhes sobre onde (IP e localização geográfica, por exemplo), quando, qual elemento e em qual dispositivo, sistema operacional, navegador etc. a mudança ocorreu.

Finalmente, oferecem a tecnologia RASP (Runtime Application Self Protection), permitindo responder automaticamente às ameaças em tempo de execução. Dentre os recursos fornecidos, destacam-se:

- Forçar autenticação escalonada.
- Modificar os aplicativos no nível funcional.
- Fechar os aplicativos atacados.

Que vantagens adicionais oferecem?

Além das funcionalidades básicas deste tipo de aplicativo, algumas soluções podem oferecer uma série de recursos que aumentam seu valor:

- Sem um único ponto de falha: Muitos programas usam senha, biometria ou assinatura digital para controlar o acesso. Esse tipo de proteção cria um único ponto de falha, que um invasor pode facilmente identificar, remover ou modificar. Esses produtos podem implementar uma rede de proteções interdependentes que não exponha um único ponto de ataque.
- Segurança integrada: As defesas não dependem do sistema operacional ou de programas externos ao binário protegido.
- Segurança personalizada: Pode ser projetado um esquema de proteção que atenda às necessidades de uma organização, que complemente ou substitua o perfil recomendado pela ferramenta.

Quais são os benefícios dos produtos de proteção automatizada?

A integração desse tipo de aplicativo nos fluxos de trabalho CICD permite criar um software seguro na velocidade do DevOps, sem a necessidade de executar determinadas tarefas comuns que atrasariam as entregas dos aplicativos.

Em todo caso, o benefício mais importante proporcionado por tais produtos é que eles protegem a segurança perimetral de forma automatizada.

VULNERABILIDADES

Receba nosso boletim informativo completo e de vulnerabilidade inscrevendo-se aqui.

Microsoft

CVE-2023-21674
Data: 10/01/2023

Descrição. A Microsoft relatou uma vulnerabilidade explorada ativamente que permite escalar privilégios no sistema. Mais especificamente, a vulnerabilidade aparece na chamada de procedimento local avançado (ALPC) do próprio Windows, o que pode levar à fuga da área restrita do navegador e permitir que os invasores tenham privilégios SYSTEM em várias instalações do Windows e do Windows Server.

Link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
https://www.helpnetsecurity.com/2023/01/10/patch-tuesday-cve-2023-21674/

Produtos afetados. Qualquer sistema que utilize o Windows Advanced Local Procedure Call.

Solução: Atualizar os sistemas

Cisco

CVE-2023-20025
Data: 13/12/2022

Descrição. A Cisco tornou pública a informação sobre uma nova vulnerabilidade que permite fazer bypass de autenticação na interface de administração web apresentados por certos modelos de seus roteadores VPN e interfaces Cisco Small Business, presentes principalmente em pequenas empresas.
Os códigos de vários PoCs foram divulgados, mas não há evidências de exploração maliciosa. Além disso, a Cisco disse que não corrigirá as vulnerabilidades porque, em sua opinião, os produtos afetados são obsoletos e não deveriam ser usados.

Link:https://www.helpnetsecurity.com/2023/01/12/cve-2023-20025-cve-2023-20026/
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-cisco-85

Produtos afetados.

- Cisco RV Series Small Business Routers:
  - RV016 Multi-WAN VPN,
  - RV042 Dual WAN VPN,
  - RV042G Dual Gigabit WAN VPN,
  - RV082 Dual WAN VPN.
- IP Phone 7800 e 8800 Series.
- Cisco Industrial Network Director (IND).
- Cisco BroadWorks Application Delivery Platform Device Management Software.
- Cisco BroadWorks Xtended Services Platform.

Solução: Instalar os patches de segurança correspondentes.

PATCHES

Juniper Networks

Data: 12-01-2023

Descrição. A Juniper Networks publicou várias atualizações de segurança, um total de 36, para solucionar vulnerabilidades que afetaram vários de seus produtos. Essas vulnerabilidades podem levar ao controle do sistema da vítima se encadeadas. A organização recomendou consultar sua página de segurança para que cada administrador de um sistema avalie sua causa e veja sua solução.

Link:https://digital.nhs.uk/cyber-alerts/2022/cc-4015
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/12/juniper-networks-releases-security-updates-multiple-products
https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&f:ctype=[Security%20Advisories]

Produtos afetados:

- Juniper Networks Junos OS
- Juniper Networks Junos OS Envolved
- Juniper Networks MX Series
- Juniper Networks SRX Series

Solução: Consultar o seu portal de ajuda e segurança e instalar as atualizações correspondentes.

