CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

Nicollas Albert Araújo
Paulo César Pinheiro da Câmara Neto
Pedro Paulo da Câmara do Nascimento

O CRESCIMENTO DOS ATAQUES CIBERNÉTICOS NAS EMPRESAS

RECIFE/2021

Nicollas Albert Araújo
Paulo César Pinheiro da Câmara Neto
Pedro Paulo da Câmara do Nascimento

O CRESCIMENTO DOS ATAQUES CIBERNÉTICOS NAS EMPRESAS

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Msc Ameliara Freire Santos de Miranda

RECIFE/2021

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

A663c Araújo, Nicollas Albert
O crescimento dos ataques cibernéticos nas empresas. / Nicollas Albert Araújo, Paulo César Pinheiro da Câmara Neto, Pedro Paulo da Câmara Nascimento. Recife: O Autor, 2021.
32 p.

Orientador(a): (Msc) Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2021.

Inclui Referências.

1. Ataque cibernético. 2. Hackers. 3. Crackers. 4. Prejuízo. 5. Empresa. I. Câmara Neto, Paulo César Pinheiro da. II. Nascimento, Pedro Paulo da Câmara. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

Dedicamos esse trabalho a nossos pais.

AGRADECIMENTOS

Agradecemos a todas as pessoas especiais que estivaram ao nosso lado durante essa árdua caminhada até a conclusão do curso, como nossos familiares e amigos, que sempre nos apoiaram.

Um Agradecimento em especial a Luís Henrique Negromonte e Murilo Freire por toda ajuda e apoio durante o desenvolvimento do trabalho.

À nossa orientadora Prof.ª Ameliara Freire Santos de Miranda, que nos ajudou bastante trazendo *feedbacks* importantes para o andamento do trabalho, e também agradecemos aos demais membros do corpo docente do Curso.

“Toda ação humana, quer se torne positiva ou negativa, precisa depender de motivação.”

(Dalai Lama)

O CRESCIMENTO DOS ATAQUES CIBERNÉTICOS NAS EMPRESAS

Nicollas Albert Araújo
Paulo César Pinheiro da Câmara Neto
Pedro Paulo da Câmara do Nascimento
Ameliara Freire Santos de Miranda

Resumo: Com o avanço tecnológico e o crescimento do ciberespaço, este trabalho busca apresentar, por meio de casos reais em fontes secundárias e pesquisas bibliográficas, o crescimento exponencial dos ataques cibernéticos a empresas. Ele vai mostrar as principais formas de ataques que visam comprometer os pilares da segurança da informação e os prejuízos econômicos causados ao longo dos anos. Apresentando também algumas contramedidas/precauções que podem ser tomadas em relação aos ataques, na tentativa de prevenir ou, pelo menos, reduzir os danos causados.

Palavras-chave: Ataque cibernético, *hackers*, *crackers*, prejuízo, empresa.

Abstract: With the technological advancement and growth of the cyberspace, this work seeks to present, through real cases in secondary sources and bibliographical research, the exponential growth of cyber attacks in companies. It will show the main forms of attacks that aim to compromise the pillars of security of information and the economic damage caused over the years. Also presenting some countermeasures/precautions that can be taken in relation to attacks, in an attempt to prevent or, at least, reduce the damage caused.

Keywords: Cyber attack, hackers, crackers, damage, company.

LISTA DE FIGURAS

LISTA DE SIGLAS

AMAP	*Application Mapper*
CID	Confidencialidade, Integridade e Disponibilidade
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
GDPR	*General Data Protection Regulation*
IDS	*Intrusion Detection Systems*
IP	*Internet Protocol Address*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
NMAP	*Network Mapper*
URL	*Uniform Resource Locator*

SUMÁRIO

1 INTRODUÇÃO

O avanço tecnológico trouxe várias facilidades, tanto para a sociedade como para as organizações de grande, médio e pequeno porte, onde a Internet se tornou um dos meios essenciais para a sua consolidação no mercado, seu crescimento da marca e consequentemente gerando um aumento lucrativo. Porém também trouxe uma necessidade de atenção maior para os *crackers* criminosos, que são indivíduos dispostos a roubar seus dados e de seus usuários e lhes trazer prejuízos enormes (NAKAMURA, E.; GEUS, P. 2007).

Diferente de *hackers* que é definido por Ramalho Terceiro (2002) como alguém possuidor de grandes habilidades em computação, e geralmente usam essas habilidades sem intuito de prejudicar ninguém, os *crackers* utilizam seus conhecimentos para atacar computadores de empresas e usuários comuns (SILVA, 2018). As grandes empresas invadidas por *crackers* descobriram, da pior maneira, que negligenciar a segurança pode sair muito mais caro do que investir em sistemas de proteção (HSC BRASIL, 2019).

O principal fator de empresas serem um alvo constante de ataques é o financeiro (ZIMMER, 2020), seja através de um sequestro de dados, onde o pagamento por meio de moedas digitais é solicitado, ou até mesmo por ataque de vírus, invasão, roubo de senha, entre outros métodos e ferramentas que visam explorar seus alvos, pois “todo funcionário da empresa que utilize um computador, um dispositivo de rede, um *tablet* ou um telefone é um alvo em potencial” (LISKA e GALLO, 2017, p. 111).

Um caso de prejuízo que pode ser gerado por esses ataques é de uma das principais empresas do segmento de videogames, onde em 2011 teve sua rede invadida por *crackers*, ocasionando um roubo de dados pessoais e de cartão de crédito de mais de 78 milhões de usuários e deixando o sistema *offline* por 23 dias. Em 2014 a companhia foi alvo de outro ataque, só que dessa vez foi um ataque DDoS (*Distributed Denial of Service*) (HSC BRASIL, 2019).

De acordo com o relatório “*Cybersecurity - Fighting Invisible Threats*”, do banco suíço *Julius Baer*, em 2021, os crimes cibernéticos chegarão a custar US$ 6 trilhões à economia global. Segundo a consultoria *Cybersecurity Ventures,* em 2015, houve somente metade desse montante. O Brasil aparece em décima posição dos países mais prejudicados com US$ 7 milhões desperdiçados. Todos os dias, são perpetrados 8 trilhões de ataques pelo mundo (MOURA; HAIDAR, 2020).

1.1 OBJETIVO

Dado o cenário exposto, o objetivo deste trabalho é mostrar um possível crescimento dos ataques cibernéticos nas empresas ao longo dos anos e os principais ataques que são usados. Serão utilizados exemplos de casos reais obtidos por outras fontes e frisar a importância de uma atenção e investimento maior na segurança de seus dados.

1.2 METODOLOGIA

A metodologia usada para embasar esse trabalho será a pesquisa bibliográfica, realizada por meio de livros, revistas, artigos e fontes secundárias para que fosse possível a obtenção de uma grande quantidade de informações que pudesse enriquecer a pesquisa.

2 REFERENCIAL TEÓRICO

Este capítulo consiste em uma base teórica de acordo com os problemas abordados.

