CIBERATAQUES EM SERVIÇOS ESSENCIAIS DE TELECOMUNICAÇÕES: UMA REVISÃO SISTEMÁTICA

CYBERATTACKS ON ESSENTIAL TELECOMMUNICATIONS SERVICES: A SYSTEMATIC REVIEW

Mauricio Santos de Brito, Faculdade de tecnologia de Santana de Parnaíba
mauricio.brito@fatec.sp.gov.br

Irapuan Glória Júnior, Faculdade de tecnologia de Santana de Parnaíba
irapuan.gloriajr@fatec.sp.gov.br

Resumo

Há diversos tipos de ataques que ocorrem contra empresas que prestam serviços essenciais, como as do setor de telecomunicações. A pesquisa buscou identificar quais os tipos mais frequentes de ataques neste tipo de companhia. A pesquisa possui natureza qualitativa, utilizou como metodologia a revisão sistemática. Os resultados obtidos dentre os 8 artigos selecionados de um total de 95 avaliados foi que os tipos de ataques foram de *Ransonware, Border Gateway Protocol, Denial-of-service e Defacement*. A contribuição para a teoria está em apresentar os tipos de ataques que devem ser estudados. A contribuição para a prática é de que os Cyber Security Officer e gestores podem utilizá-lo para prevenção de ataques.

Palavras-chave: Cyber, Cibernéticos, Ataques, Serviços, Telecomunicações.

Abstract

There are several types of attacks that occur against companies that provide essential services, such as those in the telecommunications sector. The research sought to identify the most frequent types of attacks in this type of company. The research has a qualitative nature, used as methodology the systematic review. The results obtained among the 8 articles selected from a total of 95 evaluated were that the types of attacks were Ransonware, Border Gateway Protocol, Denial-of-service and Defacement. The contribution to the theory is in presenting the types of attacks that should be studied. The contribution to the practice is that Cyber Security Officers and managers can use it to prevent attacksnecessary for preventive information security actions to avoid this type of incident.

Keywords: Cyber, Attacks, Services, Telecom, Telecommunications.

1. Introdução

Conforme os avanços da tecnologia é possível notar que há a dependência da sociedade no uso de tecnologias de serviços essenciais, e em consequência disso, existe um crescimento de Ciberataques nas empresas, visando comprometer seu funcionamento parcial ou total, sobretudo em ambientes WEB (TAVARES, 2021).

Nos ambientes WEB há a necessidade de prover segurança computacional na prestação serviços, principalmente em serviços essenciais, abrangendo o levantamento dos principias tipos de ciberataques, para assim prover uma rede de proteção defensiva e ofensiva, adequada a esses ambientes (LIMA, 2020).

No contexto de serviços essenciais esse artigo terá enfoque em telecomunicações tipificando esses tipos de ataque e trazendo à tona quais são a principais políticas de segurança para mitigá-los. A análise da cibersegurança para mitigar ataques exige que sejam analisados também os aspectos materiais que constituem a internet: os cabos que compõe a rede, seguido dos servidores, e todos os outros hardwares e finalmente pessoas que interagem com a internet nesse ambiente por esse motivo orientar os hosts acerca dos perigos e riscos de ciberataques é fator principal (TAVARES, 2021).

Diante disto, este artigo possui como questão de pesquisa: "Quais são os tipos de ciberataques em serviços essenciais de telecomunicações?". Os objetivos são: (1) Identificar os principais ataques realizados contra serviços essenciais de telecomunicações; e (2) Analisar as políticas e procedimentos de segurança da informação aplicados.

2. Referencial Teórico

2.1 Serviços Essenciais

Em um contexto geral são considerados como serviços de natureza essencial às atividades que precisam ser mantidas em funcionamento e garantidas para usufruto da população, mesmo diante de circunstâncias adversas de qualquer natureza (LINHARES, 2018).

As infraestruturas essenciais de um estado, podem ser definidas como aquelas que provem serviços considerados de grande impacto para o convívio em sociedade e para provimento do ser humano, sendo as principais empresas que forneçam serviços de energia elétrica sendo ela proveniente de qualquer fonte, abastecimento de água potável, empresas que produzem ou

processem alimentação básica, indústrias farmacêuticas e empresas que fornecem serviços de telefonia, telecomunicações e internet, por esse motivo muitos *cyber* criminosos tem mirado nesse tipo de empresa provendo ciberataques, como (JORGE ,2022) de *Ransonware, Border Gateway Protocol* (BGP), *Denial-of-service* (DDoS), entre outros os motivos desses ataques são os mais variados partindo de interesses financeiros por parte dos criminosos, até por motivos econômicos, políticos ou com intenções de Guerra cibernéticas (Gonçalves Wahl,2022).

