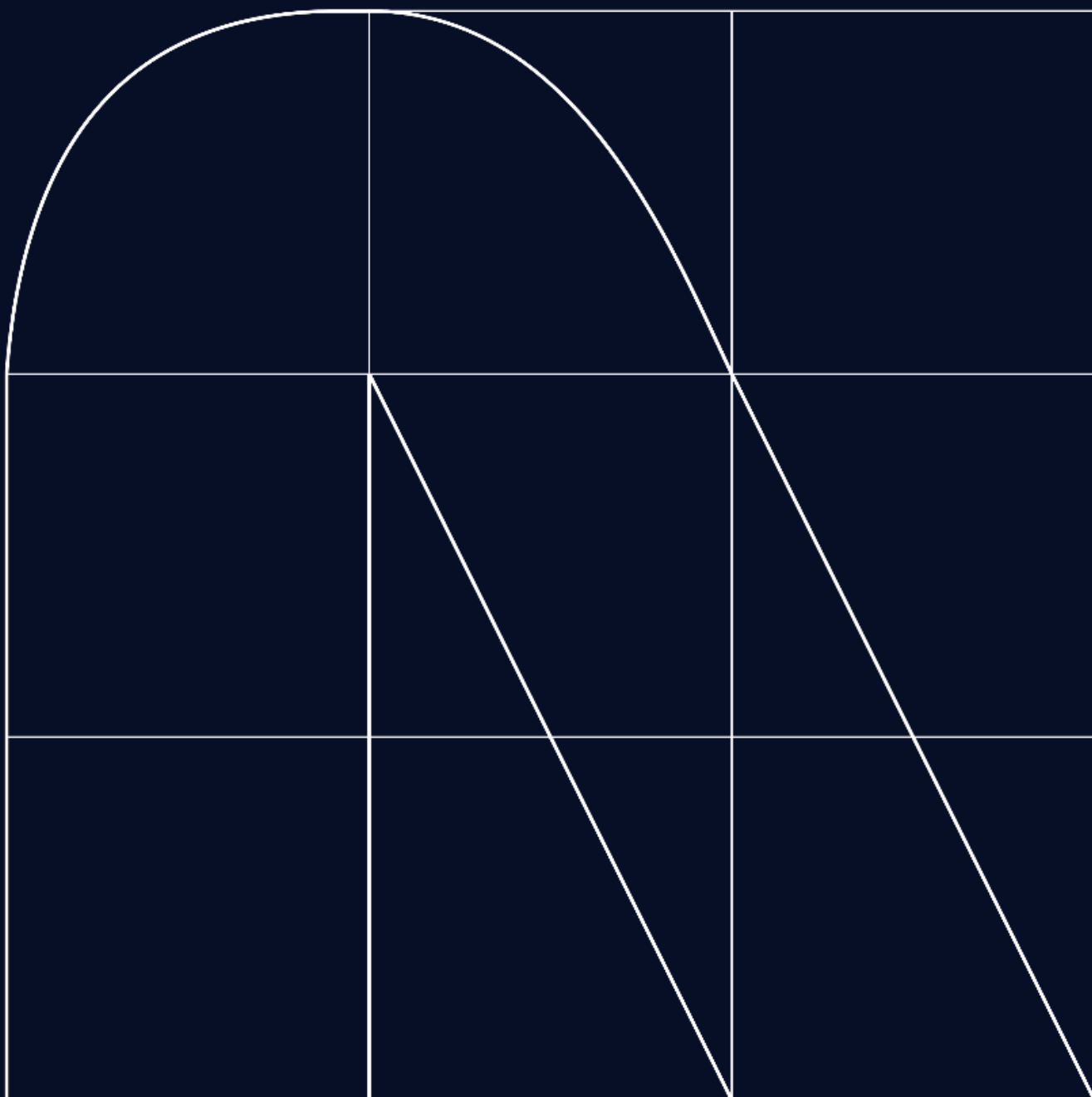
Edição 90 | maio 2024

NTT DATA

Radar

A revista da cibersegurança



Integração entre IA e ML na Detecção e Resposta a Ameaças

Em um mundo cada vez mais digitalizado, a cibersegurança se tornou uma preocupação primordial tanto de empresas e governos quanto de usuários individuais. Com o aumento constante das ameaças cibernéticas, a necessidade de soluções inovadoras é mais evidente do que nunca. Nesse contexto, a Inteligência Artificial (IA) e o Machine Learning (ML) surgem como ferramentas cruciais na defesa contra essas ameaças.

Essas tecnologias oferecem uma abordagem proativa e flexível para enfrentar os desafios cibernéticos. Ao analisar grandes volumes de dados em tempo real, a IA e o ML são capazes de detectar padrões e comportamentos anômalos, antecipando e neutralizando ameaças antes da ocorrência de danos. Essa capacidade preditiva é essencial em um ambiente no qual as ameaças evoluem constantemente, e a detecção precoce pode fazer a diferença entre um ataque bem-sucedido e uma defesa eficaz.

Da detecção de ameaças à resposta a incidentes, as aplicações da IA e ML na cibersegurança são diversas e eficazes. Essas tecnologias permitem que as equipes de segurança respondam de forma rápida e eficiente a possíveis ataques, reduzindo o erro humano e melhorando a eficiência operacional. Apesar dos benefícios, a implementação de IA e ML na cibersegurança também enfrenta desafios, como a disponibilidade de dados de treinamento adequados e a vulnerabilidade a ataques.

Apesar dos desafios, várias empresas conseguiram aplicar a IA e ML na segurança cibernética. A IBM, Darktrace, Cylance e Fortinet são apenas alguns exemplos de empresas que desenvolveram soluções inovadoras baseadas nessas tecnologias para detectar e prevenir ameaças com eficiência. Essas histórias de sucesso demonstram o potencial da IA e do ML para fortalecer as defesas cibernéticas e proteger os ativos digitais em um ambiente cada vez mais hostil e complexo.

