Timeline de Incidentes Relevantes 2024

IBRASPD

Grande Motivador

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por **meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos,** as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

IBRASPD

SOBRE O IBRASPD

IBRASPD foi criado para ser um habilitador e provedor de padrões para sociedade civil e empresas no tocante a privacidade, segurança da Informação e proteção de dados pessoais.

Um dos maiores institutos sem fins lucrativos (ONGs) com profissionais amplamente capacitados que são referências decisórias nos temas de Segurança da Informação, Proteção de dados e Privacidade no Brasil e LATAM.

IBRASPD conta com parcerias significativas no mundo de Educação como FIA e a Antebellum, em GRC como a BRA Certificadora e Associações de representação do setor como WOMCY e Cyber Security Girls.

IBRASPD promove lives, webinars, eventos e congressos com ênfase no relacionamento, troca de experiencias e oportunidades de negócios. Com um público de influenciadores e tomadores de decisão para o futuro da Proteção de Dados, Segurança da Informação e Privacidade no mercado nacional.

https://www.ibraspd.org/associe-se-ao-ibraspd

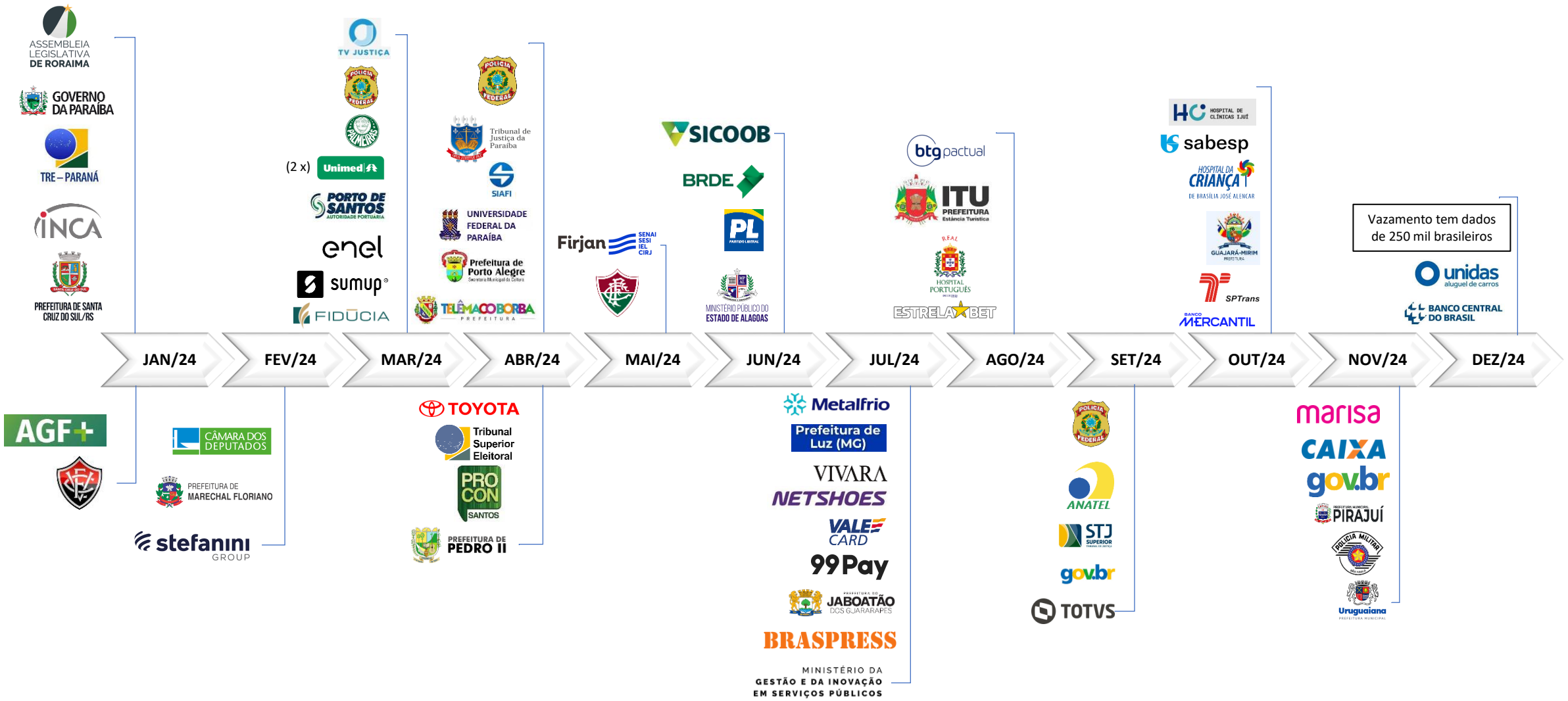
IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

IBRASPD

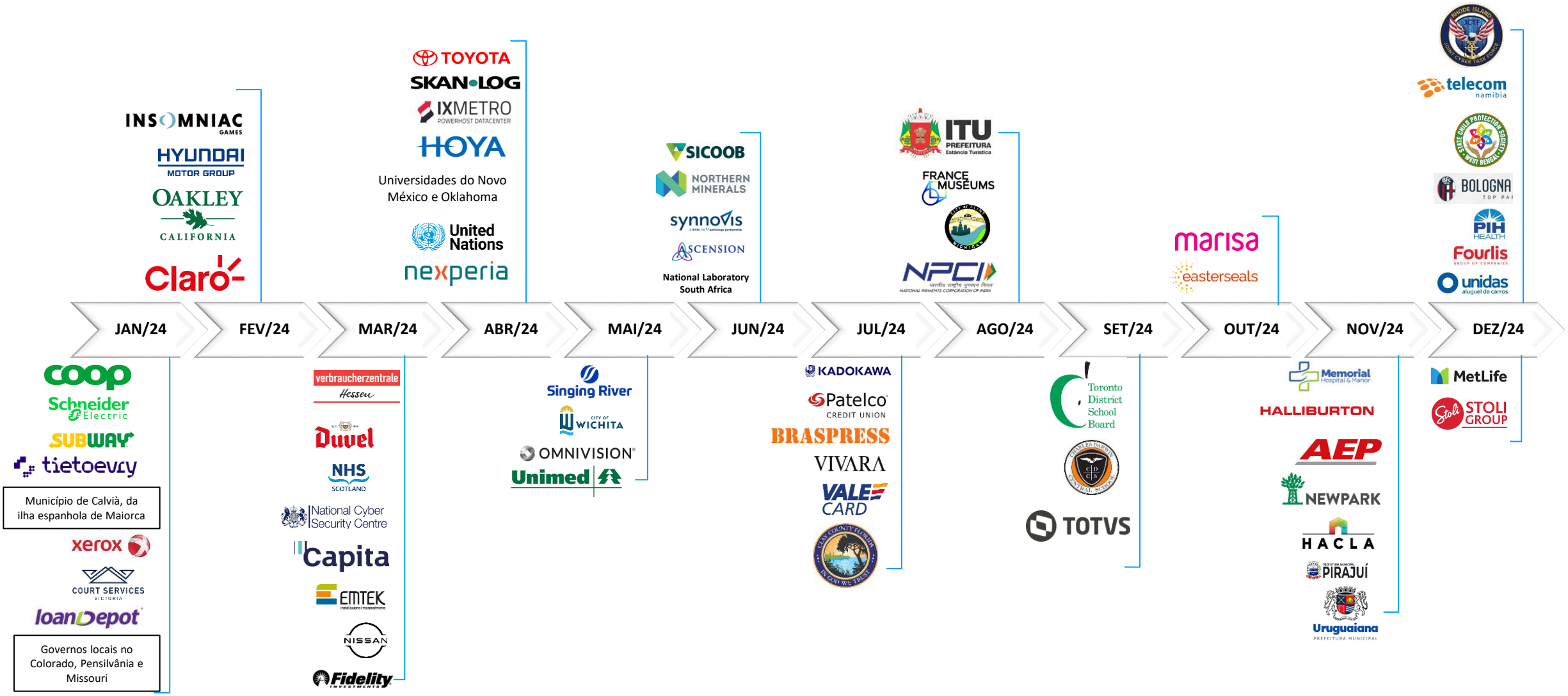
Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*



- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

IBRASPD

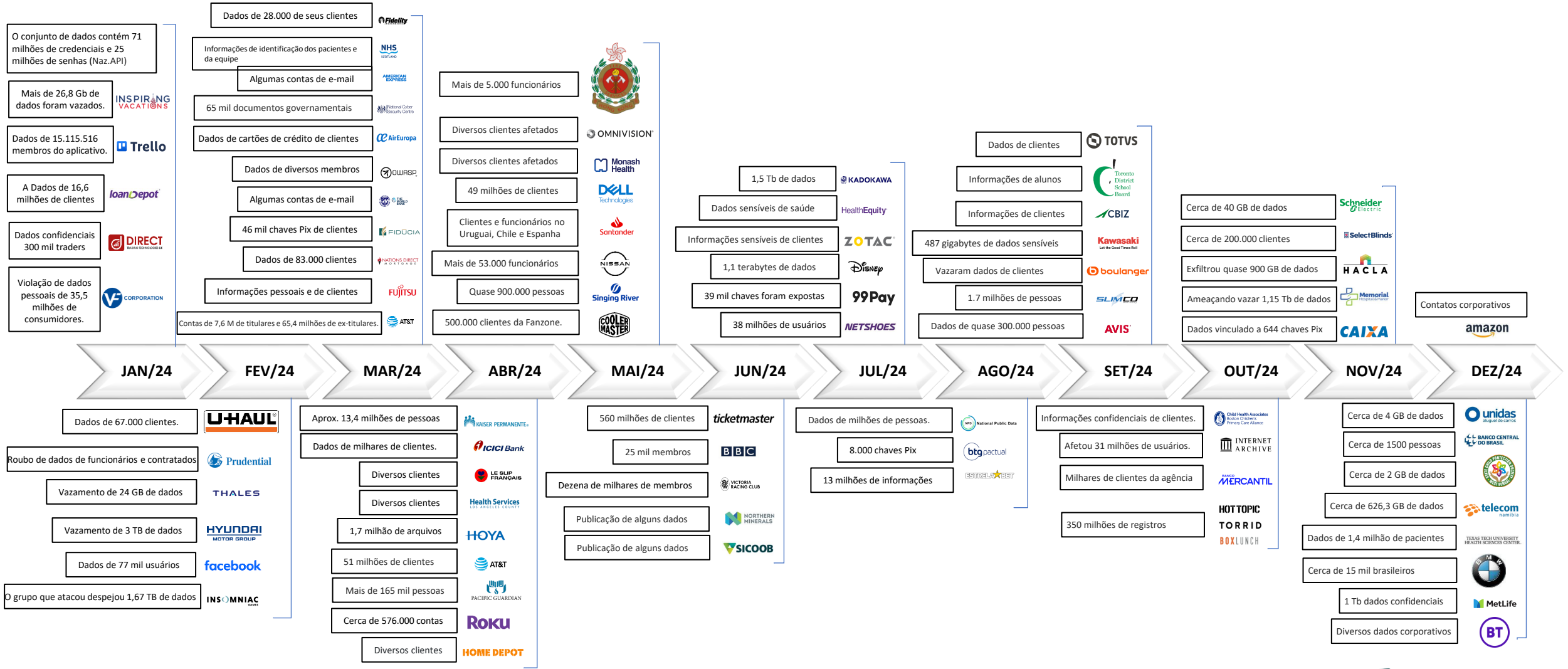
Contexto Atual – RANSOMWARE com repercussão na mídia*



- **Casos Divulgados**

IBRASPD

Vazamentos de dados pessoais com repercussão na mídia*



- **Casos Divulgados**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A LoanDepot confirmou ataque de ransomware a seus sistemas, onde informações pessoais confidenciais de 16,6 milhões de clientes foram roubadas.

Agência de viagens australiana expõe dados de clientes após deixar banco de dados acessível publicamente, onde mais de 26,8 Gb de dados foram vazados.

Maior locadora de aeronaves do mundo AerCap Holdings foi atingida por um incidente de segurança cibernética relacionado ao ransomware.

Schneider Electric sofreu um ataque de ransomware realizado pelo grupo autodenominado Cactus, que levou ao roubo de dados corporativos. O ataque atingiu a divisão de Negócios de Sustentabilidade da empresa e interrompeu a plataforma de nuvem EcoStruxure Resource Advisor

O Teatro Hispânico GALA (Washington, DC) um centro nacional de artes cênicas latinas – foi hackeado em 11 de janeiro e toda a sua conta bancária foi esvaziada num piscar de olhos.

Divisão norte-americana da Xerox Business Solutions (XBS) sofreu um ataque cibernético do grupo de ransomware INC Ransom. Informações pessoais limitadas no ambiente XBS foram afetadas.

Dados confidenciais e atividades de negociação de mais de 300 mil traders vazaram online pela empresa internacional de fintech Direct Trading Technologies.

O grupo de hackers autodenominado R00TK1T ISC assumiu a responsabilidade por um ataque cibernético à Sodexo.

Um ataque cibernético conseguiu penetrar nos sistemas da unidade financeira do Carrefour e roubar informações pessoais dos seus clientes.

O provedor de serviços de hospedagem em nuvem Tietoevry anunciou que um de seus datacenters na Suécia. Os atacantes usaram as ferramentas Akira ransomware como serviço.

A empresa de tecnologia financeira EquiLend foi atingida por um ataque cibernético que forçou vários de seus sistemas a ficarem offline.