2.2 Ciberataques

A Internet, proporciona conexões em tempo real sua abrangência é mundial, trouxe fácil acesso a um número considerável de informações, porém apresenta inúmeras vulnerabilidades. (LIMA LINHARES,2018)

Se a internet trouxe novas ameaças e vulnerabilidades, também proporcionou oportunidades, pois a internet também funciona como provedor no qual várias informações estratégicas são armazenadas, manipuladas e compartilhadas, sendo assim, repositório para armazenamento de dados, objeto que pode ser analisado como ambiente operacional, e com muitas possibilidades da aplicação de monitoramento para mitigar possíveis tentativas de ataque além de possibilitar também o monitoramento de usuários que interagem nesse ambiente (COUTINHO, 2020).

Ataque realizado pela internet, no qual são invadidos sistemas com o objetivo principal de manipular arquivos, interromper a comunicação, sobrecarregar sistemas, sites e outros serviços com foco na perca da integridade empresarial, que acontece quando ocorre a modificação ou destruição de informações de forma não autorizada. (SILVA; NOGUEIRA, 2018)

Outro tipo de ataque é o DDoS *Attack* é um tipo de ataque que tem por intuito sobrecarregar os servidores e ambientes provocando lentidão assim tornando indisponíveis os sistemas, e respectivamente sites e demais acessos.

O *Ransomware* definido como “sequestro de dados” tem como principal objetivo o bloqueio de acessos à arquivos considerados importantes de servidores. Devolvendo aos proprietários somente após o pagamento de valores determinados pelo *cyber* criminoso. *Border Gateway Protocol* (BGP) é um protocolo rede usado para roteamento que avalia os caminhos na hora do envio de dados. esse protocolo tem suas vulnerabilidades. o seu uso malicioso pode fazer o redirecionando do tráfego da internet ao comunicar de forma falsa a propriedade de prefixos de IP. nesse são roteados para um domínio falso ou inexistente

Ataques de desfiguração (*defacement*) tem por objetivo eliminar ou modificar as informações em um site ou portal de informações. É uma ferramenta usada para promover desinformação que tem a capacidade de levar os internautas a acreditarem que dados inverídicos são fidedignos (RODRIGUES; MADEIRA, 2018).

Os ataques do tipo limpadores (*wipers*) tem por objetivo excluir informações em uma rede de computadores, tornando impossível que os usuários acessem seus próprios dados (JORGE, 2022)

A estratégia de malwares *(malicious software* – programas maliciosos) que objetificam bloquear dados sensíveis, ou infectar sistemas inteiros com limpadores com intuito de promover danos aos ambientes empresariais. (NOGUEIRA, 2019).

3. Metodologia

Esse artigo possui a natureza qualitativa (GIL, 2022), com a utilização da metodologia revisão sistemática (KITCHENHAM, 2004) com a finalidade de identificar as pesquisas disponíveis a respeito de ciberataques a estruturas essenciais, conforme apresentado na Tabela 1.

Tabela 1 - Metodologias Utilizadas

Item	Conteúdo	Autor(es)
Natureza	Qualitativa	GIL (2022)
Metodologia	Revisão sistemática	KITCHENHAM (2004)

3.1. Procedimentos Metodológicos

Os procedimentos metodológicos (Figura 1) foram:

