Impactos da Segurança Cibernética na Economia Global

Cybersecurity Impacts on the Global Economy

Wanderley Martins Junior[1]

Submetido em: 31/01/2023
Aprovado em: 01/02/2023
Publicado em: 06/02/2023
DOI 10.51473/ed.al.v3i1.478

Resumo

Esse artigo tem o intuito de retratar o posicionamento das diversas entidades governamentais e privadas quando lidando com os temas referentes à segurança cibernética. É comum percebermos nas mídias sociais e digitais que o mundo vem experenciando diversos desafios quando o assunto são ataques cibernéticos, invasões em ambientes corporativos, roubos de informações, vazamento de dados, extorsões e até mesmo problemas relacionados com a privacidade. Com a expansão e a elasticidade da internet, diversas novas tecnologias têm emergido permitindo cada vez mais formas interação e possibilidades. E nessa interatividade que devemos friamente nos preocuparmos com a segurança no ponto de vista globalizado. Então, a ideia aqui é de apresentarmos e entendermos como todos esses itens podem, juntos ou separados, afetam diretamente a economia global. Muitas empresas se sentem ameaçadas pelos mais perigosos recursos que podem pô-las em risco, mas como resultado não estão preparadas para se protegerem de ataques como *Ransomware*, em que os invasores sequestram dados por pedido de resgate. Citaremos nesse trabalho alguns danos que podem ser causados por inadimplência corporativa, ou simplesmente por grupos de invasores tendo como alvo órgãos governamentais com o objetivo de destruição em massa. Por fim, identificaremos alguns recursos que podem ser favoráveis para a mitigação dessas invasões e ataques, bem como delinear formas de mantermos os riscos em um nível aceitável.

Palavras-chave: 1. Economia Global 2. Segurança Cibernética 3. *Ransomware* 4. Riscos

Abstract

This article aims to portray the position of the various governmental and private entities when dealing with issues related to cybersecurity. It is common to see in social and digital media that the world has been experiencing several challenges when it comes to cyber-attacks, invasions in corporate environments, information theft, data leakage, extortion, and even problems related to privacy. With the expansion and elasticity of the internet, several new technologies have emerged allowing more and more forms of interaction and possibilities. It is in this interactivity that we must coldly worry about security from a globalized point of view. So, the idea here is to present and understand how all these items can, together or separately, directly affect the global economy. Many companies feel threatened by the most dangerous resources that can put them at risk, but as a result, they are not prepared to protect themselves from attacks like Ransomware, where attackers hijack data for ransom. We will cite in this work some damage that can be caused by corporate default, or simply by groups of invaders targeting government agencies with the aim of mass destruction. Finally, we will identify some resources that can be favorable for mitigating these intrusions and attacks, as well as outline ways to keep the risks at an acceptable level.

Keywords: 1. Global Economy 2. Cyber Security 3. Ransomware 4. Risks

1 Mestrando em Business Administration pela Must University. Especialista em Gestão de Segurança da Informação (UNICIV). Tecnólogo em Gestão de Segurança da Informação e Defesa Cibernética (UNINTER). CV lattes: http://lattes.cnpq.br/9768260128060816 / email: wanderleymjr@protonmail.com

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

1. Introdução

A segurança cibernética é um assunto em alta desde o começo da pandemia do Covid-19. A possibilidade de teletrabalho, o lockdown obrigatório demandado pelos governos de todo mundo e as empresas sendo forçadas a mudar seus paradigmas para continuarem a sobreviver, foram de cara problemas e/ou soluções paliativas impostas por essa pandemia. Quando nos referimos a mudança de paradigma, esses foram novos *modus-operandi* criados obrigatoriamente para atender as demandas das empresas, como adequação de seus ambientes, funcionários, fornecedores e todos aqueles *stakeholders* impactados diretamente. Isso nos leva a realidade de que muitas dessas organizações tiveram que reavaliar seus ativos computacionais, introduzindo novas tecnologias e novos processos de adequação.

Devemos considerar, segundo (Bandyopadhyay, 2023, p. 1) que "novas tecnologias ou serviços introduzem novos riscos cibernéticos que precisam ser avaliados, priorizados pela análise de impacto e mitigados por meio de processo, tecnologia, habilidades e perspectiva de governança".