2.1 SEGURANÇA

Segundo Nakamura e Geus (2007), nos tempos atuais, a informática está praticamente em quase tudo que utilizamos, ajudando, otimizando e dando mais eficiência nas atividades elaboradas. Na rede, temos vários elementos conectados que vão de um mero roteador até o servidor de uma empresa, possibilitando acesso ao banco de dados com informações dos clientes vinculados, tendo privilégio a todos os dados pessoais/financeiros. As empresas que têm disponibilidade, integridade e confiabilidade em sua rede necessitam de mais proteção de suas informações. Essa proteção visa a manutenção das informações concedidas aos usuários de forma íntegra e confiável.

Assim, a segurança de redes é um fragmento fundamental para proteger as informações através da disponibilidade, integridade e discrição, resultando em um trabalho muito maior que proteger os sistemas apenas contra *crackers*, funcionários desleais ou vírus, pois também irá permitir que as empresas lucrem cada vez mais com as novas chances para negócios. Essas novas oportunidades são conseguidas devido a evolução da Internet e segurança, abrindo espaço para maior flexibilidade, facilidade e disponibilidade das informações inseridas nos sistemas (NAKAMURA, E.; GEUS, P. 2007).

As organizações deveriam encarar a segurança dos seus sistemas como algo primordial, visando maior lucratividade através da liberdade em acessar redes sem nenhum receio de ter ataques de *crackers*. No entanto, as organizações não dão a mínima atenção a este fato, por não visar a importância da liberdade em acessar sites sem medo de ataques de *crackers*. Um exemplo desses ataques foi no ano de 2000, que aconteceu um fato que gerou repercussão em toda mídia internacional. Foram os ataques distribuídos de negação de serviços que deixaram grandes empresas multibilionárias de busca e comércio online, fora do ar. Segundo a *Yahoo* os prejuízos mundiais em formato de capital, receita e com atualizações de segurança chegaram a 1,2 bilhões de dólares (NAKAMURA, E.; GEUS, P. 2007).

2.1.1 Medidas de Segurança no Ambiente Empresarial

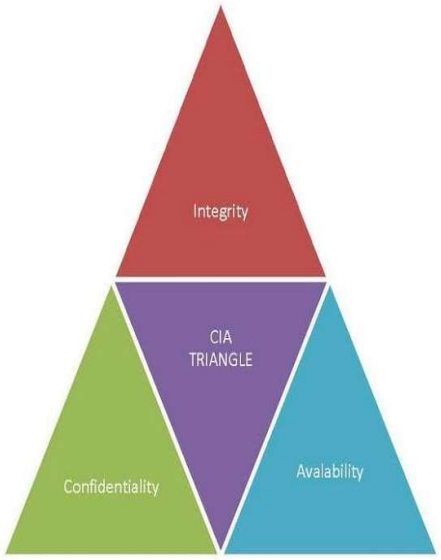
Para Baars et al. (2018) a segurança se refere a proteção e defesa de dados que, quando interpretados, se transformam em informações valiosas, tanto para um usuário comum como para uma empresa de pequeno, médio e grande porte. Portanto, sua segurança é de extrema importância para aqueles que os interessam. Através de implementações de políticas, processos, procedimentos de um conjunto adequado de controles que possam assegurar a integridade desses dados. Essas implementações devem ser estudadas e aplicadas em conjunto com outros processos de gerenciamento de negócio. Um bom gerenciamento e controle da segurança da informação pode ser essencial para abrir vantagem comercial perante seus concorrentes. Em contrapartida, uma má administração dela se torna a sua ruína iminente.

De acordo com a ISO 27002:2013, é importante entender os requisitos implementados na organização e a necessidade de estabelecer novas políticas e objetivos para a segurança da informação, controlar os riscos da informação das organizações, monitorar e revisar se realmente está sendo eficiente o Sistema de Gerenciamento de Segurança da Informação e estabelecer uma melhoria contínua baseada em medições objetivas (BAARS, et al. 2018).

2.1.2 Pilares da Segurança da Informação

Na Segurança da Informação existem três pilares fundamentais que precisam ser aplicados, respeitados e bem assegurados, que são conhecidas como a Tríade CIA (CID em português), que consiste em Confidencialidade, Integridade e Disponibilidade, conforme Figura 1: (BAARS, et al. 2018)

Figura 1. O triângulo *CIA*.



Fonte: PPETERS, 2011

2.1.2.1 Confidencialidade

A confidencialidade atua como um limitador de quem pode acessar e obter diferentes tipos de informações de acordo com as necessidades de cada setor da organização. Algumas formas bastante comuns de implementação da confidencialidade são através da criptografia de dados, preenchimento de tráfego (*traffic padding*), controle de acesso, além do próprio treinamento com o usuário de como acessar os dados que ele necessita e dos procedimentos apropriados (BAARS, et al. 2018).

2.1.2.2 Integridade

A integridade preza que os dados não sejam alterados de forma não autorizadas, mesmo que um dado seja incorreto ou não autêntico. Ele pode possuir integridade intacta, embora incorreto. Mas, se houver alterações não autorizadas, mesmo que seja para corrigir tal erro, o dado já não possui mais integridade (BAARS, et al. 2018).

Um erro bastante comum que os usuários praticam e acaba dando bastante dor de cabeça nas organizações é a quebra de integridade em um banco de dados. Uma alteração não autorizada em um banco de dados pode desencadear uma série de

erros que se a organização não estivar precavida com um *backup*, por exemplo, vai ser difícil de arrumar rapidamente (BAARS, et al. 2018).

2.1.2.3 Disponibilidade

A disponibilidade deve contar com três características indispensáveis para seu funcionamento correto, elas são: (BAARS, et al. 2018)

a) Oportunidade: A informação deve estar disponível quando solicitado.
b) Continuidade: Mesmo em casos de erro, a equipe deve conseguir continuar com seu trabalho.
c) Robustez: Deve comportar toda a equipe de trabalho, independente do seu tamanho.

Uma técnica comum para auxiliar a disponibilidade contínua do serviço é a de *backup* dos dados, precavendo ataques virtuais e até mesmo erros de *hardware*. Negação de serviço (DoS) é um método popular que *crackers* utilizam para interromper a disponibilidade do sistema da empresa. E cuidados devem ser aplicados para que não haja uma interrupção, como sistemas de detecção de intrusão (*Intrusion Detection Systems* – IDS) para monitorar o tráfego de rede e as máquinas. Um *firewall* e roteador bem configurados também conseguem dificultar bastante um ataque DoS (BAARS, et al. 2018).

2.2 ATAQUES

Os ataques são feitos com frequência e muitos ataques antigos ainda estão em funcionamento hoje. Isto indica que as empresas, tanto brasileiras como estrangeiras, ainda têm vulnerabilidade e estão devendo bastante em termos de segurança cibernética. Com a criação da Internet, as empresas ficam vulneráveis a ataques de "piratas cibernéticos" devido a visão restrita dos que gerem os sistemas. Isso ocorre por acreditarem que não estão suscetíveis a ameaças externas pela segurança das suas "caixas-pretas", tranquilizando-se com a ideia de que ninguém vai descobrir sua sistemática. Portanto, não investem em defesas básicas em seus processos de rede, ocasionando diversos ataques por meio de muitas ferramentas, visando a obtenção de dados e causando infortúnios e prejuízos para a organização (DERTOUZOS, 1997).

