AIG

CyberEdge

Seguro de Proteção de Dados e Responsabilidade Cibernética

Tiago Lino

Especialista em Riscos Cibernéticos

HISTÓRIA DO CYBER E SUAS LEIS NO MUNDO

1973 — Criada a 1ª lei nacional de Proteção de Dados na Suécia

1997 — AIG lança o Cyber nos EUA

2000 — Bug do Milênio: Preocupação com Risco Cibernético

2005 — Início da era dos maiores vazamento de dados

2012 — AIG lança o Cyber no Brasil

CyberEdge

2013/14 — Maior vazamento de dados da história (3bi de pessoas)

2017 — WannaCry

2018 — GDPR entra em vigor

2018 — SUSEP cria o Ramo 327 para Riscos Cibernéticos

SUSEP

2020 — LGPD entra em vigor

Lei Geral de Proteção de Dados Pessoais

2021 — Crimes cibernéticos causarão US$ 6 trilhões em perdas

AS AMEAÇAS

Funcionários
desonesto ou negligente

Invasores
- Hactivismo ⓘ
- Organizações Criminosas ⓘ

ⓘ Fornecedores
- Nuvem / Cloud
- Data Centers
- Fornecedores externos

ⓘ Redes Sociais

AIG

ⓘ Clique nos links acima para ver exemplos

OS SETORES EXPOSTOS

- Área Médica / Área de Saúde
- Instituições Financeiras
- Atacado / Varejo
- Manufaturas / Indústria
- Construção Civil / Imobiliário
- Telecomunicações / Mídia
  Tecnologia / Serviços de Internet
- Transporte/ Cias Aéreas
  Turismo/ Logística
- Educação
- Entretenimento
- Prestadores de Serviço (Corretores de seguro, Contadores, Advogados, Escritórios de Advocacia)
- Telemarketing / Call Centers / Centros de Processamento de Dados
- Entidades Governamentais
- **Qualquer outra Entidade Comercial que armazene informações e dados pessoais**

AIG

O RISCO CIBERNÉTICO NA EMPRESA

- Seguro Cibernético atua em 2 frentes:

