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)*

JAN/24

LUSH FRESH HANDMADE COSMETICS

water for people

Agência de prisioneiros de guerra da Ucrânia

Governos locais no Colorado, Pensilvânia e Missouri

loanDepot
INSPIRING VACATIONS
AERCAP
Schneider Electric
GALA
xerox
DIRECT
sodexo
Carrefour
tietoevry
EQUILEND

Município de Calvià, da ilha espanhola de Maiorca

DENHAM

monobank

coop
tigo
Microsoft
Global Affairs Canada
orange
SUBWAY
Hewlett Packard Enterprise
Trello
COURT SERVICES VICTORIA

FEV/24

Prudential
THALES
HYUNDAI MOTOR GROUP
EL AL
IT'S NOT JUST AN AIRLINE, IT'S ISRAEL
CLOUDFLARE
Ann & Robert H. Lurie Children's Hospital of Chicago
AnyDesk
cencora

Empresa de Hong Kong que caiu em de deepfakes.

AT&T
Canada
Robert Half Talent Solutions
TN Trans-Northern
BANK OF AMERICA
INSOMNIAC GAMES
Claro
VARTA

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

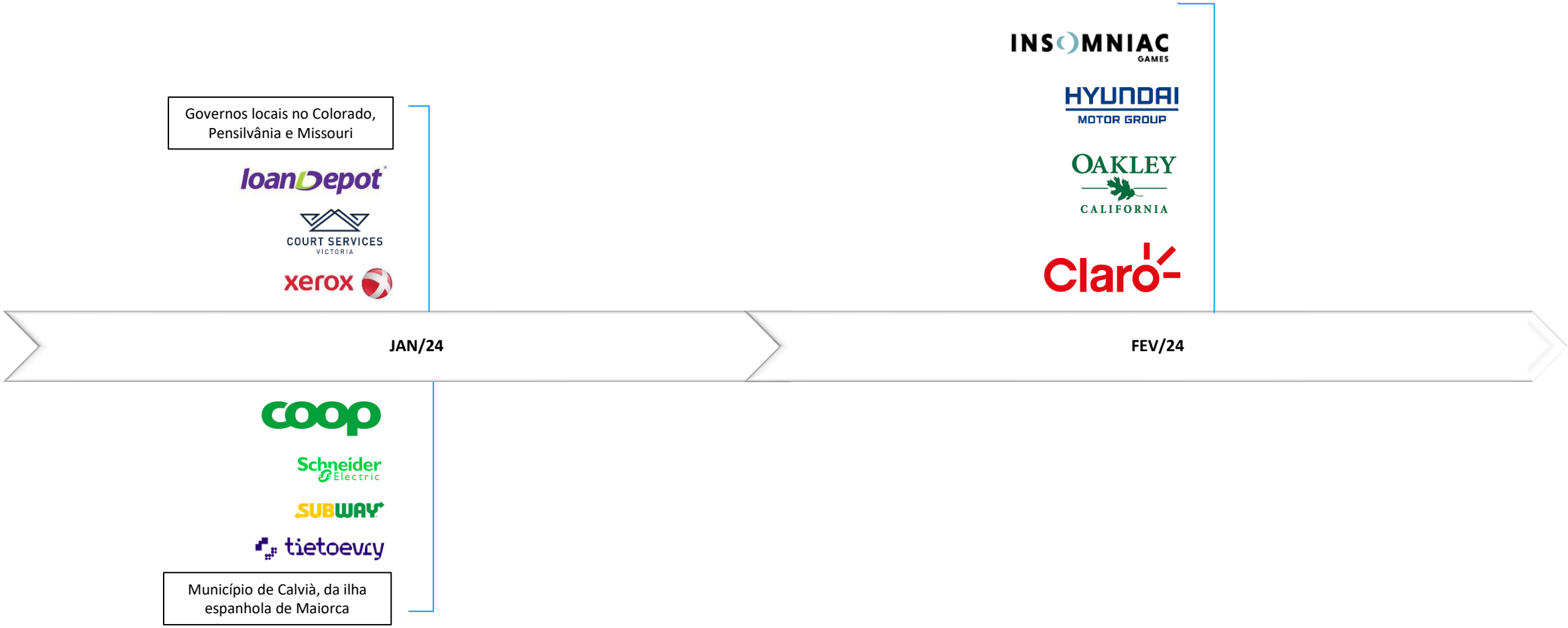
IBRASPD

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

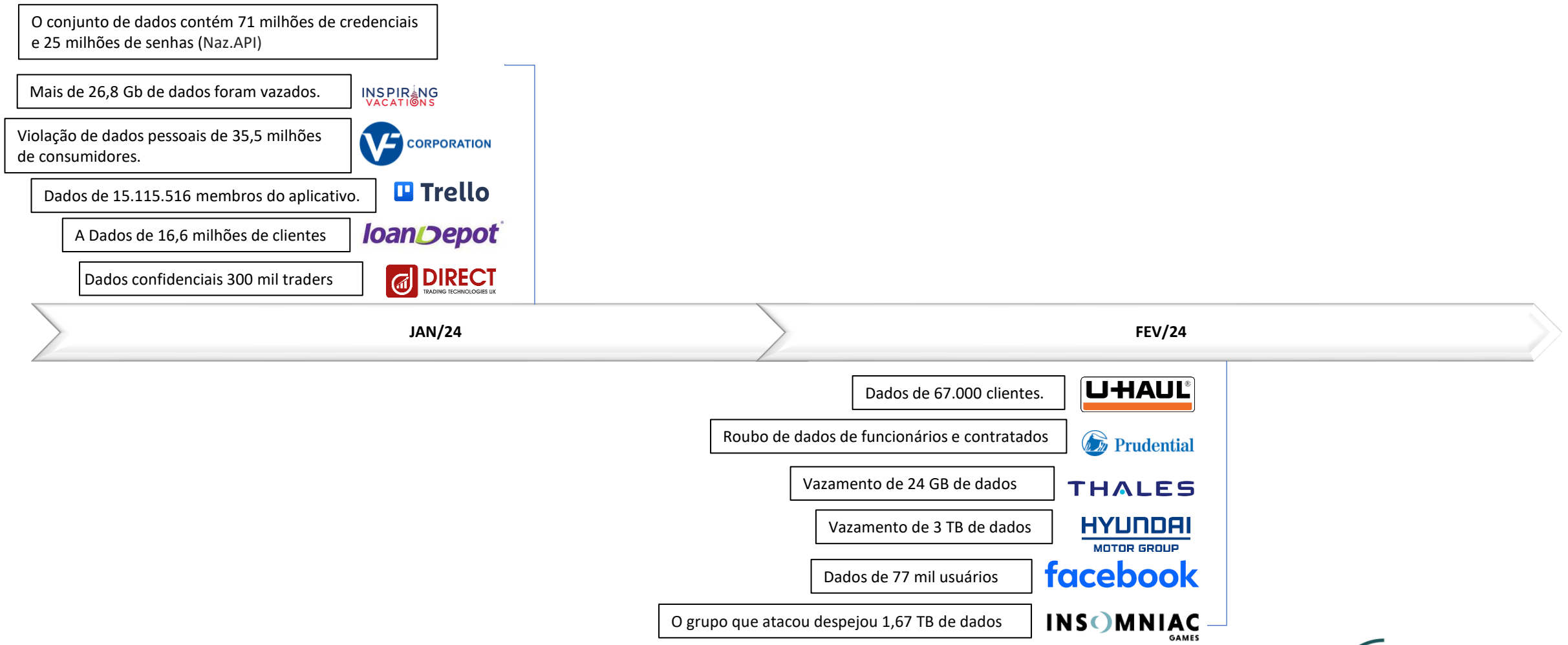
Contexto Atual – RANSOMWARE com repercussão na mídia*



- **Casos Divulgados**

IBRASPD

Vazamentos de dados pessoais com repercussão na mídia*



- **Casos Divulgados**

IBRASPD

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.

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".

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/

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.

O Monobank sofreu um poderoso ataque cibernético (DDoS).

- **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**