O primeiro passo para se perceber ou desconfiar que um ataque está sendo realizado é entender um pouco suas armadilhas. Um pouco de compreensão pode acabar sendo bastante útil e eficaz para escapar de um ataque. Existem diversas formas para que seja feito uma invasão e sequestro de dados, sendo algumas delas: (UNYLEYA, 2021)

Backdoor: é um tipo de cavalo de Troia. Concede ao invasor o acesso ao sistema infectado, permitindo ser controlado e, assim, conseguindo mexer em arquivos, dados e programas da máquina da vítima.

Phishing: É um método social que se aproveita da confiança para roubar os dados da vítima. Se passam por uma instituição ou pessoa legítima, assim conseguem pegar os dados e clonar documentos, cartões, entre outras coisas.

Spoofing: é um golpe que o atacante falsifica o endereço de IP do DNS. Esse golpe é utilizado para roubar informações confidenciais, agindo como se fosse a vítima que foi invadida usando os dados de um falsificador.

Manipulação de URL: esse ataque faz o servidor transmitir páginas que não são autorizadas para que o usuário coloque seus dados e, assim, acontecendo a captura.

Eavesdropping: o *cracker* utiliza diferentes formas para capturar os dados, mandando *e-mails* falsos, mensagem de texto e até ligações para confirmação de dados, assim conseguindo executar o golpe.

Decoy: nesse ataque, a pessoa faz *login* ou tenta se cadastrar numa interface pirata onde todos os dados colocados são coletados pelos invasores. Trabalha muito bem em conjunto com a manipulação de URL.

Os *scanners* são programas que irão descobrir as opções do sistema operacional e se ele contém algo para ser exposto e que esteja desprotegido. São chamados também de varreduras, onde os administradores vão criar instrumentos de segurança mais acertados e com propósito. Podendo destacar: *Nmap, Amap, Netcat* e *Hping*, como alguns dos *scanners* existentes (MELO, 2017).

A quebra de senhas de usuários consiste em várias combinações possíveis de caracteres na busca de encontrar uma senha/chave. São utilizados quatro tipos de ataques: (MELO, 2017)

a) Manualmente: são coletadas informações do sistema e arriscando códigos comuns, sendo uma forma com baixa efetividade;
b) Dicionário: é um tipo de mecanismo que utiliza várias palavras/caracteres de um certo dicionário. Esse tipo de ataque pode ser executado com *rainbow tables*;
c) Força bruta: são ataques fundamentados em dicionário ou função randômica utilizado para derrubar senhas, cifras e credenciais de usuários de uma rede. Facilmente reconhecida por cada investida no sistema que irá gerar uma linha de *log*;
d) Híbrido: é um conjunto empregado constituído por dicionário e força bruta ao mesmo tempo.

Uma das piores vulnerabilidades, e aquelas que mais dão dor de cabeça, são as conhecidas vulnerabilidades "*zero-day*", pois são vulnerabilidades descobertas e exploradas antes que forneçam uma correção. Um *cracker* ético, ao descobrir determinada brecha, poderia avisar ao fornecedor evitando a invasão pela mesma. A divulgação na Web, antes de qualquer correção, acarretará em vários *crackers* mal-intencionados explorando e invadindo (MELO, 2017).

Os ataques DDoS (*Distributed Denial of Service* - Negação de Serviço Distribuída) foram bastante explorados entre a época de 1999 e 2001. Mesmo sendo um ataque com um tempo considerável no mercado, ainda hoje ele é utilizado e com bastante eficácia. Seu objetivo é exclusivamente "derrubar" por completo um serviço ou servidor. Diferente do DoS, os ataques não são baseados em um único computador, é utilizado centenas ou até milhares de computadores desprotegidos e com acesso à Internet para que o ataque seja feito coordenadamente, ocasionando em um ataque em grande escala de forma remota. Esses computadores que participam do ataque DDoS geralmente são computadores de usuários comuns, que estão sendo controlados após serem infectados por um *trojan* ou *worm* (MELO, 2017).

2.3 FATOR HUMANO

Segundo Mitnick e Simon (2002), a maior vulnerabilidade de uma empresa a ataques *crackers* é o fator humano, seja explorando a inocência ou ignorância do indivíduo que tem uma falsa sensação de segurança por causa de um simples antivírus e *firewalls*. Às vezes esses ataques vêm fisicamente, onde o *cracker* consegue convencer algum colaborador da empresa a acessar tais informações, seja por chantagem, pela confiança que o *cracker* obteve do usuário, ou até mesmo por falta de conhecimento.

Existem diversos meios que o atacante pode entrar em contato com a vítima, como, por exemplo, por meio direto, ou de uma ligação. Mas um dos principais ataques, principalmente a usuários mais leigos, são os sites falsos e anexos infectados, um *e-mail* se passando de cliente enviando dados que normalmente são pedidos pela empresa e com um simples clique, o vírus está impregnado no computador, podendo abrir portas para outros tipos de vírus além do executado, comprometendo toda a rede organizacional. Se não houver um gerenciamento de segurança eficaz implementado na empresa, será necessário um gasto adicional para tentar resolver o problema, porém o ataque age muito rápido, podendo ser muito tarde em poucos segundos, levando dados importantes que geram prejuízos bilionários (MITNICK; SIMON, 2002).

2.4 ESPIONAGEM CIBERNÉTICA

Segundo Marcondes (2020) esses ataques não vêm somente de usuários comuns que fazem isso por benefício próprio, alguns desses ataques também são provenientes de outras empresas com o intuito de espionagem industrial, como, por exemplo, a *Procter & Gamble* ao tentar espionar a *Unilever* ou até mesmo a Motorola denunciando a gigante *Huawei* por espionagem. Sendo um tipo de espionagem mais comum do que se pode imaginar, geralmente com o objetivo de estar sempre a um passo à frente de sua concorrente e, por consequência, se tornar referência no mercado.

As principais formas de espionagens são: (MARCONDES, 2020)

a) Coleta de dados;
b) Vigilância velada;
c) Vírus de computador;
d) Engenharia social;
e) Grampo ilegal;
f) Entre diversas outras formas mais.

Porém essa espionagem, financiada por uma organização para obter dados e vantagens sobre a concorrente, de acordo com a lei de número 9.279/1996, Art. 195. (Lei da Propriedade industrial) se caracteriza como crime, como por exemplo:

> a divulgação, exploração ou utilização, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato; (PLANALTO, 1996).

Podendo acarretar numa detenção de três meses a um ano, ou uma multa.

2.5 TECNOLOGIA NO BRASIL

Tanto o Brasil como no mundo, a conexão e dependência ao acesso à Internet para poder realizar suas atividades do dia a dia está cada vez mais evidente. Seja para trabalho, lazer, compras, hoje se consegue fazer praticamente tudo com um celular em mãos. Contudo, esse aumento exponencial carrega consigo um aumento nos casos de crimes cibernéticos, levando a prejuízos para usuários comuns como também para as empresas. Porém o Brasil ainda sofre bastante para impossibilitar ou, pelo menos, diminuir as ocorrências de ataques *crackers* no país, ocupando a liderança nos envios de *spams* da América Latina, por exemplo. Em 2017, com a propagação do ciberataque *Ransomware*, o Brasil foi o país latino-americano mais

afetado, com a margem de 55% dos ataques direcionados ao país (SILVA; MÈRCHER, 2017).