A WEF (2023), explica que:

> A instabilidade geopolítica, tecnologias emergentes e de rápido amadurecimento, falta de talentos disponíveis, uma crescente participação de acionistas e as expectativas regulatórias representam alguns dos desafios significativos que preocupam os líderes cibernéticos e empresariais (...) as tecnologias agora são compartilhadas por várias organizações. Essas organizações, consequentemente, têm dependências ou fraquezas comuns.

E com todos esses problemas seriamente desenhados, algumas organizações de repente ficaram limitadas, expostas e desprotegidas, o que deu o início de algo que podemos chamar de "***ciberterrorismo*** em massa".

(Pinto, 2011, p. 9) define ciberterrorismo como:

> Atos fundados em motivações políticas, ideológicas ou sociais e em operações de hacking com o objetivo de causar prejuízos severos (perda de vidas humanas, prejuízos econômicos, ataques ou ameaças contra sistemas informáticos, redes e a respectiva informação neles armazenada) de forma a intimidar ou coagir um governo. Pode chegar a ser um ataque físico com o objetivo de destruir redes computorizadas de infraestruturas críticas (Internet, telecomunicações) ou a grelha eléctrica de um país ou de uma cidade.

Segundo Dijk (2019), dois anos antes da pandemia, os ataques cibernéticos e as ameaças nele contidas já se enquadravam como a quinta maior preocupação das organizações ao redor de todo o mundo e eram considerados pelo Fórum Econômico Mundial (WEF) como risco de prioridade número um, principalmente na América do norte, Europa e no leste da região Ásia-pacífico.

Esse artigo visa explorarmos os problemas socioeconômicos que ser diretamente afetados pela Cibercriminalidade no contexto do ciberterrorismo.

Utilizaremos para contexto desse artigo uma metodologia em caráter de pesquisa descritiva com foco em pesquisa bibliográfica e recursos de fontes confiáveis extraídos da internet.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

2. Ciberterrorismo aliado à Economia global

O Ciberterrorismo é um tópico emergente em diversas partes e setores em todo o mundo. Ele envolve todas as espécies de crimes que possam ser comedidos de forma digital, mais conhecidos como crimes cibernéticos. "O Ciberterrorismo é o uso disruptivo da tecnologia da informação por grupos terroristas para promover sua agenda ideológica ou política. Isso assume a forma de ataques a redes, sistemas de computadores e infraestruturas de telecomunicações" (Ciaramello, 2019, p. 1).

A Cibercriminalidade se instaurou como um terror em todo mundo. Milhares de empresas sofrem ataques cibernéticos anualmente. E, hoje, seria impossível mensurarmos o impacto que isso causa aos cofres públicos e às iniciativas privadas.

> Se fosse medido como um país, o cibercrime – que infligiu danos totalizando 6 trilhões de dólares globalmente em 2021 – seria a terceira maior economia do mundo depois dos EUA e da China. Segundo especialistas, os custos globais de crimes cibernéticos devem crescer 15% ao ano nos próximos 5 anos, chegando a 10,5 trilhões de dólares por ano até 2025, acima dos 3 trilhões de dólares em 2015. (Brasiline, 2022, p. 1)

Pinto (2011) diz que os *ciberterroristas* são normalmente jovens que são do sexo masculino, academicamente embasados (Mestres ou Doutores), que que tem a consciência de que estão violando a Lei, a ordem e causando desrespeito a sociedade, bem como descontrolando os sistemas de ordem social.

Segundo James (2023), os hackers estão constantemente mudando suas formas de burlar a segurança e realizar mais ataques em ativos comerciais. O mundo experencia em torno de 2.200 ataques cibernéticos diariamente. Dados afirmam que existe um ataque hacker a cada 39 segundos, e em torno de 300 mil malwares são criados a cada ano.

Ainda sobre economia global relacionada à cibersegurança, (Brasiline, 2022, p.1) explica que:

> Os custos do crime cibernético incluem danos e destruição de dados, dinheiro roubado, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, desfalque, fraude, interrupção pós-ataque no curso normal dos negócios, investigação forense, restauração e exclusão de dados hackeados dados e sistemas e danos à reputação.

(Pinto, 2011, p. 9) afirma que "o cibercrime é um ato baseado ou que tem como alvo os sistemas informáticos. Pode envolver o roubo de propriedade intelectual, violação de patentes, roubo de segredos de comércio, violação das leis de direito de autor e a usurpação de identidade.". Ele ainda explica que o ciberterrorismo é parecido com o cibercrime em uma versão ampliada, mas que contêm consequências piores.

