SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

O REFLEXO DA PANDEMIA NO AUMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

[ver artigo online]

Jean Carlos Moreira Prates[1]
Alax Gomes da Silva[2]
Mario de Matos Piccin[3]
Leonardo Sampaio de Lima[4]
Vinicius Nunes de Freitas[5]

RESUMO

Este artigo é o resultado de uma pesquisa que busca mostrar os incidentes de segurança da informação ao redor do globo durante os anos de 2020 e 2021, com o objetivo de mostrar quais foram os principais incidentes de Segurança da Informação ocorridos durante a pandemia da COVID-19, e o como o evento dessa pandemia pode ter influenciado nesses incidentes. A metodologia utilizada é uma pesquisa bibliográfica, descritiva, exploratória e de natureza pura, sendo utilizados vários relatos de caso sobre o tema. Os resultados mostram um aumento expressivo nas ocorrências de crimes cibernéticos e invasões, condicionados a implementação apressada e pouco planejada de soluções de trabalho remoto por parte das empresas e a falta de informação generalizada acerca do novo coronavírus que permitiu a exploração por cibercriminosos; certos tipos de cibercrimes registrando aumento de até 667%, conforme mostra a empresa de tecnologia Barracuda Networks.

Palavras-chave: Pandemia. Cibercrimes. Segurança da Informação.

ABSTRACT

This article is the result of a research that seeks to show information security incidents around the globe during the years 2020 and 2021, in order to show which were the main Information Security incidents that occurred during the COVID-19 pandemic. 19, and how the event of this pandemic may have influenced these incidents. The methodology used is a bibliographical, descriptive, exploratory and pure research, using several case reports on the subject. The results show a significant increase in the occurrence of cybercrimes and invasions, conditioned to the hasty and unplanned implementation of remote work solutions by companies and the general lack of information about the new coronavirus that allowed exploitation by cybercriminals; certain types of cybercrimes seeing an increase of up to 667%, as shown by the technology company Barracuda Networks.

Keywords: Pandemic, Cybercrimes, Information Security.

1 Graduado em Redes de Computadores, Especialista em Segurança Cibernética, Especialista em Computação Forense, São Paulo, jean.moreira@outlook.com.
2 Especialista em Segurança da Informação/Especialistas em Segurança Cibernética, São Paulo, alax.gsilva@live.com.
3 Coordenador de TI, Especialista em Segurança Cibernética, São Paulo, mario.piccin@gmail.com.
4 Tecnólogo em Redes de Computadores, Especialista em Segurança Cibernética, São Paulo, leonardo.sampaiolima@hotmail.com.
5 Tecnólogo em Gerenciamento de Marketing, Especialista em Defesa Cibernética, São Paulo, vinicius.n.freitas@gmail.com.

http://dx.doi.org/10.35265/2236-6717-228-12308
FORTALEZA-CE. EDIÇÃO 228. V.10. ANO 2022.

INTRODUÇÃO

Durante a pandemia do COVID-19, segundo relatório da consultoria de tecnologia Deloitte, houve um aumento nos incidentes de segurança da informação. O jornal americano The Hill também informa que o FBI declarou um crescimento observado de 300% no número de informe de crimes cibernéticos durante a pandemia. Em maio de 2022 a RNP - Rede Nacional de Ensino e Pesquisa publicou um relatório anual de segurança onde trouxe dados de 2021, no relatório a RNP demonstra como o ano de 2021 assemelha-se ao ano de 2022 no que se refere à continuação da pandemia e seus reflexos na vida das pessoas, ainda mais quando analisamos os impactos tecnológicos. O relatório traz dentre outras informações relevantes, um gráfico comparativo, com dados mostrando o aumento no número de vulnerabilidades médias em sistemas tecnológicos.