Graças a toda essa insegurança que o acesso à Internet passa não só para os brasileiros, mas para todos, existe um medo constante de levar algum golpe, ser *hackeado* e ter seus dados e dinheiro roubados. Com isso, uma parcela de pessoas opta em não fazer suas compras e transações online, prejudicando o lucro de empresas, principalmente as que contém um foco exclusivo em vendas ou serviços online (CERNEV; LEITE, 2021).

A impunidade aos infratores cibernéticos é algo bastante presente, “Hoje no Brasil existem apenas 4 leis que qualificam os crimes cibernéticos no país sendo, Estratégia de Defesa Nacional de 2008, especificamente o decreto 6703. Lei Azeredo (PL 84/99) Projeto de lei de Crimes Digitais de 2008. Lei Carolina Dieckmnann (PL 2793/11) e o Marco Civil da Internet de (PL 12.965/14).” Sendo ainda sim possível encontrar brechas para que se possa realizar ataques sem serem punidos, levantando inclusive pauta para que sejam criadas novas leis para amenizar essas brechas e se proteger também de ataques vindos de fora do país (SILVA; MÈRCHER, 2017).

Ao perceber a importância na reestruturação e políticas de segurança, as empresas passaram a buscar uma melhor forma de se proteger dos ataques, investindo mais na segurança dos seus dados e de seus clientes. Contudo, essa busca é dificultada pelo fato da maioria das soluções serem desenvolvidas fora do país e ao, serem importadas, acabam não sendo uma opção muito viável, financeiramente falando, principalmente para as pequenas empresas, abrindo as portas a uma realidade conhecida e antiga que se propagou quase como uma forma cultural que foi a prática à pirataria, utilizando formas ilícitas para se ter acesso a tal *software*[1] acaba abrindo portas para vários tipos de vírus, trazendo um prejuízo maior do que o preço da assinatura da mesma (SILVA; MÈRCHER, 2017).

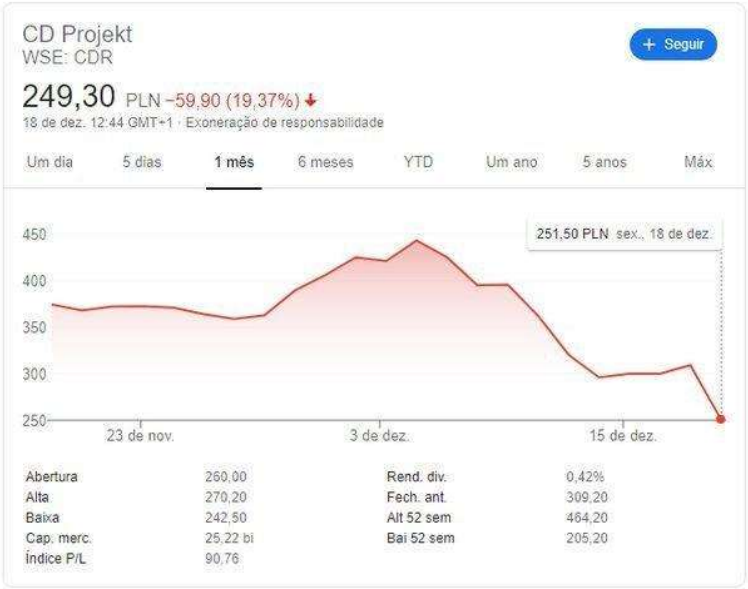
2.6 INVASÕES

A todo momento um ataque *cracker* está sendo executado com intuito de invadir alguma organização. Uma das vítimas desses ataques foi a uma empresa polonesa voltada para jogos. Em fevereiro de 2021, a empresa se deparou com uma surpresa ao notar que *crackers* invadiram sua rede interna e sequestraram seus dados dos servidores. Com isso, os criminosos tiveram acesso aos dados dos usuários, além do código fonte dos seus jogos de sucesso, e também ao jogo de lançamento recente na época, executando uma cópia das informações para uma fonte externa e tentaram chantageá-los para que eles pudessem recuperar os dados

[1] Software: Coleção de dados ou instruções que informam a um mecanismo como trabalhar;

perdidos ou eles iriam divulgar todos os dados na Web. A invasão não poderia ter sido feita numa época pior, já que a empresa estava passando por uma queda nas ações de mais de 20% após o lançamento conturbado do seu último jogo. A empresa informou que não iria negociar com os criminosos, deixando que a polícia, juntamente com sua equipe de segurança da informação, cuidassem do caso. O que minimizou, de certa forma, os danos causados por essa invasão, foi o fato de a empresa ter em sua posse um *backup* dos dados, além de seu posicionamento forte não cedendo para os criminosos. A empresa polonesa não tinha sido a única empresa de jogos a ser alvo desses ataques. Tanto ela como outras duas do mesmo ramo também foram alvos de ataques *Ransomware* (RIGUES, 2021). Na Figura 2 mostra a queda em suas ações graças aos acontecimentos:

Figura 2. Ações da Empresa Polonesa.



Fonte: WAKKA, 2020

No Brasil, em 2008, aconteceu um caso envolvendo uma empresa brasileira principal responsável pelo transporte de petróleo, onde houve sumiço de discos rígidos e *notebooks* com informações sigilosas sobre o Pré-Sal. Inicialmente foi levantada a hipótese de uma espionagem industrial, posteriormente desmentida pela Polícia Federal quando os mesmos encontraram praticamente todo o material com quatro suspeitos na zona portuária do Rio de Janeiro (CARVALHO, 2012).

3 APROFUNDAMENTO

3.1 ATAQUES CIBERNÉTICOS

Com o avanço tecnológico e globalização, os dados e informações fluem de forma muito rápida. E, por meio disso, involuntariamente se foi criando uma nova concepção chamada “espaço cibernético”, que para Oliveira (2017) o “espaço cibernético” contém três características:

1. Se encontra em uma dimensão intangível e abstrata;
2. Considerada importante desde o início da sua existência;
3. É transversal.

Junto a esse espaço cibernético criado, que, segundo Klimburg (2012) vai além de *hardware*[2] e *software,* também conta com interações sociais humanas e a troca de informações, veio a preocupação com os ataques cibernéticos, que visam violar os três pilares principais da segurança da informação: confidencialidade, disponibilidade e integridade.

Segundo o governo do Estados Unidos, uma atividade cibernética maliciosa é definida como:

> Atividade cibernética maliciosa é qualquer atividade, desautorizada ou em desacordo com a lei dos EUA, que busca comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de computadores, sistemas de informação ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informação, ou as informações nele contidos (CEA, 2018, p. 2 *apud* SILVA, 2018, p.19).

No Brasil, no entanto, para o Ministério de Defesa, ataques cibernéticos são “ações que objetivam interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014a, p.23 *apud* SILVA, 2018, p.19).

