IT Security Day

by ASCONSIT | Published on 30. November 2021

When and where does computer safety start?

Today is Computer Security Day! But what is Computer Security Day about? The first thing you'll notice

is that the term seems a bit outdated. That's because the day was first announced as Computer Security Day in 1988 by the US 'Association for Computer Security', with the aim of raising awareness for the subject. Ever since, we have celebrated Computer Security Day on 30th November of each year. But even if the term seems outdated and we tend to speak of IT security today, the issue is as urgent as ever.

IT systems and IT security are central to every business today, and almost every process is based on them. When IT systems are disrupted, this may, in a worst-case scenario, lead to the complete shutdown of a company's operations or production and cause major economic damage. This is why every business needs to protect its IT systems against existing risks and potential attacks. Preventing the failure of systems or the manipulation of data is crucial.

But where does computer security even start? Does it begin with planning your network architecture, with the selection of the right hardware and software components, with the mindset of your employees, or does it start when you log in to the system? The fact of the matter is: computer security is a complex affair that covers a wide range of aspects, such as:

- Network security
- Data storage, data protection and data encryption
- Operating systems and software (including updates and security patches)
- Connections to remote workplaces and mobile devices
- Login processes and authorisations for own and external staff

Another undeniable factor is that information technology has evolved at an amazing pace since the 1980s, and that it is constantly faced with new types of threats as cyber-criminals come up with ever new means of attack. Modern cyber criminality is often professionally organised and criminals have access to state-of-the-art technologies. Today, cyber crime creates bigger revenues than drug dealing. IT security thus means a constant race to keep up with the rising threats. Frequent forms of cyber-attacks include:

- Advanced Persistent Threats (APTs)
- Malicious software (malware)
- Ransomware
- Spam and phishing
- Botnets

IT Security starts with an in-depth analysis

What is important to bear in mind in this context is that IT security and cyber security are not merely a matter of technology. Actually, the human factor - the employee - is one of the weakest points in the system. To minimise IT risks and ensure comprehensive IT security, companies need to take both technological and organisational measures. An in-depth process and vulnerability analysis should be the starting point. Such an analysis helps determine which business processes may be vulnerable to security risks, how big the risk of these weaknesses being exploited is, and what scale of damage that would cause. It will hardly be possible to completely eliminate all IT risks, but it is crucial to clearly categorise existing risks with a view to their significance and actively manage them to the extent possible, while ensuring that every staff member is sensitised on IT security.

We at ASCONSIT can support you with the analysis of your business processes and the relevant aspects of IT security. Moreover, we specialise in Identity & Governance & Access Management. In the age of digital transformation, this is an essential part of a well thought-out and clearly funded IT security strategy, which is a crucial success factor for every company.

Would you like to find out more about us and the services we offer? Then get in touch! We look forward

to an exchange with you.