Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Franciele Cassimiro de Araujo
Jackeline Magrin Rossi

A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS

Americana, SP
2020

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Franciele Cassimiro de Araujo
Jackeline Magrin Rossi

A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Esp. Marcus Vinícius Lahr Giraldi.

Área de concentração: Segurança da Informação

Americana, SP.
2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

A689e ARAUJO, Franciele Cassimiro de

A evolução dos ataques cibernéticos. / Franciele Cassimiro de Araújo, Jackeline Magrin Rossi. – Americana, 2020.

51f.

Monografia (Curso Supeiror de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1 Segurança em sistemas de informação I. ROSSI, Jackeline Magrin II. GIRALDI, Marcus Vinícius Lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Franciele Cassimiro de Araujo
Jackeline Magrin Rossi

A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 30 de junho de 2020.

Banca Examinadora:

_____
Marcus Vinícius Lahr Giraldi (Presidente)
Professor Especialista
FATEC – Faculdade de Tecnologia de Americana

_____
Wagner Siqueira Cavalcante (Membro)
Professor Mestre
FATEC – Faculdade de Tecnologia de Americana

_____
Jose Carlos Meca Vital (Membro)
Maior Mestre
FATEC – Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradecemos, primeiramente, a Deus, que nos capacitou para realização desse trabalho.

Aos professores que durante esses anos doaram um pouco do seu conhecimento e experiências para que nós nos tornássemos pessoas e profissionais melhores.

A Prof. Dra. Maria Cristina Aranda pelo apoio, paciência e orientação.

Em especial ao nosso orientador Prof. Esp. Marcus Vinícius Lahr Giraldi, pelas conversas, pelo apoio, por não deixar de estar presente em nenhum momento, nos incentivando em cada etapa deste trabalho.

Aos colegas de turma que estiveram presentes nos grupos de estudo, que nos apoiaram e que não desistiram apesar das dificuldades.

A todos que, direta ou indiretamente, contribuíram para conclusão deste trabalho.

DEDICATÓRIA

Ao meu amado esposo Denis Delfino de Araujo pelo grato apoio e compreensão, um futuro sendo construído para o crescimento da nossa família.
Aos meus pais, pelo apoio e carinho.
E por último e não menos importante, a minha querida e amada amiga Jackeline Magrin Rossi, pela paciência e determinação.

Franciele Cassimiro de Araujo

Ao meu marido Cleber Andrez de Souza Rossi pelo apoio, compreensão e por ter tido papel fundamental na minha escolha, minha sobrinha Catarina C. Magrin e meus filhos de quatro patas Fred e Luna que foram presença constante, trazendo alegria e amor em todos os momentos.
A minha amiga, irmã de alma, Franciele Cassimiro de Araujo por compartilhar as alegrias, as decepções, as frustrações e conquistas, pelo apoio incondicional e por compreender toda minha excentricidade, você é parte essencial desta conquista.

Jackeline Magrin Rossi

RESUMO

Este trabalho conceitua a evolução dos ataques cibernéticos, a fim de demonstrar de que forma as grandes corporações têm lidado com esses ataques. Apresenta conceitos técnicos e jurídicos de terminologias que permitem ao leitor clareza no entendimento dessa pesquisa, uma linha do tempo que mostra a evolução da Internet, que contempla os principais acontecimentos responsáveis por seu desenvolvimento. Traz dados de pesquisas recentes que buscam mostrar o cenário da segurança cibernética mundial, com a classificação dos países mais e menos seguros adotando pontuação proposta pelo Índice Global de Cibersegurança (GCI). Detalha os principais ataques cibernéticos que atingiram grandes corporações e como os mesmos influenciaram o desenvolvimento da área de Segurança da Informação e a mudança de visão das organizações se tratando de segurança cibernética e, também, quais as ações foram tomadas mediante tais crises e quais as lições tomadas após os ataques. Aborda diretrizes e ferramentas essenciais como a criação de uma Política de Segurança, apresentando os principais pontos para construção de uma política eficiente, abordando metodologias para criação de uma equipe de segurança da informação, como por exemplo a metodologia SOC (Centro de Operações de Segurança) e sua importância na detecção e prevenção de ameaças. Demonstra a importância de possuir um Grupo de Resposta de Incidentes de Segurança (CSIRT), mostrando o papel fundamental do mesmo no gerenciamento de crises causados por incidentes de segurança cibernética e quais as principais diretrizes para criação de um grupo desses em uma organização. Finaliza trazendo uma reflexão sobre o cenário mundial em torno das crescentes ameaças cibernéticas e como isso têm influenciado o melhoramento das defesas e inteligência para um gerenciamento de risco eficaz.

Palavras Chave: ciberataque; segurança; Internet.

ABSTRACT

This paper conceptualizes the evolution of cyberattacks in order to demonstrate how large corporations have dealt with these attacks. It presents technical and legal concepts of terminologies that allow the reader to clearly understand this research, a timeline that shows the evolution of the Internet that contemplates the main events responsible for its development. It brings data from recent research that seeks to show the world cybersecurity scenario with the classification of the most and least secure countries adopting a score proposed by the Global Cybersecurity Index (GCI). It details the main cyberattacks that hit large corporations and how they influenced the development of the Information Security area and the change of vision of organizations when it comes to cyber security and also, what actions were taken through such crises and what lessons were taken after the attacks. It addresses essential guidelines and tools such as the creation of a Security Policy, presenting the main points for building an efficient policy, it also addresses methodologies for creating an information security team, such as the SOC (Security Operations Center) methodology and it is importance in the detection and prevention of threats. Demonstrates the importance of having a Security Incident Response Group (CSIRT), showing it is fundamental role in managing crises caused by cybersecurity incidents and what are the main guidelines for creating such a group in an organization. It concludes by reflecting on the world scenario around the growing cyber threats and how this has influenced the improvement of defenses and intelligence for effective risk management.

Keywords*: cyberattack; safety; Internet.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Antes de usarem a Internet como meio para seus crimes, os golpistas sempre foram conhecidos pela arte de fazer as pessoas acreditarem em algo muitas vezes improvável. O golpe do bilhete premiado, a venda de propriedades inexistentes, arrecadação de dinheiro para instituições filantrópicas falsas, entre tantos outros, são alguns exemplos de que a mente criminosa pode ser criativa e brilhante.

A tecnologia permitiu que, assim como o mundo, os criminosos evoluíssem; essa evolução deu aos criminosos a possibilidade de agir no anonimato e com isso elevar o nível dos golpes; também permitiu o alcance desses criminosos, pois eles são capazes de atingir diversas regiões e diversos países utilizando apenas uma conexão com a Internet.

Este trabalho visa, de forma objetiva, demostrar através de pesquisa cientifica a evolução dos ataques cibernéticos, buscando apresentar não somente os ataques cibernéticos e quais países são mais afetados, mas também os países com maior execução desses crimes, bem como os tipos de ataque mais conhecidos e as melhores formas de prevenção e combate, elucidando as maneiras que as grandes corporações têm lidado com os crimes cibernéticos.

Segundo o Juiz Federal Substituto, Emanuel Alberto Sperandio Garcia Gimenes, publicou na Revista de Doutrina TRF4:

> “O aparecimento dos primeiros casos de crimes informáticos data da década de 1960, e estes nada mais eram que delitos em que o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas.” (GIMENES, 2013)

Em 1969, nos Estado Unidos, a agência do governo ARPA (*Advanced Research and Projects Agency*), criou uma rede batizada de ARPANET (*Advanced Research Projects Agency Network*), com o objetivo de conectar departamentos de pesquisa, onde faziam trocas de pacotes através de protocolo de comutação NCP (*Network Control Protocol*), se tornando a base técnica para o surgimento da Internet.

Em 1971, surgiu o primeiro vírus informático (*The Creeper*) e em 1978 o primeiro *SPAM* (lixo eletrônico em forma de e-mails em massa ou de conteúdo duvidoso).

Em 1982, a ARPANET não era mais restrita aos Estados Unidos, se expandindo para outros países, mas foi em 1983 que pôde-se conceituar a Internet como um conjunto de redes interligadas, graças ao uso de um novo protocolo, o TCP/IP (*Transfer Control Protocol/Internet Protocol*), que permitiu um crescimento praticamente ilimitado da rede.

Com a abertura da Internet, houve um aumento das ações criminosas, que passaram a refletir, por exemplo, em manipulações de caixas bancários, abusos de telecomunicação, pirataria de programas de computador e pornografia infantil.

Desde então, os ataques têm se aprimorado e os *hackers* (pessoa que usam o conhecimento em informática para ter acesso a dados de outra pessoa, sem autorização) se tornado cada vez mais audaciosos e elevando o número de crimes.

O texto reforça a diferença entre os termos cibercrime e crimes de informática.

Há a necessidade de conscientização entre os usuários de tecnologia para que não sejam vítimas desses tipos de crime. Da mesma forma, os profissionais em segurança da informação precisam estar atualizados, para prestarem o melhor atendimento àqueles que buscam seus serviços e também orientar usuários e empresas sobre as melhores práticas para se protegerem desses ataques.

O capítulo 2 traz a revisão bibliográfica, que busca apresentar a visão de diversos assuntos sobre o tema. O capítulo 3 apresenta um cenário geral do cibercrime, com dados de pesquisas e informações dos os maiores ofensores da segurança. O capítulo 4 mostra os principais ataques cibernéticos que contribuíram de alguma forma para a evolução da segurança da informação. O capítulo 5 traz algumas soluções para combate e prevenção de ciberataques, destacando três métodos de combate. Por fim, o capítulo 6 traz as considerações finais das autoras sobre o tema abordado nessa pesquisa.

2 REVISÃO BIBLIOGRÁFICA

Esse trabalho de pesquisa buscou basear-se em autores que demonstram pontos de vista diferentes sobre o assunto, a fim de tratar do assunto em questão de forma abrangente e elucidar todos os pontos propostos nessa pesquisa.

2.1 Segurança cibernética

Araujo e Ferreira (2009) entendem que Segurança da Informação é uma disciplina relativamente nova, no que diz respeito a área do conhecimento humano, e apresenta um guia prático para elaboração e implementação de uma Política de Segurança da Informação, privilegiando o princípio da confidencialidade, pois classifica os sistemas da informação em vários níveis de segurança, partindo-se de um nível mais restrito até o nível mais básico. No entanto, os demais princípios de segurança, não são muito enfatizados.

Fontes (2006) apresenta a Segurança da Informação com foco no usuário. Ele demonstra uma visão organizacional e a importância de preparar, conscientizar o usuário na manipulação das informações, ele se preocupa principalmente em educar o usuário e assim garantir que as informações sejam manipuladas de forma segura.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, através de sua cartilha, busca mostrar a importância da Segurança da Informação na Internet. Eles apresentam os principais golpes, ataques e riscos; apresentam também mecanismos de segurança e como utilizar de maneira segura a Internet.

Laudon e Laudon (2014) baseiam-se na premissa de que conhecer sistemas da informação é essencial para criar empresas competitivas, gerenciar corporações globais e fornecer serviços e produtos uteis aos clientes. Com abordagem prática e didática, Sistema de Informações Gerenciais é voltado para aprendizagem com exemplos reais com perspectiva verdadeiramente internacional e a importância à ética e à privacidade.

Spyman (2000), trata de um assunto polêmico, porém necessário para entender como usuários de Internet se tornam *hackers* e similares, e como

empresas e usuários conectados à Internet podem evitá-los. Além disso, de forma simples, o Manual Completo *Hacker* Millenium mostra os maiores *hackers* do mundo com terminologia básica para mostrar suas diferenciações, como ser e evitá-los com programas, fontes e scripts disponíveis na Internet.