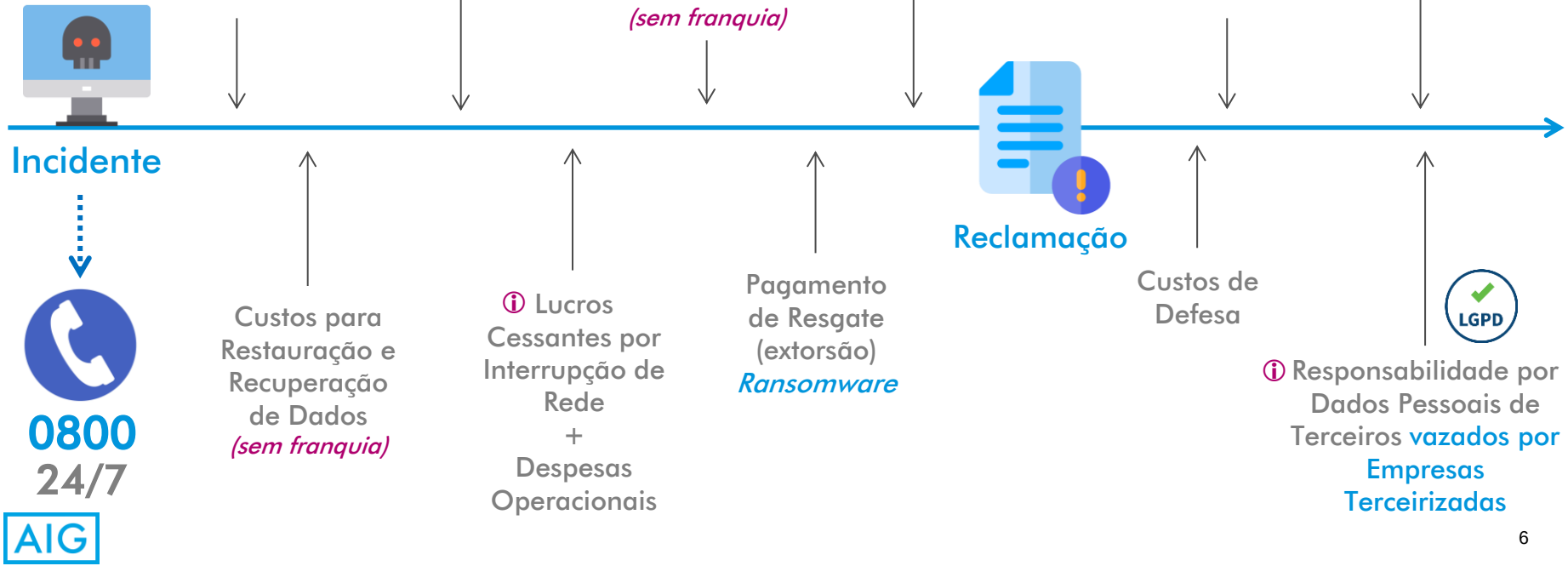
Coberturas de **Resposta a Incidentes**

Coberturas de **Responsabilidade Civil**

AIG

GARANTIAS DA APÓLICE

Clique nas coberturas indicadas com o símbolo ⓘ para ver exemplos



LEI DE PROTEÇÃO DE DADOS

Principais Pontos da Lei 13.709 de 2018

- Aplicação: Todas as empresas (pública, privada, nacionais ou estrangeiras), desde que a coleta seja feita em território brasileiro;
- Início em 14 de agosto de 2020;
- Multas de até 2% do faturamento, limitada a R$ 50 milhões;
- Obrigatoriedade de Notificação;
- Autoridade Nacional de Proteção de Dados (ANPD);

AIG

PARCERIAS E DIFERENCIAIS AIG

1

TECHGUARD® S·H·I·E·L·D™

SECURE · HOLISTIC · INTEGRATED · EMPLOYEE · LEARNING · DEFENSES

Cyber Security Awareness Training

2

poliWall®

IP and Domain Blocking

3

Vulnerability Scan

TECHGUARD®

PoliWall Sample Report

CARACTERÍSTICAS DO SEGURO

Principais Situações Excluídas da Apólice

- Danos Corporais e Danos Materiais;
- Roubo de Valores (golpe do boleto adulterado e saques em contas correntes);
- Infraestrutura: apagões, sobretensão, falhas em sistema de telecomunicação e ou transmissão via satélite;
- Valores Mobiliários: ordens de compra ou venda de valores mobiliários.

AIG

CARACTERÍSTICAS DO SEGURO

Análise do Risco | Questionário

- Segmento de Atuação;
- Tipo e Quantidade de dados armazenados;
- Relacionamento com *Stakeholders* : funcionários, fornecedores e empresas terceirizadas;
- Exposição fora do Brasil;
- Política de Proteção de Dados;
- Gerenciamento de Acesso e Recuperação de Dados: *Firewall*, Antivírus, Criptografia de Dados, Plano de Continuidade de Negócios, etc.;
- Histórico de Reclamações, Ataques, Acessos não Autorizados, etc.

AIG

Tiago Lino

AIG 100 ANOS NO MUNDO

CELEBRANDO 70 ANOS NO BRASIL

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. Products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Not all products and services are available in every jurisdiction, and insurance coverage is governed by actual policy language. Certain products and services may be provided by independent third parties. Insurance products may be distributed through affiliated or unaffiliated entities. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

Exemplos e notícias recentes

AIG

Hackers invadem site da Odebrecht e criticam envolvimento na Lava Jato

Site Odebrecht em 10/09/2015

***Fonte**: http://www1.folha.uol.com.br/poder/2015/09/1679870-hackers-invadem-site-da-odebrecht-e-criticam-envolvimento-na-lava-jato.shtml*

Anonymous derruba loja virtual que fazia apologia ao machismo

O grupo de **hacktivismo** Anonymous Brasil tirou do ar a loja virtual Alezzia, especializada em móveis, após uma série de provocações feitas pelo e-commerce a mulheres, tanto clientes quanto demais usuárias. Segundo o grupo, todos os produtos tiveram seus dados deletados.