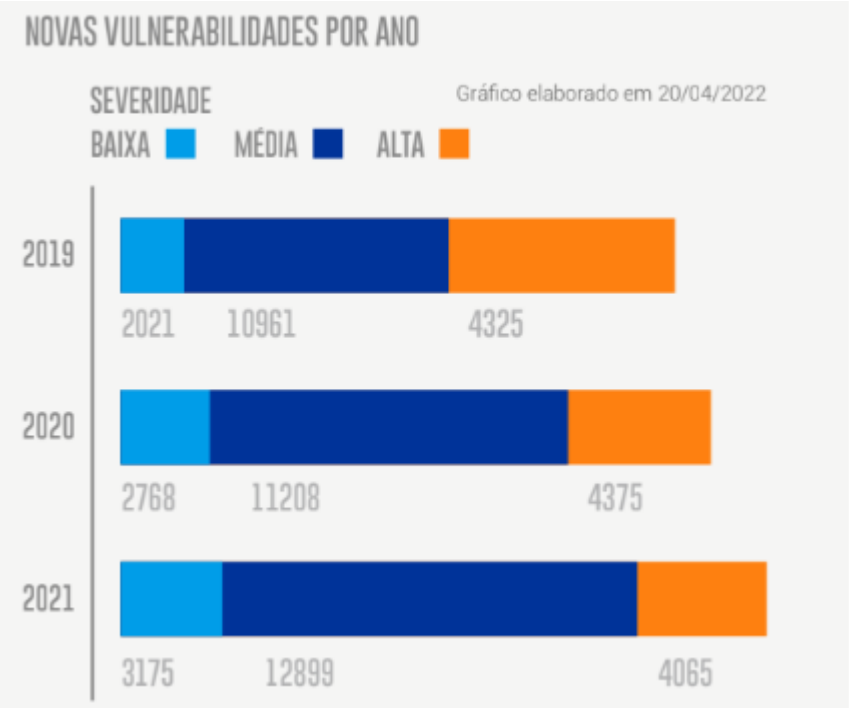

Figura 1- Novas Vulnerabilidades por ano

Fonte: Base Nacional de Vulnerabilidade – Instituto Nacional de Padrões e Tecnologias (EUA)

Plataformas de vídeo conferência, empresas do ramo elétrico e empresas do setor financeiro passaram a enfrentar tentativas diárias de ataques cibernéticos, sendo alguns bem-sucedidos e que foram noticiados em mídias e canais de comunicação.

A seguir, estão descritos o problema de pesquisa, objetivo do tema e justificativa.

Problema de pesquisa: Quais seriam os índices de aumento e os principais incidentes de segurança da informação durante a pandemia da COVID-19 e como a pandemia do novo coronavírus influenciou nesses indicadores?

Objetivo do Artigo: Identificar quais foram os principais incidentes de Segurança da Informação ocorridos durante a pandemia da COVID-19.

Justificativa: O tema justifica-se, pois, quero explicar a correlação entre a pandemia e o aumento de incidentes de Segurança da Informação. Entender como essas influências funcionam pode contribuir para o desenvolvimento de melhores medidas e processos, a fim de prevenir ou mitigar o impacto causado por esse tipo de evento ou incidentes futuros.

REFERENCIAL TEÓRICO

Será apresentado a seguir o material de referência teórica utilizado neste documento. Apresentaremos as definições de um incidente de segurança da informação, com exemplos disso; e depois iremos apresentar as definições do que define uma pandemia, da mesma maneira.

O QUE SÃO INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

De acordo com a UFPEL (2020), um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações (POSIC).

Para UFPEL (2020), são exemplos de incidentes de segurança da informação:

a) Furto de equipamentos que contenham informações institucionais; b) Vazamento de informações não públicas (considerar que esta propriedade pode variar durante o ciclo de vida da informação); c) E-mails enviados sem autorização do remetente a partir do e-mail institucional; E-mails suspeitos não classificados como SPAM que principalmente tenham por finalidade coletar informações pessoais e especialmente credenciais dos sistemas das UFPEL; d) Comprometimento da integridade da informação e perda de informações institucionais.

INCIDENTES DE SEGURANÇA NOTÓRIOS

Neste item será abordado brevemente os incidentes mais famosos, que mais exemplificam a importância e o potencial de estrago que eles possuem.

Os incidentes serão abordados conforme o estudo feito pela CSIS (Center for Strategic & International Studies) no ano de 2020, um renomado "think tank" e uma organização mundialmente reconhecida dedicada ao progresso de ideias para resolver o que definem como os maiores desafios do mundo.

Os critérios que foram usados pela CSIC para definir a notoriedade desses eventos foram os seguintes:

Ataques cibernéticos realizados em empresas de alta tecnologia, órgãos governamentais, incluindo crimes cibernéticos com perdas financeiras maiores que um milhão de dólares.

O período observado pela pesquisa realizada pela CSIS compreende desde o ano de 2006 até o ano de 2020. Destaco neste trabalho apenas alguns desses eventos, com o efeito de apenas exemplificar os de maior escala e notoriedade.

Em novembro de 2008 hackers invadiram a rede do Banco Real da Escócia, permitindo assim que clonassem 100 cartões de caixas eletrônicos e efetuassem saques de mais de 9 milhões de dólares por 49 cidades. Em fevereiro de 2009, devido a uma infecção pelo vírus Confickr, um porta-aviões francês suspendeu os voos de seus aviões.

A suspeita é de que a infecção iniciou a partir de um pendrive USB infectado. Em outubro de 2010, um exemplar de malware altamente complexo chamado Stuxnet foi descoberto no Irã, Indonésia e outros lugares; malware este criado com o propósito de interferir no funcionamento de sistemas de controles industriais. Isto levou a especulações de que se tratava de uma 'arma cibernética governamental' tendo como alvo o programa nuclear Iraniano.

Em maio de 2011, cibercriminosos se passando por membros do grupo de hacktivistas 'Anonymous' invadiram a rede da Playstation (PSN). A Sony estima que informações pessoais de 80 milhões de pessoas foram comprometidas, e de que o custo da invasão foi acima de 170 milhões de dólares.