3.2 RANSOMWARE

Um dos ataques cibernéticos utilizados contra empresas que é bastante difundido até hoje é o *Ransomware*[3] que teve sua primeira grande aparição na mídia em 12 de maio de 2017 quando um *Ransomware* denominado “*WannaCry”* atingindo 45 mil máquinas. Como foi um ataque repentino, como o COVID-19, ninguém estava preparado para essa infestação em massa. Como pode ser observada na Figura 3, ela continuou se propagando e demorou apenas cinco dias para chegar à casa de 345 mil

---

[2] *Hardware:* Componente ou equipamento físico, diferente de *software*, o *hardware* é algo palpável;

[3] Ransomware: ameaça que bloqueia o seu computador restringindo seu acesso e depois exige um resgate para que a vítima possa acessar seus dados novamente, geralmente o valor do resgate é pedido em BitCoin;

máquinas em mais de 150 países diferentes, atingindo empresas de todos os portes (OLIVEIRA, 2018). O valor inicial para o resgate dos dados era de US$ 300 dólares em *BitCoin*[4], ou um valor ainda maior dependendo do valor dos dados obtidos. Porém esse valor aumentava se o pagamento não fosse realizado em até duas horas. O curioso a se notar nesse caso é que a brecha no *Windows* para esse ataque já tinha sido identificada e corrigida desde 14 de março do mesmo ano, conhecida como a falha "*EternalBlue",* porém entra aqui novamente o fator humano. Por desleixo e falta de conhecimento, não atualizaram seus sistemas operacionais, permitindo que aquela brecha pudesse ser explorada (OLHAR DIGITAL, 2019). O primeiro indício foi notado no Sistema Público de Saúde do Reino Unido, inclusive o sistema hospitalar e os meios de telecomunicações, foram os alvos mais recorrentes do ataque. O Instituto Norte-Americano, localizado em *Wichita*, pagou em torno de US$ 17.000 dólares para que os criminosos liberassem seus dados sobre os pacientes, um valor semelhante também foi pago por outras instituições do setor de saúde (OLIVEIRA, 2018).

Figura 3. *Ransomware* pelo mundo

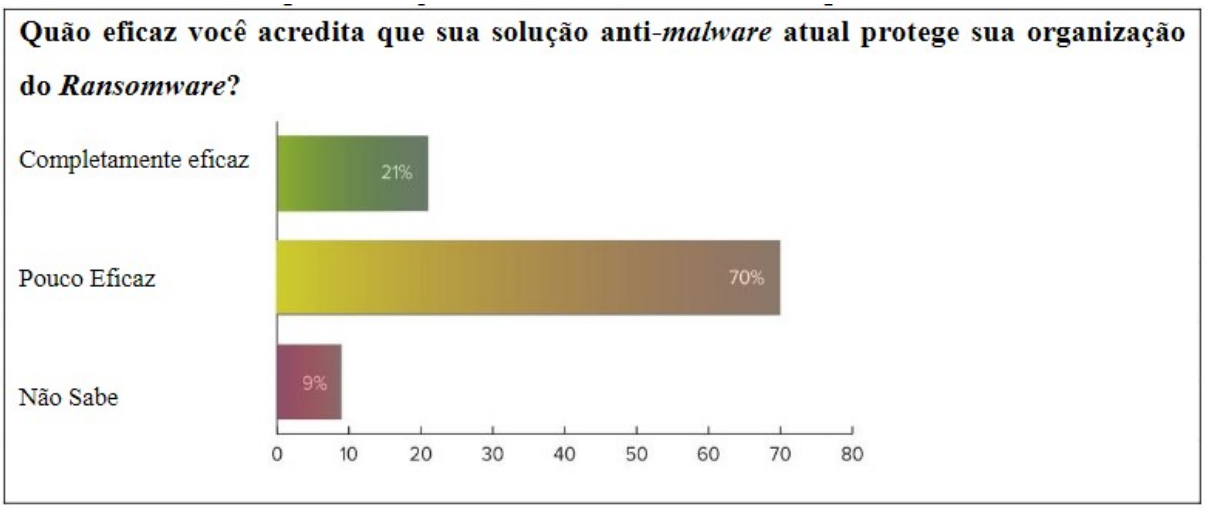
Fonte: OLHAR DIGITAL, 2019

Algumas empresas brasileiras de telecomunicação também foram afetadas pelo *Ransomware*, além de alguns serviços públicos. Estima-se que o impacto financeiro provocado pelo *Ransomware* em 2017 tenha sido de aproximadamente US$ 4 bilhões em todo o mundo (ABREU, 2021).

[4] BitCoin: Moeda virtual não rastreável;

De acordo com um estudo questionando a eficácia das soluções *anti-malwares* [5] realizado pelo site *Varonis* em 2017, onde foi realizado com 230 pessoas de organizações espalhadas pelo mundo, tanto do ocidente como do oriente, 70% acreditavam que as soluções eram poucos eficazes, 21% consideravam completamente eficazes e 9% não sabiam responder, como representado na Figura 4 (CANDIDO, et al. 2017).

Figura 4. Pesquisa de opinião sobre a eficácia dos *anti-malwares.*



Fonte: VARONIS, 2017 *Apud* CANDIDO, et al. 2017

Em 2021, por conta da pandemia, ele volta a ter destaque junto a outro ataque que tem praticamente o mesmo objetivo que ele – roubo de dados – denominado de *Phishing*, graças ao *home office*. Uma gigante brasileira e uma das maiores indústrias de alimento do mundo, em 30 de maio de 2021, sofreu um ataque de *Ransomware* onde a mesma foi forçada a parar suas atividades devido a um ciberataque que, por fim, sequestrou seus dados com exigência de resgate pelos atacantes para obtê-los novamente, a empresa interrompeu o processamento de carne por 4 dias inteiros e teve que pagar R$ 55 milhões pelo resgate. Um pouco antes já havia acontecido um ataque cibernético ao oleoduto Norte-Americano, causando escassez de gasolina na Costa Leste dos Estados Unidos, onde o governo americano precisou pagar o resgate de aproximadamente US$ 4,3 milhões em *BitCoins* (CHARLEAUX, 2021).

Mas afinal, o pagamento realmente deve ser realizado? Apesar de não haver uma resposta concreta a essa pergunta, essa questão acaba virando um verdadeiro embate psicológico, já que mediante ao pagamento nada garante a empresa que os criminosos terão honra em manter sua palavra com o acordo em devolver os dados. No entanto, se não cumprirem com sua palavra sua reputação acaba sendo manchada,

[5] *Anti-malware*: Categoria de *softwares* que tem o objetivo de combater os *malwares;*

dificultando as negociações em futuros furtos cometidos pelos mesmos. O aconselhável é não pagar o resgate, como nada garante que seus dados serão devolvidos em um mediante pagamento, que além do mais pode ser cobrado um valor bastante alto, a vítima se verá cada vez mais lesada e refém dos criminosos (NADIR; BAKHSHI, 2018).

3.2.1 Contramedidas ao Ransomware

Apesar de todo o seu poderio, a forma mais eficaz de proteção contra *Ransomware* é basicamente deixar seu *software* antivírus atualizado na versão mais recente possível e principalmente atualizar as definições de segurança do sistema operacional, além de um cuidado pessoal nos sites acessados e *e-mails* recebidos. Desse modo não só o *Ransomware* como diversos outros programas maliciosos terão dificuldades em violar seus dados (OLHAR DIGITAL, 2019).

