You won't even notice a cyber attack...

Video Transcript

Intro

In five years, your car, house, coffee maker, flower pot - just about everything will be online. And it will only be a matter of time before you too become the target of a cyber attack. I'm Michal Merta from Accenture, and I'm sure you've encountered a cyber attack. You just don't know about it.

What does a cyber attack look like?

A cyber attack is a long-term, carefully planned process that exploits vulnerabilities and a moment of surprise. After a successful initial breakthrough, the attack moves to the next phase, closer to the set goals - for example, to the domain administrator account.

The attacks that most of you have probably encountered are from the Ransomware family. It is a type of malicious program that encrypts your data so you can't work with it. Hackers behind these attacks usually shut down systems and demand money or cryptocurrency in exchange for data recovery.

Ransomware as such is therefore very interesting in terms of monetization and is becoming big business for hackers. It is enough to find a weakness, which are usually trusted employees or users. All you have to do is open a dangerous link in your email or on social networks and you have a problem.

Who is behind the cyber attacks?

Attackers are usually not the ones who embezzle your data. They are traded on black markets, so-called dark nets. The volume of transactions there is growing dangerously, attracting more and more individuals and organized groups.

And because it is often cheaper for the victim to pay a ransom than to risk losing or publishing data, this whole black market is incentivized and cybercrime is growing at an alarming rate.

Of course, the unlimited availability of a huge number of tools, training materials and online documentation is also a problem, which can turn almost any English-speaking individual into a potential cyber threat.

Every attack is something new

The failure of the human factor is not always behind a cyber attack. Attackers are actively looking for vulnerabilities not only in applications but also on any device connected to the network. We have

experience with all this and, here at Accenture, we can help you.

There are mechanisms that can detect or even stop the attacker, or predict the attack itself. Defence mechanisms include, for example, functional SIEM solutions, simulation of attacks, threat hunting, administration of privileged accounts or secure application development.

However, be aware that if you are a target to an attacker, he will try techniques for which even your existing security may not be enough, and which may not be known to the defence teams. Particularly organized groups tend to have experts in the development of zero day exploits or specialists in phishing and vishing.

That's why we've built the Cyber Fusion Centre including leading experts in security. Thanks to them, you will be able to pay more attention to your business and less to its protection. Because at Accenture we take care of security.