Em junho de 2013, Edward Snowden, um ex-administrador de sistemas da NSA (National Security Agency) traz à tona documentos que revelam, dentre outras coisas, que os Estados Unidos conduziram cyber espionagem contra alvos chineses. Mais tarde em outubro

do mesmo ano, foi revelado que até mesmo o aparelho celular de Angela Merkel, primeira-ministra da Alemanha, era monitorado.

Em fevereiro de 2016 o órgão responsável pela rede mundial de pagamentos entre bancos (SWIFT - Society for Worldwide Interbank Financial Telecommunication) alertou seus clientes de que estavam vulneráveis a 'ataques sofisticados', tendo testemunhado um 'número significativo' de ataques a seus clientes desde um ataque inicial ocorrido em Bangladesh, dos quais resultaram em roubo de valores. Em março de 2017, Wikileaks revela um conjunto de 'ferramentas hacker' da CIA, datadas entre 2013 e 2016.

Em julho de 2018 o Departamento de Justiça dos Estados Unidos anunciou a acusação de 12 oficiais de inteligência russos de realizar uma operação cibernética de larga escala contra o partido democrata na eleição presidencial de 2016. Os crimes alegados incluíam o roubo e subsequente vazamento de e-mails do comitê de campanha da então candidata Hillary Clinton, e o ataque a alvos de infraestrutura de eleições locais numa tentativa de interferir nas eleições daquele ano.

Em junho de 2019 a China conduz um ataque de negação de serviço (DoS) ao serviço de mensagens Telegram, com o objetivo de interromper a comunicação entre protestantes de Hong Kong.

Em 19 de Agosto a Lojas Renner sofreu um ataque cibernético, o qual levou a rede varejista a ficar com seus canais de venda online fora do ar por pelo menos 48 horas, ainda na semana do incidente a empresa, o Procon-SP disse que notificou a empresa, e solicitou explicações sobre o ataque cibernético. Ainda segundo o Procon-SP, empresa teria que informar quais bases de dados foram comprometidas, e, se informações de clientes foram impactadas.

Na ocasião a companhia alegou não ter realizado nenhum tipo de contato com os criminosos para negociar pagamento de resgate.

Em 17 de Outubro de 2021 a Atento soltou um comunicado informando ter sido vítima de ataque cibernético, a empresa disse ter isolado todos os sistemas envolvidos, além de interromper suas conexões de seus sistemas com os sistemas de seus clientes, ainda segundo o comunicado, a equipe de segurança cibernética da empresa já havia identificado a causa do incidente e estava atuando.

A empresa também relatou no comunicado não ter encontrado evidências de vazamento de dados de clientes.

Abaixo o comunicado publicado pela Atento, traduzido do Inglês:

> Relatórios Atento
> NOVA YORK, 17 de outubro de 2021 – Na Atento SA (NYSE: ATTO, "Atento" ou a "Empresa"), empresa líder em soluções CX e terceirização de processos de negócios (CRM / BPO) na América Latina e um dos cinco maiores provedores em todo o mundo, esta manhã detectamos um ataque de segurança cibernética contra nossos sistemas no Brasil. Imediatamente implantamos todos os protocolos de segurança cibernética disponíveis para avaliar e conter a ameaça.
> Nossa principal prioridade é garantir a proteção e integridade dos dados e sistemas de nossos clientes. A fim de prevenir qualquer possível risco para nossos clientes, isolamos os sistemas envolvidos dentro da Atento e também interrompemos as conexões de nossos sistemas aos de nossos clientes. Isso resultou em uma interrupção temporária do serviço.
> Nossa equipe de segurança cibernética interna e consultores cibernéticos externos foram capazes de identificar a ameaça e estão trabalhando para contê-la e procedendo para garantir a segurança dos ambientes afetados antes de colocá-los novamente online.
> Não encontramos evidências de vazamento de dados do cliente neste momento. Nossas investigações ainda estão em andamento e trabalharão em estreita colaboração com as autoridades competentes.
> No momento desta comunicação, o escopo deste incidente está limitado a algumas operações brasileiras e estamos trabalhando para restaurar o serviço aos nossos clientes o mais rápido possível, sempre garantindo a máxima segurança.

Nestes exemplos, o setor de segurança da informação é prevalente e estratégico em uma série de campos. Desde roubo de dinheiro, o prejuízo e interrupção de negócios, até mesmo como ferramenta de espionagem industrial e governamental; sendo até mesmo objeto de ativismo. E com o passar dos anos o assunto foi ganhando cada vez mais importância.

As consequências de incidentes de segurança da informação podem ter um impacto significativo para os negócios de qualquer corporação, e é hoje reconhecidamente um fator crítico de sucesso de uma empresa.

Dentre as principais consequências destacam-se as perdas financeiras, o vazamento de informações sigilosas da empresa e de seus clientes que podem acarretar em sanções legais, multas e até mesmo a proibição de exercer atividade econômica.