3.3 ATAQUES EM 2019

Ao fazer um levantamento dos números de ataques *crackers* do ano de 2019, no primeiro semestre houve um aumento de consideráveis 52% em relação ao mesmo período de 2018, contabilizando mais de 3.800 ataques registrados. Mesmo a gigante empresa de vendas e entregas de produtos, não se viu livre desses ataques. O inusitado foi de onde partiu essa ofensiva cibernética. Uma ex-funcionária da própria empresa chamada *Paige Thompson* foi a pioneira do ataque ao *hackear* o banco de dados do *CapitalOne*, comprometendo dados de mais de 100 milhões de clientes (LOTUFO, 2019).

Além desse, no mesmo ano ocorreram outras invasões de destaque, como, por exemplo, o ataque *Ransomware* a cidade de *Baltimore*. A cidade mais populosa de *Maryland* nos Estados Unidos se viu refém do *malware*[6] chamado *RobinHood*, cortando o acesso aos *e-mails* dos funcionários públicos e pagamento dos salários, e afetou também a compra e venda de imóveis (LOTUFO, 2019).

Novamente, graças a um ataque *Ransomware,* uma empresa espanhola de transporte e segurança de dinheiro, que se viu obrigada a parar suas operações fechando por um dia inteiro, derrubando seus próprios sites para amenizar o ataque ao ser atingido por um *malware* denominado *RYUK*[7], que trancou todos os seus dados (LOTUFO, 2019).

---

[6] *Malware: Software* malicioso que se infiltra nos dispositivos das vítimas;

[7] Alguns pesquisadores da *Deloitte* Argentina, atribuem o *Ransomware RYUK* a um grupo cibercriminoso chamado *CryptoTech;*

Mesmo ao analisar somente esses três casos entre muitos, o prejuízo obtido por essas empresas dá uma noção de como um ataque pode pegá-las de surpresa, obrigando-as a um replanejamento que custará um valor não esperado. O *CapitalOne,* após sofrer o ataque, estimou entre US$ 100 a 150 milhões para reforçar sua segurança digital. Apesar de ser algo benéfico, continua sendo um gasto não esperado. A cidade de *Baltimore,* assim que sofreu a invasão, recebeu a proposta de resgate com o valor de 13 *BitCoins,* que equivalia na época a US$ 100 mil, porém ao se negar a pagar, apesar de ser a atitude mais correta, não houve sucesso por parte das autoridades a recuperar os dados, como o tempo foi passando, estimou-se na época que a cidade gastaria não mais US 100 mil e sim US$ 18 milhões para recuperar o controle de suas operações. O *malware RYUK,* o mesmo que atingiu a *Prosegur*, conseguiu mais de 700 *BitCoins* em 5 meses na época, totalizando em mais de US$ 3,7 milhões em pagamentos de resgate (LOTUFO, 2019).

3.4 PERÍODO PANDÊMICO

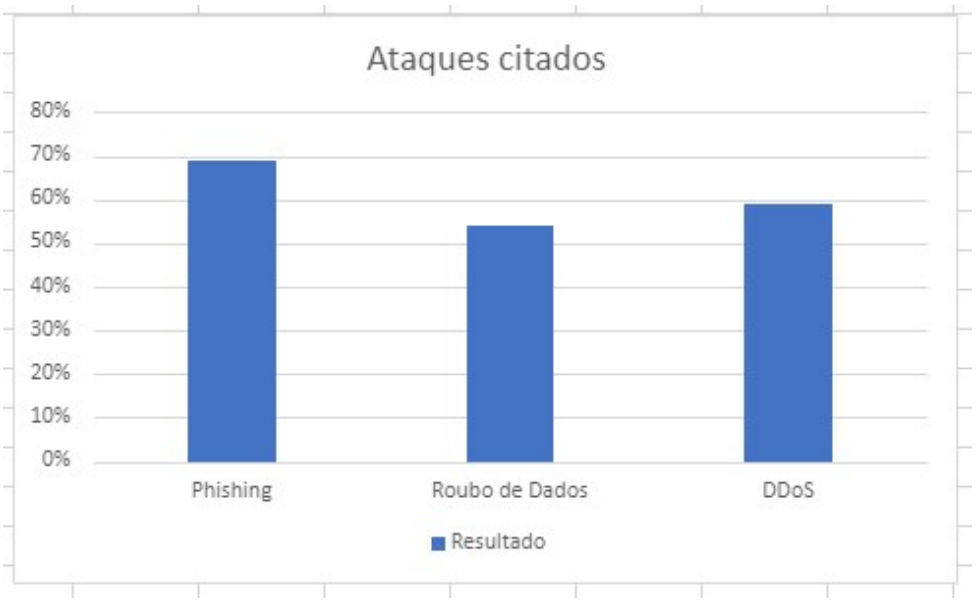
Como abordado, ao longo dos anos, com o avanço tecnológico, cada vez mais ataques *crackers* foram sofridos tanto por usuários comuns quanto por empresas de todos os portes. Com a chegada da doença denominada *COVID*-19 e a mudança de rumo do mercado onde tiveram que se adequar de forma repentina e sem nenhum planejamento realizado para a situação, agravou ainda mais os números dos crimes cibernéticos, já que em vários países adotaram a repentina quarentena – isolamento por período máximo de incubação de uma doença –, que durou em média 5 meses, muitas empresas se viram obrigadas a migrarem para o mundo *online* trabalhando em *home office*[8] com o intuito de dar andamento ao seus negócios e continuarem com as "portas abertas", disponibilizando seus serviços e produtos (EY, 2021).

Num estudo levantado pela *EY* chamado *"How Covid-19 is impacting future investment in security and privacy"* onde entrevistaram mais de 130 companhias dos cinco continentes, estima que os ataques cibernéticos aumentaram em expressivos 300% em relação ao período pré-pandemia. Uma das principais causas foi a súbita e necessária adaptação para o modelo de trabalho *home office*. As corporações se tornaram reféns de algo que não conseguiam controlar corretamente devido à distância, que foram a rede doméstica dos funcionários, e ao fator humano, onde o usuário tem que tomar cuidado com o que acessa e como manusear os dados na Internet. Essa questão fica bastante evidente quando 69% dos entrevistados alegaram que o tipo de ataque mais recorrente era o *Phishing*, que consiste em utilizar a

[8] *Home office:* Possibilidade de trabalhar em casa;

engenharia social[9] para convencer o usuário a acessar um link falso ou baixar um arquivo malicioso, para poder obter os dados da vítima e em consequência os das empresas também. A Figura 5 mostra os resultados da pesquisa (EY, 2021).

Figura 5. Ataques citados pelos entrevistados.



Fonte: Autoria Própria

Em 2020, houve diversos ataques a gigantes brasileiras de diversos segmentos. No mundo, atentaram contra uma rede social global, aplicativos de namoros e até mesmo o governo norte-americano não escapou onde um *software* da empresa *SolarWinds* chamado *Orion*, que monitora as redes de computadores, foi infectado. Esse ataque foi considerado a maior operação contra o governo em anos (ÉPOCA, 2020).

