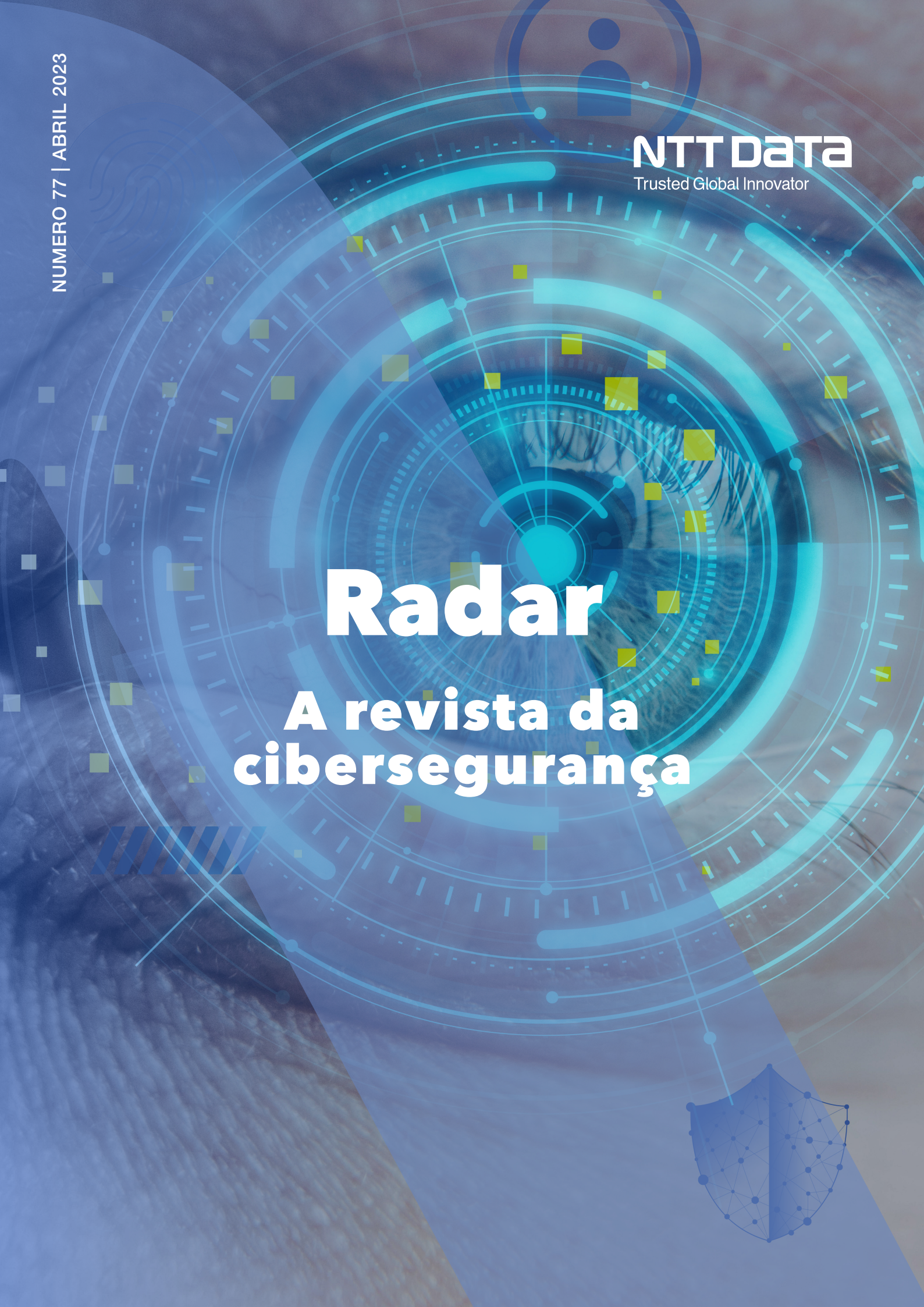
NUMERO 77 | ABRIL 2023

NTT DATA
Trusted Global Innovator

Radar

A revista da cibersegurança



SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E PROTEÇÃO DA PRIVACIDADE: ASPECTOS RELEVANTES PARA O CONSELHO DE ADMINISTRAÇÃO.

Erros humanos, falta de controle, fraudes internas ou ações criminosas no tratamento de informações são questões que passam a estar na pauta dos Conselhos de Administração das empresas, uma vez que podem provocar a paralisação do negócio, prejuízos econômicos diretos (milhões de USD), descumprimento da legislação e impacto negativo na imagem, reputação e credibilidade da empresa. Tudo isso não permite que a organização atinja adequadamente seus objetivos corporativos.

A informação é o recurso que permite o planejamento da organização e o funcionamento do seu negócio. Sem informação disponível e protegida, a organização pode sofrer um incidente que, dependendo do seu tamanho e tipo de negócio, pode tirá-la do mercado durante um tempo ou para sempre, o que afeta direta e negativamente os acionistas.

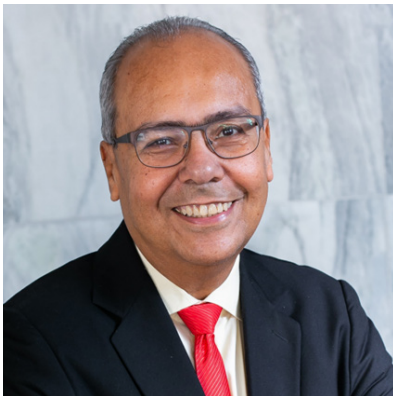
Um dos princípios da Governança Corporativa é a "Sustentabilidade da Organização". Isso significa a continuidade da informação para realizar os serviços e/ou elaborar os produtos que disponibiliza ao mercado. Portanto, é responsabilidade do Conselho de Administração garantir a existência de um processo adequado de proteção da informação.

Os acionistas, por meio do Conselho de Administração, precisam conhecer os riscos cibernéticos e a maturidade de proteção da informação da organização. Esse nível de maturidade é o resultado de uma avaliação detalhada de vários controles de segurança da informação, cibersegurança e proteção da privacidade. O Conselho precisa conhecer a existência (ou não) de controles que evitem ou minimizem a perda, roubo ou indisponibilidade da informação. Precisa conhecer a resistência da proteção da informação.