O QUE É UMA PANDEMIA?

Palavra de origem grega, foi usada pela primeira vez por Platão com um sentido genérico, referindo-se a qualquer acontecimento capaz de alcançar toda a população, e o seu conceito moderno é o de uma epidemia de grandes proporções, que se espalha a vários países, em mais de dois continentes, aproximadamente ao mesmo tempo, como foi a Gripe Espanhola, a Influenza H1N1 e, a mais recente, do COVID-19. A maior mobilidade e o número de viagens realizado em todo o planeta são a principal causa pela qual uma pandemia pode ser desencadeada.

De acordo com a Organização Mundial de Saúde, Pandemia é um termo usado para uma determinada doença que rapidamente se espalhou por diversas partes de diversas regiões (continental ou mundial) por meio de uma contaminação sustentada. Neste quesito, a gravidade da doença não é determinante e sim o seu poder de contágio e sua proliferação geográfica.

Afirmou Tedros Adhanom Ghebreyesus, diretor-geral da OMS, durante a proliferação da Covid-19 em março de 2020.

> Pandemia não é uma palavra para ser usada à toa ou sem cuidado. É uma palavra que, se usada incorretamente, pode causar um medo irracional ou uma noção injustificada de que a luta terminou, o que leva a sofrimento e mortes desnecessários (2020 apud SALOMÃO, Elisa, 2020).

HISTÓRICO DAS PANDEMIAS

Nos últimos 30 anos, tem crescido o número de surtos de vírus, proliferando assim as doenças que assolam todo o mundo. Entretanto, relatos históricos de pandemias vão além do século XX e já preocupam a humanidade há dois mil anos.

Um dos primeiros casos de Pandemia registrados é a Peste de Justiniano, acontecida por volta de 541 D.C. e que se iniciou no Egito até chegar à capital do Império Bizantino.

Provocada pela peste bubônica, transmitida através de pulgas em ratos contaminados, a enfermidade matou entre 500 mil a 1 milhão de pessoas apenas em Constantinopla, espalhando por Síria, Turquia, Pérsia (Irã) e parte da Europa. Estima-se que a pandemia tenha durado mais de 200 anos.

Em 1343, a peste bubônica foi mais uma vez a causa de outra pandemia que assolou em sua totalidade os continentes asiático e europeu. A Peste Negra, com o seu auge até o ano de 1353, a Peste ainda apareceu de forma intermitente até o começo do século XIX e matou entre 75 a 200 milhões de pessoas.

Já em 1580, existem relatos da primeira pandemia de gripe, que se espalhou por Ásia, Europa, África e América. Séculos depois, em 1889, a Gripe Russa foi a primeira a ser documentada com detalhes, com proliferação inicial de duas semanas sobre o Império Russo e chegando até o Rio de Janeiro. Ao todo, 1 milhão de pessoas morreram por conta de um subtipo da Influenza A.

Em 1918, a Gripe Espanhola causou a morte de 20 a 50 milhões de pessoas, afetando não só idosos e pacientes com sistema imunológico debilitado como também jovens e adultos. Com possível origem nos Estados Unidos, essa enfermidade quase dizimou as populações indígenas e levou a óbito cerca de 35 mil brasileiros. Com outras variáveis durante o século XX, a gripe ocasionou surtos pandêmicos nos anos de 1957 e 1968. Já em 2009, uma variação da Gripe Suína – anteriormente evitada na década de 70 assolou a América do Norte, África Europa e Ásia Oriental.

Segundo artigo escrito no site da Sanarmed (2020) e em relação ao novo Coronavírus e à mudança de classificação pela OMS, no dia 11 de março de 2020, não se deve à gravidade da doença, e sim à disseminação geográfica rápida que o vírus tem apresentado. “A OMS tem tratado da disseminação em uma escala de tempo muito curta”, afirmou Tedros Adhanom, diretor geral da Organização Mundial da Saúde, quando declarou a mudança de estado da contaminação à pandemia.

Segundo matéria escrita por Elisa Salomão no site Sanarmed (2020), desde 31 de dezembro de 2019, quando a China informou à OMS sobre o vírus desconhecido que estava se espalhando pelo país, a transmissão já se alastrou por mais de 160 países, com mais de 200 mil casos e 9 mil mortes.

Em meio a essa atual pandemia, pode-se fazer uma comparação com os primeiros casos de AIDS, que foram descritos em junho de 1981 e foram necessários mais de dois anos para identificar o vírus causador e, desde os primeiros casos do coronavírus que foram relatados na China em 31 de dezembro de 2019, no dia 7 de janeiro o vírus já havia sido identificado e seu genoma já estava disponível no dia 10 do mesmo mês.

A RELAÇÃO ENTRE A PANDEMIA DA COVID-19 E O AUMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

No ano de 2020 diversos órgãos governamentais, empresas de segurança da informação e veículos de imprensa reportam um aumento significativo de incidentes de segurança da informação.