A Alezzia ficou negativamente famosa em dezembro de 2016 ao postar diversas fotos de mulheres seminuas ou de maiô para anunciar seus produtos – as fotos não tinham conexão com os itens anunciados. A página da empresa no Facebook foi bombardeada por críticas de machismo, respondidas em tom de desafio pelo e-commerce, que incitava os internautas a diminuírem o máximo possível as notas da loja.

Na última semana, a loja contratou Gabriel Vaz, estagiário recentemente demitido pela Cantareira Construtora por usar o perfil oficial da empresa para atacar feministas.

De acordo com o Anonymous, o grupo **"está posse de todas as bases de dados, seus backups, e-mails, senhas, e todos os dados de todos os seus 10 mil clientes, que estão sendo devidamente notificados nesse (sic) exato momento por e-mail, convidando-os a processar a Alezzia pela falha de segurança"**, explicou.

Na mensagem que deixou na página, o grupo justificou o ato como forma de lutar pela igualdade de gênero e confrontar aqueles que "gritam 'liberdade de expressão' pra repetir as mesmas falas machistas que nossos avôs já diziam no século passado como se fosse uma grande novidade confrontadora do 'politicamente correto'", disse em sua postagem (confira a postagem completa no fim da matéria).

[...]

AIG

***Fonte**: https://www.ecommercebrasil.com.br/noticias/anonymous-derruba-e-commerce-apologia-machismo/*

voltar

Brasil tem os melhores hackers do mundo, diz especialista

O Brasil tem hoje os melhores hackers do mundo, ao lado da Coréia e da China. A afirmação é do americano Chris Rouland, diretor da X-Force, um grupo de especialistas da empresa Internet Security Systems (ISS) que monitora o tráfego na internet e combate a ação de hackers.

- O Brasil tem milhares dos melhores hackers do mundo e eles estão muito ocupados – disse Rouland, que está no Brasil para um ciclo de palestras sobre segurança de redes corporativas e internet em São Paulo. O diretor da X-Force ressaltou que nenhum governo ou empresa está livre de um ataque de hacker. Segundo ele, o fato de ter os protocolos de internet (IP) em seqüência torna a web brasileira muito vulnerável à ação dos invasores virtuais. No Brasil, todos os IPs começam com o número 200.

- Milhares de sistemas brasileiros são invadidos em poucas horas. O Brasil é menos seguro que a Austrália e um pouco melhor que o Japão – afirmou.

De olho no cyberterrorismo - Rouland disse também que especialistas em segurança eletrônica estão preocupados com a possibilidade de um ataque terrorista aos sistemas de informação - o chamado cyberataque - comandado pela organização terrorista Al Qaeda. Segundo ele, o grupo detectou que pessoas ligadas ao terrorista Osama bin Laden aumentaram a utilização da web.

- A Al Qaeda está usando muito a internet. Estamos preocupados que eles estejam armando um cyberataque para os próximos meses – afirmou Rouland.

De acordo com o especialista, o X-Force monitora ininterruptamente os ataques às redes e sistemas de informação em todo o mundo. Diariamente, seu grupo se reúne com equipes do FBI, a polícia federal americana, e do INPC -órgão do governo americano responsável pela proteção à infra-estrutura do país - para informá-los sobre o tipo e o local onde estão ocorrendo os cyberataques.

Rouland informou que, desde os ataques terroristas de 11 de setembro do ano passado, o governo americano tem investido US$ 1 bilhão por ano somente em sistemas de segurança e proteção de redes.

- Os sites do governo americano eram muito atacados porque, no passado, investiam pouco em segurança. Agora, o governo gasta US$ 1 bilhão somente em sistemas de segurança na rede – disse Rouland.

De acordo com levantamento da ISS, antigamente 70% das ameaças às redes vinham de dentro das próprias organizações. Atualmente, esse índice é de 30%. Entretanto, observa Rouland, os ataques feitos internamente têm um índice de sucesso maior que os de origem externa.