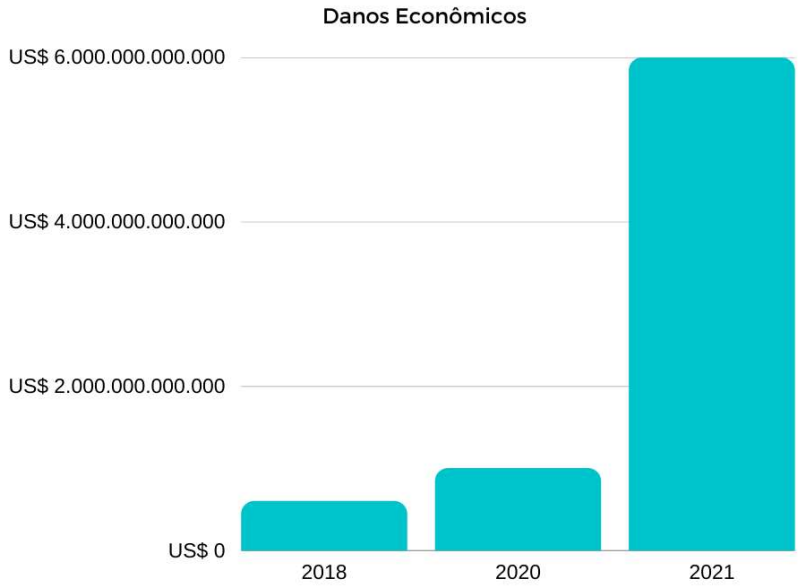
No primeiro e segundo trimestre de 2021 ocorreram grandes invasões, como um grupo da Coreia do Norte fez dos pesquisadores da área de segurança de dados da *Google Threat Analysis Group* (TAG) de alvos, com intuito de instalar um *exploit*[10] nos navegadores das vítimas; a gigante *Microsoft*[11] teve que lidar com ataques *Zero Day* em seu *Exchange Server*[12] (BALDISSERA, 2021).

Um levantamento realizado em setembro de 2021 mostra que o prejuízo no ano provocado por ataques cibernéticos chega a custar US$ 6 trilhões, que consiste em seis vezes mais em relação ao último levantamento em dezembro de 2020 e dez

[9] Engenharia social: Técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados.
[10] Exploit: Ataque que se aproveita de vulnerabilidades da máquina;
[11] Microsoft: Uma das maiores empresas voltadas para a área de tecnologia;
[12] Exchange server: Aplicação servidora de *e-mails;*

vezes mais em comparação com o levantamento de 2018, com estimativa que os ataques sejam cada vez mais aperfeiçoados e difundidos com o tempo. No primeiro trimestre de 2021, os ataques a empresas brasileiras cresceram em 220% em comparação ao mesmo período de 2020, como representado na Figura 6. Segundo o ranking criado pela consultora alemã *Roland Berger*, o Brasil já se encontra como o 5º maior alvo de ataques *crackers* a empresas do mundo, atrás somente de Estados Unidos, Reino Unido, Alemanha e África do Sul (GUIMARÃES, 2021).

Figura 6. Comparativo de danos econômicos entre 2018, 2020 e 2021.



Fonte: Autoria Própria

3.5 CONTRAMEDIDAS DE SEGURANÇA

A melhor contramedida de segurança é o planejamento prévio e investimento em segurança dos dados, ou até mesmo em cuidados simples que, realizados no dia a dia acaba dificultando o trabalho dos *crackers*, como criar regras no *Firewall* para que determinados dados sejam proibidos de trafegar, manter o antivírus e sistema operacional atualizados, realizar *Backup*[13] dos dados periodicamente se precavendo por um possível sequestro de dados, e até mesmo na contratação dos *"hackers* do bem", que são *hackers* que tem a função de encontrar brechas no sistema e informar aos contratantes sobre ela, assim podendo resolver aquele problema antes que seja explorado (OLIVEIRA, 2018; GUIMARÃES, 2021).

[13] Backup: Cópia de segurança dos dados;

Procurando formas de melhorar a segurança de dados dos usuários na Internet, foi aprovada a Lei Geral de Proteção de Dados (LGPD) que, inspirada na GDPR (Regulação Geral de Proteção de Dados), protege o usuário contra a coleta e tratamento de dados sensíveis ou não pelas empresas, onde as organizações só poderão ter acesso a essas informações mediante aprovação dos usuários. Ainda deverão ser deixadas claras quais informações serão coletados e para qual finalidade e quem terá acesso a esses dados. Isso acaba amenizando a circulação inapropriada dos dados pessoais dos usuários pela Internet, e prevenindo que um possível vazamento de dados causado por um ataque cibernético, as informações pessoais que o usuário nem fazia ideia que estavam armazenadas naquele lugar sejam utilizadas de forma inapropriada (BISSO; et. al, 2019).

4 CONCLUSÃO

Esta pesquisa se propôs a mostrar o quão vulneráveis ficamos ao estar conectados à Internet. Podemos ver que um descuido em não atualizar o *Windows* conseguiu que mais de 340 mil máquinas fossem infectadas. Trazendo uma pesquisa bibliográfica juntamente com o auxílio de fontes secundárias para obter os casos reais, se pôde perceber que a cada ano há um aumento expressivo nos ataques cibernéticos, chegando aos impressionantes US$ 6 trilhões de prejuízo econômico pelo mundo em 2021, número esse dez vezes maior que em 2018 (GUIMARÃES, 2021), isso mostra que não importa o quão avançado sejam as tecnologias disponíveis em seu mercado, se não houver uma estrutura planejada capaz de impedir, ou pelo menos amenizar os danos causados pelos ataques, o prejuízo causado acabará sendo muito maior que o esperado. A atenção ao fator humano é o principal desafio das corporações visto que por fazer parte da organização o erro/descuido/falta de conhecimento do colaborador pode acarretar uma dor de cabeça nada agradável. Mesmo com todos os cuidados, uma vez no espaço cibernético ficará sujeito a tentativa de ataques e invasões.

Apesar dos números assustadores, algumas medidas estão começando a serem adotadas que podem ajudar a amenizar esses problemas, como a Lei Geral de Proteção de Dados, que possibilita uma segurança e controle maior dos seus dados pessoais. Porém a impunidade diante dos *crackers* é uma questão que ainda terá que ser bastante trabalhada para ser revertida.

Contudo, ainda estamos longe de chegar a um sistema cibernético seguro e sem falhas, devido aos *crackers/hackers* que sempre estão buscando formas e meios de conseguir burlar, alterar e acessar informações de pessoas, empresas e sistemas.

Com isso, as empresas devem investir bastante nesse aspecto, para tentar sempre que necessário intervir antes que o problema se alastre e cause danos severos às informações de seus colaboradores e clientes. Um sistema com vasta segurança é um sistema com menos risco de sofrer ataques, entretanto a segurança e a estabilidade dos sistemas terão retornos significativos.

REFERÊNCIAS

ABREU, Mariane. **Top 5 ataques mais importantes de Ransomware**. 2021. Disponível em: https://prensa.li/prensa/top-5-ataques-mais-importantes-de-ransomware/. Acesso em: 14 out. 2021.

BAARS, Hans, et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. 3 ed., Brasport Livros, 2018.

