Intro

Small and medium enterprises are increasingly becoming cyber attacks targets. Regardless of the fact that media headlines usually cover attacks against large companies like Yahoo, Sony, Facebook etc., small and medium enterprises are actually being targeted by hackers to the same extent. Therefore, it is necessary to raise awareness of the management and employees regarding possible cyber attacks and misuse of poorly defended ICT systems of small and medium enterprises. During the company budget planning process, the management often has the "We are too small to become a target" approach which has proven to be wrong.

Trends

The 2018 statistic reports state that poorly protected information systems of small and medium enterprises are increasingly being targeted by the hackers. Actually, small and medium enterprises are targets in more than 50 percent of ransomware attack cases, due to the fact that hackers realized that managers of small and medium-sized enterprises would most often decide to pay the ransom in order to access their locked files as soon as possible, but also to protect the company's reputation, disregarding the fact that even when they pay the ransom there is no guarantee that there will be no other ransom requests for additional payment. It's similar with any other type of attack such as: Data breach, Identity theft, Phishing campaign, Social engineering, Denial of Service or Distributed Denial of Service attack (DoS/DDoS), espionage etc.

Prevention steps

However, there are measures that can be taken in order to prevent attacks and protect the ICT systems of small and medium-sized enterprises, which should include the following:

- providing the basic level of cyber hygiene within the company by establishing appropriate security procedures, conducting regular cyber security trainings for all company employees, implementing unique ID cards for accessing the ICT system, managing accounts and passwords etc.,

- creating a system employee access profiles which enable them to access only the data necessary for their job activities,
- regular updating of all hardware, system and application solutions, as well as regular backup of important documents and files,
- obligation to implement antivirus software solutions within the entire information system of the company,
- creating the incident handling procedures and the business continuity plan.

By applying the listed measures, the level of security of the company's system will be raised to a higher level, which will make the company more protected from risks and more resilient. Consequently, the possible exposure of the company to financial losses will be reduced to a minimum, which will enable enterprises to financially support other processes and safely develop their business.