Em última análise, a integração entre IA e ML na cibersegurança oferece oportunidades significativas para aumentar a proteção contra ameaças digitais, mas seu êxito irá depender de como elas são implementadas e de seu uso ético e responsável.

Por exemplo, a Symantec emprega inteligência artificial em vários dos serviços que oferece. Em seu serviço de "File Reputation Analysis" (Análise de Reputação de Arquivos), por meio da análise de bilhões de links, sites e arquivos, consegue determinar se um arquivo é confiável ou malicioso, atribuindo-lhe uma pontuação antes de chegar às equipes.

Outro exemplo da Symantec é o serviço "Email Security Cloud" (Nuvem de Segurança de E-mail), que filtra mensagens de e-mail indesejadas na nuvem e protege as caixas de correio de ataques direcionados. Este serviço possui recursos de autoaprendizagem e inteligência da Symantec para oferecer uma segurança de e-mail eficaz e precisa, sendo compatível com os provedores de e-mail mais conhecidos no mercado.

Por outro lado, recorrem ao aprendizado de máquina (ML) avançado para determinar a confiabilidade de um arquivo, reconhecendo atributos maliciosos e definindo regras para detecções. O recurso de aprendizado de máquina permite bloquear novas variantes de malwares analisando bilhões de exemplos de arquivos, maliciosos ou não, contidos na rede de inteligência global.

Outra grande empresa que já utiliza inteligência artificial é a IBM, em sua suíte “QRADAR”, que constitui uma solução modernizada de detecção e resposta a ameaças. O portfólio inclui IA e automação de nível empresarial para aumentar drasticamente a produtividade dos analistas, sendo particularmente útil para equipes com recursos limitados.
Por fim, uma das outras soluções da IBM que implementa inteligência artificial é o "IBM Security Verify". Essa solução adiciona um contexto profundo orientado por IA ao gerenciamento de acesso à identidade do consumidor e da força de trabalho, protegendo usuários e aplicativos dentro e fora da empresa com uma abordagem de software como serviço.

Desinformação e IA nos Processos Eleitorais

Cibercrônicas

A União Europeia prevê um aumento das campanhas de desinformação focadas nas eleições europeias de junho, oriundas de atuadores externos, especialmente aqueles associados ao governo russo, com o objetivo de interferir nos processos eleitorais. Essas campanhas de desinformação se adaptaram às restrições decorrentes da invasão russa da Ucrânia, com um uso predominante da internet e dos serviços de mensagens instantâneas como meio de distribuição das campanhas, em oposição aos canais mais tradicionais, como a televisão, que foram censurados na Europa.

A identificação da desinformação tornou-se cada vez mais complexa devido ao uso desses canais de distribuição, bem como à própria natureza da desinformação, que aproveita os avanços em tecnologias como a Inteligência Artificial (IA) para produzir resultados cada vez mais sofisticados com menos esforço. Os avanços nesse campo foram refletidos em estudos recentes, que documentaram o uso de IA generativa para a produção de textos, vídeos e imagens relacionados a campanhas de desinformação em pelo menos 16 países durante o ano de 2023.

Campanha de Phishing na Declaração de Impostos

Ao mesmo tempo, com a campanha de declaração de imposto de renda a todo vapor, os cibercriminosos estão aproveitando a oportunidade para aplicar golpes baseados em e-mails e mensagens em massa, pelos quais tentam enganar suas vítimas. Por meio de campanhas de phishing, eles enviam mensagens em massa, à espera de que alguém caia no golpe.

Nesses e-mails, os cibercriminosos aplicam táticas enganosas, muitas vezes alegando que a Receita reembolsará o dinheiro da vítima. Além disso, eles podem incluir links para sites fraudulentos que parecem oficiais, mas são projetados para roubar informações pessoais, como números de cartão e códigos de segurança. Esses sites são falsificados e usam logos e fontes da Receita para parecer oficiais.

Neste caso, a recomendação é pesquisar o site da Receita ou o site desejado, acessar a página oficial e autenticar-se a partir daí para verificar possíveis notificações. Em suma, a segurança on-line continua sendo uma preocupação constante. Com a temporada de impostos em curso, é importante ter cuidado e estar atento aos e-mails e mensagens que recebemos, pois muitos deles podem ser fraudulentos.

Vulnerabilidades Importantes

Há pouco tempo, foi descoberto um problema de segurança na ferramenta XZ Utils (CVE-2024-3094), de uso comum em sistemas operacionais Linux. Ela é usada para comprimir e descompactar dados no formato XZ. Andrés Freund, desenvolvedor da Microsoft, detectou códigos maliciosos ocultos nesta ferramenta enquanto investigava problemas de desempenho no SSH. O código malicioso modifica funções dentro do pacote liblzma e interfere nos dados utilizados pela ferramenta e, sob certas condições, pode permitir que um invasor obtenha acesso a um sistema afetado. No entanto, esse código malicioso não é encontrado na distribuição Git da ferramenta, apenas no pacote de download completo.

Além disso, a Fortinet divulgou detalhes sobre uma vulnerabilidade crítica de SQL Injection, presente nas versões 7.2.0 a 7.2.2 e 7.0.1 a 7.0.10 do FortiClient Enterprise Management Server. Essa vulnerabilidade permite que um invasor execute comandos ou codifique remotamente por meio de solicitações especificamente criadas, potencialmente obtendo acesso de administrador ao servidor onde o software está sendo executado.