O Centro para a Segurança do Fórum Econômico Mundial, a Internet Security Alliance e a National Association of Corporate Director (Associação Nacional de Diretores Corporativos), em seu documento Principles for Board Governance of Cyber Risk (2021) (Princípios para a Administração do Conselho de Risco Cibernético), recomendam que o Conselho de Administração e a Alta Gerência considerem uma "organização ciber-resistente":

- A cibersegurança a serviço da estratégia empresarial.
- Impulsionadores econômicos e impacto do risco cibernético.
- Alinhamento da gestão de riscos cibernéticos com as necessidades da empresa.
- Garantir que a estrutura organizacional apoie a cibersegurança.
- Integrar a experiência em cibersegurança na administração do Conselho.
- Promover resiliência e colaboração sistêmicas.

Nossa Revista Radar deste mês apresenta controles e novas tecnologias para facilitar a proteção das informações e a geração de melhores informações para o Conselho de Administração. A FAIR (Factor Analysis Information Risk), uma metodologia quantitativa de gestão de risco; Inteligência Artificial e considerações sobre ChatGPT e Tecnologia Operacional (OT) que, segundo estimativas do Gartner, possui um mercado 10 (dez) vezes maior que o de Tecnologia da Informação (TI).



Edison Goncalves Fontes
Cybersecurity Evangelist na NTTDATA Brazil

CIBERCRÔNICA

Iniciamos nossa Cibercrônica com uma preocupação que aflige muitas organizações em todo o mundo que é a GoDaddy, uma das principais empresas de hospedagem na web do mundo, relatou uma violação de segurança que comprometeu seu ambiente de hospedagem compartilhada cPanel. Segundo a empresa, invasores desconhecidos conseguiram invadir seus servidores e roubar o código-fonte, além de instalar malware nos sistemas. Apesar dos relatórios de clientes alertando a GoDaddy sobre essa violação de segurança, no início de dezembro de 2022, os invasores conseguiram obter acesso à rede da empresa vários anos antes.
Durante esse tempo, os invasores puderam usar sites comprometidos para redirecionar o tráfego para vários domínios desconhecidos. Como a GoDaddy é uma das maiores registradoras de domínios do mundo, isso é motivo de preocupação para os mais de 20 milhões de clientes em todo o mundo que usam seus serviços de hospedagem.

> “BlackLotus, um bootkit sigiloso e extensível do firmware unificado (UEFI) que se tornou o primeiro malware conhecido publicamente capaz de escapar das defesas do Secure Boot”.

Por outro lado, surgiu o BlackLotus, um bootkit sigiloso e extensível do firmware unificado (UEFI) que se tornou o primeiro malware conhecido publicamente capaz de escapar das defesas do Secure Boot, tornando-se uma ameaça potente no cenário cibernético.
“Este bootkit pode ser executado mesmo em sistemas Windows 11 totalmente atualizados com UEFI Secure Boot ativado”. Como podemos lembrar, os bootkits da UEFI são implantados no firmware do sistema e permitem o controle total do processo de inicialização do sistema operacional (SO), o que torna possível desativar os mecanismos de segurança em nível de SO e implantar cargas úteis arbitrárias durante a inicialização com altos privilégios.
Este kit de ferramentas poderoso e persistente está à venda por USD 5.000 (e USD 200 para cada nova versão subsequente) e é programado em assembler e C e tem 80 kilobytes de tamanho. Ele também possui recursos de geofencing para evitar a invasão de computadores na Armênia, Bielorrússia, Cazaquistão, Moldávia, Romênia, Rússia e Ucrânia.
Do outro lado do mundo, o grupo de ciberespionagem chinês Mustang Panda, alinhado com a China, foi visto usando um novo backdoor personalizado chamado MQsTTang como parte de uma campanha de engenharia social em andamento que começou em janeiro de 2023. O MQsTTang usa o protocolo de mensagens de IoT MQTT para as comunicações de controle e comando.
Os ataques do grupo foram direcionados a entidades europeias no contexto da invasão russa da Ucrânia no ano passado, embora ataques contra entidades desconhecidas também tenham sido observados na Bulgária e na Austrália, bem como em uma instituição governamental em Taiwan.
O backdoor MQsTTang permite a execução de comandos arbitrários recebidos de um servidor remoto e é distribuído pelos arquivos RAR que contêm um executável que apresenta nomes de arquivos com temas diplomáticos. As descobertas vêm dias depois que a Symantec revelou uma operação de ciberespionagem realizada pelo grupo estatal chinês APT41, que teve como alvo duas subsidiárias de um conglomerado asiático no setor de materiais e compostos.

Por outro lado, chegamos no México, onde foi detectada uma nova variedade de malware de caixas eletrônicos chamado FiXS, que tem como alvo os bancos desde o início de fevereiro de 2023. O FiXS se esconde dentro de outro programa

que não é malicioso e é compatível com qualquer caixa eletrônico que suporte CEN/XFS. Acredita-se que os invasores encontraram uma maneira de interagir com o caixa eletrônico por meio da tela sensível ao toque. Uma das características notáveis do FiXS é a capacidade de dispensar dinheiro 30 minutos após a última reinicialização do caixa eletrônico. O FiXS é semelhante a outro tipo de malware de caixa eletrônico chamado Ploutus. Este último, permitiu que os cibercriminosos sacassem dinheiro de caixas eletrônicos usando um teclado externo ou enviando uma mensagem de texto. O FiXS é o mais recente de uma longa linha de malware que tem como alvo caixas eletrônicos para roubar dinheiro. Deve-se levar em consideração que esse tipo de malware pode se espalhar na região e afetar caixas eletrônicos nos EUA, América Central e do Sul.

