Março 2024

NTT DATA

Radar

Powered by women

A adoção da IA nas áreas de cibersegurança

Por Maria Pilar Torres

Certamente, todos os leitores desta revista já se perguntaram várias vezes nos últimos meses até onde a IA e a IA generativa podem contribuir para nossas áreas de cibersegurança. Estamos vendo como esta tecnologia avança de forma segura em outras áreas das organizações, um fato constatado no estudo recente realizado pela NTT DATA e o MIT, sobre a adoção de IA, com foco na América Latina. Em nossa área, temos um déficit de talento especializado e muitas tarefas repetitivas onde parece que esta tecnologia poderia desempenhar um bom papel.

Para nos aprofundarmos um pouco mais neste ponto, realizamos um exercício para compreender como a IA está sendo utilizada nas áreas de cibersegurança, para o qual foi lançada uma simples pesquisa. Além de todos os detalhes que constam no relatório com os resultados, gostaria de compartilhar vários outputs.

Materialização do valor investido em IA em cibersegurança

"Mais de 95% das organizações acreditam que a IA terá um impacto médio ou alto nas áreas de cibersegurança"

A IA está gerando altas expectativas em cibersegurança e isso se reflete em orçamento investido e em apoio da organização. Isso significa que os CISOs devem materializar e quantificar o valor investido em IA em sua área, demonstrando que alguns dos benefícios esperados foram atingidos. Esse desafio tem uma maior importância nas organizações que declaram estar utilizando IA nas áreas de cibersegurança há mais de três anos.

Definição de casos de uso concretos de IA em cibersegurança

"Acredita-se que o SOC seja a área em que a IA pode oferecer mais apoio, e se formos para os domínios do NIST, há uma opinião bastante generalizada de que os domínios: identificar, proteger, detectar, responder podem ser muito beneficiados com a IA."

A definição de casos de uso permitirá explicar como a IA está sendo adotada na cibersegurança, ao mesmo tempo em que limita o escopo a avaliar e quantificar. Atualmente, podemos começar com a definição de casos de uso do SOC e posteriormente estender para os domínios do NIST e a outros campos, como governança ou riscos.

Gestão de talentos em IA e Cibersegurança

"O talento, ou melhor, a falta dele, é a principal barreira para a adoção da IA"

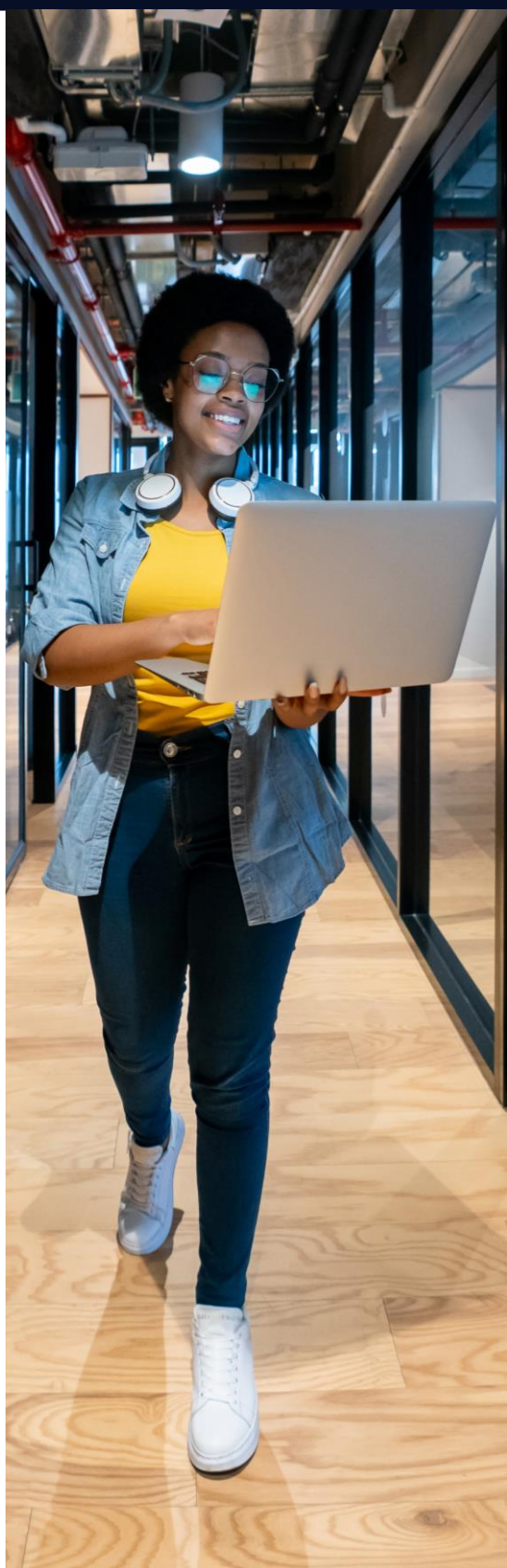
As organizações devem considerar que carreira darão aos profissionais especializados em IA e cibersegurança. Essas pessoas buscam novos desafios e, se não as encontram em uma organização, mudam para outra. Buscar resiliência na rotatividade desse pessoal chave também deve ser parte da estratégia de adoção da IA.

Consta no relatório que a presença da IA nas áreas de cibersegurança é um fato, em algumas há vários anos. Portanto, é o momento de amadurecer o papel da IA e maximizar o seu valor.

As novas regulamentações de cibersegurança de 2024

Por Marta Fernández

São muitos os desafios de cibersegurança para 2024, desde a IA, a segurança na nuvem, a falta de talentos, a conscientização dos funcionários e da sociedade até a preparação para a era quântica, mas este ano devemos destacar que, estamos diante de regulamentações que entrarão em vigor e, portanto, a conformidade regulatória e a gestão adequada de riscos serão uma das principais questões que constarão nas agendas de muitos CISOs e profissionais de cibersegurança.



Durante o ano de 2024, várias regulamentações entrarão em vigor ou serão atualizadas/revisadas. Por exemplo, o RGPD pode ficar mais rigoroso e será apresentado o primeiro pacote de normas técnicas sobre a Lei de Resiliência Operacional Digital (DORA), que entrará em vigor nas entidades financeiras de toda a UE em janeiro de 2025. Além disso, teremos novidades com a nova regulamentação NIS2, a entrada em vigor do WP.29 e a possível votação da Lei de IA da UE. Portanto, é importante compreender o alcance e o impacto de cada uma dessas regulamentações de 2024 em cada organização e se preparar, pois o descumprimento delas pode acarretar graves consequências legais, financeiras e de reputação. Neste artigo, vamos nos aprofundar no fascinante mundo das legislações e novas regulamentações de cibersegurança que entrarão em vigor este ano.

A União Europeia dá passos firmes no quesito segurança. Este ano, entra em vigor a diretiva NIS2, adotada em 14 de dezembro, cujas medidas devem ser implementadas até 17 de outubro. O novo NIS2 rompe as limitações de sua antecessora, a NIS1 (UE 2016/1148), permitindo estabelecer um nível alto e comum em toda a União. Destaca a resiliência de terceiros e prestadores de serviços de infraestruturas críticas. Tem abordagem clara na gestão de riscos, incluindo disposições específicas para notificação de incidentes de cibersegurança. Com isso, promove o compartilhamento de informações e a cooperação público-estratégica para o gerenciamento de crises cibernéticas e divulgação de vulnerabilidades. Nessa ênfase de riscos, também aborda especialmente a segurança na Cadeia de Suprimentos. A regulamentação também traz consigo medidas que levam ao monitoramento e supervisão do cumprimento para evitar sanções. Portanto, é recomendável que as organizações obrigadas ao cumprimento desta regulamentação comecem a definir um plano de cibersegurança para lidar com os novos requisitos trazidos por esta regulamentação, que têm como ponto de partida o Threat Intelligence.

Por outro lado, uma normativa que terá mais impacto e transcendência é a legislação e regulamentação sobre inteligência artificial (IA). Espera-se que a lei seja ratificada durante o primeiro trimestre de 2024 e sua aplicação total está prevista para 2026. Embora as tecnologias de IA não sejam novas, estamos vivenciando uma crescente adesão e uso acompanhados por desafios técnicos, comerciais e de segurança. Esses desafios têm um alcance global, tanto para organizações quanto para cidadãos e sociedade. Muitos debates foram abertos para responder como o uso da IA será monitorado e como os dados compartilhados através dela serão regulamentados e, por fim, como será controlada a conformidade do uso sob requisitos legais e inclusive éticos.

A prioridade do Parlamento com a publicação desta regulamentação é garantir que os sistemas de IA utilizados na UE sejam seguros, transparentes, rastreáveis, não discriminatórios e respeitosos com o meio ambiente. Em suma, a lei de Inteligência Artificial é a primeira regulamentação sobre IA em nível mundial, cujo objetivo é regular a inteligência artificial (IA) a fim de garantir melhores condições de desenvolvimento e utilização dessa tecnologia inovadora.

Em abril de 2021, a Comissão propôs o primeiro marco regulatório da UE para a IA. A lei também aborda o nível de risco, podendo ser Mínimo, Alto e Inaceitável. Estabelece-se uma avaliação categorizando os sistemas de IA, os quais podem ser modelos funcionais, modelos altamente capazes e modelos com propósitos gerais. Esta regulamentação estabelece proibições para a utilização da IA e protege os direitos dos usuários, que devem ser informados quando houver tratamento por parte da IA. O objetivo é chegar a um acordo até o final deste ano. Com base no nível de risco, a nova regulamentação estabelece obrigações para fornecedores e usuários. Vamos analisar os diferentes níveis, começando pelo de maior exposição ao risco:

- **Os sistemas de IA de risco inaceitável** são aqueles considerados uma ameaça para as pessoas e serão proibidos. Isso inclui sistemas que podem levar à manipulação cognitiva, classificação de pessoas, biometria e reconhecimento facial.
- **Sistemas de IA de alto risco** são aqueles que afetam negativamente a segurança ou os direitos. Isso inclui sistemas de IA utilizados em produtos sujeitos à legislação da UE sobre segurança de produtos e também a áreas específicas como: identificação biométrica e categorização de pessoas físicas, gestão e exploração de infraestruturas críticas, educação e formação profissional, emprego, gestão de funcionários e acesso ao autoemprego, acesso e desfrute de serviços privados essenciais e serviços e benefícios públicos, aplicação da lei, gestão da migração, asilo e controle de fronteiras e assistência na interpretação jurídica e aplicação da lei.
- **Sistemas de IA de risco limitado** devem cumprir requisitos mínimos de transparência

A IA está transformando a cibersegurança com sistemas de detecção e resposta automatizados, mas também gerando preocupações com potenciais ataques automatizados e com invasores que se utilizam dela para desenvolver ataques mais sofisticados e difíceis de detectar. Antecipar-se aos novos ataques e aumentar a capacidade de detecção e resposta é outro dos grandes desafios.