"O cibercrime é um crime de baixo risco que oferece altos retornos. Um cibercriminoso inteligente pode ganhar centenas de milhares, até mesmo milhões de dólares, quase sem chance de ser preso ou encarcerado". (CSIS, 2018, p. 4)

Muitos são os desafios causados pelos estragos feitos pelo ciberterrorismo. Com isso as empresas precisam se antecipar e montar uma estratégia para conter essa gama de ações criminosas. Uma das opções que as empresas passaram a contratar com mais frequência e vem ganhando cada vez mais popularidade no mercado é o seguro cibernético. Ele pode ser comparado com seguro de automóvel no sentido em que tem como objetivo proteger a empresa em caso de danos à infraestrutura ou danos morais. (Vandiver; Murphy, 2023, p. 1) afirmam que:

> O seguro de segurança cibernética protege as empresas contra perdas financeiras causadas por incidentes como violação e roubo de dados, hacking de sistema, pagamentos de extorsão de ransomware e muito mais. Se sua pequena empresa armazena informações confidenciais on-line ou em um computador, você deve ter pelo menos alguma cobertura de seguro cibernético.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

2.1.Hacktivismo e Hacktivistas

Traremos para nosso artigo dois tópicos bastante relevantes no mundo do ciberterrorismo. O primeiro deles refere-se ao conceito de "*hacktivismo*".

> O Hacktivismo trata da junção de dois conceitos: o ativismo online (ou ciberativismo) e a prática de hacking. Ou seja, é uma forma de manifestação que se utiliza da internet para divulgação de informações, em conjunto de métodos conhecidos pelos hackers (indivíduo com grande conhecimento em informática), normalmente ilegais, podendo ser destrutivos, a fim de que a transmissão de mensagens atinja um maior número de pessoas. (Arimura, 2016, p.1)

O segundo vem retratar quais são os autores que atuam em manifestações de *hacktivismo*, mais conhecidos como *hacktivistas*. Stouffer (2021) afirma que os *hacktivistas* são ativistas online que buscam injustiças praticadas de ordens religiosas, sociais e políticas e tentam chamar a atenção do público para uma causa que é importante para eles, com o intuito de que esses atos provoquem mudanças e melhorias.

Os *hacktivistas* se enquadram na cibersegurança como ciberterroristas, considerando que suas ações têm o mesmo foco, direcionamento e geralmente o mesmo público-alvo.

Podemos aqui citar alguns exemplos dos ataques mais comuns exercidos pelos *hacktivistas*: desfiguração e redirecionamento de sites, ataques distribuídos de negação de serviço (DDoS), vazamento de dados de informações públicas, bombardeio geográficos com intuito de revelar a localização de prisioneiros políticos e ativistas de direitos humanos, dentre outros.

Sobre grupos de *hackitivismo*, Arimura (2016) explica que o "Anonymous" é um dos mais conhecidos e influentes do mundo. Ele inclui pessoas de diferentes nacionalidades, que usam sempre o conceito de anonimato, e possuem como símbolo a máscara utilizada pelo protagonista do filme "V de Vingança" lançado em 2005 por Alan Moore.

Outros grupos *hacktivistas* de destaque são o WikiLeaks, LulzSec e Syrian Electronic Army.

3. Ransomware: a maior das ameaças cibernéticas

O *Ransomware* é um tipo de malware ou vírus designado para roubo de informações sigilosas nos mais variados sistemas operacionais, diretórios, e ativos de hardware e software em geral. Uma vez que o invasor encontre dados valiosos, ele utiliza o recurso de criptografia para que esses dados fiquem indisponíveis para o usuário responsável por ele. Esse ataque é considerado um dos mais antigos, com dados ocorridos desde os anos 90.

> Este é o mais famoso por ter sido muito usado durante a pandemia da Covid-19. Trata-se de uma espécie de malware que entra nos sistemas a fim de sequestrar dados e exigir pagamento de resgate. Uma quantidade enorme de empresas foram vítimas deste tipo de ataque nos últimos anos, gerando prejuízos financeiros e de reputação. (Mack, 2022, p.1)

A Comparitech (2022, p. 1) explica que "algumas pesquisas mostraram que as perdas para as empresas podem chegar a US$ 2.500 em média para cada incidente, com empresas dispostas a desembolsar milhões de dólares para descriptografar seus dados em alguns casos". Porém, de acordo com Armis (2023), sejam atores de estado-nação ou cibercriminosos, a anatomia utilizada por um ataque de ransomware é relativamente a mesma. OS atacantes primeiro procuram uma forma de conseguirem acesso ao ambiente através de um site comprometido, uso de *Phishing* ou um ataque direcionado. Uma vez dentro do ambiente, os invasores se movem lateralmente pela rede, escalando privilégios para conseguirem acesso como administradores e se infiltrando na rede.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Os ataques desse tipo vêm tirando o sossego de muitas empresas ao redor do mundo e acontecimentos como a guerra da Rússia-Ucrânia geralmente são uma porta de fraqueza para que gangues cibernéticas possam atacar livremente.