LUSH FRESH HANDMADE COSMETICS

De acordo com um comunicado enviado ao Recorded Future News, a Lush disse que estava "trabalhando com especialistas forenses de TI externos para realizar uma investigação abrangente".

water for people

A Water For People, uma organização sem fins lucrativos, tornou-se um alvo de grupo de ransomware Medusa.

Agência de prisioneiros de guerra da Ucrânia é atingida por ataque cibernético (DDoS)

https://therecord.media/ukraine-pow-agency-cyberattack-russia

Governos locais no Colorado, Pensilvânia e Missouri lidam com ransomware

https://therecord.media/local-governments-across-us-dealing-with-ransomware

JAN/24

A Coop, uma das maiores redes de supermercados da Suécia, disse que está lidando com um ataque cibernético que afeta lojas no condado de Värmland. A gangue de ransomware Cactus assumiu o ataque.

A Tigo Business Paraguai informou que foi "vítima de um incidente de segurança" em sua infraestrutura que afetou o fornecimento de "alguns serviços específicos a um grupo limitado de clientes".

A Microsoft divulgou que foi alvo de um grupo de hackers patrocinado pela Rússia (Midnight Blizzard), o qual extraiu informações de uma pequena porcentagem de contas de e-mail de funcionários.

Houve uma violação de dados na Global Affairs Canada envolvendo informações pessoais de alguns usuários, incluindo funcionários, e afetando o acesso remoto à rede do departamento, de acordo com o departamento.

A Orange Espanha sofreu uma interrupção nos serviços de internet, após ter sofrido um ataque hacker que teria afetado o centro de coordenação da rede IP (RIPE) da operadora de telefonia móvel. A empresa francesa garantiu que nenhuma informação de cliente foi violada.

A rede americana de fast food Subway foi alvo de um grave ataque. O grupo de ransomware LockBit assumiu a responsabilidade, que visou o banco de dados interno e levou ao comprometimento de informações confidenciais, incluindo salários de funcionários, pagamentos de royalties de franquia, pagamentos de comissões de franquia master, rotatividade de restaurantes, entre outras.

A Hewlett Packard Enterprise disse que seu sistema de e-mail baseado em nuvem foi comprometido pelo ator patrocinado pelo Estado conhecido como Midnight Blizzard ou Cozy Bear. (Dezembro)

Uma API do Trello exposta permite vincular endereços de e-mail privados a contas do Trello, possibilitando a criação de milhões de perfis de dados contendo informações públicas e privadas. Estão sendo vendidos dados de 15.115.516 membros do Trello em um popular fórum de hackers.

O sistema judicial do segundo estado mais populoso da Austrália foi atingido por um ataque de ransomware. O incidente levou à interrupção da rede de tecnologia audiovisual nos tribunais, impactando as gravações de vídeo , gravações de áudio e serviços de transcrição

Município de Calvià, da ilha espanhola de Maiorca, sofreu ataque cibernético e estão cobrando de resgate € 10 milhões.

https://www.cisoadvisor.com.br/gangue-de-ransomware-exige-e-10-milhoes-de-cidade-espanhola/

DENHAM

Em uma declaração exclusiva à equipe da Cyber Express, a DENHAM the Jeanmaker, a renomada marca de jeans fundada em Amsterdã em 2008, confirmou ter sido vítima de um ataque cibernético. O gigante do denim revelou que o ataque cibernético DENHAM foi descoberto pela primeira vez em 27 de dezembro de 2023.

monobank

O Monobank sofreu um poderoso ataque cibernético (DDoS).

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

O Governo e a Assembleia Legislativa de Roraima (ALE-RR) foram alvos de ação maliciosa que impactou os perfis oficiais dos órgãos no Instagram

Houve uma sobrecarga de acessos aos sites vinculados ao governo da Parapiba, deixando-os indisponíveis por um curto período de tempo.

O canal do Tribunal Regional Eleitoral do Paraná (TRE-PR) no YouTube ficou temporariamente fora do ar. A instituição informou que sua conta na plataforma sofreu uma tentativa de ataque cibernético.

O Instituto Nacional do Câncer (INCA) no Rio de Janeiro sofreu uma invasão hacker em seu sistema havendo a interrupção dos serviços de tecnologia

Devido a um ataque cibernético à rede de computadores da Prefeitura de Santa Cruz do Sul, no Rio Grande do Sul, alguns serviços administrativos foram suspensos.

JAN/24

O perfil oficial do Esporte Clube Vitória na rede social X (antigo Twitter) foi invadido por cibercriminoso em ato de hacktivismo. As postagens publicadas durante o incidente incluíram comentários provocativos sobre a derrota do Palmeiras na Copa São Paulo de Futebol Júnior.

A instituição de investimento AGF+ foi vítima de um ataque cibernético. Em um domínio utilizado na internet pelos operadores do ransomware Revil, foi publicado vazamento de 120Gb, com amostra de 2Gb. Empresa nega vazamento.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A Prudential Financial divulgou que sua rede foi violada e obtiveram acesso a alguns dados administrativos e de usuários da empresa.

Após suposto vazamento de 24 GB de dados na darkweb, a empresa realiza esforços para avaliar a extensão dos danos e verificar a veracidade dos dados vazados.

A montadora Hyundai Motor Europe sofreu um ataque do ransomware Black Basta, com os operadores da ameaça alegando ter roubado 3 TB de dados corporativos.

Dois voos com destino a Israel sofreram tentativas de sequestro das comunicações para desviar as aeronaves.

A Cloudflare divulgou que seu servidor Atlassian interno foi violado por um suposto "atacante do estado-nação" que acessou seu wiki do Confluence, banco de dados de bugs Jira e sistema de gerenciamento de código-fonte Bitbucket.

Hospital infantil de Chicago é atingido por ataque cibernético, forçando-o a desconectar toda a rede.

AnyDesk confirmou que sofreu um ataque cibernético que permitiu que hackers obtivessem acesso aos sistemas de produção da empresa.

A empresa farmacêutica global Cencora informou que descobriu recentemente que intrusos roubaram dados de suas redes.

Prudential

THALES

HYUNDAI MOTOR GROUP

EL AL ISRAEL AIRLINES – IT'S NOT JUST AN AIRLINE, IT'S ISRAEL

CLOUDFLARE

Ann & Robert H. Lurie Children's Hospital of Chicago

AnyDesk

cencora

VARTA

A produção da planta do fabricante alemão de baterias ficou suspensa por dias após ataque cibernético.

Empresa de Hong Kong caiu em golpe milionário, o qual permitiu que os criminosos conseguiram levar aproximadamente US$ 25,6 milhões após o uso sofisticado de deepfakes.

FEV/24

A AT&T disse que a interrupção de uma hora em sua rede de telefonia celular nos Estados Unidos foi resultado de um erro técnico, não de um ataque cibernético. A interrupção impediu o serviço de telefonia celular para milhares de usuários nos EUA.

A Real Polícia Montada Canadense (RCMP), a força policial nacional do Canadá, revelou que enfrentou um ataque cibernético direcionado às suas redes comprometendo alguns dos seus serviços.

