# ATAQUES CIBERNÉTICOS A INFRAESTRUTURA CRÍTICA DOS PAÍSES EM TEMPOS PANDÊMICOS

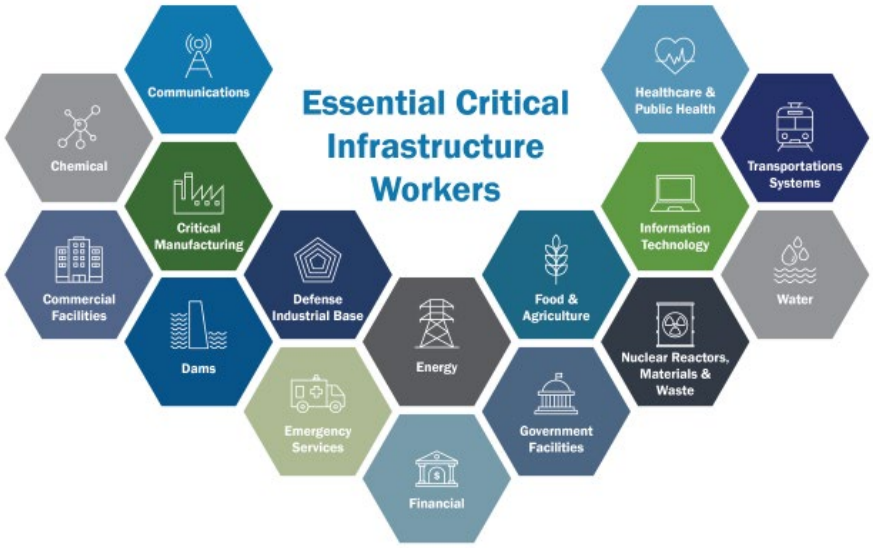
Thays Felipe David de Oliveira

Com a chegada do COVID-19 e a decretação de pandemia pela Organização Mundial de Saúde (OMS) acabou fazendo com que as pessoas começassem a trabalhar em casa e dependesse dos recursos da Tecnologia da Informação (TI). Tudo isso é considerado um cenário perfeito para os crimes cibernéticos.

Por causa dessa dependência, percebe-se que há uma grande sequência de tentativa de ataques cibernéticos a empresas e a infraestrutura crítica dos Estados. Logo, os ataques cibernéticos não é mais ficção cientifica e está cada vez mais recorrente e sofisticada.

Assim, no ano de 2020 os ataques cibernéticos a infraestrutura crítica (Figura 1) tornou-se cada vez mais recorrente chegando a ser o dobro em relação a 2019. Com a pandemia, a ideia de infraestrutura crítica teve que ser reconsiderada, tendo em vista que muitas organizações tiveram que ir para a linha de frente combater a COVID-19.

**Figura 1 –** Infraestrutura Crítica Durante a Covid-19




**Fonte:** CISA (2021)

Por causa disso, os principais alvos eram as organizações que não poderiam ter seus sistemas interrompidos – como: manufaturas e energia -, tendo em vista que se isso ocorresse iria causar sérios danos da população. O que acabou contribuindo para tal acontecimento foi porque existia uma grande vulnerabilidade nos sistemas de controle industrial (ICS) fazendo com que eles se tornassem cada vez mais vulneráveis.

De acordo com dados do Índice de Inteligência de Ameaças X Force 2021, que foi divulgado pela IBM Security, houve um aumento na quantidade de ataques cibernéticos no ano de 2020. A finalidade era atacar as organizações que são consideradas como vitais para combater o COVID-10, tais como: hospitais, fabricantes de produtos médicos e farmacêuticos, por exemplo.

É válido salientar que o índice supracitado é totalmente baseado nas percepções e observações obtidas por meio de monitoramento em mais de 130 Estados. Perante tais dados, foi inferido que a Europa recebeu o maior número de ataques cibernéticos representando 31% aos quais a X-Force respondeu. De acordo com o mesmo dado, este continente recebeu mais ataques de ameaças internas do que qualquer outra região (IBM,2021).