Clough (2010) apresenta os princípios do cibercrime na atmosfera jurídica, trazendo exemplos de crimes cometidos e analisados por quatros principais jurisdições: Austrália, Canadá, Reino Unido e Estados Unidos. Ele traz uma visão interessante para todos que buscam entender os desafios do crime cibernético.

Gragido, Molina, Pirc, Selby e Hay (2013) trazem uma abordagem especializada sobre cibersergurança, descrevendo os problemas dentro da comunidade de segurança, as facetas das diversas organizações criminosas do mundo cibernético e falam sobre espionagem industrial e cenário econômico e geopolítico da segurança cibernética. São especialistas que buscaram montar uma enciclopédia para todos que se interessam sobre crimes cibernéticos e guerras cibernéticas em geral.

2.2 Cibercrime

Antes da dar início a esse tópico, é importante frisar a diferença entre o cibercrime e crimes de informática. Os crimes de informática são qualquer conduta ilegal que envolva processamento de dados, sejam eles armazenados compilados ou em transmissão. De forma geral, cibercrime é todo delito praticado utilizando a tecnologia da informação como ferramenta a fim de causar dano a outrem. Toda e qualquer conduta ilícita praticada pelo usuário de informática, pode também ser tipificada como crime cibernético.

Os crimes virtuais, aqueles praticados utilizando a Internet como ferramenta, já são enquadrados no Código Penal Brasileiro a fim de punir dentro da lei os autores do mesmo.

Segundo Schmidt (2014), “Os crimes cibernéticos são classificados em: puro, misto e comum ou ainda como próprios ou impróprios.”

Crimes puros são aqueles que atingem a parte física (*hardware*) ou a parte virtual (*software*) de um computador. O criminoso tem como principal alvo atingir o

computador, os sistemas ou os dados armazenados no mesmo. Este é o caso do vírus Melissa, quem em 1999 causou um prejuízo de mais de oitenta milhões de dólares; esse vírus atingia os usuários do Microsoft Word.

Crimes mistos são aqueles em que o uso da Internet ou de *softwares* de computadores são condição para efetivação da ação criminosa. Um exemplo desse tipo de crime, são as transações de transferências de valores de contas bancárias utilizando o Internet Banking.

Crimes comuns são aqueles que utilizam a Internet apenas como um instrumento para ataque. Por exemplo, o crime de pornografia infantil, onde o uso da rede se dá para propagação do material ilícito, seja ele em vídeos ou fotos, *home-pages*, porém o crime essencialmente se mantém.

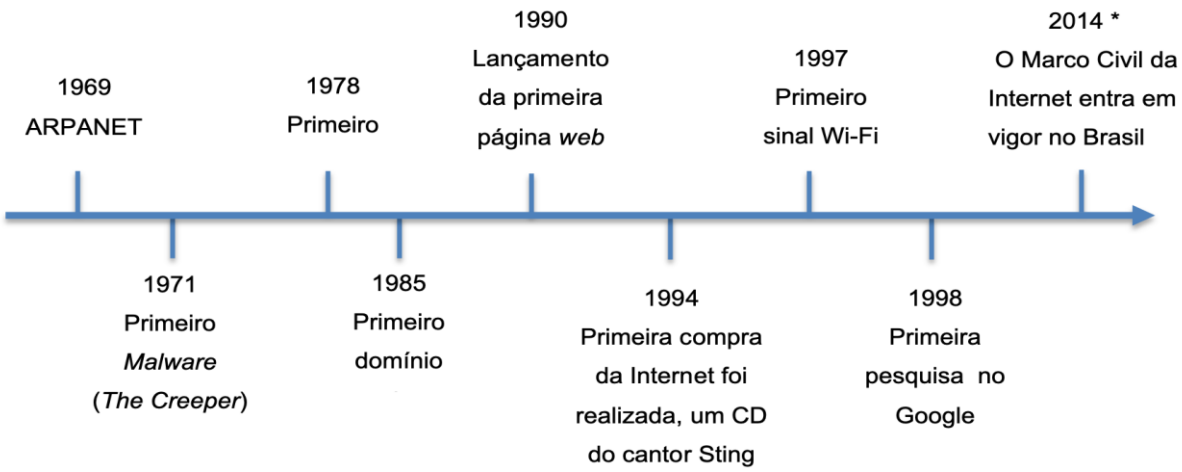
Crimes classificados como próprios são aqueles que o agente do crime precisa do computador para execução do crime. Nesse caso, a vítima afetada por esse agente também se trata de um computador. Por exemplo, quando há a invasão de um computador através da rede causada por um *hacker*, os dados roubados ou corrompidos pertencem a um computador.

Crimes classificados como impróprios também são cometidos por meio de um computador, porém a vítima pode ser atingida por diversas maneiras, não necessariamente com o computador, ou seja, pode ser atingida por um meio diverso da informática. Por exemplo, apropriação indébita, calúnia, difamação, pedofilia, estelionato, entre outros.

2.3 Cronologia dos principais acontecimentos no Brasil e no Mundo

Para melhor compreensão da evolução tecnológica, a Figura 1 apresenta uma linha do tempo com os principais acontecimentos que contribuíram para essa evolução.

Figura 1 – Principais momentos da Internet



Fonte: Elaborado pelo Autor

1969 – Nos Estados Unidos a agência do governo ARPA (*Advanced Research and Projects Agency*), criou uma rede batizada de ARPANET (*Advanced Research Projects Agency Network*), com o objetivo de conectar departamentos de pesquisa, onde faziam trocas de pacotes através de protocolo de comutação NCP (*Network Control Protocol* – Protocolo de Controle de Rede). Se tornando a base técnica para o surgimento da Internet. (RIBEIRO, 2020)

1971 – O Primeiro *Malware* (*The Creeper*), foi criado por Bob Thomas e era apenas um programa experimental e foi testado infectando um PDP-10, um computador de grande porte. Basicamente, o vírus invadia a máquina e apresentava no monitor uma mensagem dizendo: "*Im the creeper, catch me if you can*!" – Eu sou assustador, pegue-me se for capaz!. Após o recado aparecer em uma máquina, ele saltava de sistema em sistema repetindo a mensagem diversas vezes. (KLEINA, 2011)

1978 – Primeiro SPAM - O marqueteiro norte-americano Gary Thuerk, disparou material de divulgação de equipamentos; a mensagem foi encaminhada para 393 clientes da ARPANET (*Advanced Research Project Agency Netw*ork, em sua tradução Rede de Agências para Projetos de Pesquisas Avançadas). (SOUZA, 2018)

1985 – O primeiro domínio (DNS – Sistema de Nomes de Domínios) registrado foi o symbolics.com, por uma fabricante de computadores em Massachusetts, nos Estados Unidos. Foi o recurso criado para traduzir os endereços IP (*Internet Protocol* - é um número identificador dado ao seu computador, ou roteador, ao conectar-se à rede). (CABRAL, 2018)

1990 – Lançamento da primeira página *WEB* (*World Wide Web*- "www"). O primeiro site lançado foi criado por Tim Berners-Lee, um cientista do CERN, um centro de pesquisa na Suíça. O projeto foi concebido, originalmente, para que cientistas pudessem se comunicar mais facilmente. (BORNELI, 2015)

1994 – Primeira compra pela Internet foi realizada por Phil Brandenberger, da Filadélfia, comprou um disco de áudio compacto "Ten Summoners 'Tales" by the rock músico Sting. De sua estação de trabalho na Filadélfia, Brandenburger acessou o computador em Nashua e usou um código secreto para enviar o número do cartão de crédito Visa para pagar US $ 12,48, mais os custos de envio. (LEWIS, 1994)

1997 - Primeiro sinal Wi-Fi (*Wireless Fidelity*) é criado - O termo Wi-Fi é uma marca registrada pela Wi-Fi Alliance. Embora apresentado em 1999 para as empresas, a tecnologia Wi-Fi surgiu em 1997, com a criação do IEE 802.11, que permite a conexão entre diversos dispositivos sem fio. (DAROS, 2014)

1998 - Primeira pesquisa Google - Em vez de gerar spams e mostrar links aleatórios para os usuários conforme o valor pago pelos anunciantes, a companhia "roubou" a ideia de uma outra empresa chamada Idealab e a aprimorou: começou a separar resultados orgânicos dos anúncios, melhorando sua tecnologia para atingir uma meta ambiciosa: eles queriam organizar toda a informação do mundo e torná-las facilmente acessível. (MACEDO, 2015)

2014 - O Marco Civil da Internet entra em vigor no Brasil - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (PLANALTO, 2014)

3 O CENÁRIO DO CIBERCRIME

De acordo com a matéria publicada por Naveen Goud para a *Cybersecurity Insiders*, a mesma apresentou em seu artigo material produzido pela CompariTech que, assim como o *Wikileaks,* mostrou ao mundo que detém documentos válidos para provar que a CIA (Agência de Inteligência Americana) tem o potencial de invadir qualquer telefone inteligente, Smart TV ou dispositivo relacionado à Internet das Coisas (IoT – *Internet of Things*) existente no mundo. Estima-se que as pessoas também estariam interessadas em conhecer alguns fatos relacionados a esse gênero.

Deste modo, a empresa de tecnologia *CompariTech* apresentou algumas estatísticas mais recentes que fornecem informações sobre os países que estão melhor, bem e mal preparados para ataques cibernéticos, juntamente com aqueles que são os alvos mais suscetíveis aos cibercriminosos. Com tantos dados pessoais armazenados on-line, a cibersegurança é da maior importância.

Em 2019, a *CompariTech* analisou sessenta países e encontrou enormes diferenças em várias categorias, desde taxas de *malware* até legislação relacionada à segurança cibernética. Todos os países que foram analisados precisavam de algumas melhorias significativas. Em anexo, a Tabela 1 demonstra a classificação geral de segurança cibernética (da pior à melhor).

A análise feita pela *CompariTech* reuniu sessenta países que foram classificados entre os menos seguros e os mais seguros se tratando do ambiente cibernético, com base em sete critérios:

i. A porcentagem de dispositivos móveis infectados com *malware*;
ii. A porcentagem de computadores infectados com *malware*;
iii. O número de ataques financeiros com *malware*;
iv. A porcentagem de todos os ataques de telnet por país de origem;
v. A porcentagem de usuários atacados por mineradores de criptomoedas;
vi. Os países mais bem preparados para ataques cibernéticos;
vii. Os países com a legislação mais atualizada sobre segurança cibernética.

Além dos dois últimos, todas as pontuações foram baseadas na porcentagem de ataques em 2018. Os países mais bem preparados para ataques cibernéticos foram pontuados usando as pontuações do Índice Global de Cibersegurança (GCI).

> "O Índice Global de Cibersegurança (GCI) é uma referência confiável que mede o compromisso dos países com a cibersegurança em nível global - para aumentar a conscientização sobre a importância e as diferentes dimensões do problema. Como a segurança cibernética tem um amplo campo de aplicação, abrangendo muitas indústrias e vários setores, o nível de desenvolvimento ou engajamento de cada país é avaliado em cinco pilares: (i) Medidas legais, (ii) Medidas técnicas, (iii) Medidas organizacionais, (iv) Capacitação e (v) Cooperação - e depois agregados a uma pontuação geral." (ITU, 2020)

A legislação mais atualizada foi pontuada com base na legislação existente (e rascunhos) que abrangeu sete categorias (estratégia nacional, militar, conteúdo, privacidade, infraestrutura crítica, comércio e crime). Os países receberam um ponto por ter legislação em uma categoria ou meio ponto para um projeto.