***Fonte**: https://www.ecommercebrasil.com.br/noticias/anonymous-derruba-e-commerce-apologia-machismo/*

Hackers exploram falhas em sistemas de ar condicionado e máquinas de salgados

Cibercriminosos monitoram sistemas de empresas terceirizadas para obter informações de seus alvos

[...]
Incapazes de invadir a rede de computadores numa grande empresa de petróleo, hackers infectaram com um malware o cardápio online de um restaurante chinês muito utilizado pelos funcionários. Ao escolherem seu almoço, eles acidentalmente baixaram um código que deu aos agressores uma base na ampla rede computacional da empresa.

Especialistas em segurança convocados para corrigir o problema não foram autorizados a divulgar os detalhes da invasão, mas a lição com o incidente ficou clara: **empresas buscando proteger seus sistemas contra hackers e espiões do governo precisam procurar vulnerabilidades nos locais mais improváveis.**
[...]
É difícil encontrar números do percentual de ataques virtuais que podem ser ligados a vazamentos de terceiros, em grande parte porque os advogados das vítimas encontram qualquer motivo para não divulgar uma invasão. Mas uma pesquisa com mais de 3.500 praticantes globais de TI e segurança virtual, conduzida no ano passado por uma firma de pesquisa de segurança, o Ponemon Institute, descobriu que **23 por cento das invasões eram atribuíveis à negligencia de terceiros.**

AIG ***Fonte***: *https://tecnologia.ig.com.br/2014-04-26/hackers-exploram-falhas-em-sistemas-de-ar-condicionado-e-maquinas-de-salgados.html*

4 Lições que devemos aprender com o ataque sofrido pela Target

Em 2013, a rede da Target, grande varejista de roupas dos Estados Unidos, sofreu um ataque que gerou o vazamento de 110 milhões de números de cartões de crédito, senhas e dados pessoais. O vazamento acabou resultando na demissão do CIO da empresa e sérios problemas à imagem e aos negócios. Para o consultor de segurança da Real Protect, Rovercy de Oliveira, uma situação dessa magnitude chama muita atenção e gera algumas lições que podem ser aplicadas a outras companhias para que o mesmo não ocorra...
[...]

4. O ponto mais crítico da sua segurança é algo que você não considerou

O ataque à Target começou quando um técnico terceirizado, que foi à sede da empresa para consertar o termostato de um ar condicionado, conectou um dispositivo à rede wireless, no chamado lado fraco do firewall. "Os hackers estão cada vez mais sofisticados, planejam com muito cuidado uma oportunidade como essa para fisgar um alvo tão lucrativo, e eles irão exatamente onde você não está olhando. É por isso que a segurança deve ser internalizada na cultura da empesa, todo e qualquer procedimento deve estar de acordo com as normas." finaliza.

Fonte: *https://realprotect.net/blog/4-licoes-que-devemos-aprender-com-o-ataque-a-target/*

voltar

Hackers brasileiros lançam golpe no WhatsApp para roubar dados pessoais

...

As mensagens utilizam os links “ *bbit.ly/extracupom* ” e “ *bbit.ly/carrefourcupom* ”, que aparentemente pertencem a algum serviço encurtador de URLs, para levar a vítima para os sites falsos “ *extra.supermarket.gift* ” e “ *carrefour.supermarket.gift* ”. O encurtador de links verdadeiro é o “bit.ly”. No caso do golpe em pauta, o site convida a vítima potencial a preencher um formulário para coletar seus dados pessoais e solicitar a indicação de dez contatos para ter acesso ao suposto cupom de R$ 500 de desconto.

Após encaminhar a mensagem de **phishing** para os novos alvos, o usuário é direcionado para uma página que pede que ligue para o número 0911778787940 antes de ganhar o suposto cupom. Trata-se de um número premium que cobrará pela chamada. De acordo com os relatos de algumas vítimas que efetuaram a chamada, uma gravação solicita que sejam respondidas 25 perguntas, na tentativa de prolongar a ligação pelo maior tempo possível e onerar ainda mais a cobrança da vítima.

...