A cibersegurança também se aplica a produtos como carros, que cada vez incluem mais funcionalidades baseadas em software e conectividade. Por isso, desde julho de 2022, todos os fabricantes de automóveis devem cumprir o novo regulamento WP.29 UN R155/R156 para obter a homologação do veículo. WP.29 é o nome do Fórum Mundial para a Harmonização da Regulamentação de Veículos, que faz parte da Comissão Econômica das Nações Unidas para a Europa (UNECE).

A partir de julho de 2024, o requisito de homologação sob esta regulamentação será obrigatório para todos os novos veículos vendidos na União Europeia, independentemente de quando o fabricante tenha obtido a homologação do tipo de veículo. De fato, é possível que, a fim de cumprir o regulamento, alguns modelos mais antigos que ainda estão em produção tenham que passar por mudanças para serem homologados novamente. O objetivo desta regulamentação é garantir que exista um marco de gestão de segurança sobre os carros. A partir deste ano, os carros deverão ser certificados nesta regulamentação, garantindo que estejam seguros diante da possibilidade de uma ameaça cibernética ou de um possível ataque através de vulnerabilidades do software do veículo, sensores ou qualquer outro serviço conectado.

Resumindo, as regulamentações visam fornecer o marco normativo para padronizar e estabelecer requisitos mínimos que garantam sempre a segurança dos dados e das pessoas. Estamos vivenciando um momento de transformação, com novas tecnologias, produtos e elementos da cadeia de suprimentos, entre outros. O controle e a mitigação do risco de segurança que acompanham essa transformação são cruciais para evitar catástrofes e grandes perdas, bem como para a resiliência diante de possíveis ameaças. As regulamentações fornecem um marco excelente e guia para cumprir essa missão.

Hackeamento Extremo

Por Mª Ángeles Gutiérrez

Primeiro foi no mundo da IT (TI): ao conectá-la à internet, a tornamos vulnerável e suscetível a ataques de hackers; depois, conectamos ao mundo da OT (TO), as fábricas, os caixas eletrônicos; há alguns anos também a IoT; e, agora, em nós mesmos. Recentemente, foi anunciado que um chip cerebral foi implantado com sucesso, o que permitirá, entre outras coisas, controlar o telefone ou o computador e, através deles, quase qualquer dispositivo, apenas com o pensamento...

É verdade que há anos estamos incorporando diferentes dispositivos em nosso corpo, estamos falando de: marca-passos, implantes cocleares (estimulação direta do nervo auditivo), neuroestimuladores (para tratar epilepsia ou dor crônica através da estimulação direta de áreas do cérebro ou nervos periféricos), monitores de glicose implantáveis, implantes retinianos oculares (restauram parcialmente a visão ao estimular a retina com sinais elétricos), chips RFID subcutâneos (dispositivos de identificação por radiofrequência), próteses neurocontroladas, sensores de pressão (usados para monitorar a pressão intracraniana), biomarcadores implantáveis (detectam e monitoram biomarcadores específicos no corpo para fornecer informações sobre a saúde em geral), mas os últimos anúncios, como o do NeuraLink, vão um pouco além... conectamos nosso próprio cérebro, nos tornamos um terminal a mais. Conectados à rede? Expostos como qualquer dispositivo a ser hackeado?

A convergência entre tecnologia e corpo humano certamente apresenta novos desafios; a crescente integração de dispositivos eletrônicos no corpo, conhecida como corpo conectado ou cibernético traz desafios significativos.

A coleta constante de dados biométricos e de saúde permitidos por esses dispositivos preocupa a privacidade individual e introduz novas vulnerabilidades; os dispositivos implantáveis podem ser suscetíveis a ataques cibernéticos, comprometendo a integridade e a confidencialidade dos dados médicos e até mesmo colocando em risco a saúde do indivíduo com novas infecções e manipulações. Manter esses dispositivos seguros ao longo do tempo por meio de atualizações é um desafio técnico ainda não resolvido. Faltam padrões universais comuns que dificultam a interoperabilidade e a adoção em massa. Eles não se integram com segurança e eficiência ao sistema biológico sem efeitos colaterais.

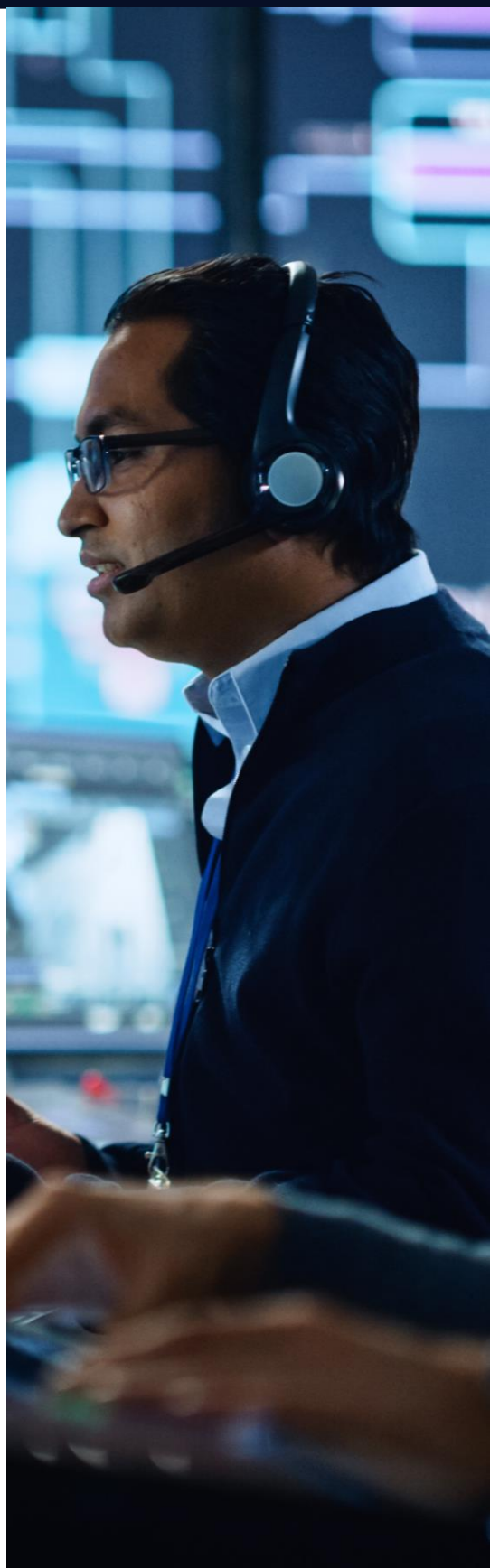
Por outro lado, ainda falta analisar a aceitação dessas tecnologias por parte da população e como isso afeta a percepção da identidade e autonomia individual, assim como o impacto na autoestima. A pressão para se conformar com padrões de beleza ou desempenho pode criar uma cultura de insegurança e insatisfação com o corpo natural, assim como intensificar as desigualdades, criando lacunas entre aqueles que têm ou não acesso às mesmas. Como isso afetará as relações interpessoais é outra incógnita. Além disso, a dependência excessiva desses dispositivos pode afetar gravemente a capacidade do corpo de funcionar naturalmente, e a obsolescência tecnológica pode deixar as pessoas em situações de risco se os dispositivos falharem ou se tornarem incompatíveis com as novas tecnologias.

Resumindo, tudo o que está conectado à rede ou possui um sistema “wireless” é suscetível a ser hackeado. Portanto, para não renunciar aos benefícios que certamente o "corpo conectado" nos trará (o que será uma grande oportunidade para milhares de pessoas paraplégicas, com ELA, perda de visão, afasia,...), e para prevenir e evitar a grande tentação que certamente representará tentar acessar informações sobre nossa saúde, e até mesmo diretamente aos nossos pensamentos, manipulando-os, para evitar esse "hackeamento extremo", devemos disponibilizar para esses novos usos todo o conhecimento adquirido sobre segurança, tanto do ponto de vista técnico quanto normativo e regulatório. Não cometamos novamente o erro de implantar em larga escala tecnologias imaturas do ponto de vista da cibersegurança, pois muito está em jogo, neste caso, a saúde e até mesmo a vida.

Governança de identidades

Por Andea Muñoz

Desde a era da Revolução Industrial, as empresas evoluíram e, com isso, se adaptaram às necessidades de um mercado mutável, com base nas novas descobertas e requisitos da indústria. No entanto, desde a chegada da internet, essa evolução deu uma volta muito grande e iniciou uma aceleração exponencial, exigindo as empresas a se adaptarem mais rapidamente às mudanças. Um dos pilares dessa evolução é a transformação digital, que pode ser resumida como a adoção de tecnologia em todos os processos de negócios.



Em 2020, com a Covid-19, essa transformação foi forçada e as empresas foram obrigadas a se adaptar. Mas o que significa ter uma empresa no mundo digital? O que significa para as empresas não controlar os dados e informações que passam por ela? Todos esses desafios começaram a se tornar perguntas que exigiam uma resposta imediata. Antes da transformação digital, todos os dados e informações das empresas estavam fisicamente nelas, então os esforços eram direcionados para proteger o perímetro e evitar vazamentos de informações. Mas com a transformação digital, a necessidade de mobilidade, trabalho remoto e adoção da nuvem, o perímetro se expande tornando-se impossível de controlar, deixando as empresas sem fronteiras. A identidade das pessoas e os sistemas de autenticação se tornam relevantes para a proteção dos dados das empresas agora descentralizadas.

Outro ponto que gerou novas brechas de segurança e preocupações entre as áreas de segurança, mas que, no entanto, é uma tendência global e que facilita o trabalho das empresas, é a migração para a nuvem.

Conforme mencionado anteriormente, soma-se a mudança de gerações, que se tornam não apenas a força de trabalho mais importante, mas também o grupo consumidor mais forte. As gerações Millennials e Centennials já representam 59% da força de trabalho das empresas, e têm uma mentalidade à qual as empresas precisam se adaptar. É um pensamento que requer agilidade e atenção imediata às suas necessidades, uma vez que são gerações que cresceram com a tecnologia como parte fundamental de suas vidas.