A jornalista Maggie Miller no jornal americano The Hill (2020), por exemplo, informa em matéria uma declaração do FBI em que houve um aumento de 300% no reporte de crimes cibernéticos em sua divisão especializada do assunto (Internet Crime Complaint Center, ou IC3).

A média normal de reportes de crimes recebidas pelo órgão, normalmente de 1.000 incidentes, saltou para cerca de 4.000. Miller Maggie também escreve outro artigo no jornal The Hill (2020) onde também reporta que um grupo de pesquisadores da empresa de tecnologia Barracuda Networks notaram um aumento de 667% no aumento de crimes de phishing.

Os especialistas que realizaram esses levantamentos notam que os criminosos estão se aproveitando da pandemia para promoverem as referidas campanhas criminosas, aproveitando-se do grande interesse, ineditismo e desinformação generalizada pela população acerca do tema.

DESENVOLVIMENTO

1. Método adotado

A metodologia da pesquisa utilizada foi a pesquisa bibliográfica de materiais disponíveis na internet por diversas instituições que abordam o assunto. Também é uma pesquisa descritiva, que é o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador; segundo Barros e Lehfeld (2007 apud Pós-Graduando, 2012).

2. Relato de casos

No que diz respeito a natureza da pesquisa, foi escolhida por uma de natureza pura. Conforme definição de Assis (2009) o pesquisador pode ter a pretensão de desenvolver novas teorias, criar modelos teóricos novos, estabelecer novas hipóteses de trabalho nos vários campos do conhecimento humano, por meio dos métodos de dedução, indução ou analogia. Esta definição compreende o tipo de natureza de pesquisa utilizado nesse artigo.

Conforme descrito anteriormente, para desenvolver a problemática proposta, foi realizada pesquisa bibliográfica nos principais órgãos e veículos de informação relevante do meio. A intenção é realizar um estudo comparativo dos incidentes de segurança da informação

que ocorreram entre os anos de 2019 e 2020, e a partir de análise e categorização desses eventos, determinar de quais maneiras a pandemia da COVID-19 influenciou nos incidentes atuais.

Os órgãos e veículos de imprensa consultados foram os seguintes:

a) CSIS – Center for Stategic & International Studies
b) Site de notícias The Hack
c) Site de notícias Computerworld
d) Site de notícias Canal Tech
e) Site oficial do Twitter Inc.
f) Site de Notícias Tecmundo
g) Site da empresa Deloitte
h) Site do jornal americano The Hill
i) Site de notícias Infomoney
j) Site de notícias Ciso Advisor
k) RNP - Rede Nacional de Ensino e Pesquisa

Por meio de informações compiladas dessas fontes, foi possível reunir os principais incidentes de segurança da informação ocorridos em 2019 e 2020, e também informações sobre a natureza desses incidentes: quais foram os alvos, os danos envolvidos e informações conhecidas sobre os métodos empregados.

Dentre os diversos incidentes levantados, destacam-se os seguintes por sua magnitude e proporção:

a) Campanha de ransomware paralisou a Honda

De acordo com informações da Kaspersky, que revelou mais detalhes sobre o ataque sofrido pela Honda por obra de um ransomware conhecido como Snake.

Duas fábricas da Honda no Brasil foram atingidas pelo ataque de ransomware, que aconteceu no dia 7 de junho de 2020 e cujas causas ainda estão sendo investigadas. De acordo com a montadora, a unidade de Manaus (AM) teve sua operação interrompida temporariamente, enquanto a de Sumaré (SP) também foi atingida, mas sua capacidade não foi reduzida pois a planta já operava de forma restrita devido à pandemia do novo coronavírus. Em ambas, a situação já foi normalizada.

b) EDP do setor de energia, sofre ciberataque nos Estados Unidos

De acordo com a empresa de segurança Bleeping Computer, a empresa sofreu um ataque ransomware, no qual os criminosos retêm parte dos dados e cobram um valor para devolver ou apagar as informações. No caso, a ameaça utilizada parece ser o Ragnar Locker, do qual os operadores são conhecidos por segmentar entidades corporativas e não o público em geral.

Nesse caso, a nota registrada pelo ransomware exigia 1580 Bitcoin (BTC), ou aproximadamente US$ 10 milhões. Os Ciberataques alertaram a EDP de que mais de 10 TB de informações foram retiradas de sistemas afetados e, como prova, o grupo estava disposto a descriptografar alguns arquivos gratuitamente.

c) Incidente de Segurança: Twitter

Em nota o blog do Twitter esclareceu algumas informações sobre o ataque sofrido em julho de 2020.

