Deloitte.

Security in a hyper connected world

Network Protection: the right steps to secure your network

Telecom Engineering Centre of Excellence (TEE)

EMEA Centres of Excellence

Network security landscape

The IT environment is more sophisticated than ever, with companies being exposed to complex network threats and attacks.

Network threats and attacks main figures

4.1 billion records **were exposed** by data breaches in the first six months of 2019.

67% of industrial **organizations don't report security incidents** to regulators.

Only **38% of global organizations** **claim they are prepared** to handle a sophisticated cyber attack.

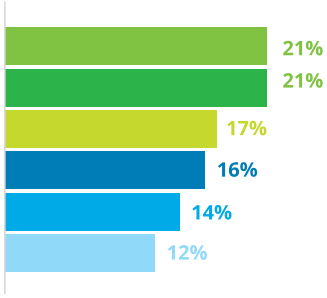
There is a **hacker attack every 39 seconds.**

The **top 5 cyber-attacked industries** over the past 5 years are: **Healthcare, Manufacturing, Financial services, Government, and Transportation.**

Retail, Energy and Utilities, Media and Entertainment, Legal, and Education will round out the **top 10** industries for 2019 to 2022.

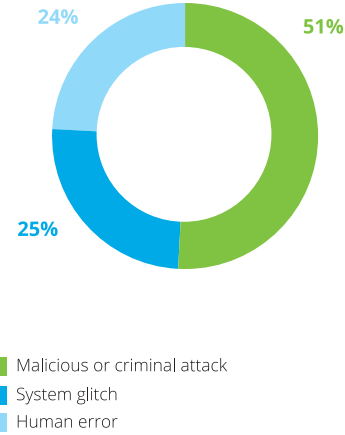
The impact of network attacks

Network attacks damages are expected to cost the world **$6 trillion** by 2021, against the **$3 trillion** by 2015. **Revenues, trust and reputation** are some of the areas impacted after a network attack, as detailed below:



Data breach causes

Malicious attacks are the leading cause of security breaches in 2019.



Sources: Gartner, Cybint, IBM, Forbes, Security Intelligence, CyberSecurityVentures, Deloitte

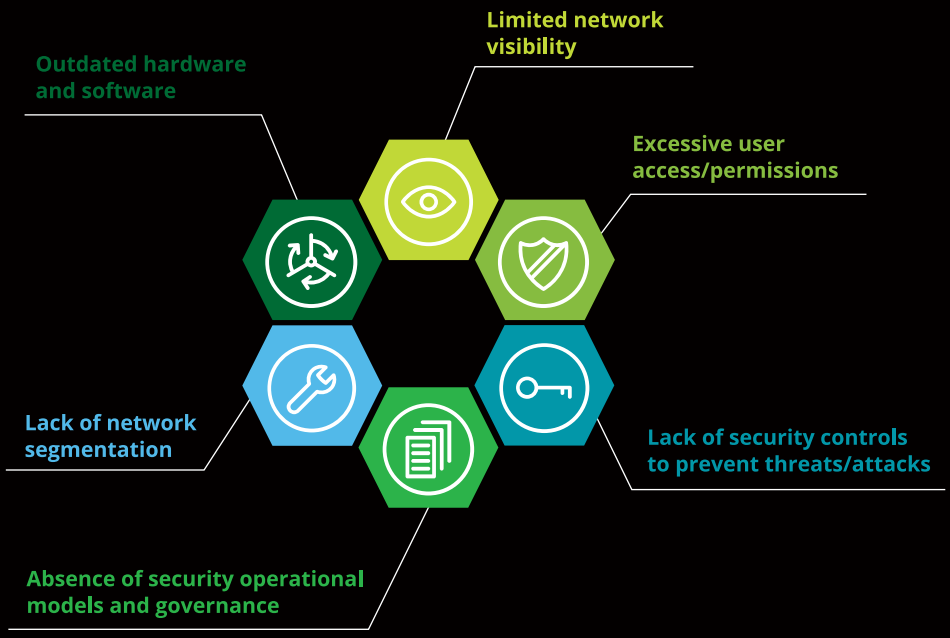
TEE Network Protection

Network Protection should be a priority to companies in order to be prepared to the increasing number and complexity of cyber threats.