Para essas gerações, a necessidade de mais tempo livre, flexibilidade no trabalho e possibilidade de trabalho remoto são alguns dos pontos-chave para manter o talento. Essas gerações também têm a expectativa de que os processos sejam realizados de maneira rápida e, em geral, por meio de aplicativos, sem filas, sem contato físico, melhorando a experiência do usuário. Tudo isso leva para as empresas a necessidade de se transformarem, a fim de permanecerem relevantes no mercado. Um exemplo claro disso é observar que as empresas maiores e com maior crescimento atualmente são empresas de tecnologia.

Com base em tudo isso e com o aumento das ameaças cibernéticas, cada vez mais empresas estão priorizando a segurança da identidade como um ponto-chave em suas estratégias de segurança, visando assim mitigar riscos e proteger seus ativos digitais. Isso é refletido no aumento das aquisições de tecnologias como IAM (*Identity and Access Management* ou Gerenciamento de Identidade e Acesso), PAM (*Privileged Access Management* ou Gerenciamento de Acesso Privilegiado) e MFA (*Multifactor Authentication* ou Autenticação Multifator), assim como nas recomendações de entidades como a Gartner, que destacam algumas dessas tecnologias como essenciais na estratégia das empresas e ressaltam sua importância.

As contas privilegiadas trazem consigo outros problemas que devem ser considerados, dependendo do sistema que está sendo gerenciado. Muitas senhas estão escritas no código do sistema, o que é uma prática ruim, embora mais comum do que se pensa. No entanto, se isso é feito para proteger a disponibilidade dos sistemas, pode resultar em senhas que não são alteradas por anos. Além disso, a brecha de segurança aumenta ainda mais quando se trata de ex-funcionários.

A tudo isso, devem ser somados os possíveis erros humanos. Os humanos são a parte fundamental das organizações, no entanto, várias brechas de segurança são geradas no recurso humano. Entre os erros mais comuns e devido à falta de treinamento em tecnologia da informação, está guardar senhas em locais inadequados, como em uma planilha do Excel, compartilhar senhas e deixar sessões abertas. Tudo isso aumenta a probabilidade de serem alvo de ataques.

O que é e o que envolve a governança de identidades?

A Governança de Identidades *(Identity Governance*) refere-se ao conjunto de processos, tecnologias e políticas utilizadas para gerenciar a identidade digital dentro de uma organização. Isso inclui a definição de funções das identidades (quais sistemas, como e com quais privilégios e autorizações uma identidade pode acessar) e garantir o gerenciamento adequado dessas atribuições. Uma identidade digital pode ser tanto uma pessoa que faz parte da organização, quanto um fornecedor ou um sistema com identidade digital. A governança de identidades inclui o provisionamento e desprovisionamento de identidades, bem como a gestão dos acessos das mesmas.

O que considerar para uma boa governança de identidades?

Para que uma empresa possa adotar a governança de identidades de forma eficaz, deverá considerar as seguintes recomendações:

Identificar as identidades e sua abrangência, tanto internas quanto de seus parceiros estratégicos e fornecedores, e os riscos associados ao seu gerenciamento. Da mesma forma, é necessário identificar os usuários com altos privilégios e as contas a que têm acesso. Para isso, é recomendada uma consultoria de governança de identidades.

Desenvolver políticas e procedimentos que permitam determinar de forma clara a gestão das identidades na empresa, como os usuários serão criados, como serão desativados, com quais autorizações e sob qual esquema e procedimento, que devem estar alinhados com as melhores práticas de segurança e privacidade de dados.

Analisar e implementar as tecnologias adequadas tanto de IAM quanto de PAM; para isso é recomendável elaborar uma matriz de necessidades a serem atendidas, quantidade de usuários que terão acesso à tecnologia e qual a abrangência desejada em termos de casos de negócio e tecnologias da empresa que devem ser integradas. Esta análise prévia é fundamental para o sucesso da adoção da tecnologia, permitindo que a empresa possa explorar adequadamente o que foi adquirido e evitar a subutilização de tecnologias.

Para o ponto anterior, é muito importante contar com um parceiro estratégico para consultoria, implementação e implantação da tecnologia. Ter um parceiro adequado com experiência e conhecimento em governança de identidade, bem como em outros aspectos de segurança, é fundamental para o sucesso.

Envolver e educar os usuários que fazem parte da organização sobre como manter suas senhas e acessos protegidos, bem como a importância da adoção tecnológica, facilitará o caminho e reduzirá a resistência à mudança.

Monitorar e revisar continuamente a conformidade com as políticas de gerenciamento de identidades, a consistência dos dados manipulados e a eficácia dos controles aplicados, para isso, podem ser realizadas auditorias e análises constantes do gerenciamento de identidades.

Outra boa prática é a integração das soluções de IAM e PAM com outras ferramentas de segurança para detecção e resposta oportuna a incidentes de segurança.

Por fim, é importante considerar a conformidade regulatória aplicável à indústria e ao país onde esteja situada, levando em conta aspectos como a lei de proteção de dados pessoais e padrões de segurança, como a ISO 27001.

Maximizando a resiliência cibernética

Por Almudena Abolafia

No sempre dinâmico panorama da cibersegurança, a prevenção proativa e a preparação são essenciais.

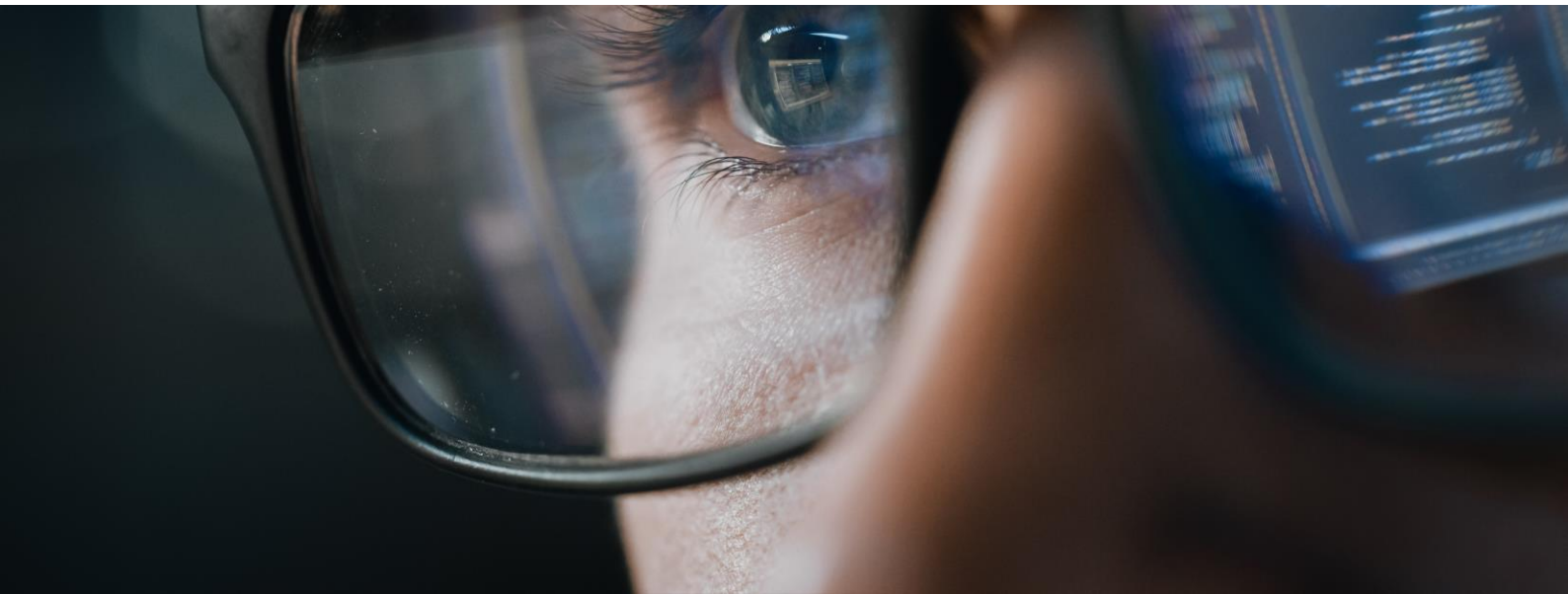
Neste artigo, exploraremos como a integração estratégica de *Cyber Threat Intelligence* (Inteligência de Ameaças ou CTI – siglas em inglês) e a Simulação de Adversários pode potencializar a resiliência cibernética das organizações. Essas duas disciplinas, se combinadas de maneira eficaz, oferecem uma abordagem holística para identificar, avaliar e mitigar as principais ameaças cibernéticas.

Quando falamos de CTI, não estamos apenas falando sobre coletar dados; é muito mais do que isso. Trata-se de um processo dinâmico e contínuo de coleta de dados, análise minuciosa e aplicação de informações específicas sobre ameaças, agentes maliciosos ou *threat actors*, como são mais comumente conhecidos, e suas motivações. Essa inteligência pode vir de fontes externas como, por exemplo, feeds de ameaças e IOCs publicados, bem como de fontes internas, como registros de eventos de segurança identificados pelas equipes de Blue Team ou atividades de threat hunting na rede interna de uma organização para identificar indícios de atividade maliciosa ou não autorizada. Ao compreender as táticas, técnicas e procedimentos (TTPs) dos adversários, as organizações podem se antecipar e prevenir esses ataques por meio da criação de regras de detecção (detection rules) baseadas nessas TTPs e enfrentar as ciberameaças de maneira eficiente.

Por outro lado, a Simulação de Adversários, frequentemente confundida com "exercício de Red Team", vai além do clássico *pentesting* ou teste de intrusão, onde o foco está na identificação de vulnerabilidades. Neste caso, estamos falando de emular threat actors e replicar, na medida do possível, as TTPs que eles usam em seus ataques, o que permite avaliar a resiliência da postura de segurança de uma organização e fornecer uma visão realista de sua capacidade de detecção e resposta às possíveis vulnerabilidades e fraquezas que enfrentariam em um ciberataque real. A principal diferença entre um exercício de Simulação de Adversários e um exercício de Red Team reside, precisamente, na necessidade de colaboração entre a equipe de CTI e a de Red Team durante a fase de preparação do exercício.

Como uma equipe de CTI enriquece uma equipe de Red Team?