Um grupo de cibercriminosos afirma ter violado a empresa com sucesso pela segunda vez, gabando-se do roubo de uma quantidade substancial de dados. Os dados roubados estão à venda no site de venda de dados ilegais na dark.

A Trans-Northern Pipelines (TNPI) confirmou que sua rede interna foi violada em novembro do ano passado e que agora está investigando um suposto roubo de dados feito pela gangue de ransomware ALPHV/BlackCat.

O banco americano está alertando sobre uma violação de dados que expôs informações pessoais de seus clientes depois que um de seus provedores de serviços, foi hackeado no ano passado

A empresa confirmou o ataque tipo ransomware a seus sistemas através de um breve comunicado publicado nas contas das redes sociais das suas operações na Guatemala, El Salvador, Honduras, Nicarágua e Costa Rica.

Ataque DDoS ao sistema judiciário da Pensilvânia derruba sistemas de arquivamento e site de pagamento de fiança

AT&T

Canada

Robert Half Talent Solutions

Trans-Northern

BANK OF AMERICA

Claro

INSOMNIAC GAMES

A subsidiária da Sony, Insomniac Games, notificou seus funcionários sobre uma violação de dados cuja informações pessoais foram roubadas e vazadas online após um ataque de ransomware. O grupo Rhysida despejou 1,67 TB de documentos em seu site de vazamento na dark web.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

A Câmara dos Deputados abriu investigação interna e acionou a polícia para apurar um ataque cibernético em seu perfil oficial na rede social “X”, antigo Twitter.

A Prefeitura de Marechal Floriano, no Espírito Santo, sofreu um ataque cibernético em seus sistemas. Segundo o Setor de Informática, os cibercriminosos invadiram e bloquearam os dados.

Ex-funcionário teria invadido e apagado servidor de cliente, além de causar transtornos entre os funcionários.

FEV/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A companhia aérea espanhola Air Europa sofreu um ataque cibernético ao seu sistema de pagamento online que deixou dados pessoais expostos de seus clientes.

O McDonald's alegou que a culpa pela interrupção global dos seus sistemas de ponto de venda (PoS), que forçou o fechamento de muitos dos restaurantes da rede de fast-food, foi a mudança de configuração de um provedor de serviços terceirizado, e não um ataque cibernético

A gigante de tecnologia japonesa Fujitsu confirmou que foi vítima de um ataque cibernético que provavelmente resultou no roubo de informações pessoais e de clientes.

A Agência de Segurança Cibernética e de Infraestrutura (CISA) dos EUA foi obrigada a colocar dois sistemas off-line no mês passado, depois que hackers violaram suas defesas por meio de falhas de segurança nos produtos Ivanti.

Autoridades suíças descobriram que 65 mil documentos governamentais contendo informações confidenciais e dados pessoais sensíveis foram vazados após um ataque de ransomware no ano passado a um de seus fornecedores de TI.

Capita, a empresa de terceirização britânica foi atingida por um ataque de ransomware provocado pelo grupo Black Basta

Electro Marteix foi anunciada como vítima pela gangue de ransonware ALPHV/Blackcat, mas ainda não houve confirmação pela empresa.

Instagram e Facebook, redes sociais da Meta, passam por instabilidade e ficaram fora do ar para muita gente durante algumas horas.

Cidades dos Estados Unidos tem serviços interrompidos devido a ataques cibernéticos, muitos deles ransomware.
(Birmingham, um condado de Illinois, municípios do Texas e Geórgia, St. Cloud, Pennsylvania)

https://therecord.dia/network-outage-birmingham-alabama-ongoing-cyberattack
https://therecord.media/illinois-county-gov-college-hit-with-ransomware
https://therecord.media/texas-georgia-municipalities-face-disruptions-from-ransomware
https://therecord.media/st-cloud-hit-with-ransomware-florida-string
https://therecord.media/pennsylvania-scranton-school-district-ransomware-attack

Os especialistas cibernéticos da Inteligência de Defesa da Ucrânia realizaram outra operação especial contra o estado agressor da Rússia, o que permitiu acesso a software, cifras, documentos secretos

https://gur.gov.ua/en/content/soft-shyfry-sekretni-dokumenty-kiberfakhivtsi-hur-zlamaly-minoborony-rosii.html

MAR/24

Verbraucherzentrale Hessen, centro de aconselhamento ao consumidor na Alemanha, confirmou que foi vítima de um ataque cibernético em fevereiro realizado pela ALPHV/BlackCat.

No final de fevereiro de 2024, depois de receber alguns pedidos de suporte, a Fundação OWASP tomou conhecimento de uma configuração incorreta do antigo servidor da Wiki OWASP, levando a uma violação de dados envolvendo membros com dezenas de anos

American Express está alertando os clientes de que os cartões de crédito foram expostos em uma violação de dados de terceiros depois que um processador comercial foi hackeado.

A Nations Direct Mortgage, com sede em Nevada, disse que mais de 83.000 clientes foram afetados por uma violação de dados no final de 2023 que vazou números da Previdência Social e outras informações confidenciais.

A Fidelity Investments Life Insurance Co. disse que mais de 28.000 de seus clientes podem ter tido suas informações pessoais comprometidas durante uma violação de dados envolvendo o provedor de serviços terceirizado Infosys McCamish Systems (IMS) em outubro de 2023

O Fundo Monetário Internacional (FMI) emitiu um comunicado, informando sobre um incidente cibernético, depois que invasores violaram 11 contas de e-mail.

Um ataque cibernético interrompeu as operações da MarineMax, um dos maiores empresas de serviços recreativos de barcos, iates e superiates do mundo.

A cervejaria Duvel Moortgat foi atingida por um ataque de ransomware interrompendo a produção de cerveja nas instalações de engarrafamento da empresa.

NHS Dumfries e Galloway (parte do NHS Escócia) tem confirmado que um ransomware foi capaz de "acessar uma quantidade significativa de dados, incluindo informações de identificação do paciente e da equipe," e publicou dados "clínicos relativos a um pequeno número de doentes."

Várias agências governamentais francesas foram atingidas por ciberataques " intensos

https://therecord.media/france-government-ddos-incident

O Conselho da Cidade de Leicester anunciou que vários dos serviços críticos da autoridade local ficaram indisponíveis por dias após um ataque cibernético.

https://therecord.media/leicester-uk-cyberattack-local-council

A empresa de finanças descentralizadas (DeFi) Prisma Finance sofreu um ataque cibernético

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

- TV Justiça teria sido alvo de um ciberataque mirando seus sistemas internos, STF nega incidente cibernético, mas seguem apurando fato.
- PF apura crimes cibernéticos contra políticos no interior de São Paulo, os quais foram vítimas de vítimas de invasões cibercriminosas.
- Unimed Cuiabá sofre paralização em seus sistemas após ataque cibernético.
- Palmeiras tem incidente cibernético com e-mails corporativos, o qual permitiu exposição de dados pessoais.
- Outras unidades da Unimed sofreram incidente cibernético, desta vez afetou as unidades do Vale do Taquari e Rio Pardo.
- O site oficial do Porto de Santos ficou fora por diversas horas, em decorrência de uma sobrecarga inesperada de acessos ao portal.