Um ataque que veio a mídia recentemente, foi o ataque cibernético ao sistema de saúde irlandês em maio de 2021 por um *ransomware* ‘ *Conti’* , que acabou desativando vários sistemas que estavam interligado a este. Para controlar, foi desligado os sistemas, mas acabou gerando um grande impacto no serviço de saúde irlandês.

Destaca-se também o caso da Espanha que apenas em janeiro de 2021 o setor de saúde sofreu 626 ataques por uma organização. De forma geral, os ataques foram de sequestro a *botnet*, execução remota de código e negação distribuída de serviço (DDoS). Para evitar tais casos o governo espanhol lançou um pacote urgente em maio de 2021 de ações sobre segurança cibernética ( REES, 2021).

Um outro ataque cibernético que aconteceu na Austrália foi ao sistema da farmacêutica Oxford/ AstraZeneca no ano de 2020 por meio de oferta de emprego

falsa. O hacker enviou nos documentos um código malicioso que tinha sido projeto para obter acesso ao computador da vítima (WARREN, 2021).

Um país que é extremamente visado é o Estados Unidos da América, que em fevereiro de 2021 *hackers* acabaram comprometendo a estação de tratamento de água de uma pequena cidade da Flórida aumentando o nível de hidróxido de sódio para 11.100 partes por milhão, que é extremamente alto para o normal (LUCKEHART, 2021). No mesmo mês foi detectado um ataque de *ransomware* contra a infraestrutura crítica de uma instalação de compressão de gás natural, para isso, o invasor teve que utilizar o *spear phishing* para acessar as redes da organização e isso fez com que a instalação fosse fechada por dois dias. É válido salientar que, houve tentativa com essa mesma tática em várias usinas nucleares em todo território estadunidense (JACKSON, 2021).

Para se proteger o governo Biden criou uma iniciativa de cibersegurança para proteger a infraestrutura do país, especialmente contra os grupos de APT. O plano prevê a modernização das medidas segurança cibernética, prevenção, detecção de resposta e das capacidades forenses.

Nesse sentido, o que resta aos Estados é buscar proteger suas infraestruturas críticas contra esse tipo de ataque cibernético. Para isso, requer uma maior atenção a redes de TI, OT (*Operational Technology*) e consequentemente, ao sistema SCADA. De forma complementar, é indispensável que haja um maior monitoramento da vulnerabilidade, para que se possa identificar os atores que estão frente a ameaça APT. Além disso, é necessário que se busque investir em gestão de risco para que se possa lidar com essas ameaças que estão extremamente sofisticadas.

## REFERÊNCIAS

IBM. **Relatório de IBM Security: Dobram os ataques às indústrias que dão suporte aos esforços em resposta à COVID-19 .** Disponível em : https://www.ibm.com/blogs/ibm-comunica/ibm-security-ataques-ciberneticos/ > . Acesso em 10 julho de 2021.

JACKSON, D. **Cybersecurity for U.S. critical infrastructure a 'national-security imperative,' NSC official says .** Disponível em: https://urgentcomm.com/2021/06/01/cybersecurity-for-u-s-critical-infrastructure-a-national-security-imperative-nsc-official-says/ > . Acesso em 07 de julho de 2021.

LUCKEHART, A. **U.S. Critical Infrastructure: Addressing Cyber Threats and the Importance of Prevention.** Disponível em: < https://www.tripwire.com/state-of-security/featured/critical-infrastructure-addressing-cyber-threats-importance-of-prevention/ > . Acesso em 5 de julho de 2021.

NAGLI, L. PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19 . Congresso Transformação Digital 2020, 2020. Disponível em: http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2020/paper/viewFile/7614/2308 > . Acesso em 07 de julho de 2021.

REES, D. **Cyber attacks in healthcare: the position across Europe.** Disponível em : < **https://www.pinsentmasons.com/out-law/analysis/cyber-attacks-healthcare-europe** > . Acesso em 07 de julho de 2021.

WARREN, M. **Critical Infrastructure in the COVID-19 Age .** Disponível em : < https://www.rmit.edu.au/news/acumen/critical-infrastructure> . Acesso em 07 de julho de 2021.