Desta forma, encerramos nossa Cibercrônica, continuaremos informando sobre as notícias atuais do mundo da cibersegurança

A IMPORTÂNCIA DE UMA GESTÃO EFICAZ DE RISCOS DE CIBERSEGURANÇA NAS ORGANIZAÇÕES

Por: NTT DATA Europa & Latam

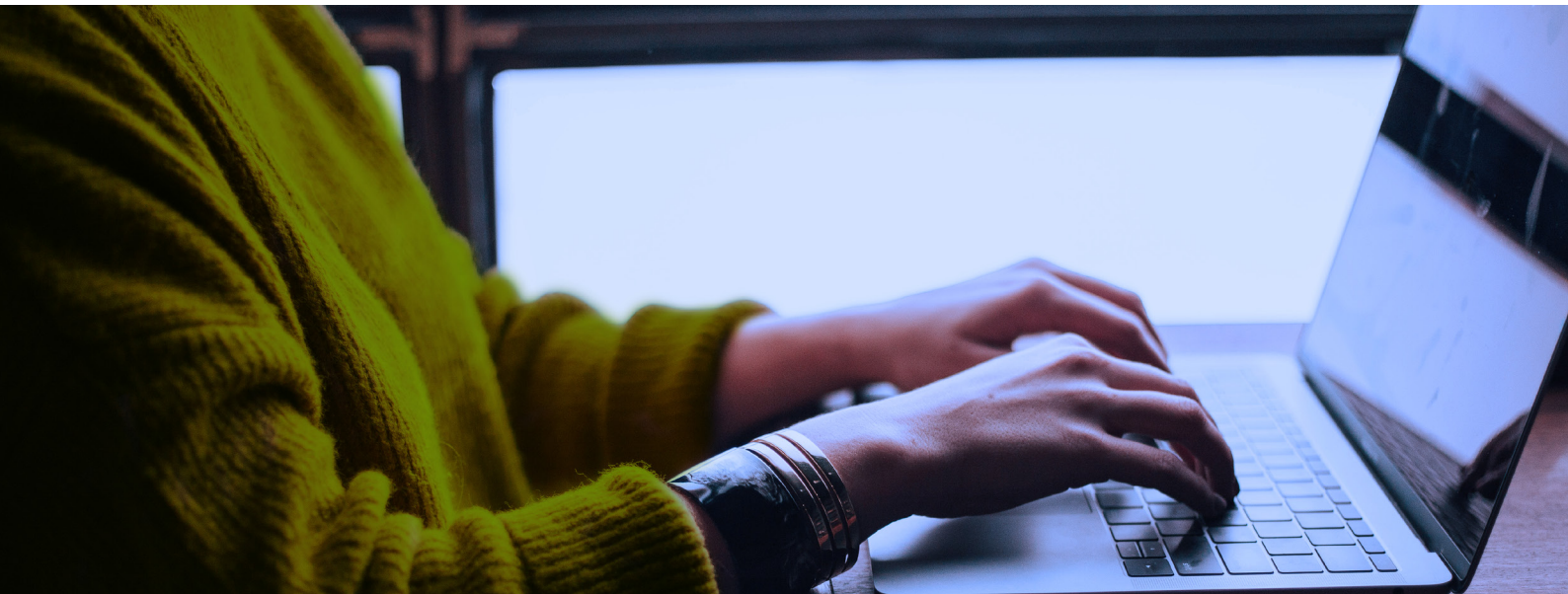
A gestão de riscos de segurança da informação e cibersegurança busca garantir ações que respaldem a integridade, confidencialidade e disponibilidade dos ativos da informação dentro das organizações. Muitas empresas já possuem uma metodologia de gestão de riscos de segurança da informação definida e madura, além de estarem comprometidas em tomar ações para tratar e mitigar seus riscos, passando por diferentes etapas de identificação, análise e avaliação, bem como tratamento do risco.

Atualmente, existem muitas metodologias e quadros de referência publicados e aplicados para a gestão de riscos, nos quais observamos que a maioria das organizações opta por alinhar-se com métodos de avaliação qualitativos, o que serviu para determinar o valor que os riscos representam em termos de impacto e probabilidade. Embora em determinados casos, a metodologia definida atribua intervalos quantitativos de exposição de risco, esta atribuição é uma "possibilidade", mas não uma "probabilidade", como tal, sustentada em informações que a suporte.

Em relação aos riscos SI, as principais partes interessadas, tais como CISOs, Gestores de riscos de segurança, responsáveis por Tecnologia, executivos e parceiros, entre outros, estão questionando o seguinte:

- A gestão que realizamos é suficiente para responder e sustentar os investimentos em segurança que precisamos fazer?
- Os resultados da gestão de riscos que aplicamos são utilizados para sustentar a avaliação de riscos críticos para a empresa?
- O impacto final que representa para a organização analisa valores com base em declarações de possibilidade próximas da realidade?
- A metodologia de riscos é um suporte para sustentar o planejamento das ações a serem realizadas como parte do programa de segurança da informação em um horizonte de curto, médio e longo prazo considerando a urgência e as principais dificuldades que temos?

A alternativa de usar métodos quantitativos que ajudem a definir melhor as decisões a serem tomadas está gerando maior interesse devido à importância de sustentar os custos que poderiam ser comprometidos no caso de apresentar e implementar uma, bem como a necessidade de sustentar investimentos em segurança. Além disso, tomar decisões corretas com base em informações relevantes representa um grande desafio em qualquer processo da empresa. A gestão de riscos de segurança da informação e a cibersegurança não são exceção: analisar a informação para conhecer mais de perto a



probabilidade de ocorrência de um evento de risco ajudará a agir de forma proativa, aplicando os controles necessários. Pelo contrário, agir de forma reativa quando o "incêndio" já ocorreu pode ter um impacto enorme.

É por isso que os responsáveis procuram melhorar a sua análise de risco e focar em valores tangíveis em termos monetários de perda, o que lhes dá a capacidade de levar a gestão de risco para o próximo nível, podendo sustentar os investimentos necessários. Além disso, poderão definir com este valor a atribuição de um horizonte de implementação a curto, médio e longo prazo.

Para aplicá-lo, uma boa alternativa é o uso da estrutura FAIR definida inicialmente para riscos de cibersegurança (pode ser utilizada para analisar outros tipos de riscos). Essa estrutura analisa o risco com base em uma taxonomia hierárquica, na qual um primeiro nível é composto por "frequência do evento de perda" e "magnitude da perda". Esses termos nos níveis seguintes são compostos por outros valores que, em suma, ajudarão a chegar aos dados do valor do risco de forma independente, considerando o cenário em que se encontra.