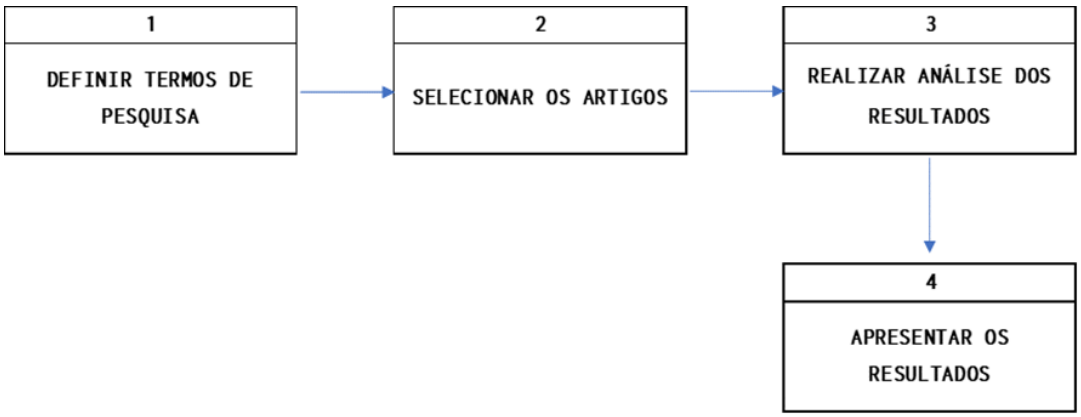
Passo 1: **Definir termos de pesquisa.** Por meio de definições fornecidas pela literatura foram baseados aos termos a serem pesquisados e a concepção de *string* de busca para *Engine* do Google Scholar (www.scholar.google.com.br)

Passo 2: **Selecionar artigos**. A utilização dos mecanismos de pesquisa retornou alguns possíveis candidatos, mas apenas após a aplicação dos critérios de seleção estabelecidos, do qual resultarão nos itens que serão considerados nessa pesquisa.

Passo 3: **Analisar os Resultados**. Realizar à identificação de artigos que qualificam os tipos de ataques cibernéticos que ocorrem em estruturas essenciais.

Passo 4: **Apresentar os Resultados**. Foram apresentados os resultados das evoluções das pesquisas em ciberataques a estruturas essenciais.

Figura 1 – Procedimentos Metodológicos



3.2. Critérios de seleção

A revisão sistemática irá considerar os seguintes itens:

(1) O período de 2018 até 2022;

(2) Utilizou somente artigos científicos publicados, sendo descartados monografia, dissertação, tese, livros e qualquer outro periódico;

(03) Apresentou em seus textos conceitos de ataques de cyber segurança e suas tipificações.

3.2 Termos de Busca

Relacionado aos termos de pesquisa, foram empregados o uso "Ataques cibernéticos" e "serviços de telecomunicações" conforme apresentado na Tabela 2.

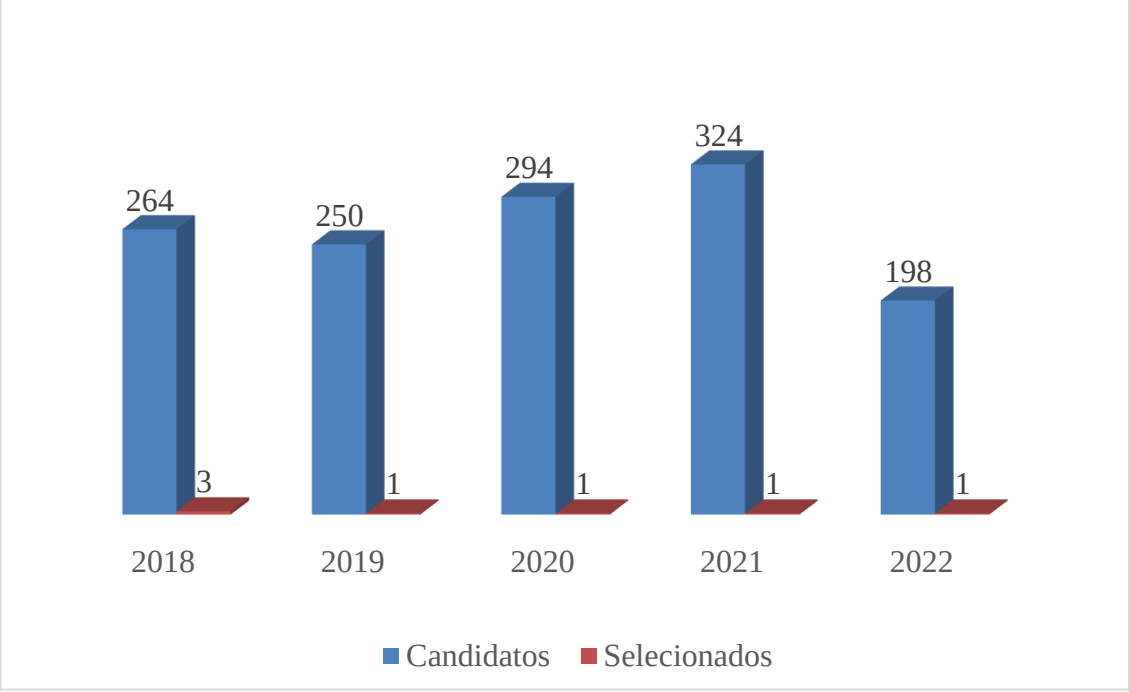
Tabela 2 - *String* de Busca

Base	String
Google Scholar www.scholar.google.com.br	("Cyber" OR "Cibernéticos" OR "Ciberneticos") AND ("Ataques") AND ("Serviços") AND ("Telecom" OR "Telecomunicações") AND ("Empresa" OR "Empresas" OR "Setor")