MAR/24

- O Banco Central (BC) divulgou que mais de 46 mil chaves Pix de clientes da Fidúcia vazaram na internet
- O site oficial da Enel possuía uma brecha que permitia a qualquer pessoa fazer o download das faturas de outros clientes. Para tanto, bastava saber um endereço específico e complementar a URL com um número de identificação.
- Banco Central do Brasil (BC) informou a ocorrência de incidente de segurança com dados pessoais vinculados a chaves Pix sob a guarda e a responsabilidade da Sumup Sociedade de Crédito Direto S.A. (Sumup SCD), em razão de falhas pontuais em sistemas dessa instituição.

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

O programa internacional de fomento alertou, para a ocorrência de um incidente contra o data center da ONU localizado em Copenhague, na Dinamarca

Gangue de ransomware que atacou a fabricante japonesa de lentes está exigindo o pagamento do valor para não divulgar os supostos 1,7 milhão de arquivos roubados.

A AT&T informou ao gabinete do procurador-geral do Maine, EUA, que a violação de dados recentemente divulgada afetou mais de 51 milhões de clientes

O ataque à seguradora Pacific Guardian Life Insurance, resultou em vazamento envolvendo dados sensíveis de mais de 165 mil pessoas,

Provedor de serviços de streaming Roku informou que identificou um segundo ataque cibernético que afetou cerca de 576.000 contas adicionais enquanto investigava uma violação que afetou 15.000 contas de usuários no início deste ano.

Um fornecedor de SaaS terceirizado inadvertidamente tornou pública uma pequena amostra dos nomes dos associados da Home Depot, endereços de e-mail de trabalho e IDs de usuário durante o teste de seus sistemas

IxMetro PowerHost, um data center e provedor de hospedagem com sede no Chile, teve seus servidores VMware ESXi e backups comprometidos por um ataque de ransomware SEXi

A Nexperia, uma empresa chinesa de semicondutores com sede na Holanda, anunciou ter sido hackeada depois que um grupo de ransomware enviou o que alegou ter sido roubado documentos confidenciais para um site de extorsão da darknet.

ABR/24

Um dos maiores fabricantes de acessórios de tecnologia teve suas operações comerciais “temporariamente interrompidas” após um ataque cibernético que começou em 5 de abril.

A empresa de análise de dados Sisense sofreu um incidente de segurança cibernética que pode ter exposto as informações sigilosas, confome relatou a CISA.

O Centro Hospitar de Cannes – Simone Veil foi alvo de um ataque cibernético, não houve demanda por resgate ou roubo de dados. Investigações foram abertas.

O provedor de serviços de saúde Kaiser Permanente divulgou um incidente de segurança de dados que pode afetar 13,4 milhões de pessoas nos Estados Unidos.

Skanlog, um distribuidor crítico da Systembolaget, a cadeia de varejo de propriedade do governo sueco sofreu um ataque de ransomware.

O ICICI Bank, um dos principais bancos privados da Índia, confirmou a exposição de informações confidenciais de cartão de crédito pertencentes a milhares de clientes.

A Hedgey Finance, uma plataforma de infraestrutura de token, sofreu duas explorações paralelas no valor total de $44,7 milhões de fundos perdidos.

A LeSlipFrançais, renomada marca francesa de roupas íntimas, confirmou uma violação de dados que afeta sua base de clientes.

O Departamento de Serviços de Saúde do Condado de Los Angeles divulgou uma violação de dados depois que informações pessoais e de saúde de milhares de pacientes foram expostas em uma violação de dados resultante de um recente ataque de phishing

A Omni Hotels & Resorts confirmou que um ataque cibernético causou uma interrupção de seu ambiente de TI, deixando-o inoperante por dias, enquanto a equipe de TI realizava os procedimentos para restauração do ambiente.

A provedora americana de telecomunicações Frontier Communications restaurou seus sistemas depois que um grupo de cibercrime violou alguns de seus sistemas de TI em um ataque cibernético.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

- Polícia Federal interrompe emissão de passaportes por tentativa de ciberataque
- Parte do site do Tribunal de Justiça da Paraíba fica fora do ar após suposto ataque hacker
- O Siafi, usado na execução de pagamentos financeiros, foi alvo de uma invasão cibernética
- Hacker derruba site da UFPB em ‘protesto’ contra assédio sexual na instituição
- O site da Prefeitura de Porto Alegre sofreu um ataque cibernético, o site foi retirado do ar pela Procempa
- Hackers conseguiram roubar R$ 6,5 milhões da prefeitura de Telêmaco Borba-PR, por meio de uma fraude sofisticada que permitiu roubar a identidade de um servidor municipal.

ABR/24

- Toyota Brasil apura possível vazamento de documentos internos
- O ataque virtual sofrido pelo Tribunal Superior Eleitoral (TSE) desviou R$ 1,2 milhão a uma empresa terceirizada de tecnologia da informação
- Portal do Procon-Santos fica fora do ar e suspende serviços remotos
- A prefeitura do município de Pedro II informou que um incidente cibernético causou a indisponibilidade do portal oficial durante algumas horas

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- O corpo de bombeiros de Hong Kong descobriu uma violação em seu sistema de computador que expôs as informações pessoais de mais de 5.000 funcionários do departamento
- Autoridades do governo em Wichita, Kansas, alertaram o público que os serviços seriam limitados após um ataque de ransomware
- O Monash Health, o maior serviço de saúde de Victoria (EUA), se viu envolvido nas consequências de uma violação de dados, que comprometeu informações confidenciais
- A empresa de assistência médica móvel DocGo confirmou que sofreu um ataque cibernético. Os agentes de ameaças violaram seus sistemas e roubaram dados de saúde de pacientes
- Dell sofre invasão e 49 milhões de clientes têm dados roubados
- Santander relata violação de dados de clientes e funcionários no Uruguai, Chile e Espanha
- A Nissan descobriu a violação de novembro de 2023 expôs dados pessoais pertencentes a mais de 53.000 funcionários atuais e antigos.

MAI/24

- O Singing River Health System alerta que estima que 895.204 pessoas foram afetadas por um ataque de ransomware sofrido em agosto de 2023.
- O fabricante de hardware de computador Cooler Master sofreu uma violação de dados depois que um invasor invadiu o site da empresa e alegou roubar informações de 500.000 clientes da Fanzone.
- O fabricante de produtos de imagem digital OmniVision divulgou uma violação de dados após o ataque de ransomware de 2023.
- Vazamento revela segredos do algoritmo de busca do Google
- A Europol, agência da União Europeia para a cooperação policial, confirmou que o portal da Plataforma Europol para Peritos (EPE) foi violado
- A famosa casa de leilões britânica Christie's disse que um ataque cibernético a forçou a retirar seu site do ar e realizar um leilão de forma presencial.