BALDISSERA, Olívia. **Os maiores ataques cibernéticos de 2021 (até agora)**. 2021. Disponível em: https://posdigital.pucpr.br/blog/ataques-ciberneticos. Acesso em: 13 out. 2021.

BISSO, Rodrigo; et. al. **Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados**. 2019, https://sol.sbc.org.br/index.php/errc/article/view/9230/9133. Acesso em: 28 out. 2021.

CANDIDO, Jeferson William, et al. **SEGURANÇA DA INFORMAÇÃO COM FOCO NA PROPAGAÇÃO IMINENTE DE RANSOMWARE NAS CORPORAÇÕES**. 2017. Disponível em: https://simtec.fatectq.edu.br/index.php/simtec/article/view/270/220. Acesso em: 20 out. 2021.

CARVALHO, Luciana. **10 casos de espionagem industrial**. 2012. Disponível em: https://exame.com/negocios/10-casos-de-espionagem-industrial/. Acesso em: 24 ago. 2021.

CERNEV, Adrian Kemmer; LEITE, Jaci Corrêa. **Segurança na Internet: a Percepção dos Usuários como Fator de Restrição ao Comércio Eletrônico no Brasil**. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924694. Acesso em: 20 set. 2021.

CHARLEAUX, Lupa. **JBS pagou R$ 55 milhões em resgate de dados após ataque ransomware**. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/218972-jbs-pagou-r-55-milhoes-resgate-dados-ataque-ransomware.htm. Acesso em: 22 set. 2021.

DERTOUZOS, Michael. **O que será: Como o Novo Mundo da Informação Transformará Nossas Vidas**. São Paulo: Companhia das Letras, 1997.

ÉPOCA. **Retrospectiva 2020: os maiores ciberataques do ano**. 2020. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/12/retrospectiva-2020-os-maiores-ciberataques-do-ano.html. Acesso em: 07 out. 2021.

EY. **Ataques cibernéticos a empresas aumentam 300% na pandemia**. 2021. Disponível em: https://istoe.com.br/ataques-ciberneticos-a-empresas-aumentam-300-na-pandemia/. Acesso em: 21 out. 2021.

GUIMARÃES, Fernanda. **Brasil já é o 5º maior alvo global de ataques de hackers a empresas**. 2021. Disponível em: https://economia.uol.com.br/noticias/estadao-conteudo/2021/09/12/brasil-e-5-maior-alvo-de-cibercrimes.htm. Acesso em: 12 out. 2021.

HSC BRASIL. **Conheça 6 grandes empresas invadidas por hackers**. 2019. Disponível em: https://www.hscbrasil.com.br/grandes-empresas-invadidas-por-hackers/. Acesso em: 23 ago. 2021.

KLIMBURG, Alexander. **National Cyber Security Framework Manual**. NATO CCD COE Publications, 2012. Disponível em: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. Acesso em: 15 out. 2021.

LISKA, Allan; GALLO, Timothy. **Ransomware: Defendendo-se da extorsão digital**. 1 ed., São Paulo: Novatec, 2017.

LOTUFO, Érico. **Os maiores casos de violação de dados de 2019**. 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/12/os-maiores-casos-de-violacao-de-dados-de-2019.html. Acesso em: 07 set. 2021.

MARCONDES, José Sérgio. **Espionagem Industrial (Empresarial/Corporativa) O que é? Exemplos.** 2020. Disponível em: https://gestaodesegurancaprivada.com.br/espionagem-industrial-empresarial-corporativa/. Acesso em: 28 ago. 2021.

MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP**. 3 ed., Starlin Alta Editora, 2017.

MITNICK, Kevin D.; SIMON, Simon L. **Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. Pearson Education do Brasil Ltda., 2003.

MOURA, Marcelo; HAIDAR, Daniel. **Os ataques cibernéticos explodem durante pandemia e expõem vulnerabilidades das empresas**. 2020. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html. Acesso em: 18 ago. 2021.

NADIR, Ibrahim; BAKHSHI, Taimur. **Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques**. 2018. Disponível em: https://www.researchgate.net/publication/322656267_Contemporary_Cybercrime_A_Taxonomy_of_Ransomware_Threats_Mitigation_Techniques. Acesso em: 14 out. 2021.

NAKAMURA, Emilio T.; GEUS, Paulo L. **Segurança de redes em ambientes cooperativos**. 1 ed., Novatec, 2007.

OLHAR DIGITAL. **Entenda o ciberataque que afetou mais de 200 mil PCs em 150 países**. 2019. Disponível em: https://olhardigital.com.br/especial/wannacry/. Acesso em: 22 out. 2021.

OLIVEIRA, Jéssica C. Ransomware - **Laboratório de Ataque do WannaCry**. Universidade de Brasília, 2018, https://bdm.unb.br/bitstream/10483/23052/1/2018_JessicaCristinaDeOliveira_tcc.pdf. Acesso em: 20 out. 2021.

OLIVEIRA, Marcos A. G.; et. al. **Guia de Defesa Cibernética na América do Sul**. Recife: Ed. UFPE, 2017.

PLANALTO. **LEI Nº 9.279, DE 14 DE MAIO DE 1996**. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9279.htm. Acesso em: 28 ago. 2021.

PPETERS. **Diagram CIA Triangle**. 2011. Disponível em: http://ppeters3005.blogspot.com/2011/05/diagram-cia-triangle.html. Acesso em: 03 set. 2021.

RIGUES, Rafael. **CD Projekt, produtora de Cyberpunk 2077, é hackeada**. 2021. Disponível em: https://olhardigital.com.br/2021/02/09/noticias/cd-projekt-produtora-de-cyberpunk-2077-e-hackeada/. Acesso em: 24 ago. 2021.

SILVA, Lillyanne Karolline de Melo; MÈRCHER, Leonardo. **Falta de Segurança e o Crescimento dos Cyber Crimes no Brasil**. 2017. Disponível em: https://repositorio.uninter.com/bitstream/handle/1/290/1188090%20-%20LILLYANNE%20SILVA.pdf?sequence=1&isAllowed=y. Acesso em: 23 set. 2021.

SILVA, Washington R. **Análise Econômica dos Impactos dos Ataques Hackers**. Universidade de Brasília, 2018, https://repositorio.unb.br/bitstream/10482/34838/3/2018_WashingtonRodriguesdaSilva.pdf. Acesso em: 27 out. 2021.

TERCEIRO, Ramalho. **O problema na tipificação penal dos crimes virtuais**. 2002. Disponível em: https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais. Acesso em: 20 out. 2021.

UNYLEYA. **Conheça os 10 principais ataques cibernéticos da atualidade**. Disponível em: https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos/. Acesso em: 16 out. 2021.

WAKKA, Wagner. **Cyberpunk 2077 é removido da PlayStation Store e ações da CD Projekt despencam**. 2020. Disponível em: https://canaltech.com.br/games/cyberpunk-2077-e-removido-da-playstation-store-e-acoes-da-cd-projekt-despencam-176476/. Acesso em: 03 set. 2021.

ZIMMER, Kelvin. **Hackers x Empresas: Quais os ataques cibernéticos mais comuns?** 2020. Disponível em: https://www.lumiun.com/blog/hackers-empresas-quais-os-ataques-ciberneticos-mais-comuns/. Acesso em: 20 ago. 2021.