3.3 Artigos Selecionados

Com base na pesquisa pode ser constatado os índices crescentes relacionados à Ciberataques a serviços de telecomunicações, de acordo com o Gráfico, serão analisados artigos correlacionados ao tema datados a partir de 2018 até o primeiro semestre de 2022.

Gráfico 1 – Artigos Candidatos/Selecionados



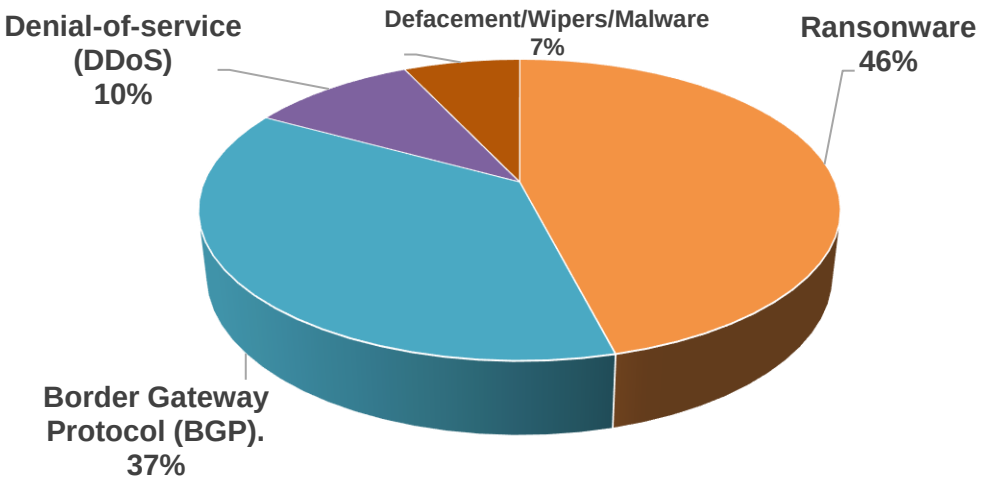
4. Resultados e Discussões

4.1 Focos dos Artigos Selecionados

No contexto de ciberataques a serviços de telecomunicações, há várias áreas até relacionadas que vão desde entidades pertencentes ao ministério da defesa á trabalhos que analisam ataques a serviços essenciais em tempos de guerra.

Conforme apresentado no Gráfico 2, com base nos artigos analisados o tipo de ataques mais tentado contra o setor de telecomunicação são os ataques de Ransonware com 46% de ocorrências o segundo tipo de ataques mais tentado são os ataques que se utilizam de *border Gateway protocol* (BGP), que é um ataque que se baseia no protocolo de roteamento de borda para desviar o trafego do servidor de empresas para o servidor de usuários maliciosos, com 37% de ocorrências, em terceiro lugar há os ataques DDoS (*denial-of-service*) com 10% de ocorrências.

Gráfico 2 – Principais tipos de ataques contra serviços de Telecom



4.2 Discussão

A internet proporcionou uma evolução notória no que diz respeito da forma como se presta serviços essenciais, quando segmentado ao setor de telecomunicações existe uma diversidade de aspectos de segurança de informação que devem ser aplicados, por serem consideradas empresas sensíveis, pois possuem a capacidade de causar impactos expressivos

caso seus serviços sejam interrompidos, focando nesse aspecto considerando a abordagem feitas nos artigos que embasam esse estudo a área de telecomunicações deve focar em aspectos relacionados a segurança em redes, visando se proteger de ataques do tipo BGP, também deverá adotar as práticas recomendadas para as políticas de treinamento e atualizações de segurança da informação para seus colaboradores visando a mitigação de ataques de Ransonware.

Outro ponto que deve ser observado com relação ao *Pentest* voltados ao stress de sistemas, sites e serviços visando se prevenir de ataques DDoS. Mesmo não blindando essas empresas contra ciberataques, essas práticas podem reduzir muito a recorrência desses incidentes e mais que isso pode preparar as empresas para atuarem de forma contingencial em caso de ataques definindo times para atuação defensiva e ofensiva.