A sinergia entre a equipe de CTI e a de Red Team é crucial para uma postura eficaz de cibersegurança. A Inteligência de Ameaças (CTI) informa e personaliza os cenários de simulação de adversários, melhorando significativamente a capacidade da equipe de Red Team de projetar um cenário de ataque adaptado às principais ameaças que a organização enfrenta. Por exemplo, a identificação pela equipe de CTI do APT38 como um agente malicioso que se concentra em instituições financeiras permite que uma equipe de Red Team que presta serviço a um banco modele ataques específicos com base nas mesmas TTPs e artefatos que este threat actor utiliza, ajudando a organização a identificar seus principais pontos fracos e aumentar seu nível de maturidade em cibersegurança, através da melhoria de sua capacidade de detecção e resposta a ciberataques.



Para que essa sinergia seja bem-sucedida, devem ser realizadas as seguintes atividades:

Identificação dos principais threat actors que operam no setor da organização-alvo e/ou que recentemente afetaram seus concorrentes, fornecendo contexto sobre as TTPs utilizadas e os objetivos do ataque. Este exercício é realizado pela equipe de inteligência de ameaças (CTI) durante a chamada "fase de preparação" de um exercício cibernético ou ciberataque.

Modelagem de ataques com base nas informações do CTI obtidas anteriormente, o que permitirá projetar cenários de ataque realistas.

Personalização dos cenários de ataque, levando em consideração as ferramentas (artefatos) e técnicas específicas utilizadas pelos grupos de threat actors que serão emulados contra a organização-alvo.

Análise das vulnerabilidades que serão alvo de exploração durante o exercício. Compreendê-las permitirá que as organizações identifiquem onde devem concentrar seus esforços para uma detecção proativa e uma resposta rápida que melhore sua postura de segurança e minimize o impacto de possíveis brechas de segurança.

Ao alinhar as simulações do Red Team com ameaças específicas, as organizações podem maximizar a eficiência de seus recursos de segurança, concentrando-os nas áreas mais críticas. Além disso, o feedback constante entre a equipe de CTI e Red Team garante uma melhoria contínua do serviço, adaptando a postura de segurança da organização às ameaças emergentes.

Na NTT DATA, acreditamos que a integração profunda dos serviços de Threat Intelligence e Simulação de Adversários representa um marco crucial na evolução das estratégias de cibersegurança. Por isso, dentro do nosso catálogo de serviços, promovemos a realização desses exercícios, pois ao unir essas duas disciplinas, as organizações se beneficiarão na defesa contra ameaças atuais e se posicionarão estrategicamente para enfrentar desafios emergentes que possam afetar seu setor. A resiliência cibernética e a cibersegurança efetiva vão além da proteção; são o resultado de uma mentalidade proativa e evolutiva.

A sinergia entre a Threat Intelligence e a Simulação de Adversários é o caminho para uma postura de segurança mais sólida e adaptativa, maximizando a resiliência cibernética de qualquer organização.

Inteligência Artificial: Navegando na fronteira entre defesa e ataque

Por Mafalda Maciel

Descobrimos que a Inteligência Artificial não é apenas uma nova palavra da moda ou uma tendência "sexy" no mundo da tecnologia. De fato, a Inteligência Artificial incorpora campos que já conhecemos há muito tempo, como Aprendizado de Máquina (Machine Learning) e Aprendizado Profundo (Deep Learning), com provas demonstradas, e agora tem um novo foco e seu uso se democratizou. No entanto, sua rápida evolução e uso pela sociedade, como já demonstraram vários estudos, preocupam os profissionais de cibersegurança. Além disso, diria que a sociedade inevitavelmente terá que enfrentar.

Podemos ver o problema a partir de duas perspectivas. Por um lado, sabemos que essa tecnologia mudará a forma como trabalhamos, acelerará processos lentos, permitirá aumentar a produtividade e combater a falta de profissionais nesse campo. As organizações que não embarcarem no trem da inovação inevitavelmente ficarão para trás, como já vimos historicamente. Por outro lado, sabemos que a linha que separa os aspectos positivos dos perigos iminentes que a Inteligência Artificial nos traz é tênue, e que, geralmente, os invasores sempre tentam estar um passo à frente. Como qualquer herói, a Inteligência Artificial também terá seu vilão.

Os impactos positivos que a Inteligência Artificial traz para a cibersegurança são inegáveis: uma automação maior e melhor na detecção e resposta a ameaças, com a possibilidade de analisar volumes massivos de dados com uma velocidade sem precedentes e, portanto, identificar anomalias mais rapidamente, permitindo que as equipes de segurança antecipem riscos e ameaças de forma mais eficaz, e também ajudem nessa crise de recursos humanos especializados que estamos enfrentando; uma análise de padrões e comportamentos mais rápida; sistemas adaptativos que evoluem para lidar com novas ameaças; aumento da previsibilidade e da capacidade e velocidade de tomada de decisões baseadas em dados e informações concretas. Em suma, a Inteligência Artificial pode e deve ser utilizada como uma ferramenta aliada, que nos ajuda em termos de produtividade, análise de informações e rapidez de resposta neste ambiente de rápida transformação em que vivemos.

No entanto, assim como qualquer tecnologia, também traz novos riscos e, para a cibersegurança, representa um novo fator de rapidez, sofisticação e alcance dos ataques. À medida que as barreiras de defesa evoluem, também progridem as táticas utilizadas por agentes maliciosos. A automação leva à exploração de vulnerabilidades em grande escala que, aproveitando-se também da adaptabilidade dos sistemas, aprendem novas formas de contornar as barreiras de segurança à medida que as encontram; táticas de engano e evasão que imitam o comportamento humano legítimo, dificultando sua detecção; o reconhecimento orientado por Inteligência Artificial que permite uma análise minuciosa e mais rápida de possíveis alvos, identificando vulnerabilidades e pontos de entrada na infraestrutura de uma organização; a capacidade de criar mensagens de phishing, smishing e vishing altamente direcionadas e convincentes, que, juntamente com o uso de deepfake, eleva todo o campo da engenharia social a um nível mais sofisticado, imprevisível e difícil de detectar, e traz uma nova disrupção no que diz respeito às precauções e mecanismos de defesa que devemos fornecer aos nossos colaboradores.

Além do conflito moral e ético que surge do uso da Inteligência Artificial Generativa - sobre a qual cada vez mais instituições, estatais e não estatais, estão investigando - e dos perigos relacionados ao compartilhamento não intencional de dados pessoais e informações sensíveis, seja por desconhecimento, falta de medidas tecnológicas para prevenção, ou até descuido, surge uma exposição aumentada do que muitos consideram o elo mais fraco e, para outros, a primeira linha de defesa das organizações: o elemento humano.

O uso massivo desta nova tecnologia acabou de começar, e já tem um alcance maior do que qualquer outra tecnologia ou plataforma vista anteriormente, e as consequências já estão sendo sentidas. Embora ainda não existam estudos em larga escala sobre o impacto que a Inteligência Artificial terá na segurança da informação e na cibersegurança do ponto de vista do risco humano, nem análises estatísticas muito concretas, já estão surgindo os primeiros casos de ataques perpetrados com base em tecnologias de Inteligência Artificial Generativa.

A conscientização dos colaboradores e da sociedade em geral sobre Segurança da Informação continua sendo um dos pontos menos evidentes e de maior dificuldade de execução. Ainda enfrentamos o desafio de preparar e alertar os colaboradores das organizações sobre os riscos e a importância da segurança, e fazer isso de forma eficaz e com resultados, resultados estes difíceis de medir, porque as variáveis são muitas e difíceis de quantificar e qualificar.

Então, como devemos proceder diante dessas novas e aprimoradas ameaças? Como ensinamos a detectar ataques cada vez mais convincentes, à primeira vista? Como detectamos comportamentos anômalos quando eles se assemelham cada vez mais aos nossos? Teremos que nos reinventar e reinventar a forma como conscientizamos nossos colaboradores? Neste momento, surgem dúvidas para as quais, por enquanto, temos poucas respostas concretas.

As equipes de segurança devem repensar sua abordagem, adotando uma postura proativa e se adaptando à nova realidade gerada pela implementação de tecnologias defensivas avançadas, com foco na maximização da automação, detecção de ameaças, agilidade operacional e melhoria da tomada de decisões. A necessidade urgente de superar as limitações de recursos é, sem dúvida, uma área onde a Inteligência Artificial emerge como uma aliada essencial.

A dependência da IA não apenas como uma solução para a falta de recursos, mas como uma abordagem estratégica para enfrentar riscos e ameaças em constante evolução, é imperativa. Nesse sentido, a reorganização das equipes de segurança deve incorporar não apenas a implementação de tecnologias avançadas, mas também a contínua exploração de novas metodologias alinhadas com os desafios emergentes.

A construção de uma cultura de segurança sólida é crucial para a eficácia a longo prazo, envolvendo não apenas o treinamento dos colaboradores com conhecimentos atualizados, mas também a promoção de uma mentalidade vigilante nas atividades diárias, tanto profissionais quanto pessoais. Devemos incentivar a análise crítica, uma atitude de ceticismo saudável e a aplicação de boas práticas em todos os aspectos da vida cotidiana, estabelecendo, assim, uma linha de defesa sólida.

Por fim, a convergência da tecnologia e da cibersegurança é uma área desafiadora que requer a união estratégica da Inteligência Artificial com as capacidades humanas. Reconhecer a inevitabilidade dessa batalha tecnológica de titãs e abraçar a Inteligência Artificial como um aliado indispensável é a chave para fortalecer as organizações contra as ameaças emergentes.

Panorama de ameaças no setor de mineração

Por Julissa Emily Calderon

A evolução tecnológica no setor de mineração, a digitalização e a adoção de tecnologias avançadas para otimizar seus processos produtivos, como perfuratrizes e caminhões autônomos, gêmeos digitais, entre outros, criam um ambiente operacional cada vez mais conectado, o que introduziu novos riscos e ampliou a superfície de ameaças cibernéticas enfrentadas pelas empresas deste setor.

Ciberespionagem
A maioria das minas em todo o mundo são alvo de ataques para coleta de informações de inteligência de negócios. Os cibercriminosos podem ser patrocinados por grupos de interesse que veem as empresas de mineração como um "tesouro" ou até mesmo estados nacionais que lançam campanhas de espionagem, pois a mineração é um setor economicamente relevante para qualquer país.