Para cada critério, o país recebeu um ponto com base em sua classificação entre os países com classificação mais alta e mais baixa. Os países com a menor pontuação de segurança cibernética receberam 100 pontos, enquanto os países com a maior pontuação de segurança cibernética receberam zero pontos. Todos os países entre essas duas pontuações receberam uma pontuação percentual, dependendo de sua classificação. A pontuação total foi alcançada pela média da pontuação de cada país nas sete categorias.

Todos os dados usados para criar esse sistema de classificação são os mais recentes disponíveis, e incluiu apenas países que atenderam todos os critérios de pontos dados. A seguir alguns dados apresentados no artigo.

3.1 Infecção por *Malware*

Os códigos maliciosos (*malware*), são *softwares* desenvolvidos especificamente para executar ações nocivas e atividades maliciosas em um dispositivo computacional (desktops, servidores, smartphones, tablets, dentre outros).

A Cartilha do Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil (CERT.br), mostra que existem diversas formas como os códigos maliciosos podem infectar ou comprometer um computador:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pelo auto execução de mídias removíveis infectadas, como pen-drives;
- pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

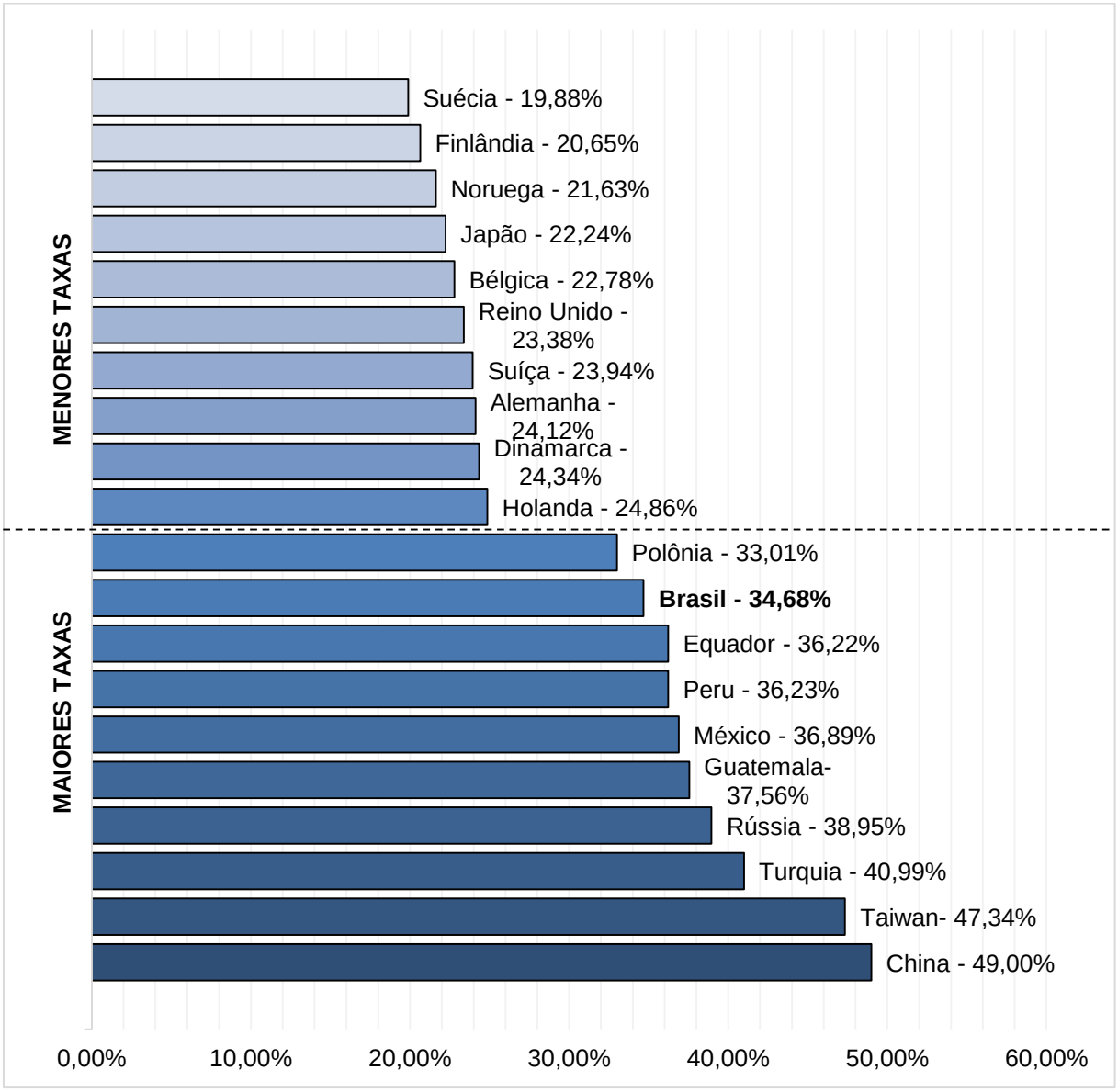
Depois que o *malware* é instalado no dispositivo, ele passa a ter acesso aos dados armazenados, podendo executar ações em nome do usuário, de acordo com as permissões de cada usuário, trabalhando assim para o cibercriminoso.

As motivações mais frequentes são a obtenção de vantagens financeiras, roubo de dados confidenciais, vandalismo e autoproclamação. Para tal, escolhem os alvos de acordo com o que os motiva.

A Figura 2 apresenta a diferença entre países com maiores e menores taxas de infecção por *malware* em computadores, que segundo Mark Yates é:

> "... o PIB per capita. Embora correlação não seja causalidade, isso sugere que a riqueza faz a diferença quando se trata de segurança de PC e laptop. ... Outros motivos apontados foi a maturidade da infraestrutura, prontidão tecnológica, treinamento de TI, conscientização de segurança e a lista continua. Mesmo a relação entre segurança de dispositivo e riqueza é uma hipótese que precisa de testes adequados.
> Mesmo assim, PCs em nações mais ricas ainda são infectados." (YATES, 2016)

Figura 2 – Taxa de Infecção por Malware



Fonte: Elaborado pelo Autor – Dados Comparitech (BISCHOFF, 2020)

3.2 Ataques por *Ransomware*

Ransomware é um tipo de *software* malicioso que geralmente usa criptografia para bloquear um sistema inteiro ou um conjunto de arquivos de um equipamento e que exige um resgate, geralmente feito via criptomoedas, como *bitcoins,* para devolver o acesso ao usuário. As formas mais comuns de propagação segundo a cartilha CERT.br são:

- e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um *link*;

- explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

A cartilha CERT.br mostra também, que existem dois tipos de *ransomware*:

- *Ransomware Locker*: impede que se acesse o equipamento infectado;
- *Ransomware Crypto*: impede que se acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

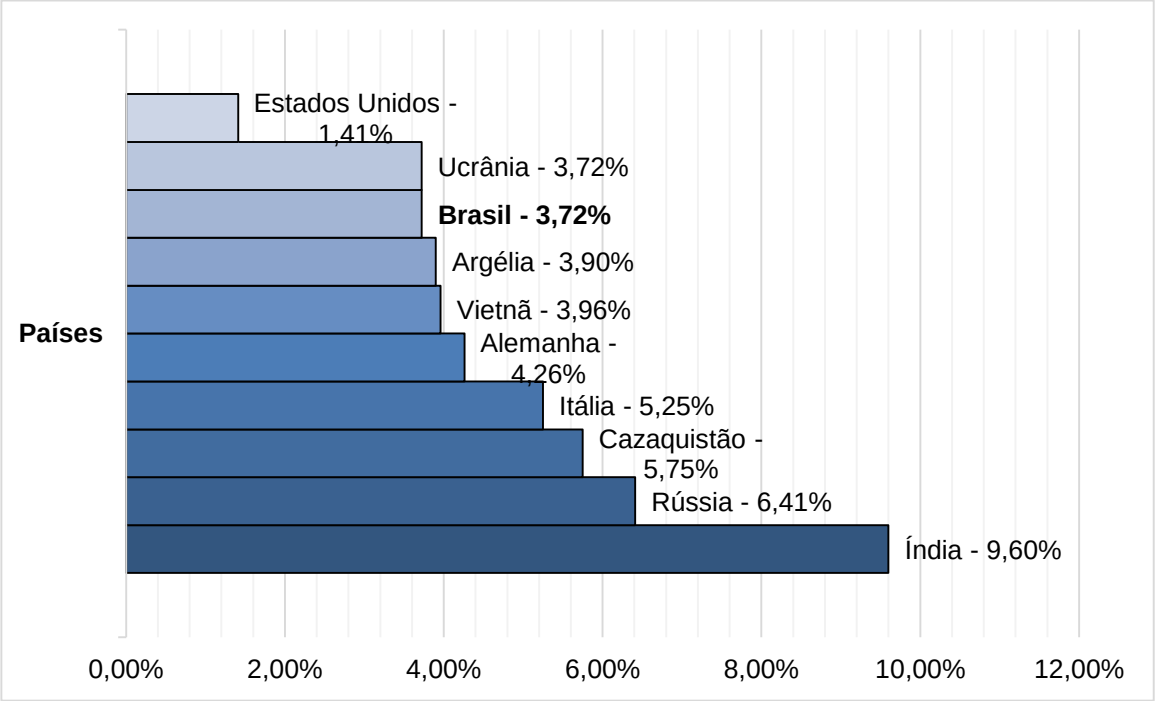
Além de infectar o equipamento, o *ransomware* também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também. Embora qualquer empresa seja um possível alvo de *ransomware*, algumas são mais propensas a estar na mira dos cibercriminosos.

Segundo o artigo publicado pelo jornalista de Tecnologia James A. Martin:

> “Sua vulnerabilidade a um ataque de *ransomware* pode depender de quão atraentes são seus dados para *hackers* criminais, de quão crítico é que você responde rapidamente a uma demanda de resgate, de quão vulnerável é sua segurança e de quão vigoroso você mantém os funcionários treinados sobre *e-mails* de *phishing*, entre outros fatores.” (MARTIN, 2017)

Para as organizações não ficarem inativas e manter sua reputação, pagam o resgate de seus dados para a retomada das operações. A Figura 3 apresenta os países que mais sofreram ataques por *Ransomware* em 2019:

Figura 3 – Taxas de Ataque por Ransomware - Países mais atacados



Fonte: Elaborado pelo Autor – Dados Comparitech (BISCHOFF, 2020)

3.3 Ataques DDoS – Negação de Serviço

Ataques de DDoS (*Distributed Denial of Service*) recebe o nome de negação de Serviço Distribuída por aproveitar os limites da capacidade específicos que se aplicam a todos os recursos de rede, usando um conjunto de dispositivos de modo coordenado e distribuído, tirando de operação um serviço, um computador ou uma rede conectada à Internet.