Fortinet

Data: 04/01/2022

Descrição. A Fortinet publicou várias atualizações de segurança para solucionar uma vulnerabilidade presente em várias versões do FortiADC. A exploração bem-sucedida da vulnerabilidade pode permitir que um invasor remoto execute códigos e comandos não autorizados usando solicitações HTTP específicas. A empresa recomenda que a atualização seja feita o mais rápido possível, dada a criticidade da vulnerabilidade.

Link: https://www.fortiguard.com/psirt/FG-IR-22-061
https://www.cybersecurity-review.com/news-january-2023/fortinet-releases-security-updates-for-fortiadc/

Produtos afetados:

- FortiADC version 7.0.0 through 7.0.1
- FortiADC version 6.2.0 through 6.2.3
- FortiADC version 5.4.0 through 5.4.5
- FortiADC all versions 6.1
- FortiADC all versions 6.0

Solução: Atualizar as novas versões dos produtos afetados.

EVENTOS

CactusCon 2023

27 a 28 de janeiro de 2023

A conferência anual de hackers e segurança conhecida como CactusCon é amplamente considerada um dos maiores eventos da indústria no estado do Arizona (Mesa). Em sua reunião mais recente, contou com a presença de quase 1.500 pessoas de todas regiões dos Estados Unidos. Ao longo dos últimos nove anos, o evento consolidou sua posição como uma conferência de segurança de primeira linha e rapidamente se tornou um evento educacional e de networking.

A CactusCon se adapta continuamente para atender aos requisitos e está em constante desenvolvimento para acompanhar a comunidade de segurança da informação. O evento atrai líderes do setor muito procurados, apresenta oficinas sobre temas de última geração e oferece amplas oportunidades para relacionamento e contato com pessoas que possuem interesse semelhante em segurança da informação.

Link: https://www.cactuscon.com/cc11

Barcelona Cybersecurity Congress

31 de janeiro a 2 de fevereiro de 2023

Esta feira, organizada pela FIRA Barcelona e pela Agência de Cibersegurança da Catalunha, é um dos principais eventos de cibersegurança de nível internacional. O ponto de partida é colaborar para melhorar e aumentar a rede de empresas e clientes. Com base nisso, a organização se concentrou nas novidades e desafios futuros em matéria de cibersegurança.

Para esta quarta edição, a diretoria do Barcelona Cybersecurity Congress espera receber mais de 16.000 visitantes de 120 países. À sua disposição estará uma área de exposição na qual cerca de trinta empresas terão seu próprio estande. De acordo com as últimas edições, a organização manteve sua aposta nas startups, criando um espaço para que 12 destas empresas se tornem conhecidas.

Link: https://www.barcelonacybersecuritycongress.com/

Dia da Internet Segura

7 a 9 de fevereiro de 2023

Em 7 de fevereiro de 2023, é comemorado mundialmente o Dia da Internet Segura, ou Safer Internet Day #SID2023, com o tema desta edição sendo “Juntos por uma internet melhor (Together for a better internet)”.

O Dia da Internet Segura, ou Safer Internet Day (SID), é um evento internacional organizado pela rede INSAFE/INHOPE de Centros de Segurança na Internet na Europa, com o apoio da Comissão Europeia. Esta iniciativa é realizada em todo mês de fevereiro para promover o uso seguro e positivo da tecnologia, especialmente entre crianças e jovens.

Link: https://www.incibe.es/sid

ManuSec Europe

27 a 28 de janeiro de 2023

MauSec é uma plataforma exclusiva para líderes de segurança de TI e TO da indústria de manufatura da Europa trocarem conhecimentos aprofundados sobre cibersegurança. Profissionais de cibersegurança compartilham conhecimento em primeira mão por meio de casos reais, debates etc. jovens.

Link: https://europe.manusecevent.com/

RECURSOS

CFSSL

A geração de certificados é um dos principais problemas para os administradores, no sentido de fazê-los de forma correta e rápida. A Cloudflare gerou uma ferramenta para gerar os bundles de forma simples. Esta ferramenta é escrita na linguagem Go e os binários podem ser baixados do repositório ou compilar a partir do código-fonte do mesmo site.

Blog da Cloudflare: https://blog.cloudflare.com/introducing-cfssl/

LInk: https://github.com/cloudflare/cfssl

Winpeas (Windows Privilege Escalation Awesome Scripts)

Ferramenta que permite auditar um sistema Windows, permitindo o escalonamento de privilégios dentro do ambiente.