Informações sobre exploração geológica, valor dos recursos naturais, estratégias corporativas de preços e patentes tecnológicas de exploração, extração e processamento contêm dados confidenciais e de propriedade intelectual atrativos para esses invasores.

Terceiros com acesso
A mineração é um setor com muitos fornecedores externos que trabalham em toda a cadeia produtiva, muitas vezes sem seguir boas práticas de segurança, podendo comprometer significativamente as operações.

Os incidentes relacionados a ataques de cadeia de suprimentos são uma modalidade em ascenção e representam um grande risco, pois os cibercriminosos buscam atingir o alvo por meio de fornecedores de confiança, que são parte fundamental da cadeia de valor e processos críticos das empresas. A falta de estabelecimento de regras e permissões com o mínimo de privilégio em sua conexão às redes deixa as portas de acesso “sem chave“, abertas a vulnerabilidades como *malwares*, podendo infectar a rede e até mesmo chegar aos sistemas de controle industrial, considerando que muitas empresas ainda não têm suas redes TI/TO segmentadas com controles de segurança perimetral robustos. Recentemente foi revelado que os ataques APTs em empresas industriais têm usado fornecedores como uma porta de entrada sigilosa que comprometeu a continuidade operacional.

Campanhas de Phishing:
As campanhas de phishing têm como alvo pessoas do setor de mineração, não apenas altos executivos, mas também superintendentes de operações, supervisores de sistemas de controle, técnicos de instrumentação e operadores.

Um ataque público ocorreu na empresa de mineração canadense Goldcorp que, devido a essa ameaça, perdeu aproximadamente 16 GB de informações confidenciais, incluindo informações de identificação, credenciais de funcionários e documentos orçamentários.

Por isso, ter um programa de conscientização direcionado aos funcionários de acordo com seu papel e funções na empresa, que compreendam sua participação e papel na cibersegurança, é de suma importância. Nem todo o pessoal está exposto da mesma forma ou terá um vetor de ataque em comum, portanto, é importante ter programas especializados para cada perfil, a fim de prepará-los para qualquer situação de perigo.

As ameaças no setor de mineração estão evoluindo a um ritmo crescente, portanto, é importante que os responsáveis pela operação compreendam o atual panorama dos riscos com os quais estão lidando continuamente. Existe um desafio significativo ao definir ações que permitam às empresas gerenciar os riscos que possam afetar e comprometer as operações industriais, por isso é crucial estar preparado para proteger seus principais ativos, a fim de prevenir ameaças em tempo real e bloquear ataques emergentes, aplicando controles e políticas de "zero trust" que os protejam contra qualquer ataque.

Navegando pela privacidade de um mundo interconectado

Por Emily Pereda

Na era da hiperconectividade, nossa vida cotidiana foi profundamente transformada pela tecnologia, oferecendo comodidades e eficiências que eram inimagináveis há apenas algumas décadas. Dispositivos IoT, sistemas de domótica e veículos conectados transformaram o que antes eram conceitos futuristas em componentes integrais de nossa realidade diária; no entanto, essa transformação digital vem acompanhada de crescentes preocupações sobre a privacidade e segurança dos dados pessoais. Como profissional em cibersegurança e, mais recentemente, como mãe, minha percepção sobre a tecnologia evoluiu para uma reflexão mais crítica sobre como essas inovações afetam a privacidade e segurança de nossas famílias.

IoT e Domótica: Comodidade às Custas da Privacidade?
A promessa de um lar inteligente se concretizou por meio de dispositivos IoT e sistemas de domótica, nos proporcionando controle remoto sobre iluminação, climatização e segurança; no entanto, a conveniência desses dispositivos vem com riscos inerentes. Cada dispositivo conectado representa um potencial vetor de ataque para cibercriminosos, que podem acessar dados pessoais sensíveis ou manipular a funcionalidade dos sistemas domésticos. Por exemplo, um ataque direcionado poderia comprometer câmeras de segurança, revelando detalhes íntimos de nossa vida cotidiana ou permitindo que intrusos monitorem nossos movimentos.

Quantas vezes nos deparamos com histórias ou vídeos sobre crianças desenvolvendo medo das câmeras de vigilância? Essas ferramentas, instaladas por nós para nos proporcionar tranquilidade ao poder observar os pequenos enquanto nos ocupamos de outras tarefas ou mesmo para monitorá-los à distância enquanto estamos no trabalho, deveriam ser um recurso seguro e confiável. No entanto, a realidade pode ser diferente. O medo nas crianças surge quando seu espaço, que deveria ser de segurança e conforto, é violado. Os incidentes documentados mostram como pessoas não autorizadas conseguem acessar essas câmeras, interagindo com as crianças e transformando um ambiente de proteção em um de vulnerabilidade e medo.

Essa invasão não apenas quebra a barreira física de segurança que tentamos manter ao redor de nossos filhos, mas também mina a confiança e a sensação de segurança que esses dispositivos são destinados a oferecer. Quando uma criança se sente ameaçada em sua própria casa, o dano vai além de um simples ato de invasão de privacidade; torna-se uma questão de segurança emocional e psicológica. A pergunta que surge então é crucial: Como podemos garantir que a tecnologia projetada para proteger nossos entes queridos não se torne uma fonte de ansiedade e medo para eles?

Responder a essa preocupante pergunta implica abordar o problema de várias maneiras, priorizando tanto a segurança tecnológica quanto a comunicação aberta e a educação. Em primeiro lugar, é fundamental selecionar dispositivos de vigilância de marcas reconhecidas que ofereçam altos níveis de segurança, incluindo criptografia avançada e autenticação de dois fatores, para dificultar o acesso não autorizado. Além disso, manter o software desses dispositivos constantemente atualizado garante que qualquer vulnerabilidade conhecida seja corrigida rapidamente.

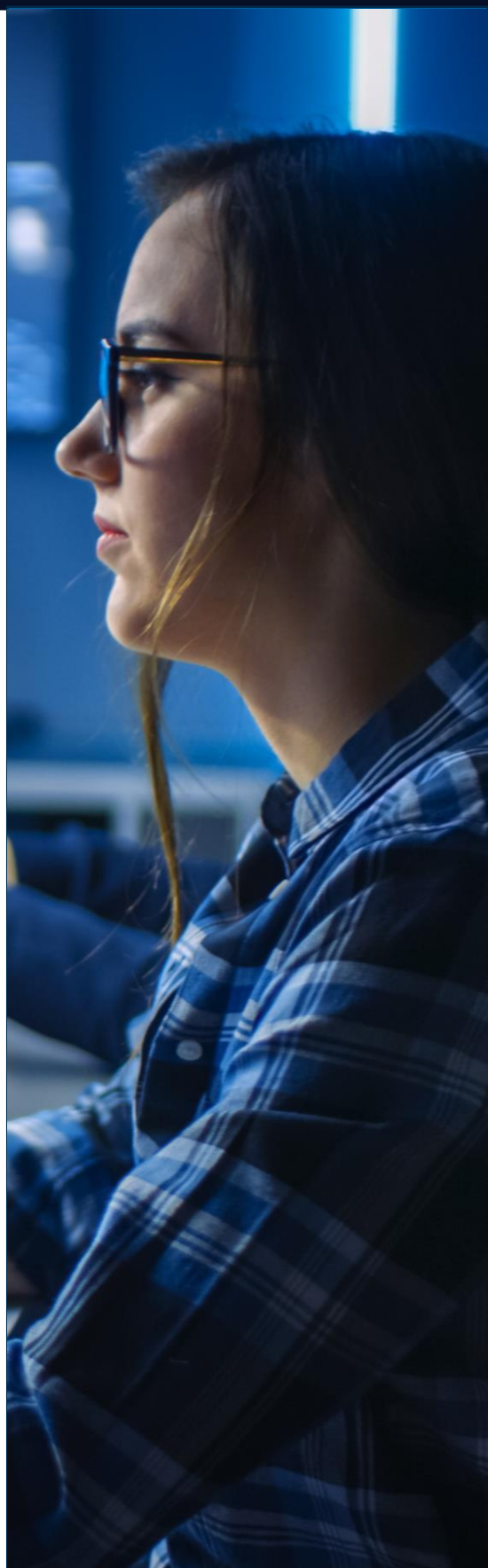
Por outro lado, a educação e a comunicação desempenham um papel crucial. É essencial ensinar às crianças sobre a tecnologia de uma maneira apropriada para sua idade, explicando como essas câmeras funcionam e qual é o propósito delas, reforçando a ideia de que são projetadas para mantê-las seguras. Além disso, é importante ouvir e validar seus sentimentos se expressarem medo ou preocupação, garantindo-lhes que estão protegidos e que as medidas de segurança estão em vigor para o seu bem-estar. Com medidas de segurança tecnológica robustas e comunicação eficaz e empática, podemos usar a tecnologia de vigilância para maximizar a segurança sem comprometer a sensação de segurança e conforto das crianças em seus lares.

No caso de crianças mais novas, que ainda não conseguem falar ou se expressar claramente, a situação é mais desafiadora, pois não podem comunicar diretamente o que estão sentindo. Aqui, a configuração que fazemos desempenha um papel fundamental para enfrentar essas dificuldades.

A evolução continua: além da biometria

Por Nelvys Pamela Porras

Com o avanço implacável da tecnologia, a inteligência artificial (IA) emerge como um elemento fundamental na transformação da gestão de acessos. A capacidade da IA de analisar e se adaptar aos padrões de comportamento do usuário oferece uma camada adicional de segurança. Os sistemas baseados em aprendizado automático podem identificar atividades anômalas e detectar possíveis ameaças antes que se materializem, proporcionando uma resposta proativa em vez de reativa.



A busca por novas formas de autenticação não para em biometria e autenticação multifatorial. A autenticação baseada em comportamento surge no horizonte como uma possível fronteira futurista. Esta abordagem envolve analisar como um usuário interage com dispositivos e plataformas, avaliando padrões de comportamento únicos. À medida em que os algoritmos melhoram, essa forma de autenticação promete ser mais resistente a ameaças e menos invasiva para a experiência do usuário.

As senhas tradicionais continuam sendo um ponto fraco na segurança digital. As ameaças de ataques de força bruta estão em constante evolução, aproveitando a crescente potência de computação e a sofisticação das técnicas. Hoje, observamos como essas ameaças emergentes desafiam a integridade das senhas e como a indústria responde a esses desafios em constante evolução.