Entretanto, as empresas que desejam começar a utilizar uma metodologia de análise de risco quantitativa devem passar por processos de transformação e transição, especialmente para poder medir as perdas, a resiliência de seus controles e a porcentagem de sucesso dos invasores. Como parte do processo de adoção da nova metodologia estará a medição dessas variáveis ou a implantação de novos controles que permitam à organização ter informações válidas nos meses seguintes.

Para iniciar a jornada, as organizações podem utilizar informações baseadas no setor, por exemplo, desde que representem uma boa fonte de dados. Isso servirá para desafiar as premissas e efetuar a análise com estimativas mais precisas, que serão de maior valor para as empresas.

Nesse processo de adoção, por fim, as empresas podem olhar para as metodologias de análise de risco quantitativa e qualitativa como complementares, não sendo necessário que a qualitativa desapareça. É possível decidir realizar a análise quantitativa nos cenários de maior impacto para a organização e concentrar-se na obtenção de informações apenas desses casos.

Uma frase famosa de Peter Drucker diz que "O que não pode ser medido não pode ser controlado; o que não pode ser controlado não pode ser gerenciado; o que não pode ser gerenciado não pode ser melhorado." Portanto, o lado positivo dessa nova abordagem é que ela permite medir e quantificar o impacto econômico de um ataque a uma organização. E isso nos permitirá controlar, gerenciar e melhorar o processo de gestão de riscos.

IMPACTO DOS CIBERINCIDENTES NA INFRAESTRUTURA CRÍTICA EM NOSSA VIDA DIÁRIA

Por: NTT DATA Europa & Latam

A última edição da revista de segurança informática "Cybersecurity Today" divulgou os recentes ataques cibernéticos em ambientes industriais e a necessidade de melhorar a segurança nessas áreas. Nos últimos meses, ocorreram vários ataques cibernéticos no setor que causaram interrupções na produção e perdas financeiras consideráveis. Um dos ataques mais notáveis foi o que atingiu uma importante fábrica de produção de petróleo e gás no Oriente Médio, que foi obrigada a fechar temporariamente devido a uma invasão em seu sistema de controle industrial.

Cibersegurança industrial, risco de vidas humanas

A cibersegurança industrial é de vital importância para proteger a vida das pessoas. As infraestruturas críticas, como usinas de energia, estações de tratamento de água e instalações de transporte, são altamente automatizadas e dependem de sistemas de controle industrial para funcionar adequadamente. Um ciberataque nesses sistemas pode causar sérios danos à saúde pública, ao meio ambiente e à economia.

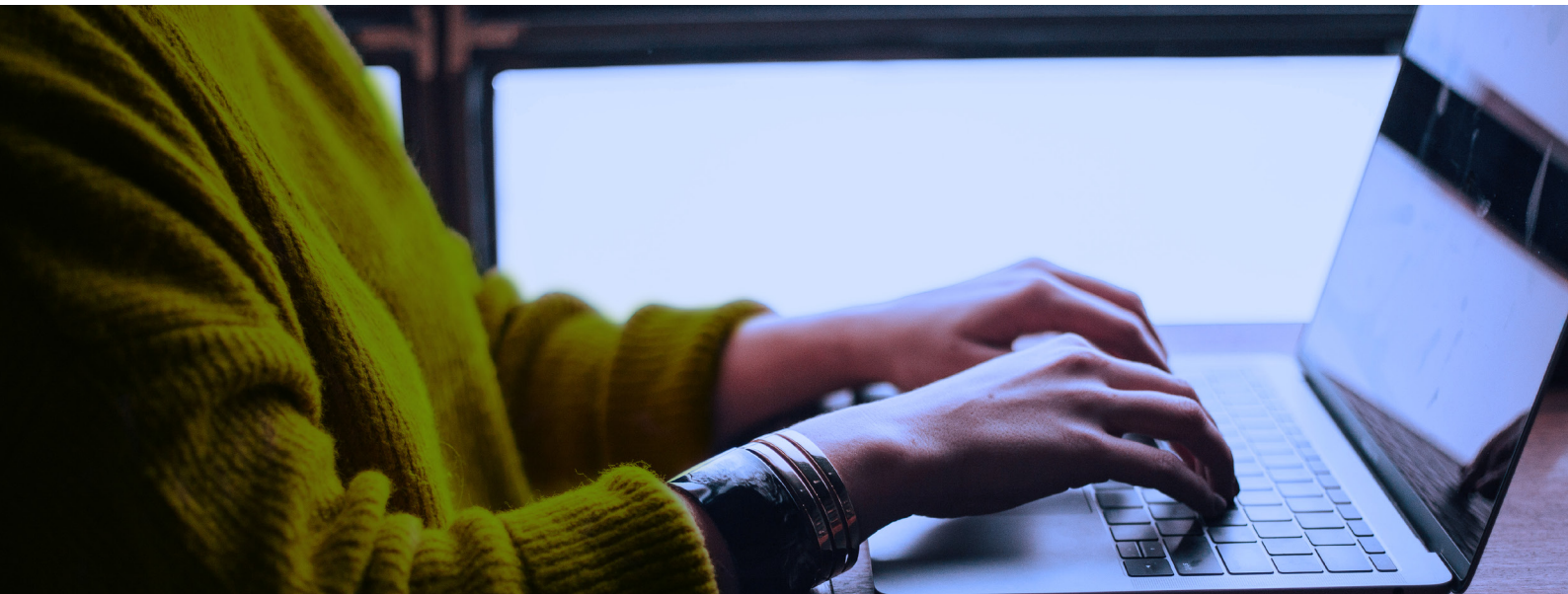
Portanto, é crucial que essas instalações tenham sólidas medidas de segurança para proteger seus sistemas de controle industrial contra possíveis ameaças cibernéticas. A cibersegurança industrial não apenas protege as infraestruturas críticas, mas também ajuda a garantir a continuidade da produção e o fornecimento de bens e serviços essenciais à sociedade. Em resumo, a cibersegurança industrial é fundamental para salvaguardar a vida das pessoas e proteger a economia dos possíveis efeitos nocivos de um ciberataque.