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

- A Unimed Vales do Taquari e Rio Pardo (Unimed VTRP) confirmou que foi vítima de um ataque cibernético
- FIRJAN admite incidente de Segurança e promete tomar medidas cabíveis
- Hackers invadem portal do Fluminense FC e anunciam contratação de Haaland

MAI/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- A Ticketmaster, plataforma de venda de ingressos, confirmou o vazamento de dados que pode ter exposto 560 milhões de clientes — ticketmaster
- Ransomware atinge o Hospital Ascension e coloca a vida de pacientes em risco. — Ascension
- Violação da BBC coloca 25 mil membros do plano de pensão em risco — BBC
- Data center nacional da Indonésia criptografado com variante do ransomware LockBit — Governo da Indonésia
- A rede corporativa da TeamViewer foi violada em um suposto hack APT — TeamViewer
- Google "bobeia" e compromete privacidade de usuários — Google
- Hospitais de Londres ficam em estado crítico após ataque de ransomware — synnovis
- Empresa de mineração australiana divulga violação após vazamento de dados da BianLian — Northern Minerals
- Laboratório nacional de saúde da África do Sul é atingido por ataque de ransomware — National Laboratory South Africa

JUN/24

- QuoteWizard, outro cliente da Snowflake, confirma violação — QuoteWizard by lendingtree
- Cidade de Cleveland desliga sistemas de TI após ataque cibernético — City of Cleveland, Ohio
- O conglomerado de mídia japonês Kadokawa ficaram offline quatro dias após um grande ataque cibernético. — KADOKAWA
- Funcionário demitido deletou 180 máquinas virtuais de QA — ncs
- Maxicare confirma violação de dados em plataforma de reservas de terceiros — Maxicare Live your best life
- As concessionárias de automóveis dos EUA e Canadá sofrem incidente cibernético no provedor de dados CDK Global — CDK GLOBAL
- A fabricante de empilhadeiras Crown Equipment sofreu um ciberataque que interrompeu a fabricação em suas plantas — CROWN
- O Victoria Racing Club foi atingido por um ataque cibernético expondo os dados de dezenas de milhares de membros — Victoria Racing Club
- Ataque DDoS atinge a partida de abertura da Eurocopa da Polônia — UEFA EURO2024

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

O Sicoob informa que identificou um incidente cibernético no ambiente local de uma das cooperativas

O Banco Regional de Desenvolvimento do Extremo Sul (BRDE) confirmou que seus sistemas digitais foram alvo de um incidente cibernético

Membros da bancada do partido na Câmara tiveram sites oficiais e contas nas redes sociais invadidas por cibercriminosos

Ministério Público de Alagoas confirma tentativa de ataque cibernético

JUN/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- Kadokawa, gigante japonesa de anime e jogos, admite vazamento de dados após ataque de ransomware
- Órgão regulador da Fórmula 1 divulga violação de dados após hacks de e-mail
- A empresa na área de saúde, HealthEquity, alertou sobre um incidente de violação de dados
- A cooperativa de crédito americana Patelco Credit Union fechou vários de seus sistemas bancários para conter um ataque de ransomware
- A Universidade de Ciências Aplicadas de Frankfurt anunciou que foi alvo de um ataque que levou ao desligamento total de seus sistemas de TI.
- O fabricante de hardware Zotac expôs de forma online informações sensíveis de clientes.
- 1,1 terabytes de dados vazados do Slack interno da Disney
- Plataforma de criptografia indiana WazirX confirma US$ 230 milhões roubados durante ataque cibernético

JUL/24

- A Leidos Holdings Inc., gigante no fornecimento de serviços de Tecnologia da Informação (TI) dos EUA, teve documentos internos bastante sensíveis expostos.
- Os escritórios do Condado de Clay foram fechados durante um ataque de ransomware.
- Atualização do Crowdstrike impediu o boot em cerca de 8,5 milhões de máquinas Windows, causando parada nas operações em diversas empresas no mundo todo.

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

- Ataque criptografa 280 servidores na Braspress
- A Prefeitura de Jaboatão dos Guararapes informou que sofreu um ataque, afetando vários serviços
- BC comunica novo vazamento de chaves Pix: 39 mil chaves foram expostas
- ValeCard confirma que sofreu um ataque de ransomware
- A Netshoes tomou conhecimento que foi vítima de um incidente cibernético, que pode ter resultado no vazamento de arquivos contendo dados de clientes.

JUL/24

- Metalfrio comunica ao mercado ocorrência de incidente
- Invasão no sistema da Prefeitura de Luz, no Centro-Oeste de Minas Gerais, resultou em roubo de mais de R$ 1,3 milhão.
- Vivara é atacada por ransomware Medusa
- O Ministério da Gestão e Inovação teve serviços indisponíveis devido a um incidente grave de segurança cibernética.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- Microsoft diz que ataque cibernético provocou interrupção no Azure
- Quase 40 museus franceses foram afetados por ataque de ransomware
- A National Public Data, confirma vazamento de dados sensíveis de milhões de pessoas.
- Ataque de ransomware na cidade de Flint causou interrupções de rede e internet.
- Ataque de ransomware no sistema de pagamento indiano
- Aeroporto e porto de Seattle isolam sistemas após ataque cibernético.

AGO/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

BC informa vazamento de dados de mais de 8.000 chaves Pix sob guarda do BTG Pactual

Sistemas da prefeitura de Itu paralisados por ransomware

O Real Hospital Português informou que sofreu um incidente de segurança cibernética

Casa de apostas confirmou vazamento de dados no mesmo dia em que pediu regularização no Brasil

AGO/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

- O Conselho Escolar do Distrito de Toronto (TDSB) confirmou que informações dos alunos estavam envolvidas em um ataque de ransomware
- Agência alemã de controle de tráfego aéreo confirma ataque cibernético e diz que operações não foram afetadas
- A CBIZ Benefícios & Seguros (CBIZ) divulgou um vazamento de dados que envolve o acesso não autorizado às informações de clientes armazenadas em bancos de dados específicos.
- Rede de transportes de London anunciou incidente de cyber segurança
- Serviços interrompidos após ataque cibernético no Conselho de Tewkesbury, Inglaterra
- Planned Parenthood em Montana confirmou que sofreu um ciberataque
- Ataque de ransomware força escola secundária em Londres a fechar e mandar alunos para casa

SET/24

- Acesso indevido a um limitado número de arquivos da Fortinet
- Informação de cartão de crédito de 1.7 milhões de pessoas são expostos pela Slim CD
- Boulanger confirma que criminosos acessaram dados de clientes
- 487 gigabytes de dados sensíveis supostamente roubados da Kawasaki Motors Europe
- Estação de rádio alemã é forçada a transmitir 'fita de emergência'
- MoneyGram diz que incidente cibernético causou interrupções na rede
- A Agence France-Presse afirma que o ataque cibernético teve como alvo sistemas de TI
- Dados de quase 300.000 expostos no ataque cibernético da Avis

IBRASPD

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

- Após Moraes determinar o bloqueio do X (antigo Twitter), rede interna da PF ficou fora do ar devido a ataque cibernético
- Ataques de negação de serviço afetaram sistemas da Anatel
- STJ sofre ataque hacker, mas nega prejuízo ao sistema
- GOV.br foi alvo de ataques DDoS e sites deixaram de funcionar
- Totvs é vítima de ataque com ransomware

SET/24

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A agência de notícias global AFP (Agence France-Presse) está alertando sofreu um ciberataque, que afetou os sistemas de TI e os serviços de entrega de conteúdo para seus parceiros.