Estratégias de Compliance

Por Soledad Romero

Em um mundo cada vez mais globalizado, as organizações zelam pelo compliance regulatório de diversos modos. Fazê-lo de forma eficaz e econômica requer a definição de uma estratégia sólida que envolva os diferentes atores e partes interessadas necessários ao processo. A complexidade do compliance regulatório em um mundo globalizado

Atualmente, todas as organizações enfrentam um cenário regulatório complexo e em constante mudança em escala global. A proliferação de leis e regulamentos em diferentes segmentos e jurisdições apresenta desafios significativos para as entidades que procuram operar dentro dos limites da legalidade.

Ao reconhecer que o cumprimento das leis é essencial para manter a integridade e a confiança nas instituições e mercados (sejam locais, regionais, nacionais ou internacionais), cada organização busca aderir a regulamentos que sejam aplicáveis e relevantes não apenas para economizar custos, evitar incidentes de cibersegurança ou penalidades, mas também com o objetivo de antecipar tendências, fortalecer sua reputação e relacionamento com as partes interessadas.

Em um ambiente tão dinâmico como o atual, a preparação para responder de forma eficaz representa um grande desafio, que torna fundamental planejar e estabelecer uma estratégia de compliance sólida e bem estruturada. Requer não apenas identificar o nível de maturidade do compliance dentro da organização, mas também avaliar se há um conhecimento e compreensão aprofundados a respeito dos regulamentos. Além disso, é importante garantir a flexibilidade e capacidade de prever e adaptar-se rapidamente a eventuais novas exigências legais.

Tudo isso torna o compliance regulatório um aspecto crítico que requer atenção constante e uma estratégia proativa para garantir o sucesso e a sustentabilidade em longo prazo de qualquer organização. Essa estratégia proativa exige desde o início uma atitude consciente e diligente entre os principais atores que intervêm a partir de seu planejamento e funções, a saber:

- Diretor de Compliance: responsável por planejar e executar o plano de compliance e comunicar as medidas a serem seguidas para toda a organização.
- Alta Direção: deve estar comprometida com a cultura de compliance e garantir que os recursos necessários sejam alocados.
- Departamento Jurídico: aconselha sobre as implicações legais e auxilia na interpretação dos regulamentos aplicáveis.
- Departamento de TI: implementa e mantém soluções tecnológicas para respaldar o compliance.
- Recursos Humanos: é responsável pelo treinamento e conscientização dos colaboradores sobre questões de compliance.
- Auditores Internos e Externos: verificam a conformidade e a eficácia das políticas e procedimentos.
- Colaboradores: todos os membros da organização devem ser informados e seguir as políticas de compliance.

Entre as recomendações e melhores práticas mais comuns ao estabelecer a estratégia, destaca-se:

1. Estabelecer uma referência: a partir de uma auditoria para entender o estado atual do compliance e os regulamentos aplicáveis.
2. Desenvolvimento de procedimentos: acessíveis e facilmente aplicáveis dentro da organização e revisados periodicamente.
3. Monitoramento e rastreamento: a fim de garantir uma conformidade e atualização contínuas, conforme necessário pela entidade.
4. Envolvimento da alta administração: conforme mencionado acima em relação às principais partes interessadas.
5. Treinamento contínuo: os colaboradores devem estar bem informados a respeito dos regulamentos e sobre como afetam suas funções. Nesse sentido, um plano de treinamento sob medida deve ser regular e adaptável às mudanças na legislação.

Por fim, mensurar o sucesso de uma estratégia de compliance envolve avaliar como as atividades da organização se alinham aos regulamentos e leis aplicáveis. A mensuração por meio de KPIs específicos, pesquisas, análises de risco ou avaliações de risco, entre outros, fornece uma visão quantitativa e qualitativa do desempenho da estratégia de compliance e ajuda as organizações a ajustar suas práticas para garantir um aperfeiçoamento contínuo.

O objetivo final é criar uma estrutura que faça frente aos riscos de compliance e ajude a evitá-los, garantindo que a organização esteja preparada para desafios futuros no cenário regulatório.

Precisamos padronizar a Inteligência Artificial

O uso de Inteligência Artificial na UE será regulada pela Lei de Inteligência Artificial, a primeira lei abrangente do mundo sobre IAs. A prioridade do Parlamento é garantir que os sistemas de IAs utilizados na UE sejam seguros, transparentes, rastreáveis, não discriminatórios e ecológicos. Os sistemas de IAs devem ser supervisionados por humanos, e não por automação, para evitar resultados prejudiciais. O Parlamento também visa estabelecer uma definição uniforme e tecnologicamente neutra de IA que possa ser aplicada a futuros sistemas de IA.

O Parlamento e seus países membros começaram a elaborar regulamentos e leis para delinear a IA. Em particular, o Parlamento Europeu aguarda a aprovação do "REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO QUE ESTABELECE REGRAS HARMONIZADAS SOBRE A INTELIGÊNCIA ARTIFICIAL (LEI SOBRE INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO".

Entre os estados membros, a Espanha desponta como uma das principais líderes após a aprovação, em 22 de agosto de 2023, do RD 729/2023, que aprova o Estatuto da Agência Espanhola de Supervisão de Inteligência Artificial. Além disso, a AEPD (Agência Espanhola de Proteção de Dados) desenvolveu dois guias sobre IA. O primeiro em fevereiro de 2020 para adaptar os tratamentos de IA ao GDPR e um segundo em janeiro de 2021 sobre os Requisitos para Auditorias de Tratamentos que incluem IA.

Neste contexto político, a Comissão Europeia propôs um quadro regulamentar sobre inteligência artificial com os seguintes objetivos específicos:

- Garantir que os sistemas de IA introduzidos e utilizados no mercado da UE sejam seguros e cumpram a legislação atual em matéria de direitos fundamentais e valores da União;
- Garantir a segurança jurídica para fomentar o investimento e a inovação em IA;
- Melhorar a governança e a implementação efetiva da legislação atual em matéria de direitos fundamentais e os requisitos de segurança aplicáveis aos sistemas de IA;
- Promover o desenvolvimento de um mercado único para permitir o uso legal, seguro e confiável de aplicativos de IA e evitar a fragmentação do mercado.