Entender um pouco sobre as tendências dos usuários, os fatores que contribuem para a escolha de senhas fracas e a tendência à reutilização é importante. Compreender esses aspectos proporciona uma visão mais profunda de como as práticas de segurança podem se adaptar para lidar não apenas com as ameaças tecnológicas, mas também com os comportamentos humanos que colocam a segurança em risco.

Embora as impressões digitais e o reconhecimento facial tenham sido pioneiros na adoção da biometria, melhorias recentes podem ser observadas. Tecnologias como o escaneamento de retina, reconhecimento de voz e análise da dinâmica da escrita estão se tornando mais comuns, oferecendo uma gama mais ampla de opções biométricas. Essas tecnologias avançadas abordam os desafios de segurança e privacidade associados à biometria.

A biometria não se limita apenas ao desbloqueio de telefones ou gerenciamento de fotos; está se integrando em setores como o bancário, o de saúde e transporte, transformando a forma como interagimos com serviços essenciais e garantindo uma autenticação mais segura em vários cenários.

A preocupação com a privacidade e segurança dos dados biométricos continua sendo um tema central; para enfrentar essas preocupações, soluções inovadoras são observadas, como a descentralização de dados e o uso de *blockchain*, que buscam abordar essas preocupações; da mesma forma, regulamentações governamentais e padrões da indústria estão evoluindo para proteger a integridade dos dados biométricos.

São evidentes os avanços tecnológicos que estão fortalecendo a biometria, desde a melhoria na precisão dos sensores até a integração de inteligência artificial para a detecção de tentativas de falsificação ou roubo de identidade. Esses desenvolvimentos buscam abordar desafios prévios e melhorar a aceitação geral da biometria como método seguro e confiável.

A eliminação de senhas e a adoção da biometria visam melhorar a experiência do usuário; o design centrado no usuário molda interfaces intuitivas e processos de autenticação seguros, acessíveis e amigáveis para todos, independentemente de seu nível de experiência tecnológica.

Analisar a resistência à mudança na adoção de novas tecnologias de autenticação, bem como compreender a psicologia por trás da resistência à mudança permitirá o desenvolvimento de estratégias eficazes para a transição para métodos de autenticação mais seguros e avançados.

Além da biometria e da autenticação multifatorial, e examinar as novas formas de autenticação que poderiam surgir no futuro, desde a autenticação cerebral até a baseada em DNA, torna-se relevante determinar os limites da inovação e como poderiam revolucionar ainda mais a segurança digital.

A transformação constante no âmbito tecnológico traz desafios inesperados; antecipar-se a possíveis dilemas éticos, de segurança e de privacidade que poderiam surgir com novas tecnologias de autenticação e identificar esses desafios permitirá que a indústria se prepare e mitigue riscos potenciais.

A eliminação de senhas e a adoção da biometria não representam apenas uma mudança na gestão de acessos, mas o início de uma revolução mais ampla na segurança digital; os marcos alcançados até agora destacam como a indústria está liderando a vanguarda da inovação e delineando as perspectivas para um futuro digital seguro, eficiente e centrado no usuário.

Awareness no seu dia a dia ... Por que não?

Por Stephanie A. Ramos

Quando pensamos em awareness, sempre vem à mente se os usuários nas empresas entendem e têm conhecimento do que essa palavra, atividade ou ação implica, e a realidade é que, se olharmos para a maioria das empresas, ainda é um assunto pouco abordado. Agora, se pensarmos como indivíduos em nosso dia a dia, quem realmente aborda temas de awareness com regularidade?... Pouquissimas pessoas.

Se compartilhássemos este tema tão significativo com a importância que ele requer, com certeza evitaríamos muitos incidentes de segurança, não apenas na vida profissional, mas também no dia a dia; daríamos menos oportunidades para formas de extorsão, não exporíamos as empresas onde trabalhamos, os colegas de trabalho e os entes queridos.

Você já se perguntou como começaria uma estratégia a partir de seu contexto pessoal? O que você deixaria de fazer? Como comunicaria isso aos seus familiares e amigos? Sabemos que, estando em um mundo de cibersegurança, o assunto pode ser um pouco mais simples, pois temos o contexto à mão, e não apenas por uma questão profissional. Nós, da área de cibersegurança, entendemos e somos conscientes do contexto global. É o cúmulo que, tendo este contexto e toda essa informação em primeira mão, não estejamos fazendo nada. Continuamos postando fotos pessoais sem o devido cuidado com o que mostramos nelas, nos cadastramos em sites cuja segurança não temos certeza, continuamos aceitando termos de privacidade que nunca lemos completamente, continuamos respondendo mensagens de texto e WhatsApp sobre coisas que não conseguimos entender como chegaram até nós. E quando fazemos uma retrospectiva do como e do quando, caímos nessa pequena linha que nos torna tão vulneráveis.

O que é awareness? Se pesquisarmos no Google, a tradução literal é "consciência".

Awareness ou conscientização em cibersegurança refere-se a uma formação sobre a importância dela, capacitando os usuários por meio de simulações automatizadas e personalizadas de ataques de phishing e malwares, reduzindo de forma bem-sucedida o número de ciberataques nas empresas.

Agora, realmente, temos "Consciência de segurança"? O quanto estamos conscientes do que fazemos em nosso dia a dia? Se tivéssemos essa informação sempre presente sobre o que não devemos expor e, ao mesmo tempo, a aplicássemos e a compartilhássemos com nosso círculo familiar, seria muito mais fácil criar essa rede de boas práticas. Isso mesmo, seria muito mais fácil, pois compartilharíamos essas boas práticas de forma natural, com um simples "Não poste fotos de casa", ou “Apague a informação sobre onde você trabalha das suas redes sociais, existem plataformas específicas para isso", ou “Filho/filha, tenha cuidado com as imagens que compartilha da sua escola", ou “Cuide das senhas da sua conta", entre outras.

Bem, estando conscientes de tudo o que nos é compartilhado no trabalho sobre boas práticas, tudo o que colocamos em ação em nosso dia a dia profissional, estamos cumprindo adequadamente as capacitações? Realmente entendemos as diretrizes? Como poderemos estar atualizados se não estivermos prestando atenção à informação em primeira mão, que tem a melhor intenção de nos conscientizar sobre a segurança?

Muitas perguntas, poucas respostas, certo... vamos fazer com que valha a pena ter boas práticas de conscientização em nosso dia a dia. As recomendações são realmente simples:

Não compartilhe suas informações em qualquer plataforma.

- Certifique-se de que os códigos QR, que parecem tão inocentes e práticos, sejam os do local para o qual você deseja entrar.

- Não abra e-mails desconhecidos por curiosidade! ... nada é de graça e o que parece mais lógico pode não ser realmente.

- Desconfie ao receber mensagens ou chamadas de desconhecidos e, principalmente, se forem de "conhecidos" que façam perguntas ou solicitem algo incomum para nós. Por que não perguntar ou questionar? No final das contas, se é um conhecido ou familiar, é claro que há confiança e tranquilidade. E se for um colega, ainda mais razão para isso.

- Se sabemos que usamos na empresa uma MFA ou como poderíamos chamá-la de forma mais casual? Essa verificação dupla de acesso a um aplicativo, sistema, conta etc., e por que não pedir aos nossos familiares que a apliquem em suas atividades? Com uma conversa casual de apenas cinco minutos, podemos explicar isso em casa...

- Muitas pessoas costumam colocar em suas senhas o seu nome, data de nascimento, nome de seus animais de estimação. Sejamos criativos com nossa segurança. Pense que se você coloca uma senha em algo, é porque certamente guarda informações importantes para você.

- E quanto aos recibos que jogamos indiscriminadamente fora? Não temos o cuidado de verificar se eles contêm algum dado que qualquer curioso ou alguém interessado em nós possa coletar. E você provavelmente pensa: "Isso só acontece em filmes". Bem, sim, mas já pensou que os filmes acabam se tornando realidade?

Por que usar dispositivos pessoais para assuntos profissionais quando podemos fazê-lo de maneira segura? Conforme abordamos neste tópico de awareness e conscientização e, no nosso caso, conscientização em cibersegurança, utilizando muito esses dois termos neste artigo. Por que esquecemos de ser conscientes sobre o cuidado das informações que administramos em nossos dispositivos móveis? É simples: não faço donwload de assuntos da empresa, não os compartilho por meios não autorizados e pronto. Ah, mas, e se eu compartilhar o extrato bancário como se fosse um documento qualquer ou o famoso pack? Eu sei, isso soa engraçado, mas se você pensar bem, é uma realidade.

Eu poderia continuar com mais alguns pontos, no entanto, é muito importante que, ao terminar a leitura, você tenha em mente como aplicar as questões de awareness no dia a dia no escritório, em casa, com os amigos e em sociedade, para que não facilitemos o trabalho para aqueles que querem nossas informações ou nos veem como uma porta de acesso a dados que nem mesmo nos pertencem.

Que possamos tornar essas práticas nossas, compartilhá-las, criar essa rede ou estratégia a partir de nossa trincheira, para que o acesso à nossa privacidade seja dificultado.

Cibercrônica Fevereiro 2024

Começamos a cibercrônica deste mês com a notícia de um relatório apresentado pela empresa de cibersegurança ESET que descreve o panorama das ameaças na Espanha e no mundo. No relatório, a Espanha se destaca como um dos países com mais detecções de ameaças, ficando apenas atrás do Japão e dos Estados Unidos.

A ameaça mais popular detectada continua sendo o phishing, representando quase um terço de todas as ameaças detectadas. O relatório alerta sobre um aumento nas técnicas utilizadas pelos cibercriminosos, sendo cada vez mais proeminente o uso de inteligência artificial. Essas técnicas adicionam uma camada de sofisticação aos ataques, gerando conteúdos falsos, montagens de fotos, deepfakes ou roubos de identidade de pessoas relevantes. Prevê-se que a tendência nesse tipo de tentativa de ataque aumente devido à rápida expansão dessas ferramentas e ao seu acesso cada vez mais fácil; de fato, isso já está acontecendo e nos leva a outros termos, como smishing e vishing.

Esse tipo de phishing por meio de sms segue uma estrutura muito semelhante à dos e-mails. Consiste em enviar iscas em massa, esperando que os usuários caiam no golpe. As duas formas mais comuns de operação são: a falsificação de empresas de entrega, empresas telefônicas ou bancos e roubo de identidade de familiares ou conhecidos.