> A engenharia social que ocorreu em 15 de julho de 2020, teve como alvo um pequeno número de funcionários através de um ataque de phishing. Um ataque bem-sucedido permitiu que os invasores obtenham acesso à nossa rede interna, bem como credenciais específicas de funcionários que lhes concedessem acesso às nossas ferramentas de suporte interno. Nem todos os funcionários que foram inicialmente alvo tinham permissões para usar ferramentas de gerenciamento de contas, mas os invasores usavam suas credenciais para acessar nossos sistemas internos e obter informações sobre nossos processos. Esse conhecimento permitiu, então, que eles visassem funcionários adicionais que tinham acesso às nossas ferramentas de suporte à conta. Usando as credenciais dos funcionários com acesso a essas ferramentas, os invasores direcionaram 130 contas do Twitter, enfim, tweetando a partir de 45, acessando a caixa de entrada DM de 36, e baixando os Dados do Twitter de 7 delas.
>
> Os hackers acessaram sistemas internos do Twitter em 15 de julho para invadir algumas das principais contas da plataforma, incluindo o candidato presidencial dos EUA Joe Biden, a estrela de TV Kim Kardashian, o ex-presidente dos EUA Barack Obama e o bilionário Elon Musk, e as usaram para pedir doações em bitcoin. (TWITTER.INC., 2020)

d) Natura tinha brecha de segurança que expôs mais de 250 mil clientes

A descoberta foi feita por um time de pesquisadores da Safety Detectives, liderado por Anurag Sen. Dados pessoais e sensíveis de mais de 250 mil clientes da Natura foram expostos

na internet a partir de uma falha em dois servidores da empresa de cosméticos, que está entre as mais reconhecidas do segmento no Brasil. Além de registros identificáveis dos clientes, os volumes também traziam 40 mil tokens de acesso ao Wirecard, sistema de gestão financeira utilizado pela empresa em seu e-commerce, junto com informações de seus usuários, entre consumidores e vendedores de produtos da marca.

Na soma, os dois servidores continham mais de 1,3 TB de dados e 192 milhões de registros sem as devidas proteções de segurança. Dados que poderiam ser usados para identificar usuários diretamente, como nomes completos, endereços, datas de nascimento, gênero, números de telefone e e-mails apareciam ao lado de informações do próprio sistema, como nomes de usuário, senhas criptografadas e cookies de acesso ao site da marca, entre outros.

Já no caso da brecha referente aos dados do Wirecard, as informações revelam histórico de compras, valores pagos e números de IPs utilizados para transações, assim como endereços de e-mail, nomes, datas de nascimento e documentos de identificação. Aqui, também é possível notar dados que pertencem a representantes da Natura, bem como consumidores cujos dados podem ou não estarem entre os 250 mil clientes expostos pela brecha citada anteriormente.

e) Vulnerabilidade no Zoom

Segundo relatório da empresa de cibersegurança Check Point Research. O popular serviço de videoconferência Zoom se encontrava com uma série de vulnerabilidades graves de segurança.

De acordo com as descobertas dos pesquisadores da Check Point, tais vulnerabilidades permitiam aos cibercriminosos gerar e verificar facilmente os IDs do Zoom Meeting para atingir vítimas. Era possível espionar as reuniões do Zoom, com permissões que, se exploradas, davam acesso intrusivo a todos os áudios, vídeos e documentos compartilhados durante todo o tempo de realização da reunião.

A Check Point informou, por meio de comunicado à imprensa, que entrou em contato com a Zoom para compartilhar suas descobertas. Posteriormente, trabalharam juntas para emitir uma série de correções e novas funcionalidades para corrigir as falhas de segurança.

f) Hackers invadem sites de universidades privadas de São Paulo

O TecMundo recebeu a informação via denúncia por uma fonte que assina como "r0ck37m4n". O ataque ao sistema do grupo Laureate International Universities, que controla, entre outras faculdades, a Anhembi Morumbi, foi revelado pelo TecMundo. Segundo o site, o banco de dados com informações pessoais já circulava no mercado de compra e venda desse tipo de informação há pelo menos seis meses.

De acordo com a universidade, hackers tentaram acessar espaços protegidos por login e senha. "Desde que identificou tal tentativa, a Universidade tratou o tema de forma imediata e com todas as providências exigidas pela lei", afirmou a direção da instituição, por meio de nota.

Já no ataque à Universidade Nove de Julho, a princípio, o hacker responsável pela invasão não vazou informações de alunos, mas apenas deixou uma mensagem no site da instituição. O invasor, que se intitula de "elsanninja", deixou a mensagem "menos propaganda, mais segurança" na home por algumas horas.

g) Ataque de ransomware que paralisou a brasileira Light.

A informação foi divulgada publicamente pela própria empresa no dia 18, através de seu perfil no Twitter; o comunicado, porém, não revelou detalhes sobre o incidente, limitando-se a garantir que seu time estaria "agindo para contê-lo" e ressaltando o funcionamento dos canais de atendimento.

O relatório da AppGate, de autoria do pesquisador Gustavo Palazolo, traz fortes indícios de que o malware utilizado contra a Light é o Sodinokibi, também conhecido como REvil. Essa variante foi inicialmente distribuída através de uma vulnerabilidade no WebLogic Server, da Oracle, e chamou atenção por excluir eventuais backups presentes no dispositivo afetado, impedindo assim qualquer tentativa de restaurar os sistemas sem pagar o resgate.