Quais problemas a aplicação desses regulamentos resolve?

Neste contexto, a IA apresenta uma série de problemas e riscos que precisam de ser mitigados tanto quanto possível por meio da legislação da UE.

Devido ao crescente uso da IA tanto nos negócios quanto no cotidiano, sua regulamentação se faz necessária pelos seguintes motivos:

- Ética e direitos individuais: a IA pode ter um impacto significativo na vida das pessoas, desde a tomada de decisões automatizada até a coleta e uso de dados pessoais. A regulamentação ajuda a garantir que os direitos individuais sejam respeitados e que práticas discriminatórias ou injustas sejam evitadas.
- Privacidade e segurança: a falta de regulamentação pode levar a vulnerabilidades de segurança e à exploração de sistemas de IA. Podem ser estabelecidos padrões de segurança e privacidade para proteger indivíduos e organizações.
- Transparência e responsabilidade: os regulamentos podem exigir transparência nos algoritmos de IA e nos processos de tomada de decisão. Além disso, eles podem estabelecer responsabilidade legal em caso de erros ou danos causados pelos sistemas de IA.
- Viés algorítmico: a regulamentação pode abordar o viés nos sistemas de IA e garantir que decisões injustas ou discriminatórias não sejam tomadas, com base em raça, gênero ou outros fatores.
- Concorrência justa: pode impedir práticas anticoncorrenciais e promover a inovação justa no mercado de IA.
- Segurança pública: os regulamentos podem abordar a segurança em aplicações críticas, como veículos autônomos e sistemas de saúde, para evitar riscos à vida e à saúde.
- Mitigação de riscos: a IA apresenta riscos significativos, como desemprego tecnológico, falta de privacidade e viés algorítmico. A regulamentação pode ajudar a resolver esses problemas e mitigar os riscos associados à IA.
- Confiança do público: promove a confiança do público na tecnologia de IA, o que pode ser crucial para a sua adoção generalizada.
- Coerência global: a regulamentação pode ajudar a estabelecer padrões comuns em um mundo cada vez mais interconectado, facilitando a cooperação internacional e o comércio de tecnologia de IA.

Em suma, a regulamentação da IA é essencial para garantir que essa tecnologia seja desenvolvida e utilizada de forma ética, segura e responsável, beneficiando a sociedade como um todo e minimizando os riscos.

Quando os regulamentos entrarão em vigor?

O principal problema ao legislar nessa área é que a inovação tecnológica é muito mais rápida do que o tempo necessário para criar, desenvolver e aprovar leis. Apesar do crescente uso da IA, ainda não há uma data definida para a aprovação da Lei de Inteligência Artificial da UE. Em 14 de junho de 2023, uma série de alterações foi aprovada no Parlamento Europeu. Deu-se início às discussões sobre a forma final da lei no Conselho, juntamente com os países da UE. O objetivo é chegar a um consenso até o final deste ano.

Quais requisitos de auditoria precisaremos atender?

Em relação à Lei de IA da UE, uma vez que ainda não foi aprovada e está sujeita a modificações, é muito cedo para determinar quais requisitos serão obrigatórios. Quanto à Espanha, a AEPD publicou dois guias sobre IA, entre os quais destacamos "Requisitos para Auditorias de Tratamentos que incluem IA". Nele, é retratado um conjunto de controles que podem ser incorporados em auditorias de tratamentos de dados pessoais que empregam componentes de IA.

É importante observar que todos os controles incluídos foram concebidos para analisar a adequação do tratamento da perspectiva da proteção de dados. Além disso, são adicionadas algumas observações metodológicas que podem ser específicas e características desses tipos de auditorias.

Em um nível muito alto, o seguinte deve ser considerado:

- Identificação e transparência do componente;
- Objetivo do componente de IA;
- Fundamentos do componente de IA;
- Gerenciamento de dados;
- Verificação e validação.

Quais organizações serão afetadas pelas regulamentações de IA?

Todas as organizações que desenvolvem, comercializam ou utilizam serviços de IA serão afetadas, mas esses regulamentos também se aplicarão a estruturas que usam serviços de IA de terceiros ou têm contratos com um provedor que usa serviços de IA para os serviços que fornecem.

Além disso, quando as organizações considerarem a escolha de um provedor de serviços de IA externo no futuro, elas devem considerar alguns fatores, como:

- Experiência e expertise;
- Transparência e ética;
- Compliance regulatório;
- Escalabilidade e flexibilidade;
- Segurança e privacidade;
- Facilidade de integração.

Em suma, precisamos nos preparar para cumprir os regulamentos de IA e garantir que nossas organizações estejam alinhadas com os regulamentos e padrões relevantes. Isso será alcançado por meio de um processo contínuo que requer um compromisso continuado com a ética, segurança no desenvolvimento e implementação de tecnologias de IA.

Manter-se atualizado sobre as mudanças nas regulamentações atuais e futuras pode ajudar significativamente qualquer organização a manter a conformidade e evitar futuras sanções.

Lei de Resiliência Operacional Digital: o fortalecimento da cibersegurança na União Europeia

A Lei de Resiliência Operacional Digital (DORA) representa um marco regulatório significativo para o setor financeiro da União Europeia, visando fortalecer a resiliência operacional digital das entidades financeiras. Apresentada em janeiro de 2023 e programada para ser aplicada em janeiro de 2025, a DORA busca harmonizar os regulamentos existentes, com foco na gestão de riscos relacionados às tecnologias de informação e comunicação (TIC) e resiliência a graves interrupções operacionais. Este regulamento é particularmente relevante nos contextos bancário e de seguros, nos quais a dependência dos serviços de TIC de terceiros é considerável e os riscos associados podem atrair significativas implicações transnacionais.