Constantin (2023) diz que houve mudanças no ecossistema do *Ransomware* no ano de 2022. A utilização do *Ransomware* como serviço (RaaS) foi reduzida para que os invasores pudessem se flexibilizar e não chamar tanta a atenção da lei. Ele ainda afirma que grupos de *Ransomware* podem ter melhorado suas alianças tendo como membros e afiliados criminosos na Rússia, na Ucrânia ou noutros países da ex-URSS.

Quanto aos tipos de *Ransomware*, podemos ver na tabela abaixo com dados fornecidos pela ESET (2022):

Tipo de Ransomware	Objetivo
Diskcoder	Utiliza o serviço de criptografia em todo o disco da máquina e impede o acesso do usuário alvo ao sistema operacional.
Screen locker	Utilizado para realizar o bloqueio da tela do dispositivo, não permitindo que usuário acesse sem conseguir o código.
Crypto-ransomware	Criptografa arquivos que ficam armazenados dentro do disco da máquina do usuário alvo.
PIN locker	Ataque aos dispositivos Android que tenta bloquear o aparelho e impedir que o usuário alvo possa acessá-lo sem um código.

Tabela 1- Tipos de Ransomware

Existem ainda muitas variantes do vírus de *Ransomware* e dentre as mais famosas podemos citar o PC Cyborg, Locky, WannaCry, Rokku e Petya. Todas essas possuem suas particularidades, mas o objetivo final geralmente é o mesmo, a extorsão. Para isso o invasor sempre busca por um valor de "resgate" para que os atacados recebam a chave para desbloquear o acesso e conseguirem seus dados de volta. Mas, Miller (2017, p. 8) adverte que:

> Não há honra entre ladrões. Embora um invasor geralmente forneça a chave de descriptografia para seus arquivos se você pagar o resgate, não há garantia de que o invasor já não tenha instalado outro malware e kits de exploração em seu endpoint ou outros sistemas em rede, ou que eles não roubarão seus dados para outros fins criminosos ou para extorquir mais pagamentos no futuro.

São muitas as estratégicas utilizadas por golpistas cibernéticos quando pensam em realizar esse tipo de ataque. Segundo a Inforchannel (2022), esses golpistas precisam ter um melhor entendimento sobre qual a relevância da informação a ser adquirida, levando em consideração etapas para a realização do ataque. A primeira delas seria o estudo sobre a vítima, principalmente se ela tem o potencial para pagar o resgate de acordo com o valor que o atacante pensa em receber. A segunda etapa seria a forma como o criminoso conseguirá acesso à rede corporativa da vítima.

4. Considerações Finais

Vivemos na famosa "era da informação" em que o aumento de possibilidades de interação digital tornou a internet um nicho para diversos atores mal intencionados cometerem crimes cibernéticos em todo o mundo. Esse aumento se potencializou pela devastação produzida pela pandemia do COVID-19, período pelo qual as organizações públicas e privadas ficam mais vulneráveis.

Nesse artigo, vimos uma síntese dos impactos causados pelo ciberterrorismo na economia global, com desafios da cibersegurança quando na mitigação, contenção e resolução dos mais diversos golpes, extorsões e outros ataques que possam comprometer as atividades de uma empresa. Fizemos uma breve menção aos conceitos de ciberterrorismo e cibersegurança, uso do seguro cibernético, bem como sobre o que é o *Hacktivismo*, seus atores e potenciais vetores.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Por fim, exploramos informações sobre o *Ransomware*, considerado uma das ameaças iminentes e mais difundidas no mundo em termos de proteção, vazamento de dados e extorsões criminosas.

Sem dúvida, nos próximos anos muitos desafios ainda virão no quesito cibersegurança. E para tanto, esperamos haja uma evolução de algumas tecnologias que permitirão a diminuição ou contenção dos ataques cibernéticos.

