accenture

Cybersecurity is a topic for each and every one of us

Video Transcript

Intro

IT technologies and online connectivity help your company grow faster, manage it more efficiently, grow business and innovate the services and products offered. On the other hand, you also become more frequently a target of cyber attacks.

My name is Michal Merta, I'm from Accenture, and if I had to define a single threat that every company should fear, it would be a cyber threat.

Cybersecurity is a topic for each and every one of us

We live in the digital age and internet connection is actually a matter of course. Our dependence on the online world and its possibilities exposes us to considerable risk, which may, sooner or later, cause us to make a mistake that attackers will undoubtedly take advantage of.

At best, this mistake will only cost you a lot of money. In the worst case, your own privacy or the security of the company you work for will be compromised. This can result in reputational damage, loss of good standing, or loss of sensitive data. In extreme cases, it can be a threat to your own life.

From my more than fifteen years of experience, I can say that it doesn't matter if the attacker attacks you, your company, or it is a random attack.

The cyber attacker needs no reason

The thought that your company is uninteresting to attackers – or hackers – may be legitimate, but cyber security is not to be underestimated. In the vast majority of cases, coincidence is what often makes your company the target of a cyber attack.

My experience is that a company accidentally gets involved in an ongoing wave of cyber attacks. The result can be data loss or theft, line decommissioning, unavailability of critical applications or the theft of know-how. And from this purely random situation it takes a long time to recover.

At Accenture, we give our own cyber protection the highest possible priority. That is why we can effectively protect our clients.

A cyber threat takes many forms

Many of us imagine the attackers as organized groups with huge financial resources, even more computing power and

the best hackers. On the other hand, there are individuals from the ranks of employees or clients who often make an unknowingly mistake and this, in combination with a digital virus or malware, can have fatal consequences.

Attacks can even be from individuals who just enjoy it. They want to prove something, tease someone, or just make some extra money. Their motivation is not great, but nevertheless the result of their activity is a big problem for the victims of the attack. The attack may also be driven by state-run organizations that use cyber attacks to address their international interests and political goals. Such attacks are often much more effective and cheaper than traditional military operations. Their targets also tend to be companies from the economic and industrial spheres.

The protection of critical infrastructure and the position of the state in the field of cyber security will increase significantly in the future. Digitalization, digital identity, online state administration systems – all this will need to be consistently secured to protect citizens, i.e. each of us.

I believe that you also perceive cybersecurity as an important topic concerning your business which must not be overlooked or taken lightly. That's why I'm offering you a helping hand and a partnership with Accenture.