A estrutura da DORA está assentada em cinco pilares primordiais: gerenciamento de riscos de TIC, resposta e comunicação de incidentes, testes de resiliência operacional digital, gerenciamento de riscos de terceiros e compartilhamento de informações e inteligência. Esses pilares foram concebidos para garantir que as entidades financeiras possam efetivamente identificar, proteger, detectar, responder e se recuperar de ameaças cibernéticas. Além disso, a DORA estabelece requisitos rigorosos para contratos com prestadores de serviços de TIC, incluindo cláusulas sobre direitos de auditoria, subcontratação e rescisão.

Quais são os principais desafios da DORA?

A implementação da DORA apresenta vários desafios para as entidades financeiras na União Europeia. Em primeiro lugar, a necessidade de um alinhamento abrangente com os requisitos de gerenciamento de riscos de TIC pode exigir uma revisão significativa das práticas atuais. As entidades precisarão estabelecer uma estrutura de gerenciamento de riscos robusta e adaptável que abranja todos os aspectos da resiliência operacional digital, desde a prevenção de incidentes até a recuperação.

Outro desafio é o gerenciamento de riscos de terceiros, em particular em um ambiente no qual muitas operações dependem de serviços de TIC prestados por entidades externas. As entidades financeiras precisarão garantir que os contratos com provedores incluam disposições rigorosas sobre segurança cibernética e mecanismos de resposta a incidentes, que podem ser complexos de negociar e implementar.

Além disso, a DORA exige que as entidades financeiras realizem testes de resiliência operacional digital, envolvendo o desenvolvimento e a execução de uma série de testes avançados para avaliar a capacidade de resistir e se recuperar de graves interrupções operacionais. Isso requer investimentos em tecnologia e expertise, bem como o estabelecimento de processos internos para realizar esses testes com regularidade.

A notificação de incidentes relacionados às TIC também é um aspecto crítico desta lei. As entidades devem ser capazes de detectar e relatar incidentes às autoridades relevantes dentro de um curto período, exigindo sistemas de detecção e comunicação eficientes e confiáveis.

A troca de informações e inteligência sobre ameaças cibernéticas é outro requisito da DORA que pode ser desafiador, pois requer a implementação de canais seguros e eficazes para a troca de informações entre entidades financeiras e autoridades, bem como entre entidades financeiras e seus pares ou partes interessadas relevantes, respeitando a confidencialidade e a proteção de dados.

Por fim, este regulamento estabelece uma estrutura de supervisão para provedores críticos de TIC, o que significa que as entidades financeiras precisarão se adaptar a um novo nível de escrutínio e compliance por parte das autoridades reguladoras. Isso pode envolver ajustes significativos nas operações e governança de TIC para atender aos padrões estabelecidos.

Como superar os desafios impostos pela DORA?

Para superar os desafios impostos pela implementação da Lei de Resiliência Operacional Digital (DORA), as entidades financeiras podem adotar uma variedade de estratégias eficazes. Em primeiro lugar, é crucial desenvolver uma compreensão profunda dos requisitos da DORA, o que pode ser alcançado por meio de programas internos de treinamento e conscientização. Isso inclui familiarizar-se com os cinco pilares da DORA: gerenciamento de riscos de TIC, resposta e comunicação de incidentes, testes de resiliência operacional digital, gerenciamento de riscos de terceiros e compartilhamento de informações e inteligência.

Uma abordagem proativa para o gerenciamento de riscos de TIC é essencial, o que significa identificar, avaliar e mitigar os riscos. As entidades devem estabelecer uma estrutura de gerenciamento de riscos robusta que seja integrada em toda a organização, garantindo que as medidas de segurança cibernética estejam alinhadas com os objetivos de negócios da entidade e com a tolerância ao risco.

A colaboração com prestadores de serviços de TIC é outro aspecto crítico. As entidades financeiras devem garantir que os contratos com terceiros incluam cláusulas detalhadas sobre segurança cibernética, direitos de auditoria e mecanismos de resposta a incidentes. Além disso, a realização de *due diligence* rigorosa e monitoramento contínuo dos provedores é importante para garantir a conformidade com a DORA.

O teste de resiliência operacional digital é fundamental para avaliar a capacidade de resistir e se recuperar de interrupções operacionais. As entidades devem implementar um programa de testes abrangente que inclua testes básicos e avançados para identificar vulnerabilidades e melhorar as estratégias de resposta.

A notificação imediata de incidentes relacionados às TIC às autoridades competentes é um requisito da DORA. Nesse sentido, as instituições financeiras precisam de sistemas eficientes de detecção e notificação de incidentes para poder responder de forma rápida e adequada.

O compartilhamento de informações sobre ameaças cibernéticas é vital para a resiliência operacional digital. As entidades devem estabelecer canais seguros e eficazes para a troca de informações e inteligência sobre ameaças cibernéticas, tanto internamente quanto com outras entidades e autoridades reguladoras.

Por fim, as entidades financeiras devem estar preparadas para a nova estrutura de supervisão para provedores críticos de TIC estabelecida pela DORA. Isso pode exigir ajustes nas operações e governança de TIC para cumprir os padrões de supervisão.

Conclusão

Em resumo, a conformidade com a DORA é um processo complexo que requer uma abordagem estratégica e compromisso contínuo com a melhoria da resiliência operacional digital. Superar seus desafios requer uma abordagem holística e estratégica, envolvendo investimento em tecnologia, processos e capital humano. A conformidade com a DORA não é apenas uma questão regulatória, mas também uma oportunidade para as entidades financeiras fortalecerem sua resiliência operacional digital e protegerem suas operações e clientes de interrupções e ameaças cibernéticas. A colaboração e o compromisso contínuo com a melhoria da resiliência operacional serão cruciais para o sucesso nessa trajetória.