Ciberataque a usinas de água

Em fevereiro de 2021, foi informado um ciberataque a uma usina de tratamento de água na cidade de Oldsmar, na Flórida, nos Estados Unidos. Segundo as autoridades locais, um hacker desconhecido conseguiu acesso aos sistemas da usina e aumentou o nível de hidróxido de sódio (NaOH) na água tratada.

O ataque foi rapidamente detectado por um operador da usina, que notou um aumento no nível de NaOH na água tratada e o corrigiu antes que qualquer dano fosse causado. A usina foi temporariamente desconectada da Internet e uma investigação foi realizada para determinar a natureza do ataque e sua origem.

As autoridades locais e federais confirmaram que o ataque foi perpetrado por um hacker externo e que foi realizado por meio de um software de acesso remoto não autorizado. A usina de tratamento de água melhorou suas medidas de segurança e implementou novas medidas para proteger seus sistemas de controle industrial.



Este incidente destaca a necessidade de melhorar a cibersegurança em infraestrutura crítica, como usinas de tratamento de água, para evitar possíveis danos à saúde pública e ao meio ambiente. As autoridades locais e federais pediram a todas as instalações críticas que revisassem seus sistemas de segurança e atualizassem suas medidas de proteção contra possíveis ciberataques.

Que medidas a indústria deve tomar para se proteger com ferramentas de cibersegurança em ambientes industriais?

Aqui listamos algumas destas medidas:

1. **Implementar uma política de segurança:** A indústria deve estabelecer uma política de segurança clara e detalhada, que descreva os procedimentos de segurança a serem seguidos para garantir a proteção dos sistemas de controle industrial. Isso pode incluir regras de acesso, políticas de senha e medidas de segurança física.
2. **Utilizar ferramentas de segurança:** A indústria deve implementar ferramentas de segurança, como firewalls, sistemas de detecção de invasão e software antivírus, para proteger os sistemas de controle industrial contra possíveis ameaças. Essas ferramentas podem ajudar a detectar e prevenir ataques cibernéticos antes que causem qualquer dano.
3. **Atualizar regularmente o software:** A indústria deve atualizar regularmente o software dos sistemas de controle industrial para garantir que estejam protegidos contra as últimas ameaças de segurança. Isso pode incluir a aplicação de patches de segurança e atualizações de software para fechar vulnerabilidades conhecidas.
4. **Limitar o acesso:** A indústria deve limitar o acesso aos sistemas de controle industrial apenas aos funcionários que precisam de acesso para realizar suas funções. Controles de acesso físico e lógico podem ser implementados para garantir que apenas pessoas autorizadas tenham acesso aos sistemas.
5. **Realizar testes de penetração:** A indústria deve realizar testes de penetração regulares para avaliar a eficácia de suas medidas de segurança. Isso pode ajudar a identificar possíveis vulnerabilidades e áreas que precisam de melhorias na proteção de segurança.

Por que é importante desenvolver um Plano de Emergência?

Um plano de emergência para ataques cibernéticos à indústria OT deve ser integral e abranger todas as fases do processo, desde a prevenção até a recuperação. As organizações, dada a superfície de ameaça atual e devido à proliferação de novos cibercriminosos, devem não apenas estar cientes das campanhas com objetivos industriais, mas também considerar sistematicamente os pilares defensivos para minimizar o impacto de um ataque direcionado à sua organização.

A seguir estão as principais ações que devem ser incluídas em um plano de emergência eficaz:

- Preparação: identificar os ativos críticos e os pontos vulneráveis da infraestrutura OT, avaliar os riscos e estabelecer medidas de segurança apropriadas para prevenir ataques.
- Detecção: estabelecer sistemas e ferramentas de identificação de invasão para detectar ataques em tempo real.
- Contenção: isolar os sistemas afetados e impedir a propagação do ataque.
- Investigação: determinar a causa e o escopo do ataque, coletar informações e documentar os fatos.
- Mitigação: implementar medidas para minimizar os danos causados pelo ataque.
- Recuperação: restaurar os sistemas e a funcionalidade da infraestrutura OT para o seu estado anterior ao ataque.
- Avaliação: revisar o plano de emergência e as ações tomadas, identificar possíveis melhorias e ajustar o plano de acordo.

É importante ressaltar que um plano de emergência eficaz deve ser prático, acessível e atualizado regularmente. Além disso, é essencial que todos os funcionários estejam familiarizados com o plano e saibam qual é o seu papel em caso de um ataque cibernético. A colaboração e o trabalho em equipe são essenciais para uma resposta eficaz a um ataque cibernético na indústria de OT.

A prevenção de incidentes OT é um processo contínuo e requer compromisso contínuo da organização. Ao adotar medidas de segurança eficazes e trabalhar em colaboração com especialistas em segurança, as organizações podem proteger seus ativos industriais e garantir a continuidade do negócio

TENDÊNCIAS

GPT: Uma porta que abre caminhos

Embora em nossa última edição tenhamos explicado algumas generalidades do ChatGPT (chatbot desenvolvido pela OpenAI) em termos de definição, objetivo, prós e contras para o usuário comum, também é necessário falar sobre o impacto que começa a ser forjado em um nível corporativo pela sua adoção e graças à evolução do modelo GPT.

Desde que foi lançado para uso em novembro de 2022, o ChatGPT tem sido foco de um debate constante sobre segurança. No entanto, é importante fazer uma retrospectiva para perceber seu progresso e o papel de tê-lo como um aliado para conferir a ele esse tom de confiabilidade no âmbito empresarial.

Como todos sabem, a OpenAI é uma empresa governada pela organização sem fins lucrativos -OpenAI Incorporated- mas também composta por outra subsidiária com fins lucrativos -OpenAI Limited Partnership. Desde que começaram a desenvolver sua ideia em 2015, foi somente em 2019 que passaram a se relacionar com um dos gigantes da tecnologia -Microsoft- para treinar seus modelos com a tecnologia Azure, possibilitando assim, que a OpenAI não desista de seu propósito de pesquisa e, por outro lado, a Microsoft continuará amadurecendo seus produtos como seu fornecedor exclusivo na nuvem a ponto de implementar uma interface de aplicativo (API) que permita atingir tanto o mundo empresarial quanto os desenvolvedores para construir soluções de forma mais segura em seus modelos GPT, CODEX e DALL-E

Em termos simples, vamos defini-los:

- O GPT executa uma variedade de tarefas de linguagem natural, é usado para executar perguntas e respostas, resumos de texto, tradução automática e conversação IA.
- O CODEX, baseado em GPT-3, converte linguagem natural em código. Não se destina a substituir o trabalho dos programadores, destina-se a ajudá-los a codificar certos fragmentos de rotina ou otimizar código existente.
- DALL.E, cria imagens a partir de uma descrição em linguagem natural.