Diferente de um ataque *malware,* a motivação para um ataque de DDoS é apenas exaurir recursos e causar indisponibilidade ao alvo, ficando impossibilitados de acessar ou realizar as operações desejadas. Segundo a cartilha CERT.BR os ataques de negação de serviço podem ser feitos de várias maneiras:

- Através do envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;

- pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;

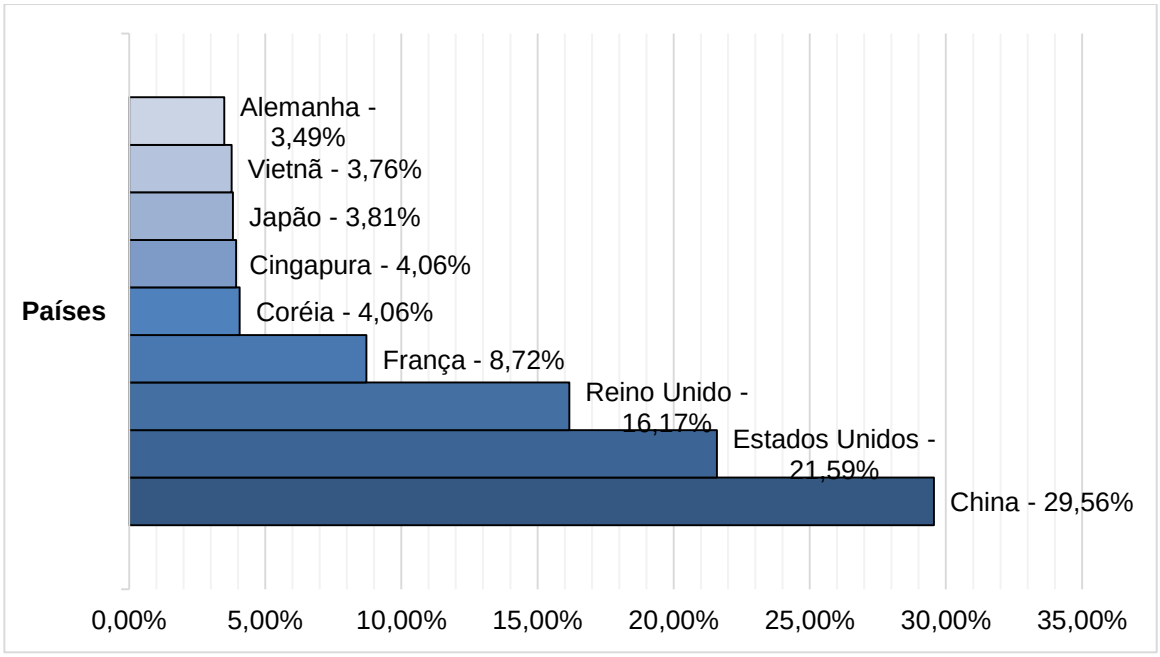
- pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.

Nas situações onde há saturação de recursos, caso um serviço não tenha sido bem dimensionado, ele pode ficar inoperante ao tentar atender as próprias solicitações legítimas. Segundo um artigo da empresa Zillion Cybersecurity:

> “Os alvos geralmente são servidores de empresas, governo e sites web... ... Toda a empresa que tem algum serviço na Web pode ser atacada, seja um ERP que vendedores acessam externamente, seja um site de notícias, ou uma loja virtual.” (ZILLION, 2018)

A *Figura 4* apresenta os países mais afetados com ataques por DDoS em 2019.

Figura 4 – Taxas de Ataque por DDoS - Países mais atacados



Fonte: Elaborado pelo Autor – Dados Comparitech (BISCHOFF, 2020)

3.4 Países mais atingidos pela espionagem cibernética

A espionagem cibernética é a ação realizada por um agente adverso que busca obter, de maneira ilícita, acesso a informações sensíveis ou sigilosas de um

governo ou de instituições para beneficiar outros países, organizações, grupos de interesse ou empresas.

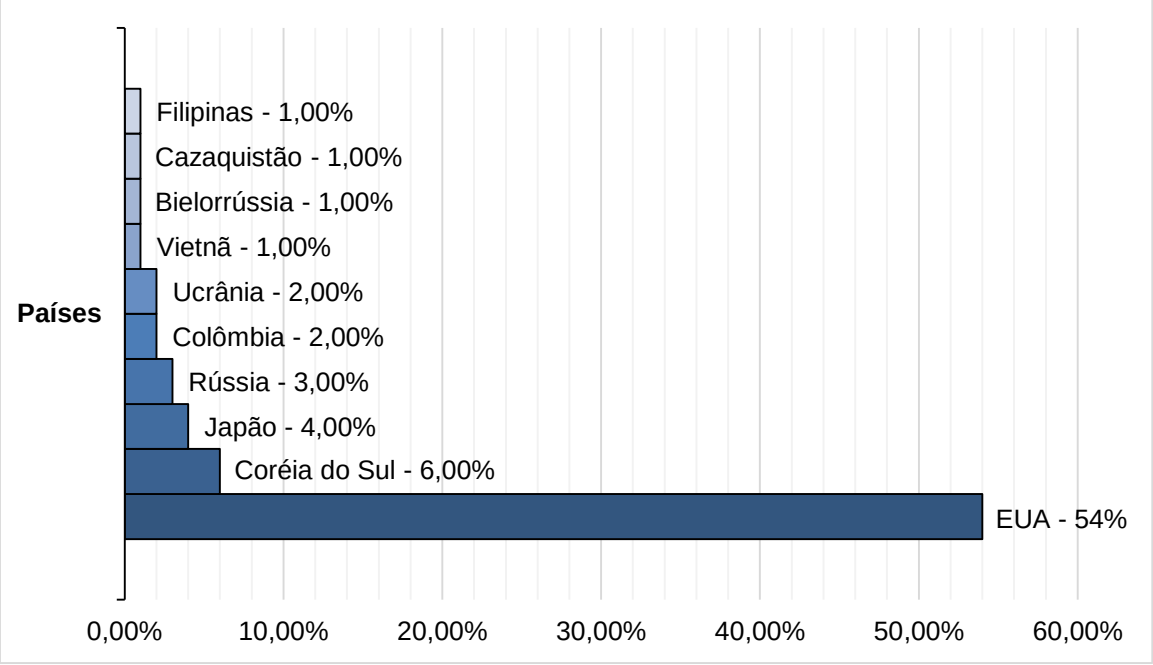
Ações de espionagem permitem a agentes adversos aos interesses do país o acesso indevido a conhecimentos sensíveis, como o domínio de tecnologias avançadas ou decisões tomadas na condução das relações internacionais.

A obtenção destes dados por espiões prejudica a competitividade econômica do país, compromete objetivos estratégicos nacionais e afeta a condução da política exterior. Por meio de ações de espionagem, o agente adverso busca acessar dados que não estão disponíveis em fontes de informação abertas.

O intuito é fornecer ao seu patrocinador vantagens de natureza política, geopolítica, militar, econômica, tecnológica ou científica. O acesso não autorizado à informação sigilosa pelo agente adverso pode ocorrer não apenas de forma física e presencial – como no caso da obtenção de cópia de documento sigiloso – mas também de maneira remota, por meio de operações de espionagem cibernética.

A Figura 5 apresenta os países com maiores taxas de espionagem cibernética em 2019.

Figura 5 – Espionagem Cibernética



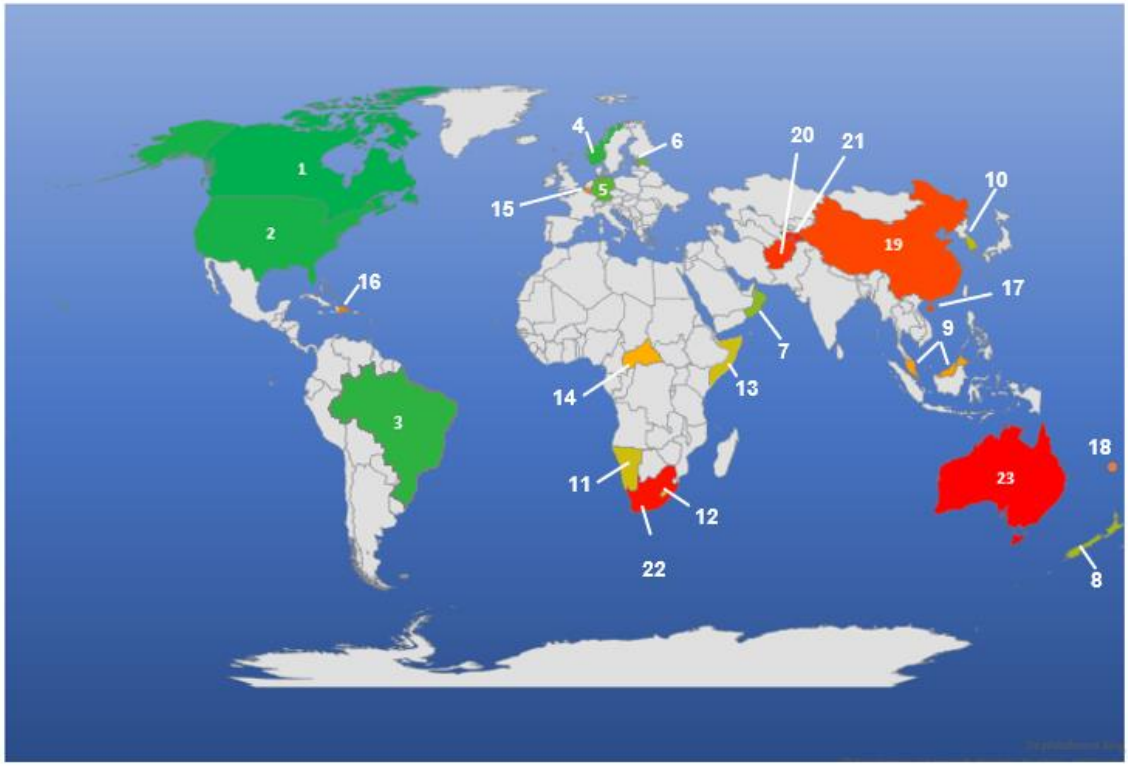
Fonte: Elaborado pelo Autor – Dados Comparitech (BISCHOFF, 2020)

3.5 Cenário mundial de preparação contra ataques cibernéticos

A preocupação de instituições e governos em investir em proteção contra *hackers* vem aumentando, passando a investir mais em processos e projetos que, de modo constante, contribuam em proteger contra os riscos de vazamento de dados.

A Figura ***6*** apresenta os países mais bem preparados, bem preparados e vulneráveis aos ataques cibernéticos em 2019.

