How good is your system's cybersecurity?

by  Štefan Lukáč, ESET Security Sales Representative

Hackers are often regarded as modern-day pirates. But this is a romantic view of people with the ability and willingness to steal and misuse you, your data, your privacy and your money. And don't think that they have to be software geniuses. Extensive technical knowledge isn't needed anymore, as there are many pre-built, ready to be used malicious programs to be had for free or at low cost. Furthermore, there are known "holes" in IT systems, which if not tested for and patched, allow attackers easy access to your environment to either insert malicious code or take your data.

Situations when your PC, or wider IT systems are affected, can be difficult to identify, especially if no visible destructive actions have taken place. These situations are clearly dangerous for your company. An attacker might create a back-door to your system, insert code, and then a command will activate the malware and steal something from you and return it to its control center. This malicious code can sit in a system for months or even years, and then in an instant allow the leakage of data, steal typed passwords as you type them (while logging in to internet banking), activate microphones or PC cameras, offer you fake webpages instead of the page you wanted, collect data and/or redirect communications.

Using these tactics, an attacker can hide their footprints, create additional opportunities for malicious activities and make it difficult or impossible for them to be caught.

Just to give you an example of the potential pain your organization could experience, we give some real life cases. Many cases are hidden from the public, due to efforts to avoid compromising the image and reputations of the affected companies.

In the US in 2013, there was a cyberattack on a dam in Rye Brook, N.Y., which was only publicly announced in 2016. Hackers were successful in taking control over some of the dam's systems.

In 2015, there was massive leak of US federal government data, including information on CIA agents.

In 2015, and again in 2016, attacks on Ukraine's energy distribution network put 230,000 people in the capital, Kiev, in the dark due to an electrical power outage. In 2016, a water utility in the US was attacked and hackers were able to change the levels of chlorine at a water filtration station.

You may remember, or may have been affected, by WannaCry in 2017. At least 40 hospitals in the UK were forced to stop providing services, and CAT scans, x-rays and cooling devices were impacted. In Slovakia, this ransomware spread to the computers at a hospital, around 50% of machines were affected and the rest switched off to mitigate the impacts.

Often a number of days are needed to solve these kinds of issues and return to normal operations. Two to three days of near paralysis is a real possibility, where the primary task following the identification of an attack is to analyze the issue and decide if the computers' operating systems should simply be reinstalled, or whether they should be reimaged with full data loss. The next phase may last a week, and operations will be slowed until full recovery of normal functions. However, the costs of data leakage, data loss, missed deadlines or organizational reputation are much more difficult to estimate.

Hackers are often regarded as modern-day pirates. But this is a romantic view of people with the ability and willingness to steal and misuse you, your data, your privacy and your money.

There are some basic steps that can be taken to make your future safer. Even in smaller organizations, SMBs, and for the self-employed, it makes sense to use a good cybersecurity solution, with a solid reputation and use regular threat database updates and encrypted data on PCs and mobile phones. Otherwise, you are taking a huge risk, just to save relatively small amounts of money.

Organizations with their own web or mobile applications, for example, those used for communications with partners, customers, employees, or organizations that need to be aligned with recent GDPR legislation, should take additional steps to test and prove their systems' strength, and identify the existence of issues in hardware and software configurations. This penetration testing can identify vulnerability issues, due to missing updates and architectural and process mistakes. Penetration tests are controlled simulations of hacker attacks to determine your systems' resilience. This goes beyond just automatic scanning by a program tool, and includes more complex processes led by specialists and based on standards and a given methodology.

These tests can be done in two to five days at organizations that have more basic infrastructure or applications. This makes penetration testing accessible even for smaller companies. Bigger organizations can expect higher costs and a longer duration of testing based on the number of applications. This also has a strong correlation with the total GDPR penalty risk amount.

The last point I would like to emphasize is training. If you don't want to pay for face-to-face training, there are some great e-learning possibilities for free. I would recommend these for every company to decrease the risk of employee mistakes or a lack of knowledge, as these are among the leading causes of opportunities for attackers to access your valuable data, or disrupt your business assets.