Para entidades que já possuem certificação ISO 27001, uma norma internacional para sistemas de gerenciamento de segurança da informação ou implementaram estruturas como o NIST, o caminho para a conformidade com a DORA pode ser mais suave. A ISO 27001 fornece uma estrutura que se alinha aos princípios de gerenciamento de riscos da DORA, enquanto o NIST oferece orientação para identificar, proteger, detectar, responder e se recuperar de ameaças cibernéticas. No entanto, a certificação ISO 27001 ou a implementação do NIST não equivale à conformidade automática com a DORA. É essencial que as entidades realizem uma análise de lacunas para identificar áreas em que as práticas existentes podem precisar de ajustes para atender aos requisitos específicos desta lei.

Vulnerabilidades

Vulnerabilidade crítica na Biblioteca XZ Utils

Data: 1 de abril de 2024
CVE: CVE-2024-3094

CVSS: 10

CRÍTICA

Descrição
Um código malicioso foi descoberto nos tarballs do XZ Utils, começando com a versão 5.6.0. Através de uma série de ofuscações complexas, o processo de compilação da liblzma extrai um arquivo de objeto precompilado de um arquivo de teste disfarçado no código-fonte, que é então usado para modificar funções específicas no código da liblzma.

Isso resulta em uma biblioteca liblzma modificada que qualquer software vinculado pode usar, interceptando e modificando a interação de dados com esta biblioteca.

Produtos afetados
Foi indicado que os pacotes afetados estão presentes apenas no Fedora 41 e no Fedora Rawhide dentro do ecossistema da comunidade Red Hat. Nenhuma versão do Red Hat Enterprise Linux (RHEL) é afetada.

Solução
Os usuários afetados são aconselhados a atualizar para versões que não incluam o código malicioso.

As versões comprometidas das bibliotecas XZ Utils são 5.6.0 e 5.6.1, incluídas apenas no pacote de download do tarball.

Os usuários são aconselhados a verificar e limpar seus sistemas dessas versões afetadas.

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

Vulnerabilidade nos dispositivos NAS da D-Link

Data: 3 de abril de 2024
CVE: CVE-2024-3272 e mais 1

CVSS: 9,8

CRÍTICA

Descrição
As vulnerabilidades identificadas como CVE-2024-3272 e CVE-2024-3273 são classificadas como críticas e de alta gravidade, respectivamente.

A vulnerabilidade crítica existe no URI nas_sharing.cgi dos dispositivos NAS da D-Link.

Atualmente, existe uma exploração para a vulnerabilidade crítica, que poderia permitir a coleta de credenciais por meio da manipulação de argumentos. Além disso, o ataque pode ser iniciado remotamente.

Produtos afetados
Os modelos afetados por essa vulnerabilidade são aqueles que atingiram seu fim de vida (EOL) e, portanto, não recebem mais atualizações de firmware. Eles incluem:
- DNS-340L
- DNS-320L
- DNS-327L
- DNS-325

A D-Link confirmou que esses modelos estão expostos à exploração devido à vulnerabilidade e recomenda sua remoção.

Solução
Dado que a D-Link não planeja lançar uma atualização de firmware para esses modelos EOL, a recomendação oficial é remover e substituir esses dispositivos vulneráveis. Os usuários são avisados de que, se continuarem a usar esses dispositivos contra a recomendação da D-Link, devem garantir que tenham o firmware mais recente disponível no site legado da D-Link, atualizar regularmente a senha exclusiva do dispositivo para acessar sua configuração da web e manter a criptografia Wi-Fi habilitada com uma senha exclusiva.

Referências
- nvd.nist.gov
- nvd.nist.gov
- thehackernews.com

Patches

CRÍTICA **Atualizações de segurança críticas para o Google Chrome**

Data: 2 de abril de 2024
CVE: CVE-2024-3156 e mais 2

Descrição
O Google lançou uma série de atualizações de segurança para resolver vários problemas que afetam o produto Google Chrome. A atualização corrige um total de três vulnerabilidades, todas críticas em termos de gravidade.

A vulnerabilidade CVE-2024-3156, categorizada como uma implementação inadequada no mecanismo JavaScript V8 do Google Chrome, pode ser explorada para executar código arbitrário ou acessar informações confidenciais no sistema.

A vulnerabilidade CVE-2024-3158 ocorre quando um programa acessa uma área de memória após ter sido liberado, o que pode resultar em comportamento imprevisível ou execução não autorizada de código.

A vulnerabilidade CVE-2024-3159 também afeta o mecanismo JavaScript V8 devido ao acesso incorreto à memória fora dos limites, o que pode levar a comportamentos imprevisíveis por meio de manipulações específicas de JavaScript ou até mesmo permitir a execução de código malicioso.

Produtos afetados
As versões do Google Chrome afetadas por essas vulnerabilidades são:

- Versões anteriores a 123.0.63.12.105, 123.0.63.12.106 e 123.0.63.12.107 para Windows e Mac.
- Versões anteriores a 123.0.63.12.105 para Linux.

Solução
Atualize o Google Chrome para a versão mais recente disponível para Windows, Mac e Linux no site oficial.

Referências
- chromereleases.googleblog.com
- www.bleepingcomputer.com

CRÍTICA **Atualização de segurança de abril do Android Pixel/Nexus**

Data: 2 de abril de 2024
CVE: CVE-2024-29740 e mais 2

Descrição
O Boletim de Segurança do Android de 2 de abril de 2024 destaca várias vulnerabilidades de segurança detectadas em dispositivos Android Pixel/Nexus de gravidade crítica e alta.