***Fonte**: https://oglobo.globo.com/economia/hackers-brasileiros-lancam-golpe-no-whatsapp-para-roubar-dados-pessoais-17566872*

Um em cada quatro brasileiros já caiu em phishing, golpe que rouba dados

Ataques que acontecem por e-mail, WhatsApp e redes sociais apelam para a curiosidade e o senso de urgência das pessoas

O número de pessoas que caiu em um golpe de phishing no último ano no Brasil é de mais de 48 milhões, quase 25% da população. O país é líder mundial nesse tipo de ameaça, que consiste em usar sites falsos para roubar dados dos usuários, principalmente, informações bancárias. Os ataques vêm por e-mail, **WhatsApp**, SMS e até ligações convencionais, e visam enganar usuários comuns, que usam o PC ou o celular em suas casas, e também funcionários de empresas. Os dados foram divulgados durante a 8ª Conferência de Analistas de Segurança para a América Latina, nesta segunda-feira (13).

A história não é nova: o usuário recebe um e-mail, mensagem ou vê um anúncio no **Facebook** com o produto que queria comprar. A propaganda mostra o nome de uma empresa já conhecida e traz um desconto interessante, mas totalmente plausível (10% a 15% mais barato, por exemplo). O consumidor clica, preenche os dados e efetua a compra sem saber que se trata de um site falso. Dias depois, descobre que teve o cartão clonado, senha trocada, entre outros problemas que terá que resolver a partir de agora.

...

***Fonte**: https://www.techtudo.com.br/noticias/2018/08/um-em-cada-quatro-brasileiros-ja-caiu-em-phishing-golpe-que-rouba-dados.ghtml*

Mercado de saúde é um dos mais atrativos para os hackers

Manter informações sigilosas protegidas e em segurança é um desafio para empresas de todos os segmentos de negócios. E no setor da saúde não é diferente. Pesquisa realizada pela KPMG aponta que **81% das organizações desta área já foram comprometidas**, ao menos uma vez, por malware, botnet ou outro tipo de ciberataque em um período de dois anos. Já um estudo sobre ransomware, organizado pela BitSight Insight em 2016, aponta que as organizações de saúde aparecem na terceira posição como alvo preferido de ataques e fraudes.

Alguns fatores contribuem para que este setor seja um alvo cada vez mais frequente dos cibercriminosos, conforme explica Rogério Reis, diretor de Operações da Arcon. **"Isso ocorre porque, para os hackers, os dados de pacientes são extremamente críticos e valorizados. Por exemplo, no mercado negro, cada cadastro de paciente é vendido por um valor acima de R$ 150,00 enquanto o valor pago pelos dados de um cartão de crédito pessoal é de R$ 3,00".** Já no outro lado, os hospitais também estão mais propensos a aceitar chantagens. "Em seus sistemas constam informações centralizadas sobre a saúde dos pacientes ou, até mesmo, acesso aos equipamentos que controlam um procedimento. O risco é significativo para as instituições e, consequentemente, aos seus pacientes. Muito mais que uma questão de privacidade, é uma questão de disponibilidade e integridade dos dados. Ficar sem acessos aos dados corretos de tratamento de um paciente ou perder o controle sobre um equipamento, em alguns casos, pode custar até vidas", alerta o executivo. [...]

Além das invasões aos sistemas com bloqueio dos dados e solicitações de resgates (ransomware), há outro golpe que vem chamando a atenção. **Hackers conseguem acesso aos prontuários e familiares de pacientes internados sofrem golpes por telefone com a solicitação de pagamentos dos procedimentos hospitalares**. Ou seja, por falhas nos sistemas de segurança da informação ou na conduta dos profissionais, os criminosos se beneficiam. Recentemente, órgãos de defesa do consumidor apontaram que as instituições hospitalares devem ser responsabilizadas e arcar com os danos e prejuízos gerados aos pacientes, independentemente dos avisos utilizados pelos hospitais para alertarem aos pacientes sobre os golpes.

