CYBERSECURITY

Organization Vulnerability Research

Contact

Cybers security team
e-mail: B2B_Security_Squad@t-mobile.pl

Contents

1. WEB application vulnerability and security research 3

2. ICT infrastructure vulnerability research 4

3. Assessment of the state of cyber security culture 5

4. Verification over the method of protecting e-mail systems 6

5. Analysis of supervision overr the point of interconnection with the Internet 7

WEB application vulnerability and security research

WEB application vulnerability assessment

WEB applications are a frequent target of cyber criminals due to the fact that they are usually exposed on the web Internet as a communication interface for an external user. In addition t o the standard configuration on implementation phase and maintenance rarely have additional layers of protection that are allowing for detection and protection against threats. The vulnerabili ties and errors of WEB applications are one of the main reasons for their occurrence of ICT security incidents related to compromising websites, data leakage customers, employees, which results in obtaining an access point to the resources of the organizat ion, and then treating it as a communication intermediary for further cybercriminal activities.

Proprietary methodology of vulnerability research

Assess the vulnerability to threats by examining the status and level of security of WEB applications and WAF protection systems.

The point of research is:

- Active checking of vulnerabilities of WEB applications in terms of known vulnerabilities
- Assessing the effectivness of WAF in detecting and blocking threats
- Dynamic analysis of the application's source code to identify programming errors
- **Identification of malware and content that can be embedded in WEB servers.**

The result of the reseach will be a report containing:

- Assessment of security status, configuration errors and vulnerabilities
- Information about detected threats
- Outlining the direction of development and changes necessary to increase the level of security in the organization
- Recommendation of corrective actions.

Why does your company need such a research?

- Increase in the level of cyber security in the organization
- Increasing the level of customer and employee data protection
- Standards and regulations (eg. the act on telecommunications law, KNF-D, the NIS directive - act on the national cyber security system)
- Audit (internal, external)
- Improvment of activities related to the process of managing cyber security incidents.

ICT infrastructure vulnerability research

ICT infrastructure vulnerability assessment

The ICT infrastructure is an essential element for the proper functioning of any organization. ICT networks are multilayer, compiled components that form a whole. Some of them are visible from the Internet, which makes them directly exposed to cyber threats and attacks. Infrastructure vulnerabilities are one of the basic reasons for ICT security breaches that result from outdated software and configuration errors arising at the implementation and maintenance stage.

Proprietary methodology of vulnerability research

Assess the vulnerability to threats by examining the condition of the ICT infrastructure.

The point of research is:

- Identification and inventory of IT infrastructure resources
- Demonstrating vulnerabilities, security gaps and configuration errors
- Proactive action against identified threats, indicating the direction of corrective actions
- Demonstrating the risks and critical areas that should be prioritized and eliminated.

The result of the study will be a report containing:

- Assessment of security status, configuration errors and vulnerabilities.
- Information about detected threats.
- Outlining the direction of development and changes necessary to increase the level of security in the organization.
- Recommendation of corrective actions.

Why does your company need such a research?

- Increase in the level of cyber security in the organization.
- Standards and regulations (e.g. the act on telecommunications law, KNF-D, the NIS directive act on the national cyber security system).
- Audit (internal, external).
- Improvement of activities related to the process of managing cyber security incidents.

Assessment of the state of cyber security culture

Employee sensitivity assessment

Employees are an important element of the security system in any organization. Due to poor awareness of threats and little knowledge of identifying them, they are often the weakest link in the system. The cause of critical incidents are usually directly human errors caused by improper processing of the received information Cyber criminals are often skilled professionals with the sole purpose of making an intentional profit. By targeting the employees of the selected organization, they gain a decisive advantage. The lack of cybersecurity awareness programs and exercises simulating individual cases is one of the main reasons for ICT security incidents.

Proprietary methodology of vulnerability research

Assess resistance to threats by examining employees' susceptibility to social engineering attacks using:

- Simulating real phishing campaigns.
- Non-invasive attacks targeted at selected groups of employees.
- Personalize the message content using dedicated templates.

The result of the research will be a report containing:

- The system vulnerability to attempts to send malicious e-mail messages
- Recommendations on the use of mechanisms increasing the level of e-mail security.
- Outlining the direction of development and changes necessary to increase the level of security in the organization.
- Recommendation of corrective actions.

Why does your company need such a research?

- Increase in the level of cyber security in the organization.
- Standards and regulations (e.g. the act on telecommunications law, KNF-D, the NIS directive act on the national cyber security system
- Audit (internal, external).
- Improvement of activities related to the process of managing cyber security incidents.

Verification over the method of protecting e-mail systems

Vulnerability assessment of mail security systems

Email is the most popular distribution channel for malicious content and the easiest way to get it into your organization. The main reasons for this are the general availability of mailbox addresses, employees' ignorance and lack of resistance to social engineering attacks. Another element is very effective methods of crafted messages that pass through e-mail gateways, which do not effectively analyze and interpret the content. A single layer of mail systems protection is the main cause of ICT security incidents.

Proprietary methodology of vulnerability research

Assess your resilience by examining your postal infrastructure protection mechanisms.

The point of research is:

- Identification of native protection mechanisms, policies and configuration of mail protection systems by generation special e-mail messages simulating popular attack techniques
- Generating e-mail messages containing malicious URLs and attachments in order to verify their identifiability and blocking.

The result of the research will be a report containing:

- The system vulnerability to attempts to send malicious e-mail messages
- Recommendations on the use of mechanisms increasing the level of e-mail security
- Outlining the direction of development and changes necessary to increase the level of security in the organization
- Recommendation of corrective actions.

Why does your company need such a research?