Dentre todas as vulnerabilidades detectadas, cabe destacar 1 de gravidade crítica e 2 de gravidade alta (zero-day), detalhadas a seguir:

- CVE-2024-29740 (crítica): vulnerabilidade de escalonamento de privilégios nos dispositivos Pixel mencionados.
- CVE-2024-29745 (alta): vulnerabilidade que pode levar à divulgação de informações confidenciais.
- CVE-2024-29748 (alta): vulnerabilidade de escalonamento de privilégios.

Produtos afetados
Você pode consultar a lista completa de produtos afetados, que impactam dispositivos Pixel compatíveis, no seguinte link: support.google.com.

Solução
A solução para essas vulnerabilidades envolve a aplicação de patches de segurança no nível da plataforma fornecidos pelo Android Open Source Project (AOSP).

Os telefones Pixel recebem atualizações para resolver problemas de segurança detalhados nos boletins de segurança pública do Android. Recomenda-se verificar e atualizar para a versão mais recente do Android Pixel, conforme indicado na página oficial.

Referências
- cybersecuritynews.com
- bleepingcomputer.com

Eventos

CONFERÊNCIA RSA 2024 SÃO FRANCISCO (6 a 9 de maio)

A RSA, fundada em 1991 pela RSA Security, emergiu como uma das conferências mais importantes no campo da cibersegurança em todo o mundo. Este evento emblemático reúne especialistas, líderes do setor e profissionais de TI para abordar os desafios atuais e emergentes em segurança de computadores. Por meio de apresentações, painéis, workshops e demonstrações, a conferência oferece um espaço vital para explorar novas soluções e melhores práticas em proteção de dados, ameaças cibernéticas, segurança na nuvem, inteligência artificial aplicada à segurança, compliance regulatório e outros temas relevantes em proteção de informações. A Conferência RSA tornou-se uma plataforma essencial para colaboração, aprendizado e inovação em um mundo digital cada vez mais interconectado.

Link

CONFERÊNCIA OSINTOMÁTICO 2024 (17 a 18 de maio)

A conferência Osintomático 2024 reúne profissionais de segurança, pesquisadores e entusiastas para compartilhar conhecimentos sobre técnicas de inteligência de código aberto (OSINT) e engenharia social. O programa inclui apresentações, workshops, mesas redondas e demonstrações práticas sobre tópicos como coleta de informações de fontes abertas, análise de dados de redes sociais, investigação de antecedentes e cibersegurança. Os palestrantes são especialistas reconhecidos em seus campos, e a conferência é uma excelente oportunidade para aprender e interagir com outros profissionais do setor.

Link

45º SIMPÓSIO IEEE DE SEGURANÇA E PRIVACIDADE (22 a 24 de maio)

Desde 1980, o Simpósio IEEE sobre Segurança e Privacidade tem sido o principal fórum para apresentar os avanços em segurança de computadores e privacidade eletrônica, e para reunir pesquisadores e profissionais da área. O Simpósio de 2024 marcará o 45º encontro anual desta conferência emblemática. Ele acontecerá de 20 a 22 de maio de 2024, e os Workshops de Segurança e Privacidade serão realizados no dia 23 de maio de 2024. Ambos os eventos serão realizados em São Francisco, Califórnia, no Hilton San Francisco Union Square.

Link

XIII FÓRUM DE CIBERSEGURANÇA (14 de maio)

O XIII Fórum de Cibersegurança, organizado pelo ISMS Forum Spain e seu grupo de trabalho Cyber Security Centre (CSC), ocorrerá em Madri no dia 14 de maio de 2024. O evento abordará as últimas tendências e desafios em cibersegurança, com foco especial em proteção de dados, gerenciamento de riscos e resposta a incidentes. O programa inclui apresentações de especialistas, mesas redondas e casos práticos, tornando-o um evento obrigatório para quem procura aprender sobre as últimas tendências e soluções em cibersegurança.

Link

CONGRESSO DE CIBERSEGURANÇA DE BARCELONA (21 a 23 de Maio)

O Congresso de Cibersegurança de Barcelona, em sua edição de 2024, se consolida como um evento-chave no campo da segurança digital na Espanha. Sob o lema "Cibersegurança na era digital: proteção e resiliência abrangentes", este congresso propiciará uma plataforma presencial e virtual para fazer frente aos desafios atuais e futuros no campo da cibersegurança. Com uma abordagem abrangente, serão explorados tópicos cruciais como identidade digital, proteção de dados e gerenciamento de riscos em um ambiente cada vez mais interconectado.

Link

IX CONFERÊNCIA NACIONAL DE PESQUISA EM CIBERSEGURANÇA (27 a 29 de maio)

A JNIC é um congresso científico que promove a troca e debate de ideias, conhecimentos e experiências entre a rede acadêmica e de pesquisa de um lado, e profissionais e empresas do outro. Ele serve como uma vitrine para os mais recentes avanços científicos no segmento e materializa um fórum de debate em que perspectivas e abordagens inovadoras em cibersegurança podem ser apresentadas, permitindo a conexão entre pesquisa e inovação e o desenvolvimento de produtos e serviços de valor para a sociedade. Pesquisadores e profissionais de diferentes partes do país apresentarão os resultados de suas pesquisas científicas de várias vertentes, mas com um elo em comum: a cibersegurança. A Conferência se concentrará em três pilares: Pesquisa, Transferência e Treinamento em Cibersegurança.

Link

Recursos

EVOLUÇÃO DAS AMEAÇAS DE DADOS EM 2024

Nesta era digital, os dados se tornaram um dos recursos mais valiosos para empresas, governos e indivíduos. No entanto, à medida que nossa dependência de dados aumenta, também aumentam as ameaças e os riscos associados a eles. No ano de 2024, uma série de novos desafios surgirá na vanguarda da segurança de dados, e os ataques cibernéticos se tornarão mais avançados, complexos e graves.

Link

O SETOR DE CIBERSEGURANÇA ESTÁ PRONTO PARA A IA?