AIG

***Fonte**: https://ecommercenews.com.br/noticias/pesquisas-noticias/instituicoes-de-saude-estao-na-mira-de-cibercriminosos/*

voltar

Ataques hackers são mais temidos por empresas que inflação e austeridade

Para empresários brasileiros, o risco de ser alvo de um ataque hacker supera a preocupação com mudanças regulatórias ou com a inflação.

A conclusão é de uma pesquisa que mede riscos corporativos, da Allianz Global Corporate, empresa de seguros. Ela contou com respostas de 1.911 empresários e corretores em 80 países, entre outubro e novembro de 2017.

Problemas macroeconômicos, como deflação (ou inflação), programas de austeridade e aumento no preço das commodities, estavam em segundo lugar (30%) entre brasileiros no fim de 2016, mas não chegaram às dez maiores preocupações neste ano.

Apesar disso, o baixo consumo no país —que, em junho de 2017, provocou deflação de 0,23%— afeta as empresas por meio de uma preocupação com baixa demanda e concorrência externa, o que a pesquisa chama de "mudanças no mercado".

No mundo, o maior risco identificado é a interrupção dos negócios (42%), item que também liderou a pesquisa no ano anterior. Era possível escolher até três riscos.

"As interrupções são momentos em que a operação tem que parar e se perde espaço para a concorrência", diz Angelo Colombo, presidente na América do Sul da Allianz Global Corporate & Specialty. "Nem todas as interrupções são cobertas por seguros. Um exemplo é quando a cadeia produtiva para devido à falta de estoque."

Europa e Estados Unidos também estão menos preocupados com a conjuntura econômica agora do que antes, segundo a pesquisa.

CATÁSTROFES

As catástrofes naturais subiram do quarto para o terceiro lugar (30%) no ranking de riscos neste ano, na esteira de desastres como os furacões Harvey, Irma e Maria, além de enchentes e incêndios.

O grupo de seguros Munique Re estima que, em 2017, o prejuízo com eventos desse tipo tenha superado US$ 330 bilhões (mais de R$ 1 trilhão).

O ano também foi marcado por ciberataques. Em maio de 2017, houve o WannaCry, ataque em massa que travou computadores e pediu um resgate dos usuários em bitcoins. Um mês depois, um vírus chamado Petya infectou dezenas de computadores.

AIG

***Fonte**: https://www1.folha.uol.com.br/mercado/2018/01/1951058-empresario-brasileiro-teme-mais-ataque-hacker-a-inflacao-e-austeridade.shtml*

voltar

LGPD: 10 pontos para entender a nova lei de proteção de dados no Brasil

Próximos meses dever ser de muitas dificuldades e planejamento dentro das corporações brasileiras

4 – Data Protection Officer: a partir de agora, as organizações devem estabelecer um Comitê de Segurança da Informação para analisar os procedimentos internos. Dentro deste órgão haverá um profissional exclusivo para a proteção dos dados e responsável pelo cumprimento da nova lei.

***Fonte**: https://computerworld.com.br/2018/09/19/lgpd-10-pontos-para-entender-a-nova-lei-de-protecao-de-dados-no-brasil/*

Fábrica da Renault em São José dos Pinhais foi afetada por ataque cibernético

Montadora suspendeu a atividade de unidades na França após detectar invasão aos sistemas

A fábrica da Renault em São José dos Pinhais, na Região Metropolitana de Curitiba, foi afetada pelo super ataque cibernético que tomou os sistemas de empresas e instituições de mais de 100 países na sexta-feira (12). De acordo com a assessoria da montadora no país, ainda não se sabe se os problemas percebidos no Brasil são consequência de um ataque direto aos sistemas locais ou da invasão sofrida pela unidade francesa. Por meio de nota, a assessoria da montadora informou que "um diagnóstico completo está sendo feito para colocar em prática as medidas apropriadas para o caso".

Não foram informadas as áreas da fábrica no Brasil afetadas pelos ataques cibernéticos. Na França, a montadora suspendeu a produção em várias unidades "para evitar a propagação do vírus", informou a direção do grupo no país europeu. Não foi divulgada, contudo, uma lista das fábricas que tiveram as atividades suspensas. O porta-voz da Renault na França apenas confirmou a suspensão das atividades de uma unidade no Noroeste da França.