Acredita-se que o Sodinokibi tenha ligações com o Pinchy Spider, nome utilizado para se referir ao indivíduo ou grupo de desenvolvedores que também foram os responsáveis pelo GandCrab, ransomware que causou muita dor de cabeça até que uma ferramenta de decriptação gratuita foi lançada pela BitDefender em parceria com o FBI e a Europol.

3. Análise dos dados coletados

Uma vez as informações sendo definidas, é possível realizar uma análise sobre esses dados.

A primeira questão que é necessário confirmar é a afirmação de que os incidentes de segurança da informação em 2020 cresceram em relação ao ano anterior. Além de constatar que todos os veículos de imprensa, associações e sites de empresas especialistas do setor de segurança da informação citados no início dessa sessão atestam em diversas matérias que houve um aumento sensível na ocorrência de incidentes de segurança da informação.

Quanto a correlação desse aumento de incidentes com a atual pandemia de COVID-19, destacam-se as seguintes hipóteses relatadas a seguir:

a) A implementação de estruturas de trabalho remoto de forma apressada, sem o devido planejamento.

A análise dos dados coletados citados anteriormente ressalta que na maioria das empresas não houve tempo hábil para realizar um correto planejamento de como implementar a estrutura de trabalho remoto para os colaboradores poderem trabalhar de suas casas.

A pandemia ocorreu de forma súbita e se mostrou um evento sem precedente na história contemporânea.

Por consequência disso, muitas soluções de trabalho remoto foram implementadas com o foco principal em fornecer apenas a conectividade, relegando preocupações como a segurança em segundo plano. Isto foi um prato cheio para que justamente cibercriminosos pudessem realizar invasões e ataques de negação de serviço (Denial of Service) a estruturas que antes não estavam disponíveis e dados sensíveis ficassem expostos na internet.

Mesmo a pandemia sendo um evento tão recente e ainda em curso, mesmo ainda sendo muito cedo para se ter a proporção real da quantidade de invasões e incidentes de segurança ocorridos; já é possível notar uma grande preocupação dos especialistas da área de segurança da informação com nesse aspecto.

b) Empregados de companhias trabalhando em regime de home office, longe das estruturas de proteção da companhia.

As empresas já há um bom tempo investem muito tempo e dinheiro na proteção de suas informações, implementando soluções e produtos de tecnologia para realizar a segurança, prevenir invasões e vazamentos e controlar de forma geral quem deve acessar o quê.

E agora com o regime de trabalho em home office, os colaboradores podem potencialmente ficar desguarnecidos de todos os mecanismos de proteção que as corporações implementaram em seus espaços físicos, e assim vulneráveis à toda sorte de riscos e ataques cibernéticos possíveis. Isso é um grande risco que, novamente, muitas corporações que implementaram o trabalho remoto não tiveram tempo hábil de contemplar e aplicar as possíveis medidas de mitigação.

E mesmo em alguns casos, os colaboradores das empresas podem ocasionalmente utilizar equipamentos não homologados para acessar remotamente os recursos de suas empresas, o que também é um outro grande fator de risco.

c) Campanhas de Phishing que se aproveitam da pandemia

Como informado anteriormente, a pandemia é um evento sem paralelo na história contemporânea, além de ser muito recente. O mundo como um todo ainda está estudando e observando este acontecimento, e novas informações, correções e principalmente notícias falsas circulam constantemente. Há um grande clima de temor e incertezas generalizado.

Cibercriminosos se aproveitam disso para realizarem golpes se aproveitando desses fatores, e com isso conseguem enganar suas vítimas obtendo assim informações sigilosas, acesso não autorizado e até mesmo a possibilidade de realizar ataques com softwares maliciosos (malware, ransomware, etc.). A maior parte das notícias relacionadas no início do capítulo atestam este fato.

CONSIDERAÇÕES FINAIS

O objetivo de identificar quais foram os principais incidentes de Segurança da Informação ocorridos durante a pandemia da COVID-19 foi alcançado porquê demonstrei os números e as análises de diversos órgãos e autoridades no assunto que atestam a influência que este evento exerceu sobre o aumento do número de incidentes.

Com base nas informações obtidas no estudo de casos, notou-se um aumento de até 667% nos informes de golpes usando e-mails falsos e de 300% de crimes na internet em geral, esse aumento se deve ao fato de que a pandemia de COVID-19 trouxe a necessidade de ações para

contenção da mobilidade social como isolamento e quarentena por todo o mundo, forçou as empresas a implementarem soluções de trabalho remota de forma desordenada, sem tempo hábil para planejar e até mesmo adequar estratégias de defesa.

Isto fez com que as soluções de trabalho remoto introduzissem novas vulnerabilidades e possibilidades de ataques por parte de cibercriminosos, e também que os trabalhadores remotos, longe das empresas e todas as soluções de defesa implementadas ao longo do tempo, também ficassem mais vulneráveis aos ataques. O próprio evento da pandemia também está em ampla exploração pelos cibercriminosos para aplicar golpes.