A desenvolvedora canadense de jogos Red Barrels alertou que o desenvolvimento de seus jogos Outlast sofrerá atrasos após a empresa sofrer um ciberataque que impactou seus sistemas internos de TI e dados.

Golpistas de criptomoedas hackearam brevemente o site da LEGO para promover um falso token Lego que poderia ser adquirido com Ethereum.

Um ataque cibernético aos sistemas usados pelo fabricante japonês de tecnologia Casio causou uma falha no sistema que resultou na indisponibilidade de alguns serviços para os clientes.

O Internet Archive, responsável pela ferramenta "The Wayback Machine", enfrentou uma séria violação de segurança que afetou dados de 31 milhões de usuários.

A desenvolvedora japonesa de videogames Game Freak confirmou que sofreu um ataque cibernético no início deste ano, resultando em um vazamento de dados.

Os moradores de Calgary tiveram acesso limitado aos serviços em suas bibliotecas locais após um ataque cibernético ao sistema de bibliotecas públicas da cidade.

OUT/24

Uma organização importante que ajuda a conectar pessoas com médicos em Nova York e Connecticut alertou os pacientes que uma violação em setembro expôs uma grande quantidade de informações confidenciais.

Plataforma de criptomoedas Radiant Capital diz que US$ 50 milhões em moedas digitais foram roubados após comprometimento de contas

A Cisco desabilitou o acesso público a um de seus ambientes DevHub depois que invasores baixaram alguns dados de clientes do site e os colocaram à venda em um fórum de crimes cibernéticos.

A organização sem fins lucrativos de serviços para deficientes dos EUA, Easterseals, foi obrigada a pagar um resgate de US$ 1,3 milhão pela operação de ransomware Rhysida , que assumiu a responsabilidade por uma invasão em abril.

Um post de um usuário que se intitula “Satanic” apareceu num fórum frequentado por cibercriminosos, anunciando vários bancos de dados relacionados a três grandes empresas de varejo dos EUA: Hot Topic, Torrid e Box Lunch. Visto como maior vazamento do varejo com 350 milhões de registros.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

Órgão de saneamento básico paulista confirmou que foi alvo de um ataque cibercriminosos que comprometeu parte de seus sistemas digitais.

O HCB informou que seus sistemas internos foram atingidos por um ataque cibernético.

A prefeitura de Guajará-Mirim confirmou que dados foram sequestrados pelo ataque, mas não comprovou a ação de um ransomware, nem se dados pessoais dos cidadãos foram atingidos.

A empresa A2 Transportes, concessionária da SPTrans na Zona Sul da cidade de São Paulo, sofreu um incidente cibernético envolvendo cibercriminosos. Devido à ocorrência, o serviço de cobrança via Bilhete Único foi paralisado, impedindo a geração de renda da organização.

O Banco Mercantil foi flagrado descartando fichas cadastrais de clientes em sacos de lixo na calçada, expondo dados confidenciais como assinaturas e informações pessoais.

OUT/24

O Hospital de Clínicas Ijuí (HCI) informou, que sofreu, no dia 24 de outubro, um ataque cibernético à sua base de dados.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A AEP, uma atacadista farmacêutica alemã sediada na Baviera, disse que foi atingida por um ataque de ransomware, e resultou na criptografia parcial dos sistemas de TI da empresa.

O Tribunal Superior do Condado de San Joaquin (California) disse que quase todos os seus serviços digitais foram desativados devido a um ataque cibernético que começou no início desta semana.

Interbank, uma das principais instituições financeiras do Peru, confirmou uma violação de dados após um ator de ameaça que invadiu seus sistemas vazar dados roubados online.

A Schneider Electric confirmou que uma plataforma de desenvolvedor foi violada depois que um invasor alegou ter roubado 40 GB de dados do servidor JIRA da empresa.

Mais de 200.000 pessoas que compraram persianas ou decorações para janelas em 2024 tiveram suas informações de cartão de crédito e outros dados roubados depois que hackers colocaram malware no site de um grande varejista.

A Housing Authority of the City of Los Angeles, ou HACLA, está lidando mais uma vez com um incidente grave de ransomware. A gangue de ransomware Cactus assumiu a responsabilidade por um ataque cibernético que supostamente exfiltrou quase 900 GB de dados confidenciais da organização.

A Newpark Resources, importante fornecedora para a indústria de petróleo, revelou ter sido alvo de um ataque de ransomware que impactou sistemas críticos e restringiu o uso de algumas aplicações empresariais essenciais.

NOV/24

Um ataque de ransomware a um importante hospital no sudoeste da Geórgia interrompeu o acesso ao sistema de prontuários eletrônicos. O ataque foi reivindicado pela gangue de ransomware Embargo, que está tentando extorquir um resgate do hospital ameaçando vazar 1,15 terabytes de dados.

A Halliburton revelou que um ataque de ransomware em agosto resultou em perdas de US$ 35 milhões depois que a violação fez com que a empresa desligasse os sistemas de TI e desconectasse clientes.

A Amazon confirmou uma violação de dados envolvendo informações de funcionários depois que dados supostamente roubados durante os ataques MOVEit de maio de 2023 vazaram em um fórum de hackers.

Hackers ligados a uma agência de inteligência chinesa conseguiram invadir a T-Mobile como parte de uma campanha de um mês para espionar as comunicações de celulares de alvos de inteligência de alto valor.

A Finastra confirmou que alertou seus clientes sobre um incidente de cibersegurança após um ator de ameaça começar a vender dados supostamente roubados em um fórum de hackers.

O fornecedor de software Blue Yonder, que fornece ferramentas de gerenciamento da cadeia de suprimentos para grandes varejistas em todo o mundo, foi atingido por um ataque de ransomware que afetou o Starbucks e alguns supermercados do Reino Unido.

