



Trends in protection against cyber attacks

Video Transcript

Trends in protection against cyber attacks

Five years ago, a unique Cyber Fusion Centre was established in the Czech Republic, in which experts from more than 30 nationalities work with different fields of expertise. They provide cybersecurity services to clients around the world.

We simulate real attacks on applications, infrastructure, machines, or the company as a whole using sophisticated scenarios. We help clients discover weaknesses in their security and propose solutions to all their deficiencies.

In addition to protection against attacks, we also help with the management of privileged accounts or, for example, with cloud security. We have our own 24/7 monitoring centre, which immediately detects and responds to incidents threatening the security of clients.

Prevention of attacks

Our primary task is to convince you, and everyone else, that cybersecurity must be seen as an integral part of business. Just as important as the accounting department.

It is difficult to help clients who are not aware of this, because they are primarily the

ones responsible for the secure handling of their employees and customers' data. We will provide them with tools and expert advice.

Whether the client decides to outsource their security or build their own security team, in both cases, Accenture is ready to deliver an end-to-end solution. There are also cases where we provide the services of a control mechanism that keeps the security activity on the client's side constantly alert. And it doesn't matter if they are clients from the products industry or banks.

The client (company) must determine what security means to them and how it needs to be set up so that his business is safe, resilient, and ready for possible cyber attacks. We can provide very good advice in this regard, because within Accenture we follow trends in all industries across continents.

We have our own Threat Intelligence team, a kind of secret service of the commercial online world. Teams of experienced analysts monitor ongoing attacks, have an overview of what is being sold on various "darknet" servers, and evaluate and then share potential threats and targets of hacker attacks with us.



Thanks to us, the client gains a competitive advantage and is one step ahead. Prediction of a possible attack is very important for the appropriate setting of security mechanisms.

Response to attack and handling consequences

However, cyber attacks are not always preventable. It is well known that the weakest link is the human factor, which fails sooner or later. Once the attack is carried out, it is necessary to react as quickly as possible and so as to cause as little damage as possible.

For example, if a production line is taken out of service. Re-launching it as soon as possible is a key task for which the company must be prepared, without the attacker himself being involved in this remedy, for example by payment of a ransom.

Shutdown of an attacked production line means a production interruption for several weeks for a poorly secured company, which not only results in fatal financial consequences, but can also significantly damage to the company's reputation.

We see into the future and we can prepare you for it. In this regard I can offer you a helping hand and a partnership with Accenture.

Copyright © 2022 Accenture
All rights reserved.

Accenture and its logo
are registered trademarks
of Accenture.