Referências

Arimura, M. (2016). **Hacktivismo: vilões ou mocinhos?** Portal de e-governo, inclusão digital e sociedade do conhecimento (E-Gov). [online]. Disponível em: https://egov.ufsc.br/portal/conteudo/hacktivismo-vil%C3%B5es-ou-mocinhos Acesso em 14 de dez de 2022

Armis. (2023). **The state of Cyberwarfare**: Armis state of Cyberwarfare and trends report 2022-2023. [online]. Disponível em: https://www.armis.com/cyberwarfare/ Acesso em 10 de jan de 2023

Bandyopadhyay, S. (2023). **Cybercrime is now the world's third-largest economy**. [online]. Khaleej Times Journal. Disponível em: https://www.zawya.com/en/legal/crime-and-security/cybercrime-is-now-the-worlds-third-largest-economy-hwpvrkdl Acesso em 20 de jan de 2023

Brasiline. (2022). **O Cibercrime como império seria a terceira maior economia do mundo**. Brasiline Tecnologia. [online]. Disponível em: https://brasiline.com.br/blog/o-cibercrime-como-imperio-seria-a-terceira-maior-economia-do-mundo/ Acesso em 20 de jan de 2023

Ciaramello, Marina. (2019). **Sequestros de informações e cyber espionagem são as principais ameaças cibernéticas para as empresas**. [online]. Disponível em: https://www.segs.com.br/info-ti/190703-sequestros-de-informacoes-e-cyber-espionagem-sao-as-principais-ameacas-ciberneticas-para-as-empresas Acesso em 25 de jan de 2023

Comparitech. (2022). **2018-2022 Ransomware statistics and facts**. [online]. Disponível em https://www.comparitech.com/software-supply-chain-attacks/ Acesso em 10 de janeiro de 2023

Constantin, L. (2023). **Ecossistema de ransomware diversifica-se antes de 2023**. [online]. Disponível em: https://www.comparitech.com/antivirus/ransomware-statistics/ Acesso em 18 de jan 2023

CSIS. (2018). **Economic impact of Cybercrime: No slowing down**. [online]. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf Acesso em 20 de jan de 2023

Dijk, Gina Van. (2019). "**Por que os ciberataques são uma preocupação global**". [online]. Disponível em: https://neofeed.com.br/dados-blindados/por-que-os-ciberataques-sao-uma-preocupacao-global/ Acesso em 10 de jan de 2023

ESET. (2022). O que é um ransomware? [online]. Disponível em: https://www.eset.com/br/ransomware/ Acesso em 20 de jan de 2023

Inforchannel. (2022). **Kaspersky alerta: grupos de ransomware usam ferramentas de Red Teaming**. [online]. Dis-

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

ponível em: https://inforchannel.com.br/2022/06/27/kaspersky-alerta-grupos-de-ransomware-usam-ferramentas-de--red-teaming/ Acesso em 20 de jan 2023

James, Nivedita. (2023). **160 Estatísticas de Cibersegurança 2023** – A Lista Definitiva de Estatísticas e Tendências. [online]. Disponível em: https://www.getastra.com/blog/security-audit/cyber-security-statistics/#Top_Cybersecurity_Statistics_2023 Acesso em 10 de jan de 2023

Mack, Cecilia L. (2022). **Ataques cibernéticos devem continuar em 2023**. [online]. Disponível em: https://www.segs.com.br/info-ti/366234-ataques-ciberneticos-devem-continuar-em-2023 Acesso em 15 de jan de 2023

Miller, Lawrence. (2017). **Ransomware defense for dummies®**, Cisco Special Edition. New Jersey: John Wiley & Sons.

Pinto, Marco A. G. (2011). **Teoria relativista do ciberterrorismo**. Dissertação para a obtenção do grau de Mestre em Guerra da Informação. Academia Militar. Lisboa. Disponível em:

https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf Acesso em 15 jan 2023.

Stouffer, Clare. (2021). **Hacktivism: An overview plus high-profile groups and examples**. [online]. Disponível em https://us.norton.com/blog/emerging-threats/hacktivism# Acesso em 25 de jan de 2023

Vandiver, W. & Murphy, R. (2023). **Cybersecurity Insurance: What It Covers, Who Needs It**. [online]. Disponível em: https://www.nerdwallet.com/article/small-business/cybersecurity-insurance Acesso em 20 de jan de 2023

WEF. (2023). **Global Cybersecurity Outlook 2023**. World Economic Forum. [online]. Disponível em:

https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Acesso em 25 de jan de 2023

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.