Com toda a ascensão e benefícios do ChatGPT, alguns desses modelos podem passar despercebidos, embora já estejam começando a ganhar relevância no ambiente de grandes empresas para proporcionar melhorias nos tempos de resposta, na efetividade e na experiência do usuário, fatores que têm sido decisivos nos últimos anos na interação do usuário com relação a um produto ou serviço.

Por último, é de extrema importância esclarecer que o simples fato de ter um destes módulos não significa que tudo funcionará como num passe de mágica para a organização, devemos estar cientes de que eles apenas fazem parte da solução e, em torno deles, haverá uma peça importante para trabalhar nos controles a serem implementados na comunicação dos serviços a serem definidos no backend e garantir que tanto os usuários internos quanto os externos que têm acesso sejam validados e recebam o que as suas funções lhes permitem.

Para isso, é preciso não perder de vista dois conceitos que sempre andam de mãos dadas e se complementam no sucesso de uma solução hoje, **SEGURANÇA** e **PRIVACIDADE**. A SEGURANÇA visa proteger contra ameaças maliciosas enquanto a PRIVACIDADE garante que apenas os usuários autorizados a acessar os dados possam fazê-lo.

VULNERABILIDADES

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

Fortinet

CVE-2023-25610
Data: 08/03/2023

Descrição. Em 8 de março, foi publicada uma vulnerabilidade crítica que afeta a interface administrativa do FortiOS e do FortiProxy e que pode permitir que um invasor execute o código arbitrário no dispositivo ou realize um ataque DOS na interface gráfica do usuário por meio do envio de solicitações especificamente projetadas para isso. A Vulnerabilidade CVE-2023-25610 seria provocada por um "buffer underflow" ou estouro de buffer. Nesse tipo de vulnerabilidade, o buffer do aplicativo carregaria as informações fornecidas a ele em uma velocidade inferior ao seu tempo de processamento, o que causaria uma solicitação de memória adjacente.
Link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-fortinet-0
https://www.fortiguard.com/psirt/FG-IR-23-001
Produtos afetados.

- FortiOS: 7.2.0 a 7.2.3, 7.0.0 a 7.0.9, 6.4.0 a 6.4.11, 6.2.0 a 6.2.12, 6.0 todas as suas versões.
- FortiProxy: 7.2.0 a 7.2.2, 7.0.0 a 7.0.8, 2.0.0 a 2.0.11, 1.2 todas as suas versões, 1.1 todas as suas versões.

Solução: A principal solução para corrigir essa vulnerabilidade é atualizar o Jira Service Management Server and Data Center para as seguintes versões: 5.3.3, 5.4.2, 5.5.1,5.6.0 ou posterior.

Aruba

CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750, CVE-2023-22751 e CVE-2023-22752.
Data: 01/03/2023

Descrição. No dia 1 de março, foi publicado um relatório de vários pesquisadores detalhando várias vulnerabilidades que podiam afetar os produtos da Aruba. Este relatório notifica a existência de 33 vulnerabilidades classificadas como: 6 críticas, 19 importantes e 8 moderadas. A seguir, detalharemos as vulnerabilidades críticas:

- Foram relatadas várias vulnerabilidades que poderiam levar um invasor a executar o código arbitrário, mediante o envio de pacotes especificamente criados para a porta UDP (8211) utilizando o protocolo PAPI (Aruba Netowrks Access point management protocol). Os CVEs para esta vulnerabilidade são os seguintes: CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 e CVE-2023-22750.
- As outras duas vulnerabilidades críticas que afetam os produtos da Aruba permitiriam, por meio de um estouro de buffer, a execução de código arbitrário no sistema, enviando pacotes especialmente projetados para a porta UDP (8211) utilizando o protocolo PAPI. Esta é uma vulnerabilidade de execução remota de código. Os CVEs para esta vulnerabilidade são os seguintes: CVE-2023-22751 e CVE-2023-22752.

Link:https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04454en_us
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt
Produtos afetados. As vulnerabilidades afetam os seguintes produtos da Aruba:
• ArubaOS: 8.6.0.19 e versões anteriores, ArubaOS: 8.10.0.4 e versões anteriores, ArubaOS: 10.3.1.0 e versões anteriores, SD-WAN: 8.7.0-2.3.0.8 e versões anteriores.
Solução: A solução principal é atualizar para as seguintes versões dos produtos Aruba afetados:
• ArubaOS: 8.10.0.5 e versões seguintes, ArubaOS: 8.11.0.0 e versões seguintes, ArubaOS: 10.3.1.1 e versões seguintes, SD-WAN: 8.7.0.0-2.3.0.9 e versões seguintes.
Além disso, a Aruba também publicou uma série de recomendações para minimizar as chances de ser afetada por uma dessas vulnerabilidades:
• Para minimizar as chances de exploração, a comunicação entre o controlador/gateways e o ponto de acesso deve ser restrita por um segmento único da camada 2 ou uma Vlan; Além disso, se o controlador/gateways e gateways passarem para a camada 3, é aconselhável ter regras de firewall que restrinjam as comunicações dos dispositivos. Por último, habilitar a segurança extra para o protocolo PAPI fornecido pelo fabricante evitará vulnerabilidades.

PATCHES

Cisco

Data: 07-02-2023

Descrição. A Cisco publicou uma atualização de firmware para a interface de gerenciamento da Web de seus telefones IP das séries 6800, 7800 e 8800 que corrige a seguinte vulnerabilidade crítica:

- CVE-2023-20078: Essa vulnerabilidade poderia permitir que um usuário remoto não autorizado executasse o código arbitrário ou causasse um ataque de negação de serviço na interface web de gerenciamento dos telefones IP da Cisco das séries 6800, 7800 e 8800. Esta vulnerabilidade foi causada por uma falha na validação das informações inseridas, permitindo assim, que um invasor explorasse esta vulnerabilidade enviando solicitações especialmente projetadas para isso.