Why protecting the network is important?

Security threats are increasing and **making more damage** every year. A network attack can seriously impact a company's business and reputation as it can result in the **exposure of confidential information, risk information integrity** or compromise the **availability of business systems**. To face this reality, companies must design and operate their networks considering its **security and protection** a priority.

What makes a company vulnerable?



Most companies **lack a security strategy for the network, a security governance model** and **appropriate security controls** to protect the network. Therefore, they are not prepared to **detect, protect, respond and recover** their network from threats and attacks.

Network Protection offer

Breaking down the offer into areas of expertise ensures a structured approach and an effective implementation.

Approach for Network Protection

Our offer consists in consulting services that bring expertise and knowledge to effectively secure the network.

Network assessment

- Collect information on the existing network devices, sites, business critical assets and technology landscape;
- Assess current network security capabilities (people, processes and technology) and network security maturity;
- Identify the existing network threats and vulnerabilities.

Network Protection strategy definition

- Define the Network Security Target State;
- Define a Must, Should, Could strategy to achieve the Target State;
- Define the network security baseline configuration for network devices.

Network Protection implementation

- Implement the network security baseline configuration;
- Enhance the network defenses through the implementation of the selected security controls;
- Remediate the current network devices that represent a security risk, considering the targeted security level;
- Implement the defined network security capabilities (people, processes and tools).

Network Protection sustainability

- Ensure knowledge transfer to the BAU teams;
- Guarantee the teams are properly trained to manage the enhanced security capabilities;
- Monitor if capabilities are correctly used in BAU.

Our experience

TEE has already several use cases, applying different technologies and enhancing several capabilities to achieve the expected outcomes.

Enhanced network visibility

Created an aggregated view of the **Network Topology**, detailing the majority of the known **network**. The remaining was achieved by **uplifting** the **visibility capability**.

This project enabled the Client to have visibility of its network assets and the ability to keep track of network changes, thus being able to understand where an investment in network security was essential.

Network security strategy

Strategy designed for the network security architecture providing a vision for the Client's future state, following by the enablement of next generation firewall security controls in critical areas of the network.

Defined **Strategy for Network Segmentation** stating which network security controls must exist in different areas in the network.

Security baseline configurations

Defined **Secure Baseline Configuration** based on the minimum-security standards expected **for the configuration of network devices.**

This project ensured that the Client's network devices were protected, by guaranteeing that the configurations were in place according to the defined security framework. Additionally, an efficient management of the firewall ruleset lifecycle was implemented.

Hardening network devices

Network Infrastructure Patch Management defined and implemented the processes to maintain, update and upgrade the software of the Client's network devices', following industry's best practices, which allowed to increase the security level of the devices.

Patched firewalls with the latest software version.

Network threat detection and protections

Implementation of IDS/IPS to detect and block malicious traffic coming to the Client's network.

This project implemented a security control in key network locations which allowed the Client to be able to prevent its network from malicious traffic. Additionally, the capability (people, processes and tools) to manage multiple IPS instances was uplifted.

Contacts

Experts

Luís Abreu
Telecom Engineering Centre of Excellence (TEE) Partner
labreu@deloitte.pt

Vikash Laxmidas
Telecom Engineering Centre of Excellence (TEE) Manager
vlaxmidas@deloitte.pt

Sponsors

Pedro Tavares
Telecom Engineering Centre of Excellence (TEE) Leader
petavares@deloitte.pt

Joaquim Ribeiro
Telecom Engineering Centre of Excellence (TEE) Partner
joaqribeiro@deloitte.pt

Acknowledgements

Special thanks to Deloitte TEE Team who contributed to this publication in terms of researching, providing expertise, and coordinating:

Ana Rita Ferreira | David Andrade | Fábio Martins | Filipe Monteiro | Gonçalo Horta
Luís Pinto | João Bernardo Alves | José Miguel Mesquita | Tiago Pereira Marques

Deloitte.