Nos últimos anos, houve um aumento significativo no interesse em torno do papel crucial da inteligência artificial na cibersegurança, bem como dos benefícios notáveis que ela proporciona à estratégia de negócios de cibersegurança. No entanto, este artigo aborda a questão fundamental de saber se o setor de cibersegurança está adequadamente preparado para lidar com todas as complexidades inerentes à IA, além de seus benefícios óbvios.

Link

KIT DE FERRAMENTAS DE CIBERSEGURANÇA

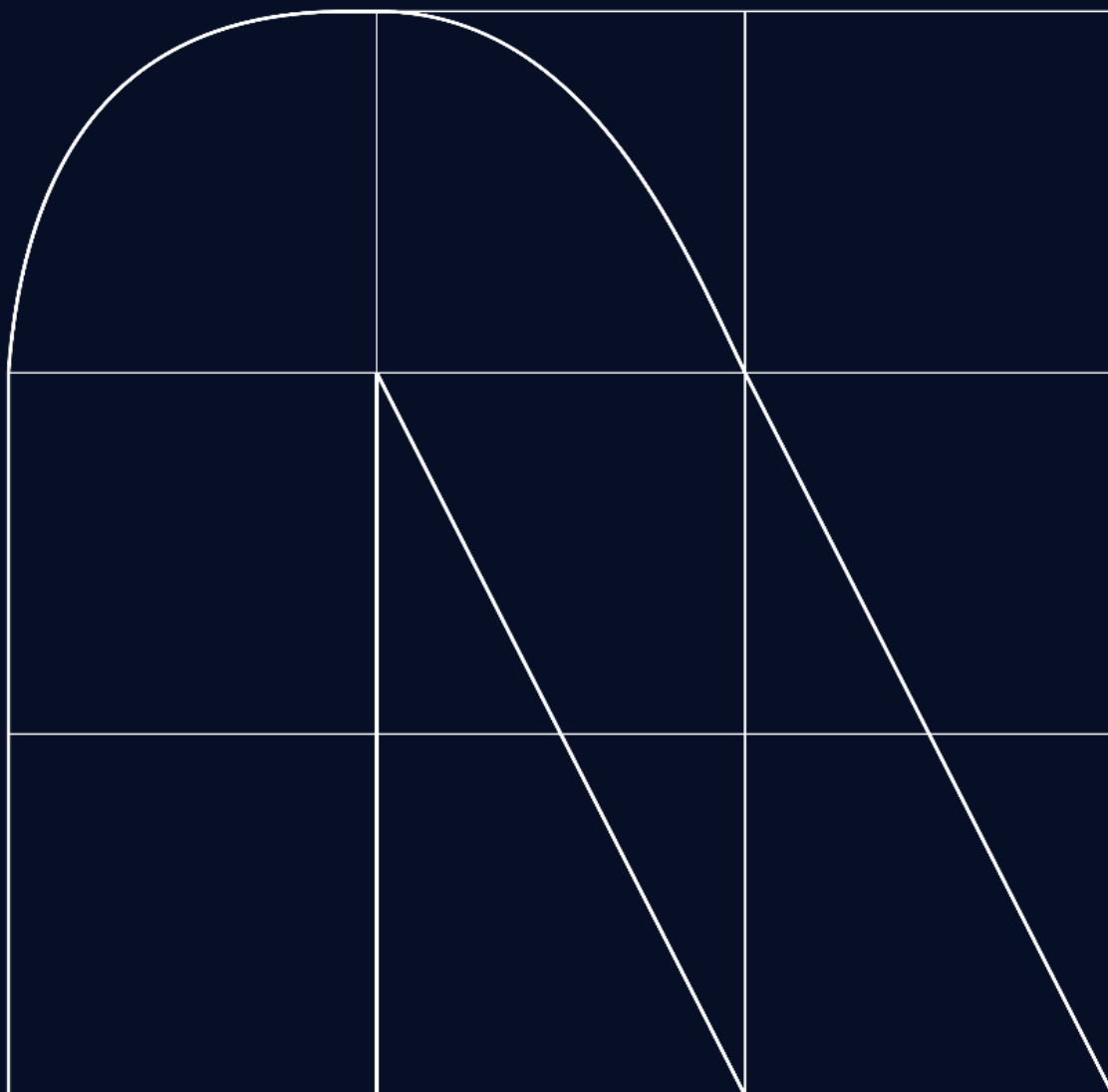
A fim de reforçar a solidariedade da UE e as suas capacidades de detecção de ameaças e incidentes de cibersegurança, preparação e resposta quando ocorrerem, bem como para aumentar a sua resiliência cibernética, a Presidência do Conselho e os negociadores do Parlamento Europeu chegaram a um acordo provisório sobre o chamado Regulamento de Solidariedade Cibernética e uma alteração específica ao Regulamento de Cibersegurança.

Link

THUNDERSTRIKE: EXECUTANDO APLICATIVOS MALICIOSOS DESPERCEBIDOS EM FACE DE SOLUÇÕES ANTIMALWARE MODERNAS

O compromisso da NTT DATA com a inovação se intensifica a cada passo que damos. No recente Congresso RootedCON, um dos eventos mais proeminentes na comunidade hispanófana, nossos colegas Antonio Pérez Sánchez e Marcos González Hermida apresentaram o Thunderstrike, uma ferramenta inovadora.

O Thunderstrike é uma ferramenta pós-exploração com técnicas avançadas de evasão que permite o carregamento e a execução de aplicativos .NET, como o Seatbelt e o Rubeus, entre outros. Essa ferramenta é capaz de fazê-lo sem ser detectada por sistemas antimalware modernos: sistemas de detecção e resposta de endpoint (EDR).



Desenvolvido pela equipe de cibersegurança da NTT DATA

es.nttdata.com