O Ministério Público de Paris abriu uma investigação por este ataque. A polícia francesa classificou de "particularmente perigosa" a forma como se propaga este "ransomware" – um vírus que bloqueia o computador e que exige um resgate, que deve ser pago em um prazo curto, para poder recuperar o controle do equipamento.

"Uma vez que a primeira máquina está infectada, se propaga ao conjunto da rede à qual está conectado, paralisando assim todos os computadores", explicou a polícia francesa.

Confira a nota da assessoria da fábrica no Brasil:

O Grupo Renault confirma que foi impactado pelo ciberataque global que começou no final do dia 12, sexta-feira. Imediatamente, foram tomadas medidas proativas para impedir que o vírus se espalhasse e para proteger o Grupo. Um diagnóstico completo está sendo feito para colocar em prática as medidas apropriadas para o caso.

AIG

***Fonte**: http://www.gazetadopovo.com.br/economia/nova-economia/fabrica-da-renault-em-sao-jose-dos-pinhais-foi-afetada-por-ataque-cibernetico-1bf8m4wxb8wgciisv2ioezuam*

LGPD: 10 pontos para entender a nova lei de proteção de dados no Brasil

Próximos meses dever ser de muitas dificuldades e planejamento dentro das corporações brasileiras

3 – Principais pontos: a lei é aplicada a todos os setores da economia; possui aplicação extraterritorial, ou seja, toda empresa que tiver negócios no país deve se adequar a ela; consentimento do usuário para coletar informações pessoais; os titulares podem retificar, cancelar ou até solicitar a exclusão desses dados; criação da Autoridade Nacional de Proteção aos Dados (ANPD); e a notificação obrigatória de qualquer incidente.

AIG

***Fonte**: https://computerworld.com.br/2018/09/19/lgpd-10-pontos-para-entender-a-nova-lei-de-protecao-de-dados-no-brasil/*

Netshoes faz acordo para notificar clientes sobre ataque hacker

O Ministério Público do Distrito Federal notificou a companhia em janeiro para que informasse os cerca de 2 milhões de usuários atingidos pelo vazamento

Por **Alberto Alerigi Jr., da Reuters**
access_time 27 fev 2018, 15h56

O Ministério Público do Distrito Federal notificou a companhia em janeiro para que informasse os cerca de 2 milhões de usuários atingidos pelo vazamento. Uma nova reunião do MPF com a empresa ocorreu semana passada sobre a forma como a notificação dos clientes ocorreria.

"Na ocasião, foi acordado que a empresa fará a comunicação pessoal, por meio de contato telefônico, a todos os clientes que tiveram seus dados disponibilizados por terceiros na internet", afirmou a Netshoes em comunicado à imprensa.

***Fonte**:https://exame.abril.com.br/negocios/netshoes-faz-acordo-para-notificar-clientes-sobre-ataque-hacker/*

voltar

LGPD: 10 pontos para entender a nova lei de proteção de dados no Brasil

Próximos meses dever ser de muitas dificuldades e planejamento dentro das corporações brasileiras

9 – Multas: a nova lei prevê sanções para quem não tiver boas práticas. Elas englobam advertência, multa ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões, passando por penalidades diárias.

AIG

Fonte: *https://computerworld.com.br/2018/09/19/lgpd-10-pontos-para-entender-a-nova-lei-de-protecao-de-dados-no-brasil/*

França multa Google em 50 milhões de euros por violação de lei de privacidade na UE

A agência de proteção de dados da França multou o Google nesta segunda-feira (21) em 50 milhões de euros (cerca de R$ 213 milhões) por violação de regras de privacidade da União Europeia.

É a maior penalidade do tipo imposta contra uma companhia de tecnologia dos Estados Unidos, relata a agência Reuters.

O regulador francês afirmou que o Google não é transparente e claro na maneira como informa usuários sobre como dados pessoais são coletados em seus serviços, incluindo o YouTube, o Mapas e o mecanismo de busca, para apresentação de anúncios publicitários personalizados.