Quanto ao vishing, a Guarda Civil recentemente alertou sobre o aumento desse tipo de fraude e recomendou à população que fosse cautelosa e tomasse precauções a esse respeito, já que os avanços tecnológicos em inteligência artificial tornam cada vez mais real o roubo de identidade de pessoas por meio de videochamadas.

Isso nos leva a falar sobre a profissionalização da fraude, que vem aumentando nos últimos anos. Existem relatos de empresas no exterior que se dedicam especificamente a montar call centers que se passam pela equipe de suporte de diferentes serviços com a intenção de enganar os possíveis usuários através da utilização de suas informações.
O usuário do youtube, conhecido como Savitar (que divulga conteúdo relacionado a hacking ético e cibersegurança), algumas semanas atrás, relatou em um de seus vídeos como um hacker se dedicava a desvendar fraudes desse tipo. A metodologia que ele utilizava era coletar informações dessas centrais após infectar todos os seus equipamentos, para posteriormente entrar em contato com as autoridades para que interviessem na central e interrompessem a atividade. O escritório de onde operavam parecia bastante profissionalizado, sendo possível até mesmo que algumas das pessoas que trabalhavam nessa atividade não estivessem cientes da ilegalidade.

Para enfatizar isso, uma notícia do portal ITUser nos conta que o cibercrime agora funciona como qualquer outra empresa e seus objetivos são equivalentes a essas (redução de custos, melhoria da eficiência e obtenção de receita), cujas atividades alcançam um valor próximo a 1,5% do PIB mundial. Paradoxalmente, a percepção da população em relação à sua vulnerabilidade a ataques cibernéticos não avança de acordo com seu impacto e popularidade. Como enfatiza o Centro de Coordenação Nacional do INCIBE: "Em geral, ano após ano, os usuários acham que são menos atacados. Mas, no entanto, a tendência real é crescente. Na verdade, a porcentagem de usuários que declaram ter malware em seus equipamentos é muito baixa, especialmente quando comparada com a realidade“.

Para encerrar a cibercrônica deste mês, é importante destacar que, dado o aumento dessa situação na qual a ciberfraude melhora a cada dia diante da falta de percepção da população, é necessário prestar atenção especial às novas tecnologias que estão cada vez mais integradas em nossas vidas. De acordo com diversas fontes, o vetor de ataque mais comum até o momento continua sendo o e-mail, através do qual os computadores ou dispositivos móveis podem ser infectados. No entanto, essa situação pode ser muito diferente em um futuro não muito distante.

Recentemente, vimos notícias em que empresas como a Apple lançaram no mercado seus novos óculos de realidade aumentada, ou até mesmo como a empresa Neuralink estava realizando testes com um chip cerebral. Acreditamos que a indústria da fraude ainda está longe de se aproximar desses dispositivos, mas à medida em que a oferta e o uso desse tipo de tecnologias aumentarem, a indústria os verá como novos vetores de ataque.

Harvest Now, Decrypt Later

Tendências

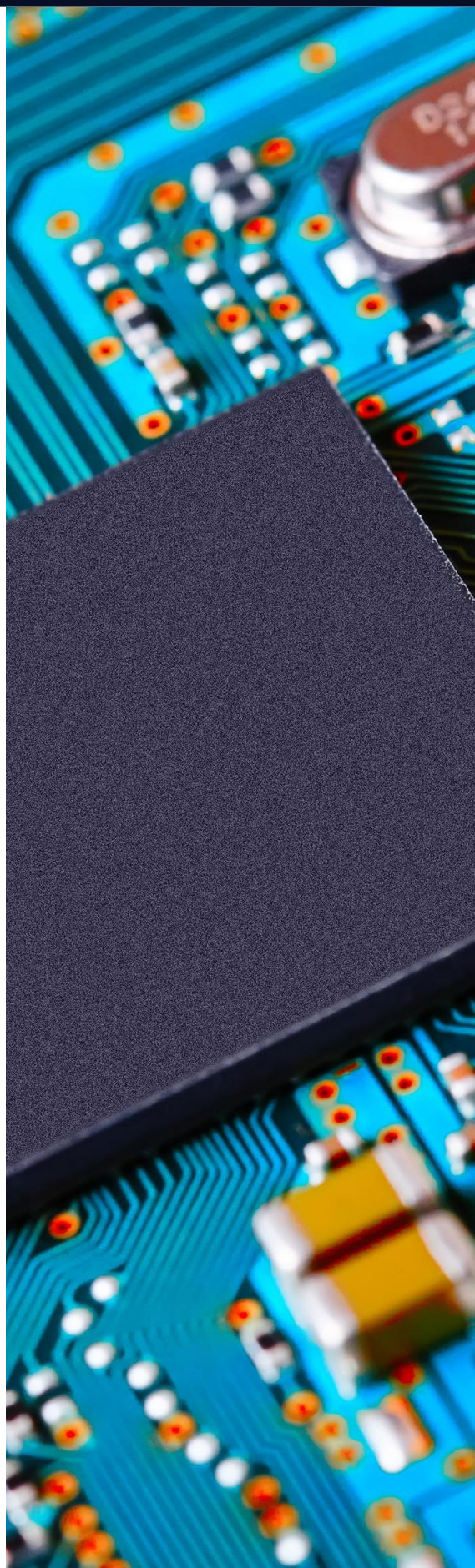
Nos últimos anos, discutiu-se de forma ampla sobre o possível impacto global que o acesso generalizado à tecnologia quântica poderia ter. À medida que seu funcionamento e desempenho estão se tornando cada vez mais relevantes, institutos internacionais de cibersegurança têm tomado medidas para tentar estabelecer medidas preventivas diante da eventual revolução que essa nova tecnologia poderia causar.

Ao contrário dos computadores clássicos utilizados hoje em dia, onde bits são usados para representar informações como 0 ou 1, os computadores quânticos usam qubits, que não apenas representam os bits clássicos, mas também incorporam um estado adicional onde representam ambos, ao mesmo tempo, através de um fenômeno chamado superposição. Isso proporciona uma capacidade para realizar cálculos exponencialmente maiores do que um computador convencional, representando uma ameaça aos sistemas criptográficos atuais que se baseiam na dificuldade computacional para resolvê-los. Por esse motivo, tem havido um interesse crescente no desenvolvimento de algoritmos criptográficos quântico-resistentes.

Até o momento, os protocolos de segurança utilizados para proteção da integridade e confidencialidade dos dados baseiam-se principalmente na criptografia RSA e ECC. De acordo com diversos estudos realizados pelo "*World Economic Forum*", além dos cronogramas estabelecidos pelo CNSA, os computadores quânticos representam uma ameaça para essas criptografias de segurança, pois passariam a ser considerados vulneráveis, devido à capacidade de computação apresentada por essa nova tecnologia. Estima-se que essa brecha de segurança em nível mundial possa ocorrer no início de 2030. Por isso, os sistemas clássicos são considerados vulneráveis ao "*Harvest now, descrypt later*" (HNDL: Colher agora, descriptografar depois), onde agentes maliciosos roubam e armazenam dados para decifrá-los mais tarde, caso obtenham acesso a computadores quânticos.

Tanto a IBM quanto a Palo Alto começaram a manifestar seus planos de ação para prevenir e combater essa futura problemática, especialmente após a mensagem publicada pelo Instituto Nacional de Padrões e Tecnologia (NIST), onde anuncia que começará ao longo deste ano a desenvolver e estabelecer padrões criptográficos seguros contra a computação quântica. Com os quatro ciframentos "*post-quantum*" (PQC) escolhidos em 2022 após seis anos de pesquisa internacional e o anúncio do NIST em agosto de 2023 sobre seus planos de padronização de três dos ciframentos vencedores, espera-se que sua aprovação e implementação ocorram ao longo de 2024. Esses ciframentos são: "Crystals Kyber", "Crystals-Dilithium" e "SPHINC+".

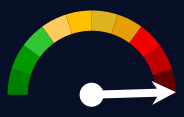
Com o avanço contínuo do desenvolvimento da computação quântica, liderado por empresas como IBM, Google, D-Wave e IonQ, entre muitas outras, a contribuição do NIST representa um apoio imenso para mobilizar todos os setores dependentes da segurança das criptografias clássicas.
A tendência observada nos últimos meses sugere que o ano de 2024 marca o início de mudanças significativas nos protocolos de segurança. Esse movimento reflete a crescente conscientização sobre a necessidade de se adaptar à era quântica, destacando a importância de desenvolver e adotar algoritmos quântico-resistentes para continuar garantindo a integridade e confidencialidade dos dados.



Vulnerabilidades

Vulnerabilidade de código remoto em produtos da Cisco

Data: 24 de janeiro de 2024
CVE: CVE-2024-20253



CVSS: 9.9

CRÍTICA

Descrição
A Cisco relatou uma vulnerabilidade crítica que afeta um grande número de seus produtos.

Trata-se de uma vulnerabilidade de execução de código remoto, devido ao processamento inadequado dos dados de entrada fornecidos pelo usuário. Um invasor poderia explorar a vulnerabilidade enviando uma mensagem especialmente projetada para uma porta de escuta do dispositivo afetado.

Ao explorar essa vulnerabilidade, um invasor poderia executar comandos arbitrários no sistema operacional do dispositivo com privilégios de usuário do serviço da web. Além disso, com acesso ao sistema operacional, o invasor poderia estabelecer permissões de acesso *root* no sistema.

Produtos afetados
A vulnerabilidade afeta os seguintes produtos:

- Unified Communications Manager (Unified CM)
- Unified Communications Manager IM & Presence Service (Unified CM IM&P).
- Unified Communications Manager Session Management Edition (Unified CM SME).
- Unified Contact Center Express (UCCX).
- Unity Connection.
- Virtualized Voice Browser (VVB).

Solução
O fabricante publicou atualizações para os produtos afetados.

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

Múltiplas vulnerabilidades em produtos da Fortinet

Data: 8 de fevereiro de 2024
CVEs: CVE-2024-23113 e mais 1

CVSS: 9.8

CRÍTICA

Descrição
A Fortinet informou na última sexta-feira sobre duas vulnerabilidades críticas em seu sistema operacional FortiOS.

A vulnerabilidade mais crítica, CVE-2024-23113, é uma vulnerabilidade de cadeia de formato controlada externamente (CWE-134), como através da entrada de um usuário no daemon *fgfmd* do FortiOS.

A segunda vulnerabilidade, CVE-2024-21762, é uma vulnerabilidade permite que um agente malicioso escreva dados fora da área de memória reservada (CWE-787).