Link: https://cve.report/CVE-2023-20078
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP#details

Produtos afetados: telefones IP Cisco versão 6800, 7800 e 8800.

Solução: Atualizar os patches de segurança publicados pelo fabricante do dispositivo correspondente

Apple

Data: 27/02/2023

Descrição. A Apple lançou um relatório de segurança indicando várias atualizações para seus dispositivos iPadOS, iOS e macOS. Esses patches corrigem as vulnerabilidades: CVE-2023-23531, com gravidade crítica, CVE-2023-23530, com gravidade alta.

- CVE-2023-23531: esta vulnerabilidade permitiria que um invasor executasse o código arbitrário no equipamento, explorando expressões de NSPredicate que poderiam ignorar a validação realizada pelo componente NSPredicateVisitor, que permite ao invasor ignorar qualquer tipo de validação.
- CVE-2023-23530: No caso dessa vulnerabilidade, um invasor poderia explorar as listas negras usadas pelo NSPredicate, o que impedia o uso de determinadas classes ou métodos que poderiam comprometer a segurança do dispositivo. A exclusão dessas listas pode permitir que um invasor execute o código arbitrário em seu equipamento.

Link: https://techmonitor.ai/technology/cybersecurity/apple-security-vulnerabilities-ios-macos-ipados
https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-advanced-research-center-discovers-a-new-privilege-escalation-bug-class-on-macos-and-ios.html

Produtos afetados: As vulnerabilidades corrigidas afetavam as seguintes versões:

- MacOS 13.2 e anteriores.
- iOS 16.3 e anteriores.
- iPadOS 16.3 e anteriores.

Solução: Atualizar os patches de segurança publicados pelo fabricante do dispositivo correspondente.

EVENTOS

Cisco Develop 2023

5 e 6 de Abril de 2023

Um evento para explorar as ideias e perspectivas do software empresarial e nativo da nuvem com visão de futuro. Os participantes se conectarão pessoalmente ou virtualmente para discutir perspectivas contemporâneas e aprendizados relevantes para trabalhar com tecnologias na nuvem.

Link: Develop 2023: Secure It, Cloud It, Code It (cisco.com)

TecnoSec

26 e 27 de Abril de 2023

O evento Altas Tecnologias de Segurança e Inteligência, Tecnosec 2023, é um ponto de encontro para instituições e órgãos de segurança de Infraestruturas Críticas. A Tecnosec é o local ideal para promover encontros nacionais e internacionais e cultivar contatos valiosos para a indústria de segurança.

Link:TECNOSEC – Feria de Tecnologías Policiales, de Seguridad e Inteligencia - TECNOSEC

RSA Conference 2023

24 a 27 de Abril de 2023

A Conferência RSA é uma das maiores e mais conhecidas conferências de cibersegurança do mundo. Acontece todos os anos em São Francisco e atrai mais de 40.000 participantes de todo o mundo. Os temas abordados na RSA incluem tudo, desde gestão de riscos e conformidade até segurança na nuvem e segurança móvel.

Link: 2023 USA | RSA Conference

SANS Pen Test Austin 2023

17 a 22 de Abril de 2023

O SANS Pen Test Austin 2023 oferece seis dias de treinamento aprofundado e prático em testes de penetração, red teaming, purple teaming e desenvolvimento de exploits para profissionais que precisam saber como encontrar vulnerabilidades em suas organizações, entender riscos e priorizar recursos com base em possíveis ataques do mundo real.

Link: SANS Pen Test Austin 2023 | Cyber Security Training

RECURSOS

Você conhece seus riscos? INCIBE

Para ajudar as empresas a avaliar o seu estado de cibersegurança e avançar para níveis mais elevados de proteção, o INCIBE oferece uma ferramenta de autodiagnóstico especialmente projetada para esse fim. Por meio de uma série de perguntas, o usuário será orientado a determinar seu estado de segurança da informação, quais riscos ameaçam o funcionamento da empresa e quais aspectos devem ser melhorados. Tudo isso, para começar a medir. Para começar a melhorar.

LInk: ¿Conoces tus riesgos? | INCIBE

CSA CCM v4.0 Addendum - IBM Cloud Framework for Financial Services

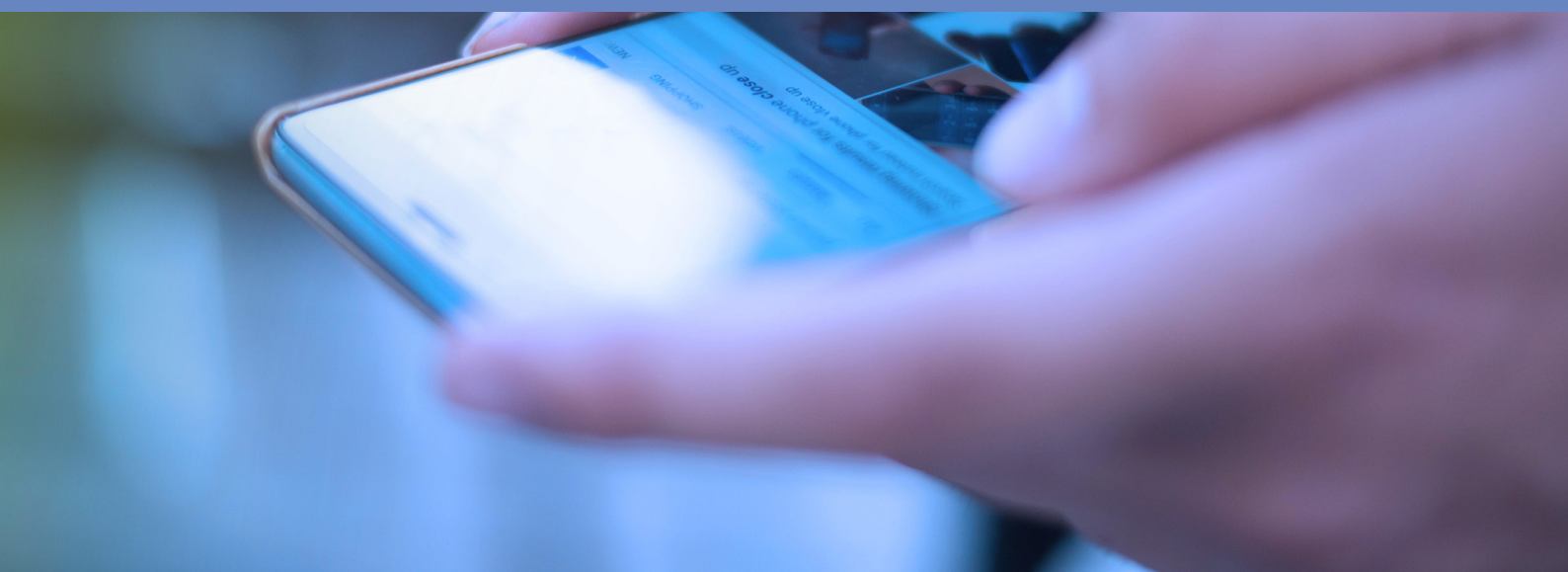
Este documento é um complemento da CSA CCM v4.0 para IBM Cloud Framework for Financial Services v1.1.0 que contém o mapeamento de controles entre o CCM e IBM Cloud Framework for Financial Services. O documento visa ajudar as organizações que estão em conformidade com o IBM Cloud Framework for Financial Services a atender aos requisitos do CCM.