Regras mais duras

A Regulação sobre Proteção Geral de Dados (GDPR) da UE, a maior reforma em leis de privacidade de dados em mais de duas décadas, entrou em vigor em maio do ano passado.

Ela permite aos usuários um melhor controle sobre seus dados pessoais e dá às autoridades o poder de impor multas de até 4% da receita global em caso de violações.

"O montante decidido e a publicidade da multa são justificados pela gravidade das infrações observadas", disse a agência francesa.

O Google afirmou que está "profundamente comprometido em cumprir as exigências de consentimento da GDPR".

...

***Fonte**: https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml*

Banco Inter fecha acordo com MP sobre vazamento e vai pagar R$ 1,5 milhão

O Banco Inter fechou nesta terça-feira (18) acordo com o Ministério Público do Distrito Federal e Territórios (MPDFT) para encerrar uma ação civil pública movida junto à 15ª Vara Cível de Brasília por vazamento de dados de clientes. No acordo, **o banco aceitou pagar R$ 1,5 milhão em indenização.** Originalmente, o MPDFT havia pedido uma indenização de R$ 10 milhões.

Segundo o Banco Inter, deste valor, R$ 1 milhão serão destinados, até 31 de julho de 2019, a instituições públicas que combatem crimes cibernéticos indicadas pelo MPDFT. Esse valor será repassado na forma de equipamentos e softwares, também indicados pelo Ministério Público. Os outros R$ 500 mil serão doados até 30 de janeiro a instituições de caridade

***Fonte**: http://economia.uol.com.br/noticias/estadao-conteudo/2018/12/18/banco-inter-fecha-acordo-com-ministerio-publico-para-pagar-r-15-milhao.htm*

Vazamento de dados da Netshoes custa R$ 500 mil à empresa

Acordo feito com o Ministério Público evita ação civil pública contra a companhia, mas exige medidas práticas para evitar novas ocorrências

Os vazamentos de dados têm custado caro para as organizações. Exposições ocorridas em 2017 e 2018 vão custar à Netshoes **R$ 500 mil como indenização por danos morais.** O acordo extrajudicial foi fechado com o Ministério Público do Distrito Federal e Territórios (MPDFT) para evitar uma ação coletiva.

O MPDFT classifica o caso como um dos maiores incidentes de segurança registrados no Brasil. Isso porque as ações espalharam informações de 1.999.704 clientes: nome completo, e-mail, CPF, data de nascimento e produtos comprados. Senhas e números de cartões de crédito não foram comprometidos.

O órgão, então, ameaçou a empresa com uma ação civil pública. Como a Netshoes colaborou com a investigação, as partes chegaram a um acordo na forma de Termo de Ajustamento de Conduta (TAC). Assim, a marca concordou em informar os clientes sobre o vazamento e pagar a indenização por danos morais coletivos.

***Fonte**: https://olhardigital.com.br/noticia/vazamento-de-dados-da-netshoes-custa-r-500-mil-a-empresa/82367*

BACEN anuncia resolução sobre uso de cloud computing no setor

Banco Central do Brasil divulga a Resolução nº 4.658 sobre a política de cibersecurity, que estabelece requisitos para a contratação de serviços de armazenamento e processamento de dados e computação em nuvem para instituições financeiras

Por: Redação, 08/05/2018 às 16h12 - Atualizado em 08/05/2018 às 16h13

O Banco Central do Brasil (BACEN) acaba de dar aval no uso de computação em nuvem para as empresas do setor. A Resolução nº 4.658, de 26/4/2018, é sobre a política de segurança cibernética, que estabelece os requisitos para a contratação de serviços de armazenamento e processamento de dados e computação em nuvem, incluindo pontos contratuais mínimos. Com base neste regulamento, os bancos e instituições financeiras autorizadas a funcionar pelo BACEN começarão a usar provedores de nuvem pública de larga escala.

***Fonte**: http://www.decisionreport.com.br/financas/banco-central-do-brasil-libera-uso-de-cloud-computing-no-setor/#.W4mB_K-WyUk*