Figura 6 – Cenário Mundial de Preparação contra Ataques Cibernéticos



Legenda					
	Melhor preparado		**Bem preparado**		**Vulnerável**
1	Canadá	10	Coreia do Sul	15	Bélgica
2	Estados Unidos	11	Namíbia	16	República Dominicana
3	**Brasil**	12	Lesoto	17	Hong Kong
4	Noruega	13	Somália	18	Samoa
5	Alemanha	14	República Centro-Africana	19	China
6	Estônia			20	Afeganistão
7	Omã			21	Tajiquistão
8	Nova Zelândia			22	África do Sul e
9	Malásia			23	Austrália

Fonte: Elaborado pelo Autor – Dados Comparitech (BISCHOFF, 2020)

NOTA - As estatísticas foram preparadas pela CompariTech com base em recursos como telegraph.co.uk, freedomhouse.org e statista.com

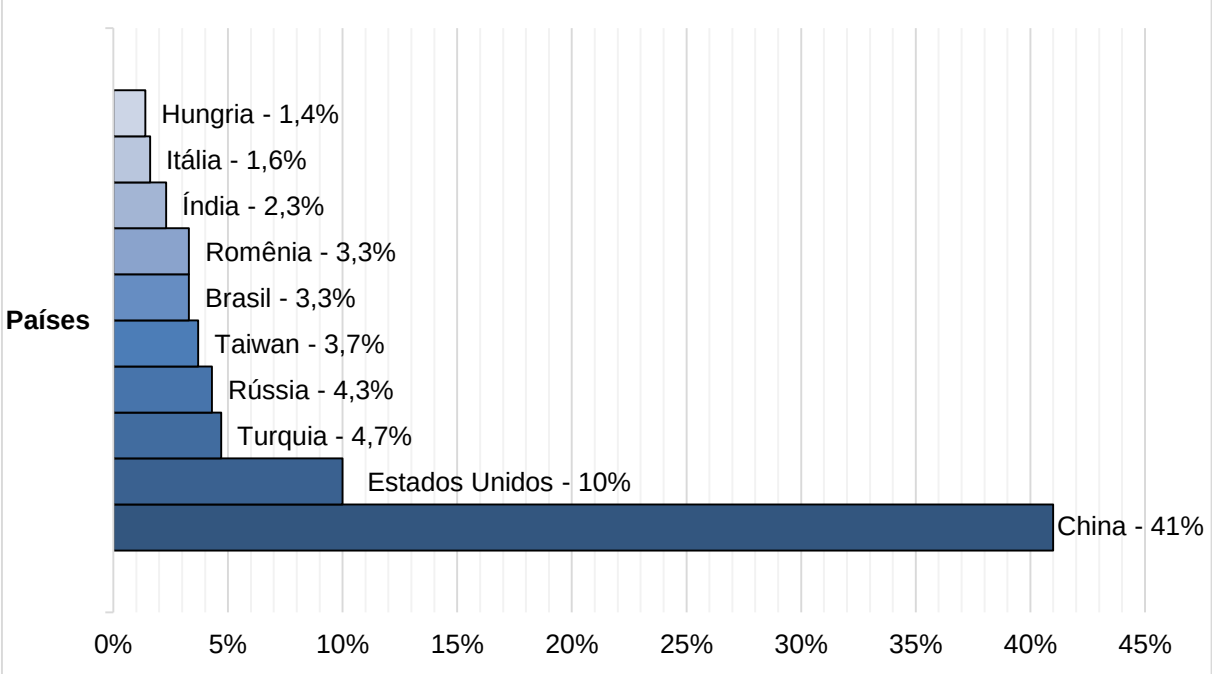
3.6 Os dez países com maior origem de ataques cibernéticos

Os ataques cibernéticos são motivados por vários aspectos diferentes, dentre elas, ganho financeiro, ativismo, desafio, entre outros.

A rede de distribuição de conteúdo (CDN - *Content Delivery Network*) GoCache fez um estudo e apontou que as principais fontes de ciberataques no mundo são a China, os EUA, Turquia, Rússia e Taiwan.

A seguir a Figura 7 mostra a lista dos 10 países com maior origem de ataques cibernéticos em 2017.

Figura 7 – Os 10 países com maior origem de ataques cibernéticos



Fonte: Elaborado pelo Autor – Dados Gocache (GOCACHE, 2017)

4 OS PRINCIPAIS ATAQUES QUE CONTRIBUIRAM PARA EVOLUÇÃO DA SEGURANÇA DA INFORMAÇÃO

Os ataques cibernéticos nas empresas têm se tornado um grande problema, visto que esta área está envolvida com a proteção de todos os dados fundamentais de uma organização, como relatórios, informações de clientes, dados fiscais, planejamentos, entre outros.

Em geral, os ataques são feitos em plataformas com excelência em coletar um grande volume de informações, como sites de instituições financeiras, bancos, grandes varejistas, organizações médicas, entre outros.

4.1 *Ransomware WannaCry*

Em maio de 2017 um ataque *hacker* atingiu computadores em quase cem países. O ataque foi detectado primeiro no sistema de saúde britânico e atingiu o governo Russo, serviços de entregas de encomendas americano, universidades na China e Indonésia, sistemas de trens na Alemanha, empresas de telecomunicações na Espanha e em Portugal, dentre outras.

No Brasil, o GSI (Gabinete de Segurança Institucional) da Presidência da República divulgou nota informando que o ataque ocorreu "em grande quantidade, por meio de e-mails com arquivos infectados". Na mesma nota, o GSI afirma que “foram confirmados incidentes pontuais em estações de trabalho de servidores do INSS. Até o momento, não há registros e evidências de que a estrutura de arquivos dos órgãos da Administração Pública Federal (APF) tenha sido afetada". (BRASÍLIA, 2017)

O ataque consistia em: O usuário recebia um e-mail aparentemente confiável e quando o mesmo clicava no anexo, o computador era infectado e tudo o que estava ligado à rede que fazia parte; os dados do computador eram criptografados e um pedido de resgate, mínimo de US$ 300,00 (o equivalente a R$ 1.000,00 em 2017), era exigido para liberação dos dados. Estima-se que os *hackers* tenham conseguido mais de um bilhão de dólares.

Companhias privadas de segurança identificaram o *ransomware* com uma espécie de bloqueio que cobrava um resgate em criptomoedas (moeda digital) para

que o acesso fosse restabelecido, do contrário os arquivos poderiam ser perdidos e até mesmo publicados, como uma variação do “*WannaCry*”, que tem a habilidade de automaticamente se espalhar por grandes redes ao explorar um conhecido erro no sistema operacional *Windows*.

A polícia europeia não descobriu quem estava por trás dos ataques, mas já se sabe quem desenvolveu a tecnologia, o Governo Americano - através da NSA (Agência de Segurança Nacional dos Estados Unidos). A NSA produz as armas da guerra virtual, vírus que atacam sistemas cibernéticos para espionar terroristas e outros Governos, por exemplo. O problema é que várias dessas armas virtuais da NSA foram roubadas por *hackers* em 2016 e uma delas foi usada para fazer o vírus que atacou o mundo em 2017.

- **Medidas tomadas após o ataque para resolução do problema**

A Microsoft (2019) disponibilizou soluções para proteger seus clientes. As medidas foram projetadas para atender os indivíduos e as empresas, fornecendo atualizações a todas as plataformas do *Windows*, tornando-os seguros.

Além disso, a Microsoft impôs atualizações automáticas do *Windows,* que corrige a vulnerabilidade explorada por ataques *WannaCry.* Para se proteger de ataques *ransomware,* a Microsoft recomenda:

- Fazer backup de arquivos importantes regularmente. Usar a regra 3-2-1, mantenha três (3) backups de seus dados em dois (2) tipos de armazenamento diferentes e, pelo menos um (1) backup externo;

- Aplicar as atualizações mais recentes aos seus aplicativos e sistemas operacionais;

- Instruir os funcionários da organização para que possam identificar engenharia social e ataques de *spear phishing* (prática onde um e-mail fraudulento é enviado através de um remetente conhecido ou confiável, que busca coletar informações confidenciais do alvo);

- Controlar o acesso às pastas, o que pode impedir o *ransomware* de criptografar arquivos e manter os arquivos para resgate.

O Presidente e Diretor Jurídico da Microsoft, Brad Smith citou sobre esse ataque:

> “Os governos do mundo devem tratar este ataque como um alerta. Precisam adotar uma abordagem diferente e levar ao ciberespaço as mesmas regras aplicadas às armas no mundo físico. Precisamos que os governos considerem o dano causado aos civis por armazenar essas vulnerabilidades e usar programas que as exploram.” (BRAD SMITH, 2017).

4.2 *Malware* paralisa quatro plataformas das empresas do grupo *Kolbenschmidt – Rheinmetall Automotive*

A empresa situada no Brasil há 52 anos, possui uma de suas plantas no interior do estado de São Paulo, na cidade de Nova Odessa. *Rheinmetall Group* são empresas de armas e autopeças, porém, somente o ramo automotivo foi afetado.

No dia 24 de setembro de 2019 a empresa de autopeças teve problemas de operação por ter sido afetada por um ataque *malware*. No dia 30 de setembro a Divisão MS Motorservice Brazil - KSPG *Automotive* disponibilizou uma nota no site oficial informando sobre a interrupção dos processos operacionais:

> “Pela presente carta informamos que a infraestrutura de TI da divisão Automotive do Rheinmetall Group nas fábricas no Brasil, México e EUA foi afetada por um ataque de *malware* desde a noite de 24 de setembro de 2019. Por essa razão, os processos e o funcionamento normal destes locais sofrem atualmente grandes perturbações.
> De acordo com as informações mais recentes, os demais sistemas de TI do Grupo não estão afetados.
> A empresa está fazendo todos os esforços para eliminar a falha nas fábricas afetadas o mais rápido possível e manter o máximo possível a capacidade de fornecimento aos clientes. Embora a capacidade de fornecimento seja garantida a curto prazo, não é possível fazer nenhuma declaração sobre a duração da falha. Nos cenários mais prováveis pode demorar entre duas e quatro semanas.” (KSPG AUTOMOTIVE BRAZIL, 2019)

Segundo o porta-voz da *Rheinmetall*, Peter Ruecker, “A infraestrutura de TI na região foi desativada e está sendo reconstruída atualmente”, frisando que a empresa não poderia dizer quem estaria por trás dela.

Apesar da empresa não comunicar qual tipo de ataque, apenas que era um *malware*, alguns funcionários da plataforma Brasileira afirmaram que o ataque paralisou parcialmente as operações e que foi pedido resgate através de *bitcoins*, caracterizando um ataque *ransomware*. Até onde se sabe, o resgate não foi pago.

O Grupo acredita que o impacto financeiro nos resultados operacionais chegou de 3 a 4 milhões de euros por semana.

4.3 Vazamento de Dados na *Target* – 2013

A rede *Target Corp*. sofreu um ataque *hacker* na *Black Friday* de 2013.

Segundo a jornalista Nicole Perlroth, em publicação no jornal *The New York Times* (NYT):

> "...o alvo foi atingido durante a época de compras de feriado quando os sistemas de detecção fraude tiveram dificuldades em identificar transações legítimas de falsas." (PERLROTH, 2013)

Na mesma publicação Paul Kocher, presidente da *Cryptografhy Research* (Empresa que desenvolve tecnologias para prevenir fraudes) disse: "Esta é a tempestade perfeita", para a vulnerabilidade a *hackers.*

Em outro artigo do NYT a jornalista Nicole Perlroth (2014) informou que, "... *hackers* conseguiram invadir através da empresa de gerenciamento de aquecimento e refrigeração do varejista."

No primeiro momento houve roubo das credenciais de um fornecedor de serviços da Target, o qual foi infectado por meio de uma campanha de *phishing* (em inglês corresponde a "pescaria", tem o objetivo de "pescar" informações e dados pessoais importantes através de mensagens falsas) por *e-mail*.

As credenciais foram utilizadas para conseguir infiltrar nos serviços da Web hospedados pela Target, destinado a fornecedores. Através de uma vulnerabilidade, fizeram um envio de um arquivo malicioso, fazendo parecer algo legítimo ocultando à vista da equipe de segurança.

Obtendo êxito, conseguiram consultar o *Active Directory* com ferramentas internas do *Windows* usando o protocolo LDAP (*Lightweight Directory Access Protocol* - Protocolo de acesso aos diretórios leves) padrão.

Tendo acesso ao diretório os atacantes criaram uma conta de administrador para ter os privilégios e obter o controle da conta, além da senha. Depois de contornar os dispositivos de segurança os invasores utilizaram ferramentas de

scanner de rede para saber quais computadores estavam conectados à rede, tendo acesso aos sistemas de destino, passaram a executar remotamente códigos nos servidores comprometidos.

