1. General Overview on the SMEs in Poland

According to the annual report [1] the general overview data related to enterprises in **Poland** indicates that there are ~2.2 M enterprises and 99.8% are SME's and among them: 97.0% are micro, 2.2% are small and 0.7% are medium. Working people: 10.01 M – the number of working people in enterprises, 6.75 M – the number of people working in SMEs, among them there are: 4.12 M – in micro, 1.05 M – in small, 1.58 M – in medium; 3.26 M – in large. 4.53 – the average number of working people per enterprise

2. Analysis of the risk situation:

What IT security gaps have SMEs?

According to data given in [2] we can note that:

- 33% of all and 42% of large enterprises have struggled with cybersecurity breaches in 2021,
- 6% of large companies have experienced multiple attacks,
- 45% of cybersecurity threats were related to malware,
- 43% of companies reported attempts to break into IT systems,
- 29% of all companies noticed phishing attempts.

What are the major risks in the SMSs?

The problem of major risks in cyber security can be shown as it is in Table 1 done according to data given in [2]:
Table 1. Major risks in Polish SMEs.

Risk	Total	SME	Big
breaking into the company's IT systems	43%	37%	47%
the operation of malware, including ransomware	45%	37%	50%
identity theft	8%	16%	3%
theft or disclosure of data	18%	11%	23%
phishing	29%	26%	30%
other	8%	11%	7%

Are there any differences between big companies and SMSs on Cyber-Security attacks?

Some difference can be show depending on the size of companies. According to data given in [2] we can show that the most frequent cybersecurity attacks related to SME's refers to:

Digital infrastructure:	1016 cases,	9,75%
Retail trade	1437 cases	13,79%
Media	2568 cases	24,64%

What type of risks and attacks are peculiar to SMEs?

According to [2] we can show that the most peculiar to SME's incidents are:

Phishing	7622 cases	73,15%
Spam	336 cases	3,22%
Open websites prone to abuse	29 cases	0,28%

Many of incidents are unclassified (~18%)

What kind of measures are taken in the SMEs to protect themselves?

According to [2] we can indicate the following measures – Table 2:

Table 2. Measures related protect IT resources in SMEs

Measure	
we use anti-virus software	85%
we secure mobile devices and the Internet of Things, including those connected to the network in the BYOD model	67%
encryption, including mobile devices, laptops and documents	51%
we use security at the edge of the network	88%

we use typical security procedures such as software updates, regular backups	72%
we secure and monitor employees' workstations	68%

What kind of skills are needed?

We can indicate the following needed skills [3] also confirmed by report available in [4]:

- identifying security gaps, risk analysis and detection of hacker attacks or other incidents,
- evaluation of the level of safety, in terms of technical, legal and ethical aspects,
- design, configuration and diagnosis of ICT networks,
- taking care of the technical efficiency of the system - removing failures and defects,
- administration of the system and devices for detecting incidents of IT security breaches,
- planning and implementing cybersecurity solutions,
- developing emergency procedures, attack response scenarios,
- cooperation with programmers,
- support for employees of other departments in the field of safe use of the Internet or devices,
- conducting security tests of applications and websites,
- preparing reports.

Are SME's prepared for targeted attacks on reputable customers?

According to data given in the report [5] (2018) for Polish SMEs we can indicate that:
44% of companies have suffered financial losses as a result of attacks,
62% of companies experienced disruptions and downtime
21% were victims of disk encryption (ransomware)
20% of medium and large companies have no cybersecurity
46% of companies do not have operational incident response procedures
on average, 3% of the IT budget is spent on security - that's at least three times too little
20% of the respondents have not started preparations yet
50% of companies rate their readiness at 30% or less
3% of the companies are fully operational in cyber security
8% of the surveyed companies are matured in terms of information and cyber security

Is there any IT security concept?

On August 1, 2018, the President of the Republic of Poland signed the Act on the National Cybersecurity System, implementing into the Polish legal system the Directive of the European Parliament and of the Council (EU) on measures for a high common level of security of network and information systems in the territory of the Union (Directive 2016/1148), the so-called The NIS Directive.

The purpose of the act on the national cybersecurity system prepared by the Ministry of Digitization was to develop legal regulations enabling the implementation of the NIS directive and the creation of an effective ICT security system at the national level.

The national cybersecurity system aims to ensure cybersecurity at the national level, in particular:

- uninterrupted delivery of key services and digital services,
- achieving a sufficiently high level of security of ICT systems used to provide these services.

The system includes operators of key services (e.g. from the energy, transport, health and banking sectors), digital service providers, CSIRTs (Computer Security Incident Response Team) at the national level, sectoral cybersecurity teams, entities providing cybersecurity services , authorities competent for cybersecurity matters and a single point of contact for communication within the framework of cooperation in the European Union in the field of cybersecurity. Operators of essential services are required to implement effective security measures, assess cybersecurity risks and report and handle serious incidents in cooperation with the national CSIRTs. The above-mentioned entities are also required to appoint a person responsible for cybersecurity of the services provided, handling and reporting incidents, and sharing knowledge on cybersecurity. Public administration bodies as well as telecommunications undertakings will also be included in the national cybersecurity system - in a manner harmonized with the existing regulations in this area.

References:

[1] A. Skowrońska, A. Tarnawa: Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce, 2021, https://www.parp.gov.pl/component/site/site/raport-o-stanie-sektora-msp-w-polsce, Access: 28 January 2022.

[2] Cyberbezpieczeństwo polskich firm 2021, https://www.computerworld.pl/whitepaper/3727-Cyberbezpieczenstwo-polskich-firm-2021.html

[3] https://www.praca.pl/poradniki/rynek-pracy/specjalista-ds-cyberbezpieczenstwa-praca,wymagania,wynagrodzenie_pr-855.html

[4] https://itwiz.pl/najwazniejsze-kompetencje-specjalistow-cyberbezpieczenstwa-nowej-generacji/

[5] Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście, 2018 https://www.pwc.pl/pl/pdf/cyber-ruletka-po-polsku-raport-pwc-gsiss-2018.pdf