- Increase in the level of cyber security in the organization.
- Standards and regulations (e.g. the act on telecommunications law, KNF-D, the NIS directive act on the national cyber security system).
- Audit (internal, external).
- Improvement of activities related to the process of managing cyber security incidents.

Analysis of supervision over the point of interconnection with the Internet

Assessment of the security sensitivity over the point of the inter connection with the Internet

The point of interconnection with the Internet plays a fundamental role in ensuring cyber security and identifying threats. It is an intermediary in traffic, connecting with the outside world, which should be closely monitored and treated as a border point. Direct supervision over outgoing and incoming traffic is one of the pillars of effective monitoring of the ICT infrastructure. The lack of proper monitoring and analysis over events at the interconnection with the Internet is one of the main reasons for the occurrence of ICT security incidents.

Proprietary methodology of vulnerability research

Assess your vulnerability by research on your edge infrastructure.

The point of research is:

- Edge architecture analysis.
- Verifying the ability to detect high-risk applications and content in the network traffic.
- IPS functionality check- detection and blocking of known exploit threats.
- Detecting threats at the level of firewall functional modules.

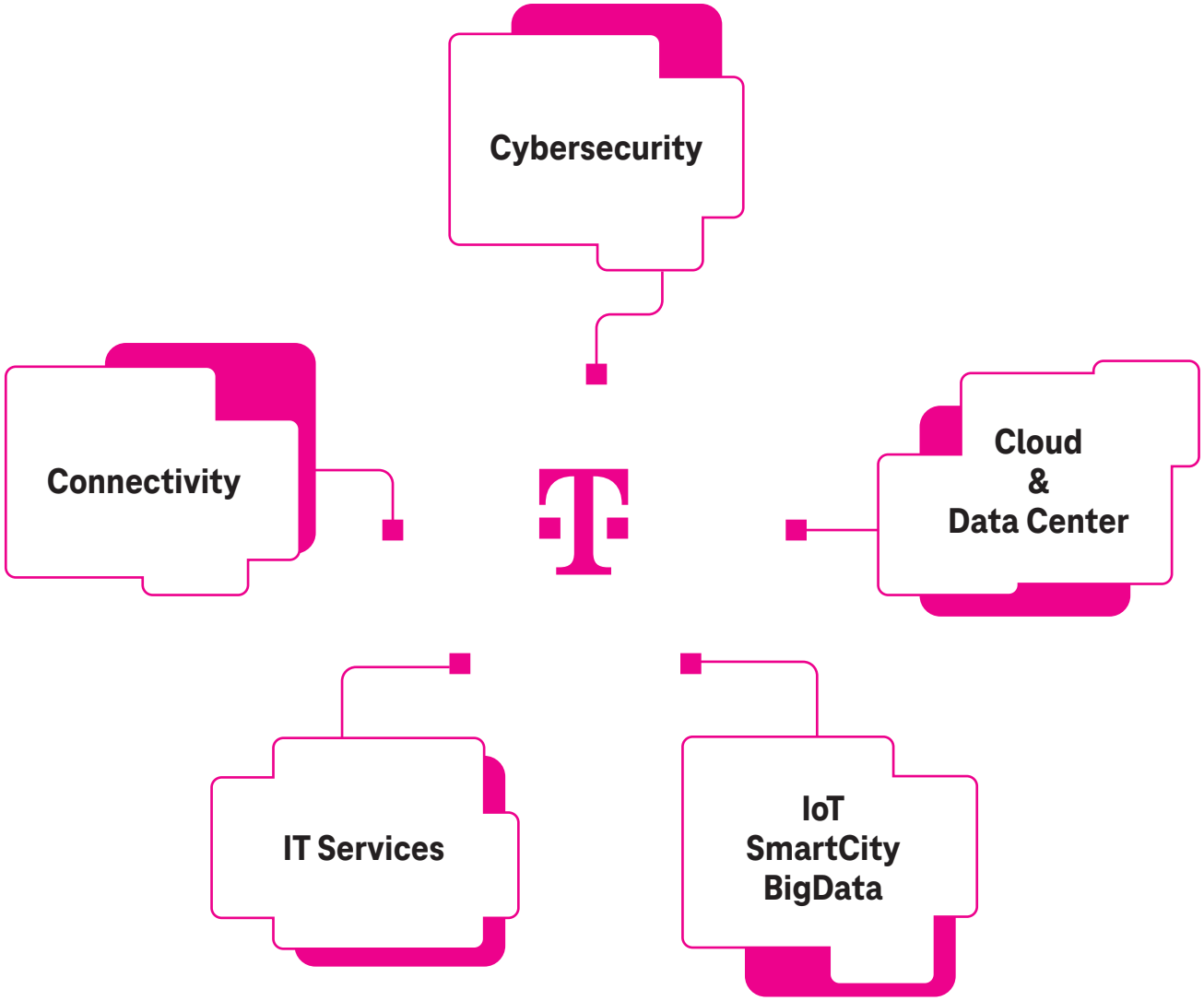
The result of the research will be a report containing:

- The system sensitivity to attempts to transmit malicious content in network traffic.
- Identifying threats at the edge of the Internet.
- Outlining the direction of development and changes necessary to increase the level of security in the organization.

Why does your company need such a research?

- Increase in the level of cyber security in the organization.
- Standards and regulations (e.g. the act on telecommunications law, KNF-D, the NIS directive act on the national cyber security system
- Audit (internal, external).
- Improvement of activities related to the process of managing cyber security incidents.

Comprehensive services
for large and medium-sized companies



POLSKA

OFICJALNY SPONSOR REPREZENTACJI

T-Mobile Polska S.A.
ul. Marynarska 12
02–674 Warszawa

More information about the services:
www.t-mobile.pl/biznes