Hackers invadiram os sistemas do banco central de Uganda e desviaram 62 bilhões de xelins (equivalentes a US$ 17 milhões), segundo informações do jornal New Vision.

amazon

A Amazon confirmou, que foi notificada do vazamento de parte dos dados corporativos de seus funcionários, por meio de um incidente cibernético ocorrido em um de seus fornecedores terceirizados. De acordo com a nota, o incidente teria vazado contatos corporativos e localizações de prédio da Big Tech

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

A Prefeitura de Uruguaiana (RS), informou por meio de nota que enfrentou um incidente cibernético. Os sistemas internos foram invadidos por um agente hostil, que criptografou os arquivos locais de todas as secretarias da cidade.

A Lojas Marisa informa que foi vítima de um ataque cibernético do tipo ransomware. A empresa adotou medidas de segurança e de controle apropriadas para mitigação dos impactos e do restabelecimento da normalidade operacional, incluindo o isolamento e a suspensão temporária do funcionamento parcial de seus sistemas para proteção de suas informações.

Banco Central comunica vazamento de dados de clientes da Caixa, onde foram afetados dados cadastrais vinculados a 644 chaves Pix e não foram expostos dados sensíveis, tais como senhas ou saldos financeiros.

Hackers e golpistas estão tendo acesso ao sistema de vigilância Córtex, utilizado pelo Poder Executivo Federal, sob responsabilidade do Ministério da Justiça e Segurança Pública, denunciam a Coalizão Direitos na Rede, a campanha Tire Meu Rosto da Sua Mira e entidades parceiras

NOV/24

A prefeitura de Pirajuí (SP), foi alvo de um incidente cibernético que paralisou diversas funções públicas do município, como Finanças, Compras, Recursos Humanos, Secretaria de Saúde, Educação, além do Sistema de Águas e Saneamento Básico e a Fundação Educacional em março.

A Polícia Militar do Estado de São Paulo informou que está investigando um possível acesso não autorizado aos sistemas de inteligência da corporação, responsáveis por dar suporte tecnológico às operações de policiamento diários.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*

A gangue de ransomware Brain Cipher começou a vazar documentos roubados em um ataque à plataforma de serviços sociais "RIBridges" de Rhode Island. RIBridges é um sistema integrado de elegibilidade (IES) usado pelo estado para gerenciar e fornecer programas de assistência social, incluindo assistência médica, assistência alimentar, creche e outros serviços.

O Bologna Football Club 1909 confirmou ter sofrido um ataque de ransomware após seus dados roubados serem vazados online pelo grupo de extorsão RansomHub.

Dois relatórios recebidos pelo TecMundo no começo de novembro expõem cerca de 15 mil brasileiros clientes da fabricante de automóveis de luxo BMW

Pacientes da PIH Health ficaram impossibilitados de se comunicar com seus provedores de saúde, após um ataque de ransomware ocorrido no início do mês, que levou ao desligamento completo da rede.

ackers atacaram o Fourlis Group da Grécia, interrompendo operações nas lojas IKEA na Grécia, Chipre, Bulgária e Romênia, bem como lojas Intersport, com um ataque de ransomware. O ataque cibernético, descrito como uma “ação externa maliciosa”, foi detectado em novembro e atingiu a infraestrutura central das operações do grupo.

A rede de donuts diz que foi atingida por um ataque cibernético que interrompeu seus sistemas online. Alguns clientes nos EUA não conseguiram fazer pedidos on-line por causa do hack, que ocorreu no final de novembro, mas só agora foi divulgado.

Os Centros de Ciências da Saúde da Texas Tech University (HSCs), em Lubbock e El Paso, foram alvos de um ciberataque significativo. O incidente resultou na exposição de dados de 1,4 milhão de pacientes, entregando uma quantidade substancial de informações valiosas para possíveis ataques de roubo de identidade e engenharia social.

A gigante das telecomunicações BT Group, uma das maiores empresas da Grã-Bretanha, confirmou "uma tentativa de comprometer" sua plataforma de conferência depois que o grupo de ransomware Black Basta afirmou em seu site de vazamento na darknet ter obtido dados corporativos da empresa.

A holding norte-americana Stoli Group, fabricante de bebidas alcoólicas, das quais a mais conhecida é a vodka Stoli, revelou que um ataque de ransomware, em agosto de 2024, contribuiu para o pedido de falência de suas subsidiárias americanas Stoli Group USA e Kentucky Owl (KO).

DEZ/24

O fornecedor de energia romeno Electrica Group confirmou ter sofrido um ataque cibernético no mais recente incidente que atingiu grandes instituições do país.

A Telecom Namibia foi alvo de um ataque do grupo de ransomware Hunters International, que roubou e publicou 626,3 GB de dados de cerca de 619.000 clientes, incluindo ministérios e empresas como Qatar Airways Namibia. A empresa orientou mudanças de senhas e alertou sobre riscos de fraudes, enquanto autoridades trabalham para mitigar os danos.

A Japan Airlines (JAL) sofreu um ataque cibernético que causou atrasos em voos domésticos e internacionais. O incidente afetou sistemas de comunicação externos, levando a JAL a suspender temporariamente a venda de passagens e a isolar um roteador problemático.

Uma falha nos sistemas de TI da American Airlines na véspera de Natal resultou em uma paralisação nacional de voos, ordenada pela FAA. O problema, que afetou processos de check-in e despacho de aeronaves, foi resolvido em cerca de uma hora, permitindo a retomada das operações.

A Volkswagen enfrentou um grande vazamento de dados envolvendo informações confidenciais de 800.000 veículos elétricos, incluindo dados de localização e detalhes de contato do proprietário.

A State Child Protection Society (SCPS) de Madhya Pradesh, uma agência governamental encarregada de implementar leis de proteção à criança, esquemas e iniciativas de bem-estar, tornou-se a mais recente vítima do notório grupo de ransomware Funksec. O grupo de ransomware Funksec assumiu publicamente a responsabilidade pelo ataque, afirmando que infiltrou 2 GB de dados confidenciais dos sistemas da SCPS

O RansomHub alega ter roubado 1 terabyte de dados confidenciais da rede da MetLife, listando servidores que seriam de operações da empresa no Brasil, Chile, México, Equador, Colômbia e Argentina.

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*

DEZ/24

A Unidas Aluguel de Carros confirmou que reagiu contra uma tentativa de acesso indevido aos seus sistemas, o grupo de ransomware Fog teria assumido a autoria do vazamento de informações.

A Banco Central comunica vazamento de dados pessoais e alerta sobre golpes. Autarquia monetária disse que 1.500 pessoas que participaram de levantamento realizado pela instituição tiveram suas informações expostas de forma indevida

Especialistas da empresa brasileira de inteligência de ameaças ZenoX, calculam que há dados pessoais de aproximadamente 250 mil brasileiros num vazamento na dark web. O material inclui dados sensíveis de clientes de pelo menos seis instituições do setor de crédito pessoal: **Sincronos, Éfeso Capital, CredCenter, GoldenBank, SemprePromotora, MegaPromotora e ProntoPay**.

Vazamento tem dados de 250 mil brasileiros

- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**