Link: CSA CCM v4.0 Addendum - IBM Cloud Framework for Financial | CSA (cloudsecurityalliance.org)

STAR Enabled Solutions FAQ

Uma Solução Habilitada STAR é um produto ou serviço que utiliza a estrutura CCM ou o Questionário da Iniciativa de Avaliação de Consenso (CAIQ). Suas tecnologias e ferramentas foram avaliadas e atendem aos requisitos de segurança estabelecidos pela CSA. Esse processo de verificação permite que as empresas implantem com mais facilidade ferramentas que estejam alinhadas ou em conformidade com o STAR, a estrutura CCM e as melhores práticas.

Link: STAR Enabled Solutions FAQ | CSA (cloudsecurityalliance.org)



RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Cibersegurança en NTT DATA Latam y Perú

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

Carla Passos Schwarzer

Directora 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

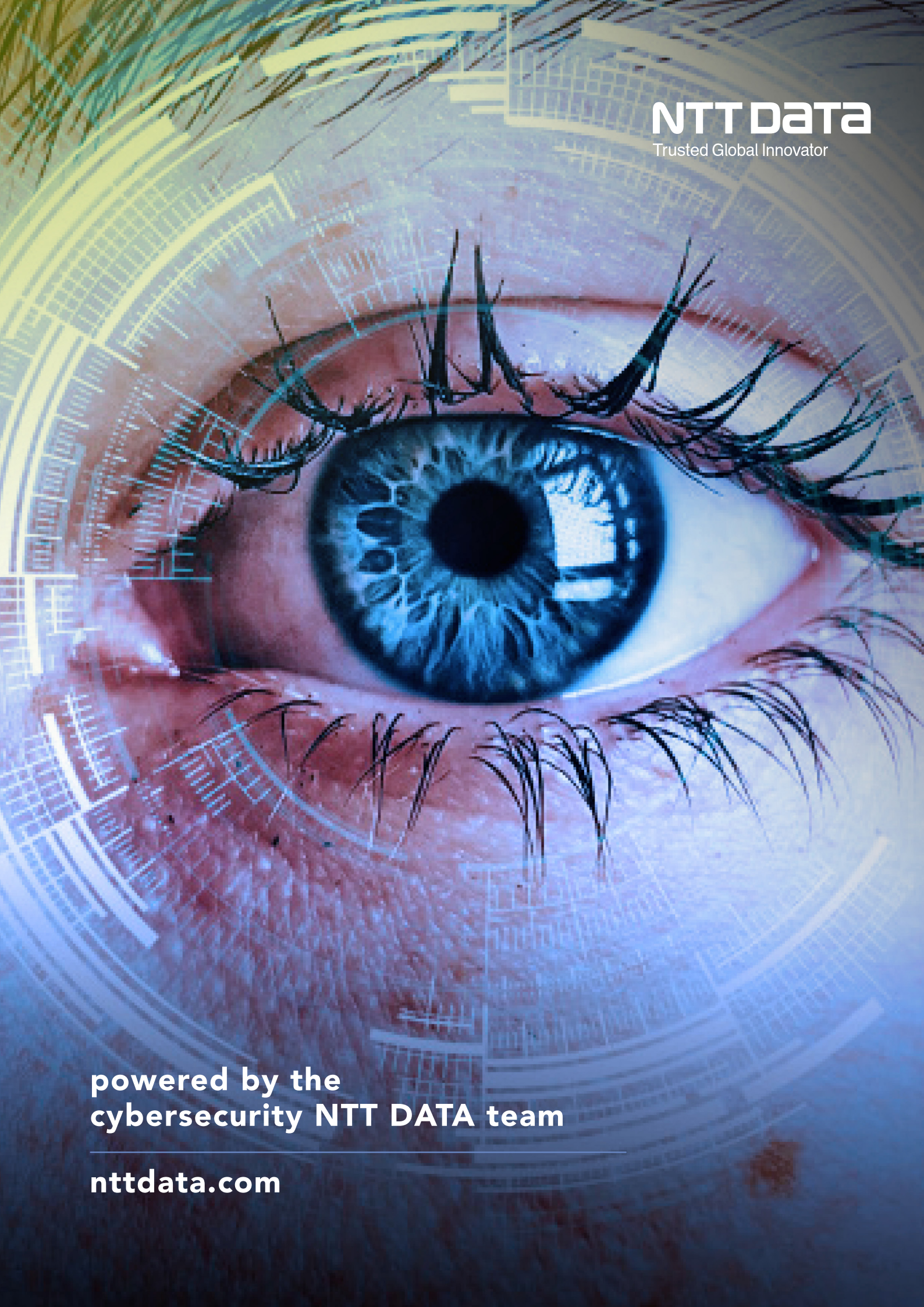
nestor.ordonez.ramirez@emeal.nttdata.com

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