Com isso, os atacantes conseguiram instalar um *malware* infectando as máquinas, que foi utilizado para verificar a memória das mesmas e salvando os cartões de crédito encontrados em um arquivo local.

A *software* de segurança da FireEye utilizado pela Target, emitiu vários alarmes avisando a equipe de segurança que não consideraram necessário acompanhamento de imediato.

Como resultado do ataque, a segunda maior rede varejista de lojas de departamento dos Estados Unidos a Target, os *hackers* obtiveram acesso de pelo menos quarenta milhões de cartões e setenta milhões de outros dados dos clientes, com um prejuízo estimado em US$ 400 milhões.

De acordo com matéria publicada pelo UOL (2014), o responsável pelo *malware* usado no ataque à Target, foi um adolescente russo de dezessete anos. Acredita-se que o adolescente não estava envolvido diretamente no ataque, ele teria apenas desenvolvido e vendido o código. A consultoria IntelCrawler afirmou que o *malware* foi comercializado para pelo menos quarenta grupos de criminosos.

- **Medidas tomadas após o ataque para resolução do problema**

O diretor financeiro e vice-presidente executivo da Target, John Mulligan disse em comunicado:

> “Os cartões inteligentes habilitados para chip contêm um minúsculo chip de microprocessador que criptografa os dados das transações compartilhadas com os terminais de vendas usados pelos comerciantes. Como resultado, mesmo se o número do cartão for roubado em uma violação de dados, os ladrões não poderão falsificar o cartão.” (MULLIGAN, 2014).

Na mesma nota, Muligan informou que:

> “Além disso, exigir o uso de um número de identificação pessoal (PIN) de quatro dígitos para concluir uma transação de vendas proporcionaria uma segurança ainda maior...A Target também está investindo em soluções que tornarão as transações móveis mais seguras...” (MULLIGAN, 2014).

4.4 Roubo de dados da *Home Depot* – 2014

A varejista americana *Home Depot* informou que cerca de cinquenta e seis milhões de cartões de créditos de seus clientes foram comprometidos.

A *Home Depot* tem 2.265 lojas nos Estados Unidos, Canadá e México, com um volume de vendas anual de 78,8 milhões de dólares. Segundo Perlroth publicou:

> "... Home Depot disse que alguém usou o nome de usuário e a senha de um de seus fornecedores para ganhar uma posição, e depois invadir diferentes partes dos sistemas da Home Depot, incluindo um banco de dados de e-mails de clientes e a caixa registradora da empresa sistemas. ... Os funcionários dizem que a Home Depot não adotou uma abordagem agressiva à segurança dos dados, confiando em software desatualizado e ignorando avisos de funcionários. Mas a empresa disse que o *malware* usado para roubar dados de seus sistemas nunca foi usado antes da violação e teria sido difícil para seu sistema antivírus detectar." (PERLROTH, 2014)

- **Medidas tomadas após o ataque para resolução do problema**

Segundo a publicação do jornal O Globo (2014) a empresa afirma que o canal de acesso dos *hackers* foi fechado, e o *software* malicioso (*malware*) eliminado da sua rede. A companhia também informou que tomou providências para *encriptar* os dados de pagamentos em todas as suas lojas americanas.

Além de custos com monitoramento de crédito, aumento de telefonistas em seus *call-centers*, e a contratação de advogados, a companhia estima um custo inicial de US$ 27 milhões a ser pago as seguradoras. Custos relacionados ao reembolso de bancos e a substituições de cartões ainda não foram estimados, assim como aqueles relacionados a possíveis processos ou investigações governamentais.

Algumas lições foram aprendidas com esses ataques as grandes organizações, entre elas podemos citar:

- Ter um controle rígido ao acesso à rede para terceiros;
- Manter controles de segurança quando *Active Directory* for utilizado pela organização, pois o mesmo é muito utilizado em ataques;

- Ter uma equipe capaz de monitorar e identificar qualquer anormalidade nos acessos;
- Utilizar autenticação de múltiplos fatores para sistemas e ambientes sensíveis;
- Investir no tratamento de alertas e escalonamento correto dos incidentes;
- Investir em ferramentas e recursos de Segurança da Informação.

4.5 Como esses ataques influenciaram a área de segurança?

Os ataques estão nitidamente evoluindo considerando que alguns são planejados a longo prazo, complexos e inovadores, com isso as soluções de segurança precisam ser implementadas seguindo uma política consistente, capacidade analítica e recursos avançados a fim de combater de forma efetiva.

O time de tecnologia precisa estar ciente e bem treinado em relação as ferramentas de monitoramento, ou, do contrário os alertas podem ser ignorados ou não identificados da forma correta. A equipe de TI precisa se manter informada, participar de grupos sobre inteligência cibernética, sobre segurança da informação etc. O conhecimento adquirido pode ser um fator de sucesso na identificação e bloqueio de ataques, como também o aprimoramento das tecnologias do setor, para que sejam capazes de detectar comportamento de um *malware* novo.

As grandes potências mundiais são os principais alvos dos ataques cibernéticos, mesmo porque o desenvolvimento tecnológico nesses lugares sempre está à frente do resto do mundo. Há também questões como economia, poder de armamento e descobertas de novas tecnologias que fazem deles os maiores alvos desses ataques.

Devido ao grande avanço tecnológico nas últimas décadas e a evolução dos dispositivos como computadores e aparelhos de telefonia, a criação da Internet, a capacidade de comunicação em tempo real, fez-se necessário criar uma categoria para os crimes cometidos utilizando esses meios.

Há diversos fatores que influenciam o crescimento dos ataques cibernéticos, podemos destacar entre eles:

- **Escala** – a Internet dá poder aos atacantes de atingir alvos distantes sem um grande custo para ele.
- **Acessibilidade** – a disponibilidade da tecnologia na palma das mãos, equipamentos cada vez menores e mais leves que permitem facilidade no acesso.
- **Anonimato** – a capacidade dos atacantes em esconder sua identidade com o uso da tecnologia.
- **Alcance Global** – a capacidade de cometer crimes em outras jurisdições, porém estarem protegidos por leis locais. Em muitos países, ainda não há legislação específica para crimes cibernéticos.

5 SOLUÇÕES PARA COMBATER CIBERATAQUES

Ao passo que a tecnologia vai avançando e novos métodos de ataques são desenvolvidos, manter a Segurança da Informação de uma organização ou instituição fica cada vez mais complexo e desafiador.

Pensando nisso, algumas das medidas mais importantes para prevenção e combate aos ciberataques são possuir um Política de Segurança eficiente, uma equipe de Cibersegurança capacitada e uma equipe que possa gerenciar as crises quando elas ocorrerem, ou seja, Grupo de Resposta a Incidentes de Segurança ou CSIRT (*Computer Security Incident Response*).

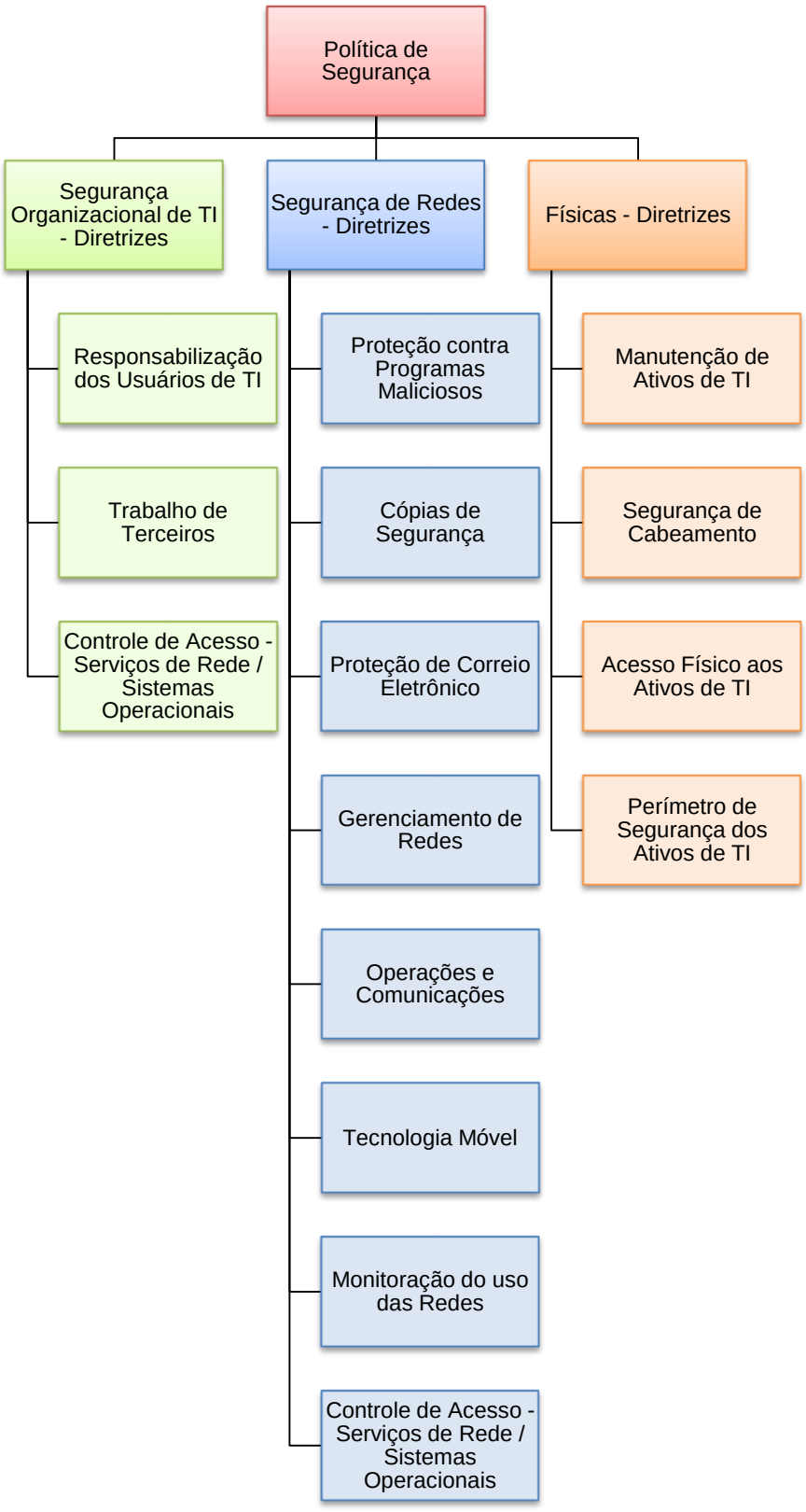
5.1 Política de Segurança

Uma Política de Segurança da Informação é um conjunto de diretrizes e normas que definem quais critérios de segurança são adotados e quais são as atividades que cada indivíduo envolvido na segurança da informação deve executar. Uma política eficiente abrange:

- Diretrizes de Segurança Organizacional;
- Diretrizes de Segurança de Redes;
- Diretrizes de Segurança Física.

Na Figura 8 é possível verificar em detalhes os principais pontos dentro de uma Política de Segurança.

Figura 8 – Política de Segurança



Fonte: Elaborado pelo Autor

As diretrizes de **Segurança Organizacional** têm como objetivo gerenciar a segurança das informações dentro da empresa. Compreende composição de senhas e segurança em estações de trabalho.

As diretrizes de **Segurança de Redes** têm como objetivo controlar os acessos da organização aos recursos de TI. Compreende configuração de sistemas operacionais, acesso lógico e remoto, autenticação, Internet, gerenciamento de mudanças e desenvolvimento de aplicativos.