5. Conclusões

A cada dia há a necessidade de criar políticas solidas de segurança da informação em empresas que provem serviços essenciais, considerando desde princípios de segurança em redes, até as políticas de nível de usuário (host), além disso deve ser ponto focal para as empresas manterem essas ações atualizadas visando combater o que é da mais recente em métodos e tipos de ciberataques.

Considerando a revisão das obras que compõe esse artigo, fica explicito a importância do treinamento de todos que interagem com o ambiente empresarial, afim de evitar comportamentos inseguros que por venturas possam ser utilizados como janelas para ataques, esses treinamentos devem ser aproximados o máximo possível da realidade considerando o mix de técnicas de engenharia social e *phishing* que se parecem cada dia mais com mensagens ou interações verídicas, fazendo com que o usuário caia no erro, considerando ser uma mensagem ou contato oficial.

A contribuição para a teoria está em apresentar os tipos de ataques que devem ser estudados. A contribuição para a prática é de que os *Cyber Security Officer* e gestores podem utilizá-lo para prevenção de ataques.

Referências

COUTINHO, Lilian. LGPD e inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas. **Revista Brasileira de Inteligência**, v. 97, p. 97, 2020.

GIL, A. **Métodos e técnicas de pesquisa social.** 6. São Paulo: Atlas,208 págs, 7ª. Edição, 2022.

JORGE, Bernardo Wahl Gonçalves Araújo. A dimensão cibernética da guerra entre a rússia e a ucrânia em 2022: uma avaliação inicial passados 100 dias do conflito. **Revista Hoplos**, v. 6, n. 10, p. 102-124, 2022.

KITCHENHAM, B. Procedures for Performing Systematic Reviews. Vol. Keele, v. 33. 1-26, 2004.

LIMA, Pedro Arthur Linhares. Segurança Cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das Infraestruturas Críticas Nacionais, Órgãos Estratégicos do Governo e Forças Armadas. Edição Especial da Revista Brasileira de Estudos de Defesa, 10º Encontro Nacional da Associação Brasileira de Estudos de Defesa (ENABED)., 2018

LIMA, Walbery Nogueira et al. Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional. **Data & Hertz**, v. 1, n. 1 jan./Dez, p. 52-59, 2020.

SILVA, Washington Rodrigues; NOGUEIRA, Jorge Madeira. Ataques cibernéticos e medidas governamentais para combatê-los. Revista o **Comunicante**, v. 9, n. 1, p. 42-57, 2019.

SOUZA, Deywisson Ronaldo Oliveira et al. Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito rússia-ucrânia. **Revista Eletrônica da Estácio Recife**, v. 5, n. 3, 2019.

TAVARES, Marcus Vinicius da Silva. EUA x HUAWEI: A importância estratégica da tecnologia 5g para o poder global. **Revista Brasileira de Estudos Estratégicos**, v. 13, n. 25, 2021.

Anexo A – Artigos Selecionados

Ano	Título / Autores	Foco
2018	Segurança Cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das Infraestruturas Críticas Nacionais, Órgãos Estratégicos do Governo e Forças Armadas Pedro Arthur Linhares Lima.	Serviços Essenciais
2018	Ataques cibernéticos e medidas governamentais para combatê-los, Washington Rodrigues da Silva Jorge Madeira Nogueira	Telecomunicações
2019	Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional Walbery Nogueira de Lima e Silva	Defesa Cibernética
2019	Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito Rússia-Ucrânia. Deywisson Ronaldo Oliveira de Souza Fernando Henrique Casalunga Alane Costa Pinheirom Augusto Ferreira do Nascimento Barbosa Caroliny dos Santos Marinho Matheus Guerra Guedes.	Serviços Essenciais
2020	LGPD e inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas Lilian Coutinho	Tratamento de Dados
2020	A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil José Euclides Oliveira de Araújo	Defesa Cibernética
2021	Eua x Huawei: a importância estratégica da tecnologia 5g para o poder global Marcus Vinicius da Silva Tavares	Telecomunicações
2022	A dimensão cibernética da guerra entre a Rússia e a ucrânia em 2022:uma avaliação inicial passados 100 dias do conflito Bernardo Wahl Gonçalves de Araújo Jorge	Serviços Essenciais