Link: https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

LinPEAS (Linux Privilege Escalation Awesome Scripts)

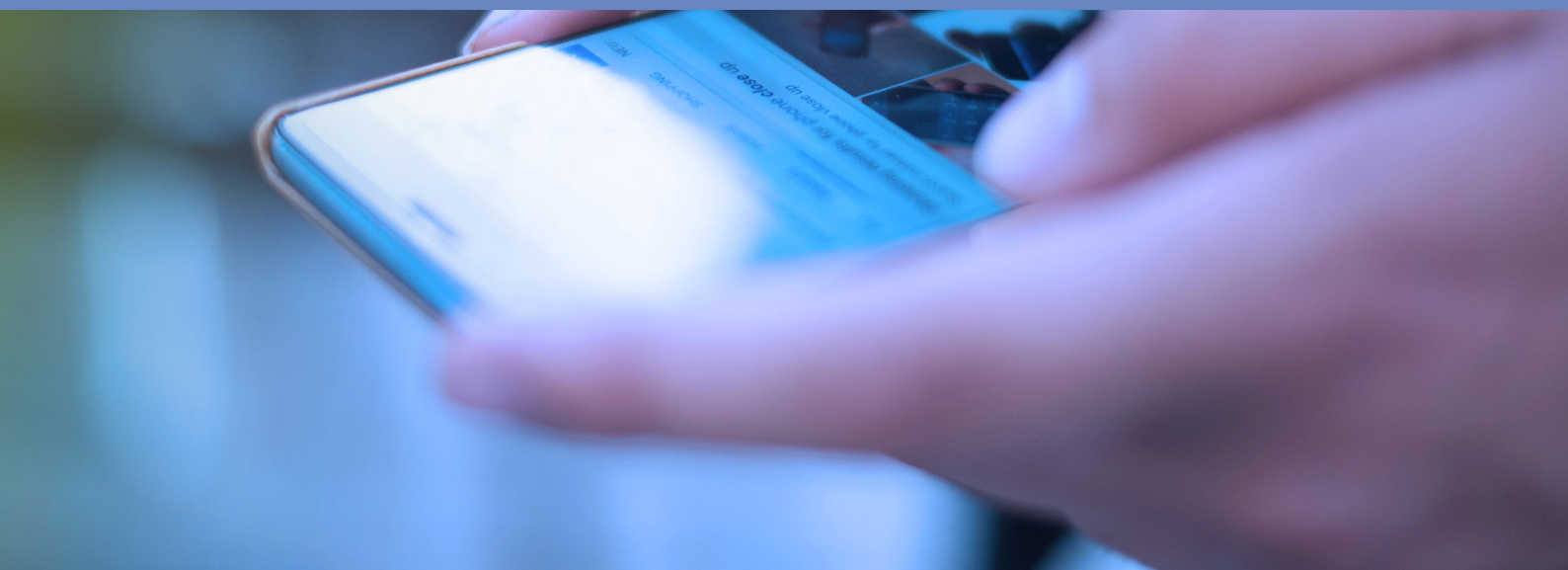
Ferramenta que permite auditar um sistema Linus, permitindo o escalonamento de privilégios dentro do ambiente.

Link: O que é e-mail spoofing e como pode ser identificado? | INCIBE

LinPEAS (Linux Privilege Escalation Awesome Scripts)

A Ashton Rodenhiser da Mind's Eye Creative criou gravações gráficas das apresentações da Cumbre SANS Pen Test HackFest. Se você perdeu alguma palestra ou quer ver a Cumbre por uma lente visual, basta checar o seguinte link:

Link: https://github.com/carlospolop/PEASS-ng



RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Cibersegurança en NTT DATA Latam y Perú

maria.pilar.torres.bruna@emeal.nttdata.com

Marcelo Nascimento

Gerente de Cibersegurança en NTT DATA Brasil

marcelo.nascimento.junior@emeal.nttdata.com

Javier Mauricio Albarracin

Director de Cibersegurança en NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

Fernando Vilchis

Director de Cibersegurança en NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Cibersegurança en NTT DATA EE.UU

nestor.ordonez.ramirez@emeal.nttdata.com

Carolina Pizarro

Director de Cibersegurança en NTT DATA Chile

carolina.pizarrodiaz@emeal.nttdata.com

Ou escreva para nossa caixa de correio principal: ciberseguridad_latam@emeal.nttdata.com


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com