As diretrizes **de Segurança Física** têm como objetivo impedir acesso não autorizado às instalações físicas da organização. Compreende acesso físico, infraestrutura do edifício e datacenter.

De modo geral deve abranger também segurança de dados – criptografia, privilégios, antivírus e plano de contingência – aspectos legais.

Para elaboração dessa política é necessário a formação de um Comitê de Segurança, formado por uma equipe multidisciplinar que represente parte dos aspectos culturais, técnicos e administrativos da organização. Esse comitê é responsável pelas atividades referentes à criação e aprovação de requisitos e demandas de segurança na organização. O documento é formado por:

- Objetivo e Escopo;
- Entrevista;
- Investigação e Análise de Documentos;
- Reunião de Política;
- Glossário da Política;
- Responsabilidades e Penalidades.

A Política final deve ser oficializada com base na aprovação pela administração da organização e deve ser comunicada a todos os envolvidos com a organização, desde funcionários a clientes. É importante deixar todos cientes das consequências do não cumprimento da mesma.

Uma política bem implementada reflete os objetivos do negócio, segurança nos processos e está de acordo com a cultura organizacional. Deve ser baseada na análise de risco e ter como principal objetivo a padronização de ambientes e processos de TI. Deve ser reavaliada sempre que se identificar a necessidade.

Segundo o CERT.br as motivações para o estabelecimento de CSIRTs incluem:

- Um aumento generalizado na quantidade de incidentes de segurança sendo reportados;
- Um aumento generalizado na quantidade e variedade de organizações sendo afetadas por incidentes de segurança em computadores;
- Uma maior consciência, por parte das organizações, da necessidade de políticas e práticas de segurança como parte das suas estratégias globais de gerenciamento de riscos;
- Novas leis e regulamentos que afetam a maneira como as organizações precisam proteger as suas informações;
- A percepção de que administradores de redes e sistemas não podem proteger sozinhos os sistemas e as informações da organização.

5.2 Equipe de Segurança da Informação

Para que a Política de Segurança seja eficiente, é necessário que seja aplicada da forma correta e acompanhada para que não perca sua efetividade, e é por isso que uma equipe de Segurança da Informação é necessária.

Essa equipe é responsável pela prevenção de incidentes de segurança cibernética, monitoramento, detecção e análise de possíveis intrusões, resposta a incidentes de segurança e fornece relatórios de status e dos incidentes, bem como de tendências e comportamento dos atacantes.

Uma equipe de Segurança da informação pode ser formada seguindo diversas metodologias de trabalho. Uma dessas metodologias é criar um SOC (Centro de Operações de Segurança), que é composta principalmente por analistas

de segurança e cada um desses analistas tem um papel a desempenhar dentro do time.

A estrutura do SOC é uma divisão por camadas ou níveis:

- **Camada 1: Analista de Alertas**

  Faz todo o monitoramento na fila de alertas de segurança e também da integridade dos sensores e terminais de segurança.

- **Camada 2: Respondente de Incidente**

  Faz a análise dos incidentes, é quem determina se um sistema foi corrompido de alguma forma e também fornece suporte para novas formas de detecção de ameaças.

- **Camada 3: *Hunter* (caçador)**

  Literalmente é um caçador de incidentes, que não espera o incidente ocorrer. Tem um vasto conhecimento de engenharia de rede, ameaças, engenharia forense e engenharia reversa. Também fornece suporte e desenvolve soluções para detecção de ameaças.

- **Camada 4: Gerente de SOC**

  Faz a gerência de recursos, orçamento, programação dos trabalhos a serem executados. É o ponto de apoio para a organização no momento de um incidente e também responsável pela estratégia geral de segurança.

Uma boa equipe de cibersegurança é aquela que consegue atender todas as necessidades da organização, diminuindo o impacto que um ataque pode trazer a mesma e restabelecer a operação quando necessário de forma rápida e eficaz, considerando sempre as boas práticas de segurança e de negócio.

5.3 CSIRT - Grupo de resposta a incidentes de segurança

Quando um incidente de segurança, evento adverso que viole de alguma forma uma política de segurança, ocorre, é necessário minimizar os danos que o

mesmo pode trazer para a organização. Uma ação rápida e eficaz irá determinar os danos que a que a mesma sofrerá, por isso é essencial que haja um CSIRT.

Os objetivos do CSIRT devem ir de encontro com os objetivos da entidade/organização que ele atende. Os membros do CSIRT precisam ter habilidade para resolverem problemas, serem comunicativos e principalmente saberem lidar com situações estressantes. Essa equipe é composta por membros de diversos setores da organização, uma equipe multidisciplinar é importante pois em um momento de crise todo o público interessado deve estar ciente de quais ações serão tomadas para que o impacto do incidente seja o menor possível.

Essa equipe fará a Gestão de Riscos, que é um conjunto de processos que identificam medidas de proteção necessárias para diminuir os riscos. O risco nesse caso é qualquer evento que possa gerar impacto no andamento da organização.

Especificamente para Segurança da Informação, é importante identificar potenciais ameaças que possa colocar o negócio em risco. Assim, é de suma importância conhecer as vulnerabilidades as quais a organização está exposta e ter em mãos um Plano de Continuidade de Negócios (PCN), que é elaborado considerando as diversas situações consideradas como possíveis crises.

No site do CERT.br é possível entender em oitos passos como criar um CSIRT, são eles:

- Passo 1: Obter o apoio e a aprovação da administração superior;
- Passo 2: Determinar o plano de desenvolvimento estratégico do CSIRT;
- Passo 3: Coletar as informações relevantes;
- Passo 4: Conceber a visão do seu CSIRT;
- Passo 5: Comunicar a visão do CSIRT;
- Passo 6: Iniciar a implementação do CSIRT;
- Passo 7: Anunciar o CSIRT;
- Passo 8: Avaliar a eficácia do CSIRT.

Implementar um grupo como esse pode variar de organização para organização, e o tempo para o que o mesmo torne operacional pode variar de dois meses a dois anos, e até 18 meses para ter todos os procedimentos e políticas finalizadas.

A maturidade de um CSIRT reflete na confiança que a comunidade tem sobre o mesmo e isso é refletido nos incidentes reportados que tendem a crescer junto com essa maturidade.

Há diversas práticas para garantir a cibersegurança de uma organização, esse capítulo demonstrou apenas algumas dessas práticas. A segurança da informação é um campo da tecnologia que está em constante mudança, assim, novas práticas para combate e prevenção a ciberataques tendem a surgir constantemente.

6 CONSIDERAÇÕES FINAIS

Este trabalho de pesquisa buscou apresentar o entendimento de seus autores sobre os temas abordados sob supervisão do orientador, bem como demonstrar o conhecimento dos mesmos e a realidade que poderão enfrentar no mercado na área de estudo que escolheram, visto que, discutir aspectos relacionados a evolução dos crimes cibernéticos frente aos desafios que os mesmos trazem, ampliam o entendimento sobre Segurança da Informação e seus conceitos.

Os temas abordados buscam trazer aos leitores entendimento de que o mundo está em constante evolução e, a evolução tecnológica traz benefícios, porém muitos perigos contra os quais algumas pessoas não possuem conhecimentos e muitas organizações não se encontram preparadas para evitá-los e combatê-los.

Os estudos apresentados demonstram através de métodos científicos e confiáveis como organizações e governos estão se preparando para enfrentarem de forma eficaz com não apenas o cibercrime, mas também os cibercriminosos, que utilizam principalmente do anonimato que a Internet lhes proporciona para cometerem seus crimes.

A falta do compartilhamento de informações sobre ciberataques que ocorrem no mundo, principalmente das grandes organizações, dificulta o trabalho de pesquisa e com isso, definição das melhores práticas para combate a esses ataques.

A formação de profissionais de Tecnologia da Informação, especializados em Segurança, cresceu nos últimos anos devido a essa necessidade do mercado de obter profissionais que possam ser capazes de ajudar na transformação que essas organizações estão sofrendo, porém de forma consciente e segura. Os crimes cibernéticos estão em constante evolução, porém os profissionais estão evoluindo na mesma proporção.

Por fim, é possível concluir que sempre haverá reflexões em torno dos cenários de ameaças, que estão se desenvolvendo gradualmente, fazendo-se necessário avanços nas defesas e inteligência, para um gerenciamento eficaz dos riscos.

REFERÊNCIAS

ARAUJO, Márcio T.; FERREIRA, Fernando Nicolau Freitas. Política de Segurança da Informação. 2. ed. -: Ciência Moderna, 2009.

BISCHOFF, Paul. Which countries have the worst (and best) cybersecurity? 2020. Disponível em: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/. Acesso em: 13 jun. 2020.

BORNELI, Júnior. Primeiro site lançado no mundo completa 25 anos. 2015. Disponível em: https://www.startse.com/noticia/empreendedores/primeiro-site-lancado-no-mundo-completa-25-anos. Acesso em: 11 maio 2020.

BRAD SMITH. A necessidade de ação coletiva urgente para manter as pessoas seguras online: lições do ciberataque da semana passada. 2017. Disponível em: https://news.microsoft.com/pt-br/a-necessidade-de-acao-coletiva-urgente-para-manter-as-pessoas-seguras-online-licoes-do-ciberataque-da-semana-passada/. Acesso em: 18 jun. 2020.

BRASÍLIA. GSI - GABINETE DE SEGURANÇA INSTITUCIONAL. . Ciberataque - Nota à Imprensa. 2017. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/notas-a-imprensa/ciberataque.pdf/view. Acesso em: 08 jun. 2020.

CABRAL, Isabela. A História dos domínios de Internet: conheça a origem, o desenvolvimento e o lucrativo mercado por trás dos endereços da internet. Conheça a origem, o desenvolvimento e o lucrativo mercado por trás dos endereços da Internet. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/a-historia-dos-dominios-de-internet.ghtml. Acesso em: 11 maio 2020.

CERT.BR. Ataques na Internet. 2017. Disponível em: https://cartilha.cert.br/ataques/. Acesso em: 07 jun. 2020.

CERT.BR. Cartilha de Segurança para Internet. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/. Acesso em: 15 abr. 2020.

CERT.BR. Códigos maliciosos (Malware). 2017. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 07 jun. 2020.

CERT.BR. Materiais de Apoio para Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs). 2018. Disponível em: https://www.cert.br/csirts/. Acesso em: 04 maio 2020.

CERT.BR. Ransomware. 2018. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 07 jun. 2020.

CLOUGH, Jonathan. Principles of Cybercrime. New York: Cambridge University Press, 2010.

DAROS, Gabriel. Wifi completa 15 anos - veja a trajetória e curiosidades da conexão sem fio de seus dispositivos. 2014. Disponível em: https://adrenaline.com.br/artigos/v/28119/wifi-completa-15-anos-veja-a-trajetoria-e-curiosidades-da-conexao-sem-fio-de-seus-dispositivos. Acesso em: 11 maio 2020.

FONTES, Edison Luiz Gonçalves. Segurança da Informação: o usuário faz a diferença. Rio de Janeiro: Saraiva, 2007.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. Revista de Doutrina da 4ª Região, Porto Alegre, v. 1, n. 55, p. 1-1, 30 ago. 2013. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao055/. Acesso em: 04 maio 2013.

GOCACHE. Veja os 10 países do mundo com maior número de hackers e crimes cibernéticos. 2017. Disponível em: https://www.gocache.com.br/seguranca/dez-paises-com-mais-ataques-de-hackers/. Acesso em: 06 mar. 2020.