Ficou entendido também que este artigo pode apresentar informações importantes para que as empresas entendam a importância de implementar de forma mais sólida soluções de trabalho remoto, que provavelmente farão parte do cotidiano daqui por diante por todas as corporações.

Os incidentes relatados, os números levantados e as análises realizadas neste artigo reforçam o papel cada vez mais importante e estratégico que a segurança da informação exerce em qualquer negócio, em qualquer atividade econômica e até mesmo em entidades, sejam elas governamentais ou não.

REFERÊNCIAS

CANALTECH, Felipe Demartini: Campanha de ransomware focado em empresas paralisou a Honda. Disponível em: https://canaltech.com.br/seguranca/campanha-de-ransomware-focado-em-empresas-paralisou-a-honda-166964/ Acesso em: 05/07/2022.

CANALTECH, Felipe Demartini Natura tinha brecha de segurança que expôs mais de 250 mil clientes. Disponível em: https://canaltech.com.br/seguranca/natura-tinha-brecha-de-seguranca-que-expos-mais-de-250-mil-clientes-165118/ Acesso em: 08/07/2022

COMPUTERWORLD, Redação: Check Point descobre vulnerabilidades graves no app Zoom. Disponível em: https://computerworld.com.br/2020/01/29/check-point-descobre-vulnerabilidades-graves-no-app-zoom/ Acesso em: 18/07/2022

COMPUTERWORLD, Redação: EDP, do setor de energia, sofre ciberataque nos Estados Unidos. Disponível em: https://computerworld.com.br/2020/07/08/edp-do-setor-de-energia-sofre-ciberataque-nos-estados-unidos/ Acesso em: 18/07/2022

CISO ADVISOR, Atento publica comunicado ao mercado sobre ataque. Disponível em: https://www.cisoadvisor.com.br/atento-publicou-comunicado-ao-mercado-sobre-ataque/ Acesso em: 18/08/2022

CSIS. Significant Cyber Incidents. Disponível em: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents Acesso em: 18/07/2022

DELOITTE, Tope Aladenusi: COVID-19’s Impact on Cybersecurity. Disponível em: https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html. Acesso em: 25/07/2022

INFOMONEY, Incidente Lojas Renner comunica restabelecimento de app e e-commerce após ataque hacker e diz que não fez contato com autores. Disponível em:

https://www.infomoney.com.br/negocios/lojas-renner-comunica-restabelecimento-de-app-e-e-commerce-apos-ataque-hacker-e-diz-que-nao-fez-contato-com-autores/
Acesso em: 18/08/2022

MILLER, Maggie: Cyber threats spike during coronavírus pandemic. Disponível em: https://thehill.com/policy/cybersecurity/490232-cyber-threats-spike-during-coronavirus-pandemic. Acesso em: 25/07/2022.

MILLER, Maggie: FBI sees spike in cybercrime reports during coronavírus pandemic. Disponível em: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic. Acesso em: 25/07/2022.

PÓS-GRADUANDO. As diferencias entre pesquisa descritiva, exploratória e explicativa. Disponível em: https://posgraduando.com/diferencas-pesquisa-descritiva-exploratoria-explicativa/ Acesso em: 11/08/2022

RNP, Confira o Relatório Anual de Segurança de 2021. Disponível em: https://www.rnp.br/noticias/confira-o-relatorio-anual-de-seguranca-de-2021
Acesso em: 18/07/2022

SALOMÃO, Elisa. Pandemia, epidemia e endemia: significados e diferenças. Disponível em: https://www.sanarmed.com/epidemia-endemia-e-pandemia-seus-significados-e-suas-diferencas-colunistas Acesso em: 11/08/2022

SANAR SAÚDE. Pandemias na História: o que há de semelhante e de novo na Covid-19. Disponível em: https://www.sanarmed.com/pandemias-na-historia-comparando-com-a-covid-19
Acesso em: 10/07/2022

TECMUNDO. Dados de 1,3 milhão de alunos e docentes da Anhembi Morumbi foram expostos. Disponível em: https://www.tecmundo.com.br/seguranca/155586-dados-1-3-milhao-alunos-docentes-anhembi-morumbi-expostos.htm.
Acesso em: 18/07/2022

THE HACK, Ramon de Souza: Tudo sobre o ataque de ransomware que paralisou a brasileira Light. Disponível em: https://thehack.com.br/tudo-sobre-o-ataque-de-ransomware-que-paralisou-a-brasileira-light/
Acesso em: 21/07/2022

TWITTER.INC. Uma atualização sobre nosso incidente de segurança. Disponível em: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.
Acesso em: 18/07/2022

UFPEL. Reportar Incidente de Segurança. Disponível em: https://wp.ufpel.edu.br/seginfo/reportar-incidente-de-seguranca/
Acesso em: 10/07/2022