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

LoanDepot
INSPIRING VACATIONS
AERCAP
LUSH FRESH HANDMADE COSMETICS
Schneider Electric
water for people
GALA HISPANIC THEATRE
xerox
Agência de prisioneiros de guerra da Ucrânia
DIRECT TRADING TECHNOLOGIES LLC
sodexo
Governos locais no Colorado, Pensilvânia e Missouri
Carrefour
tietoevry
EQUILEND

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

MAR/24

Serviços públicos de diversas cidades nos EUA
Várias agências governamentais francesas
AirEuropa
McDonald's
FUJITSU
prisma
National Cyber Security Centre
capita
EMTEK

JAN/24

Município de Calvià, da ilha espanhola de Maiorca
coop
tigo
DENHAM
Microsoft
Global Affairs Canada
monobank
orange
SUBWAY
Hewlett Packard Enterprise
Trello
COURT SERVICES VICTORIA

FEV/24

Empresa de Hong Kong que caiu em de deepfakes.
AT&T
Canada
Robert Half Talent Solutions
Trans-Northern
BANK OF AMERICA
INSOMNIAC GAMES
Claro
VARTA

MAR/24

verbraucherzentrale Hessen
OWASP
AMERICAN EXPRESS
NATIONS DIRECT MORTGAGE
Fidelity INVESTMENTS
THE WORLD BANK
MARINEMAX
Duvel
NHS SCOTLAND

- **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)*

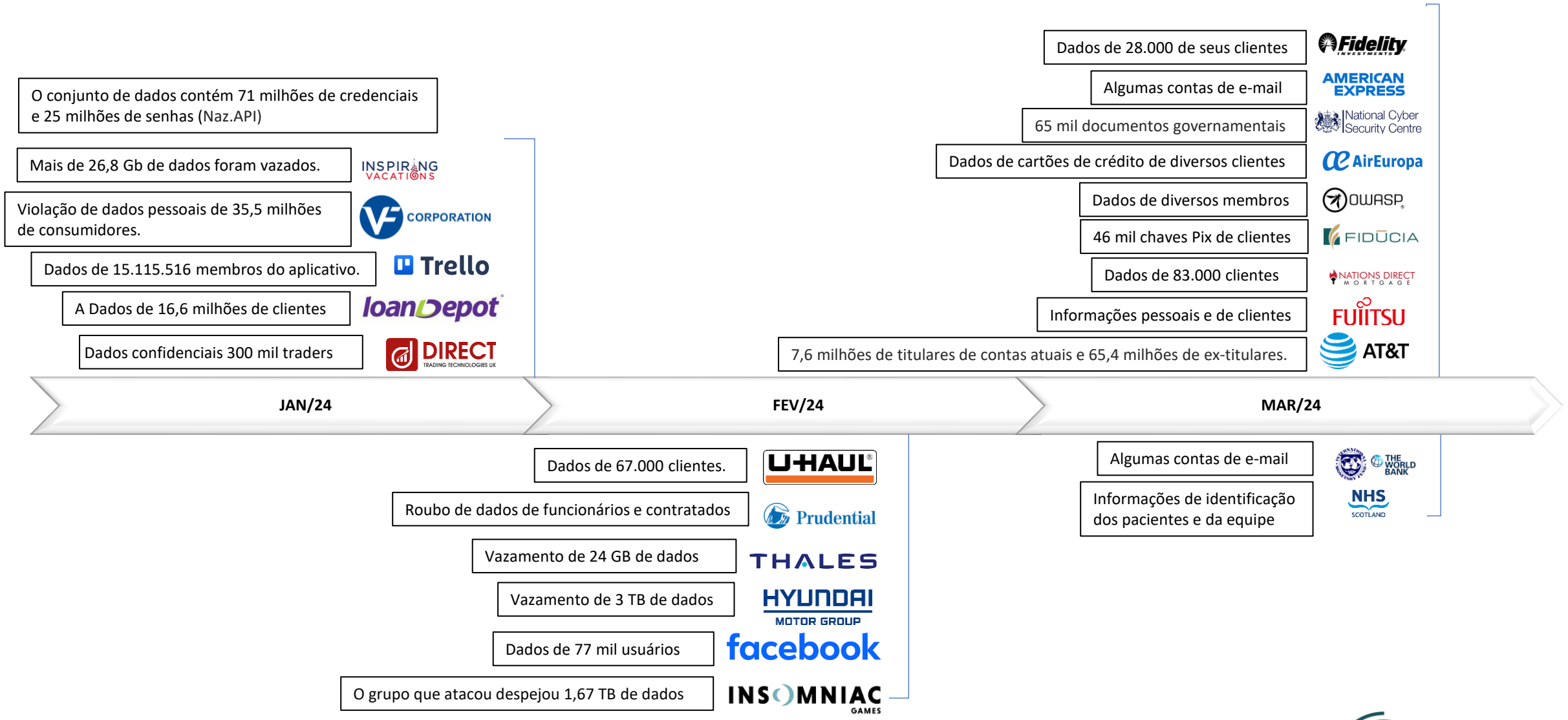
- **Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade**

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**

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.

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