GOUD, Naveen. List of Countries which are most vulnerable to Cyber Attacks. Disponível em: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/. Acesso em: 07 maio 2020.

GRAGIDO, Will; MOLINA, Daniel; PIRC, John; SELBY, Nick; HAY, Andrew. Blackhatonomics: an inside look at the economics of cybercrime. Waltham: Elsevier, 2013.

ITU. Global Cybersecurity Index. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Acesso em: 13 jun. 2020.

KLEINA, Nilton. Primeiro vírus de computador completa 40 anos. 2011. Disponível em: https://www.tecmundo.com.br/virus/9184-primeiro-virus-de-computador-completa-40-anos.htm. Acesso em: 11 maio 2020.

KSPG AUTOMOTIVE BRAZIL. Informações sobre a interrupção dos processos operacionais. 2019. Disponível em: https://www.ms-motorservice.com.br/novidades/imprensa-e-informacao/artigos/news/informacoes-sobre-a-interrupcao-dos-processos-operacionais/. Acesso em: 14 jun. 2020.

LAUDON, Kenneth; LAUDON, Jane. Sistemas de Informações Gerenciais. --: Pearson Universidades, 2014.

LEWIS, Peter H.. Attention Shoppers: Internet Is Open. 1994. Disponível em: https://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html%2011/05/20. Acesso em: 11 maio 2020.

MACEDO, Joyce. Conheça a história dos buscadores e veja como o Google alcançou o topo. 2015. Disponível em: https://canaltech.com.br/internet/conheca-a-historia-dos-buscadores-e-veja-como-o-google-alcancou-o-topo-47289/. Acesso em: 11 maio 2020.

MARTIN, James A.. Who is a target for ransomware attacks? 2017. Disponível em: https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html. Acesso em: 07 jun. 2020.

MICROSOFT. Ransomware. 2019. Disponível em: https://docs.microsoft.com/pt-br/windows/security/threat-protection/intelligence/ransomware-malware#como-proteger-contra-o-ransomwarehow-to-protect-against-ransomware. Acesso em: 20 jun. 2020.

MULLIGAN, John. Time for smartcards, an op-ed by John Mulligan, Executive Vice President and Chief Financial Officer, Target. 2014. Disponível em: https://corporate.target.com/press/releases/2014/02/time-for-smartcards-an-op-ed-by-john-mulligan-exec. Acesso em: 08 jun. 2020.

O GLOBO. Ataque hacker a varejista dos EUA expõe dados de 56 milhões de cartões de crédito: roubo de dados da home depot é maior que o sofrido pela target em 2013, quando 40 milhões de cartões vazaram. Roubo de dados da Home Depot é maior que o sofrido pela Target em 2013, quando 40 milhões de cartões vazaram. 2014. Disponível em: https://oglobo.globo.com/economia/ataque-hacker-varejista-dos-eua-expoe-dados-de-56-milhoes-de-cartoes-de-credito-13983296. Acesso em: 28 fev. 2020.

PERLROTH, Nicole. Home Depot Says Hackers Also Stole Email Addresses. 2014. Disponível em: https://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/. Acesso em: 08 jun. 2020.

PERLROTH, Nicole. Target Struck in the Cat-and-Mouse Game of Credit Theft. 2013. Disponível em: https://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html%2008/06/20. Acesso em: 08 jun. 2020.

RIBEIRO, Lígia Maria. A História da Internet. 1998. Disponível em: https://web.fe.up.pt/~mgi97018/historia.html. Acesso em: 04 maio 2020.

SCHMIDT, Guilherme. Crimes Cibernéticos. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 11 set. 2019.

SOUZA, Ramon de. Spam completa 40 anos; confira a história e fatos curiosos sobre a prática. 2018. Disponível em: https://canaltech.com.br/internet/spam-completa-40-anos-confira-a-historia-e-fatos-curiosos-sobre-a-pratica-113024/. Acesso em: 14 jun. 2020.

SPYMAN, Hacking. Manual Completo do Hacker. 3. ed. --: Book Express, 2000.

YATES, Mark. Os países mais perigosos e mais seguros para PCs. 2016. Disponível em: https://www.avg.com/pt/signal/safest-and-most-dangerous-countries-for-pcs. Acesso em: 03 jun. 2020.

ZILLION CYBERSECURITY. Conheça o que é e como funciona o ataque DDoS. 2018. Disponível em: https://www.zillion.com.br/?s=conhe%C3%A7a+como+%C3%A9+e+como+funciona+ataques+ddos. Acesso em: 07 jun. 2020.

ANEXO A

Tabela 1 – Classificação geral de segurança cibernética (da pior à melhor)

Classificação geral de segurança cibernética (do pior ao melhor)									
Classificação	**País**	**Pontuação**	**% de celulares Infectados com *Malware***	**Ataques financeiros por *Malware* (% de usuários)**	**% de computadores infectados com *Malware***	**% de ataques Telnet por país de origem (IoT)**	**% de ataques de Cryptominers**	**Melhor preparado para ataques cibernéticos**	**Legislação mais atualizada**
1	Argélia	55,75	22,88	0,9	32,41	0,01	5,14	0,432	1
2	Indonésia	54,89	25,02	1,8	24,7	1,51	8,8	0,424	4
3	Vietnã	52,44	9,62	1,2	21,5	1,73	8,96	0,245	2
4	Tanzânia	51,00	28,03	0,7	14,7	0,04	7,51	0,317	1,5
5	Uzbequistão	50,50	10,35	0,5	21,3	0,01	14,23	0,277	3
6	Bangladesh	47,21	35,91	1,3	19,7	0,38	3,71	0,524	3,5
7	Paquistão	47,10	25,08	1,4	14,8	0,4	6,07	0,447	2,5
8	Bielorrússia	45,09	9,33	0,7	31,1	0,04	9,73	0,592	3
9	Iran	43,29	28,07	0,8	12,7	1,71	4,51	0,494	2
10	Ucrânia	42,58	10,85	0,3	28,7	1,17	7,6	0,501	3
11	Nigéria	42,54	28,54	0,7	15,6	0,89	4,54	0,569	2
12	Peru	41,25	13,81	0,9	16,6	0,22	6,29	0,374	3
13	China	40,80	25,61	1,4	11,8	27,15	1,73	0,624	7
14	Sri Lanka	39,59	13,71	1,1	18,8	0,01	3,61	0,419	3
15	Índia	39,30	25,25	0,7	21,8	2,59	4,4	0,683	3,5
16	Grécia	39,06	5,78	2,3	21,6	0,73	1,77	0,475	4
17	Romênia	39,02	6,42	1,2	24,6	0,61	3,21	0,585	2
18	Equador	38,29	14,13	0,7	16,8	0,4	3,73	0,466	2
19	Azerbaijão	38,20	6,53	0,9	26,7	0,03	7,13	0,559	4
20	Egito	38,03	18,8	1,3	20,2	7,43	4,01	0,772	4

Classificação geral de segurança cibernética (do pior ao melhor)									
Classificação	**País**	**Pontuação**	**% de celulares Infectados com *Malware***	**Ataques financeiros por *Malware* (% de usuários)**	**% de computadores infectados com *Malware***	**% de ataques Telnet por país de origem (IoT)**	**% de ataques de Cryptominers**	**Melhor preparado para ataques cibernéticos**	**Legislação mais atualizada**
21	Bulgária	37,86	4,73	1,8	21,4	0,7	3,49	0,579	3
22	Coreia do Sul	37,16	7,14	2,8	14,3	3,57	3,1	0,782	3
23	Emirados Árabe Unidos	36,88	9,14	1,9	20,7	0,09	2,99	0,566	4
24	Filipinas	36,79	23,07	0,6	23,8	0,1	2,94	0,594	4
25	Marrocos	36,47	10,61	1,5	21,7	0,11	3,01	0,541	4
26	Eslováquia	35,57	5,32	0,6	22	0,13	2,76	0,362	3
27	Tunísia	35,54	9,85	1,2	21,5	0,1	2,78	0,591	3
28	África do Sul	34,39	9,9	1	13,4	0,64	2,51	0,502	2
29	Quênia	34,16	21,43	1,2	17	0,15	3,39	0,574	5
30	Brasil	33,57	7,96	0,4	21,5	10,57	2,74	0,593	4
31	Letônia	33,05	6,25	1,4	23,1	0,17	4,17	0,688	4
32	Arábia Saudita	32,99	10,15	0,7	20,7	0,11	2,72	0,569	3
33	Portugal	32,79	5,25	1,9	20,9	0,09	1,63	0,508	5
34	Tailândia	32,42	7,26	1	19,7	0,79	4,27	0,684	3
35	Malásia	31,79	15,46	2,1	21,7	0,24	2,87	0,893	5
36	Itália	28,31	5,24	1,3	18	1,75	1,14	0,626	4
37	Argentina	28,11	11,71	0,9	18,8	0,86	2,11	0,482	6
38	Rússia	28,02	10,11	0,6	23	7,87	6,89	0,788	7
39	Colômbia	27,69	12,52	0,5	16,4	0,52	2,01	0,569	4
40	Polônia	27,36	5,83	0,8	19,9	1,23	1,73	0,622	4
41	Hungria	27,30	7,28	0,8	20,2	0,3	4,19	0,534	6
42	México	27,17	10,49	0,7	19,5	0,73	1,43	0,66	4
43	Croácia	27,09	3,66	1,8	15,2	0,05	1,91	0,59	5
44	Alemanha	26,48	3,41	3	15,7	1,11	0,91	0,679	7
45	Áustria	25,76	2,94	1,4	12,3	0,12	0,84	0,639	3

Classificação geral de segurança cibernética (do pior ao melhor)									
Classificação	**País**	**Pontuação**	**% de celulares Infectados com *Malware***	**Ataques financeiros por *Malware* (% de usuários)**	**% de computadores infectados com *Malware***	**% de ataques Telnet por país de origem (IoT)**	**% de ataques de Cryptominers**	**Melhor preparado para ataques cibernéticos**	**Legislação mais atualizada**
46	Espanha	24,12	5,14	0,8	18,6	1,1	1,56	0,718	4
47	Peru	23,20	8,94	0,8	15,6	1,82	2,17	0,581	6
48	Bélgica	21,03	4,11	0,4	13,5	0,07	0,97	0,671	3
49	República Checa	20,37	5,68	0,5	10,9	0,34	1,44	0,609	4
50	Austrália	16,34	5,47	0,8	14,5	0,37	0,88	0,824	5
51	Cingapura	15,13	8,18	0,8	8,5	0,14	1,61	0,925	4
52	Países Baixos	15,00	3,71	0,6	8,1	0,32	1,06	0,76	4
53	Reino Unido	14,15	3,68	0,7	10,5	1,07	0,88	0,783	5
54	Suécia	13,78	3,15	0,4	11	0,45	1,31	0,733	5
55	Irlanda	13,41	3,73	0,5	7,9	0,06	0,85	0,675	5
56	Estados Unidos	12,20	7,68	0,5	10,3	4,47	0,71	0,919	5,5
57	Dinamarca	12,04	1,98	0,4	5,9	0,04	0,61	0,617	5
58	Canadá	11,19	3,91	0,4	14,3	0,47	0,81	09818	6
59	França	10,58	4,72	0,4	16,2	0,67	1,12	0,819	7
60	Japão	8,81	1,31	0,5	8,3	1,23	1,1	0,786	6

Fonte: Comparitech (BISCHOFF, 2020)