A exploração de qualquer uma dessas vulnerabilidades pode permitir que um invasor remoto não autenticado execute código arbitrário ou comandos por meio de solicitações especialmente projetadas.

Produtos afetados
As vulnerabilidades mencionadas afetam as seguintes versões do sistema operacional FortiOS:

- FortiOS 7.4 da versão 7.4.0 a 7.4.2
- FortiOS 7.2 da versão 7.2.0 a 7.2.6
- FortiOS 7.0 da versão 7.0.0 a 7.0.13
- FortiOS 6.4 da versão 6.4.0 a 6.4.14
- FortiOS 6.2 da versão 6.2.0 a 6.2.15
- FortiOS 6.0

Para acessar o restante dos produtos afetados, consulte os links de referência.

Solução
A Fortinet recomenda desativar SSL VPN como *workaround* e atualizar FortiOS para as seguintes versões ou superiores: 7.4.3; 7.2.7; 7.0.14; 6.4.15; 6.2.16.

Referências
- www.incibe.es
- www.fortiguard.com
- www.fortiguard.com

Patches

CRÍTICA

Novos patches de segurança para o GitLab CE/EE

Data: 25 de janeiro de 2024
CVE: CVE-2024-0402 e mais 4

Descrição
O GitLab lançou em 26 de janeiro uma série de patches de segurança para corrigir um conjunto de cinco vulnerabilidades, das quais uma é categorizada como crítica e as demais têm uma classificação de gravidade média.

A vulnerabilidade crítica, CVE-2024-0402, poderia permitir que um usuário autenticado gravasse arquivos em locais arbitrários dentro do servidor do GitLab ao criar um ambiente de trabalho. Essa brecha de segurança poderia resultar na distribuição de *malware*.

As demais vulnerabilidades corrigidas neste patch de segurança poderiam permitir as seguintes ações:

- Desencadear um ataque DoS (CVE-2023-6159).
- Acesso ou exposição de dados confidenciais (CVE-2023-5933 e CVE-2023-5612).
- Atribuir qualquer usuário sem restrições às solicitações de *merge* (MR) que foram criadas dentro de um projeto no GitLab (CVE-2024-0456).

Produtos afetados
As versões do GitLab afetadas são as seguintes:

- 12.7 anterior a 16.6.6;
- 13.7 anterior a 16.6.6;
- 14.0 anterior a 16.6.6
- 16.0 anterior a 16.5.8;
- 16.6 anterior a 16.6.6;
- Todas las anteriores a 16.6.6;
- 16.7 anterior a 16.7.4;
- 16.8 anterior a 16.8.1.

Solução
Atualizar para as versões 16.5.8, 16.6.6 e 16.7.4 do GitLab CE/EE. A versão 16.8.1 unicamente contém o patche para a vulnerabilidade CVE-2024-0402.

Referências
- about.gitlab.com
- www.helpnetsecurity.com

CRÍTICA

Novos patches de segurança para dispositivos Android

Data : 5 de fevereiro de 2024
CVE: CVE-2024-0031

Descrição
A Android lançou um novo boletim de segurança que corrige uma vulnerabilidade crítica e 45 vulnerabilidades de alta gravidade.

A vulnerabilidade crítica é um erro de escrita fora dos limites encontrado na função "attp_build_read_by_type_value_cmd", que, se explorado, permitiria que um invasor executasse código remotamente no sistema operacional do dispositivo, sem a necessidade de privilégios de execução *system*. Esta vulnerabilidade foi identificada como CVE-2024-0031.

As vulnerabilidades corrigidas no patch afetam tanto o sistema operacional quanto componentes do sistema, como Arm, MediaTek, Qualcomm ou Unisoc.

Produtos afetados
Os produtos afetados por essa vulnerabilidade são os seguintes:

- Android Open Source Project (AOSP): versões 11, 12, 12L, 13 e 14
- Componentes de Arm, MediaTek, Unisoc e Qualcomm

Solução
A Android recomenda verificar se o fabricante do dispositivo lançou um patch de segurança e aplicar a atualização correspondente.

Referências
- www.incibe.es
- source.android.com

Eventos

Innovate Cybersecurity Summit

Este evento de três dias reúne executivos e CISOs de cibersegurança de todos os EUA para discutir e aprender, dentro de um contexto de participação exclusiva. Este ano, foi realizado em Nashville, Tennessee, nos dias 25 a 27 de fevereiro.

As pessoas que participam desta experiência têm acesso a painéis e sessões de formação lideradas por CISOs que abordam as melhores práticas e desafios atuais, ao mesmo tempo em que apresentam as oportunidades e as mais recentes soluções tecnológicas em cibersegurança.

Trata-se de um evento único do qual se pode obter informações valiosas para posicionar sua organização em um bom nível de proteção e resposta às ameaças neste campo.

Link

Cyber Security World Madrid - 2024

Evento que acontecerá na capital espanhola nos dias 16 e 17 de outubro, no pavilhão 9 do Ifema Madrid. Nele se reunirão profissionais de cibersegurança corporativa, empresarial e institucional das principais empresas de cibersegurança do mundo para discutir o aumento atual dos ciberataques, suas tipologias e os investimentos neste campo para proteger os dados e as atividades das organizações.

Este ano, está prevista a participação de cerca de 400 empresas que irão expor suas soluções cloud, além de mais de 350 palestrantes que apresentarão as últimas novidades do setor.
Link

Infosecurity Europe 2024

Esta feira ocorrerá de 4 a 6 de junho no ExCeL London, no Reino Unido. Reunirá profissionais e empresas da área de cibersegurança para discutir as últimas novidades do campo e compartilhar experiências, por meio de conferências e eventos onde será possível expandir conhecimentos e networking.

É considerada uma das feiras europeias mais importantes em termos de cibersegurança, pois reúne um grande número de fornecedores de soluções.

Link

Infosecurity México 2024

Evento organizado no Centro Citibanamex da Cidade do México para discutir cibersegurança, principalmente em relação às últimas tendências e métodos de segurança da informação.

Os participantes terão contato com importantes especialistas da indústria de segurança da informação, o que pode ajudar a melhorar a proteção das empresas encontrando soluções que se adaptem aos novos tempos.

Portanto, os temas principais abordados nos dias 22 e 23 de outubro serão normativas, bem como ameaças cibernéticas e proteção, tanto para pessoas físicas quanto para empresas e instituições públicas.
Link

Recursos

Materiais de formação e treinamento para especialistas em cibersegurança da ENISA (European Union Agency for Cybersecurity)
A ENISA, desde 2008, tem fornecido material de cibersegurança para capacitar qualquer pessoa interessada em ampliar seus conhecimentos. No site da agência, há informações para professores e alunos, a fim de complementar uma parte mais prática.

A formação é composta por quatro áreas principais: Técnica (análise forense, *honeypots* ou detecção proativa são alguns dos tópicos), Operacional (elaboração de avisos de segurança ou gerenciamento de incidentes na nuvem), Cooperação e Legal (identificação, gestão de vestígios de crimes cibernéticos, cooperação com as forças policiais) e Configuração de um CSIRT (ou seja, treinamento para poder responder de maneira eficaz a um incidente de cibersegurança).
Link

Revolucionando a gestão de identidades: como a Web3 descentraliza e protege os sistemas IAM
No seguinte link, a DataVeritas explica o novo campo da Web3 e sua relação com o conceito de identidade descentralizada. Essa ideia revolucionária busca dar ao usuário controle total sobre sua identidade digital, reduzindo o número de vulnerabilidades causadas por outros tipos de gestão e as limitações do indivíduo ao utilizá-la. Tudo isso se baseia em campos como *blockchain* e outros tipos de tecnologias IAM atuais e inovadoras.

Portanto, a Web3 é uma ótima escolha para uma gestão descentralizada da identidade de forma mais segura, superando certos desafios atuais em IAM. Trata-se de uma solução que já foi testada com sucesso em setores como o bancário ou o da saúde.
Link

NIST Cybersecurity Framework (CSF) 2.0
Trata-se de um marco de cibersegurança publicado pelo instituto norte-americano NIST (National Institute of Standards and Technology). Sua origem ocorreu em 2014, quando se apresentou com o objetivo de apoiar a Lei de Melhoria da Cibersegurança dos EUA. O objetivo deste guia é gerenciar e reduzir os riscos, bem como fortalecer as medidas de cibersegurança.

Focando na própria ferramenta, o NIST Cybersecurity Framework (CSF) 2.0 Reference Tool permite estudar o rascunho do CSF 2.0 Core. Este inclui funções, categorias, subcategorias e exemplos de sua implementação, oferecendo versões legíveis por humanos e máquinas em JSON e Excel, além de permitir a busca por palavras e termos-chave. Dentro da ferramenta, podem ser encontradas as seguintes funções:

• GOVERNANÇA (GV): estabelecer e monitorar a estratégia, expectativas e política de gestão de riscos de cibersegurança da organização.
• IDENTIFICAR (ID): ajudar a determinar o atual risco de cibersegurança para a organização.
• PROTECT (PR): usar salvaguardas para prevenir ou reduzir o risco de cibersegurança.
• DETECT (DE): encontrar e analisar possíveis ataques e comprometimentos de cibersegurança.
• RESPONDER (RS): tomar medidas diante de um incidente de cibersegurança detectado.
• RECUPERAR (RC): restaurar ativos e operações afetados por um incidente de cibersegurança.

É uma ferramenta em desenvolvimento e prevê-se que seja concluída em 2024, o que permitirá integrar o CSF com marcos, padrões, guias e recursos relacionados à cibersegurança. Em versões futuras, espera-se que os usuários possam gerar sua própria versão do CSF 2.0 Core ao selecionar outras informações e recursos como referência.
Link

Radar
Powered by women

NTT DATA

Mª Pilar Torres
Diretora de Cibersegurança - IBIOL

Marta Fernández
Cybersecurity Manager

Mª Angeles Gutiérrez
Cybersecurity Manager

Andrea Muñoz
Cybersecurity Manager

Almudena Abolafia
Cybersecurity Manager

Julissa E. Calderón
Cybersecurity Project Leader

Emily J. Pereda
Cybersecurity Lead Consultant

Mafalda Maciel
Senior Lead Analyst Cybersecurity

Nelvys P. Porras
Cybersecurity Expert Analyst

Stephanie A. Ramos
Lead Analyst Cyber

Radar

Powered by women

Powered by the Cybersecurity NTT DATA team

es.nttdata.com