The Hague Centre for Strategic Studies

Stellenbosch University Iyunivesithi Universiteit
School for Data Science and Computational Thinking
ISikolo seNzululwazi ngeDatha neNgqiqo yokuBala
Skool vir Datawetenskap en Rekenaardenke

cair
CENTRE FOR ARTIFICIAL INTELLIGENCE RESEARCH

Ministerie van Buitenlandse Zaken

Mitigating against Strategic Cyber Threats

CSI
CYBER SECURITY INSTITUTE
Solutions Advisory Learning

Introduction

After conducting research on the above questions and ensuring that you understand the above issues you can progress to the next stage of this challenge.
Your team, acting as a high-level national security agency, needs to advise national critical infrastructure entities on how to begin implementing and improving their cyber security posture in line with a cyber security maturity program.

Use the following as guidance:
Should the NCI and government departments be subject to a centralised and managed cyber maturity program with regular reporting and metrics (i.e. the Australian maturity program), or should this be decentralised and each entity instructed to make use of international standards such as the NIST Cyber Security Framework (https://www.nist.gov/cyberframework) with additional sector specific measures? What are the potential advantages and disadvantages of these approaches. In the case of the last question should the approach be different for developing countries with low levels of cyber security maturity compared to developed countries? (See ITU Cyber Maturity Index). Do you think it is possible to use both approaches simultaneously – explain?

NB: It is important for this challenge to attend the lectures of Prof Brett van Niekerk and Prof Elmarie Biermann.

Objective and key tasks

Countries across the globe are analysing and planning countermeasures and controls for strategic cyber threats aiming at causing disruption and sabotage on a national level.
Study the following questions, and ensure you have a sound understanding of the issues:

- What does a strategic cyber threat look like?
- What differentiates a strategic cyber threat from other types of cyber threats?
- What are TTPs in this context?
- Strategic Cyber Threat Actors and Advanced Persistent Threats (APT)
- Is the focus on ransomware attacks diverting awareness away from other serious attack vectors?
- Define national critical infrastructure (NCI). What are examples of NCI?
- Why do attacks on NCI constitute potentially catastrophic cyber events of national significance?
- **April 16th, 12:00PM SAST is the deadline for you to hand in a video of max. 3min** to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the **final submission moment** and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Three recent cases to consider: Solar winds, Cyber attackers Lure EU Diplomats with Wine-Tasting Offers, Volt Typhoon – LOL Bin attack on US critical infrastructure. However none of these cases are ransomware incidents, yet most organisations devote a significant amount of resources to ransomware prevention – in doing so are they potentially losing sight of other vectors for advanced persistent threats?

Contributor

The Cyber Security Institute (CSI) offers specialized training and services in cyber security. Their focus includes bespoke training courses and cyber and data security guidance for both public and private sectors. CSI's services encompass advisory and consultancy, particularly in areas like ISO27001 implementation and POPIA compliance. They also provide a range of courses in cyber security, cyber investigations, cyber intelligence, cyber governance, and a comprehensive IT and cyber security program. These courses are designed to equip various professionals with practical skills and competencies in cyber security. For more details, please visit their website at Cyber Security Institute.