Cybersecurity

The Three Myths of Cybercrime and What It's Really Like

As a German cybersecurity company that consciously identifies as European, we will actively help shape future cyber developments internationally. Contact us now to ensure your company is prepared for future attacks.

Smart Cyber Security

Myth 1

„A hacker is a hacker.“

Wrong. What you have learned about hackers so far corresponded to reality until about 36 months ago. Internationally, there was a small number of people with exceptional hacking skills who often used their special talent either as nerds or as advocates for the interests of a free internet.

Sometimes, they also hacked official government websites to highlight the risks of the internet and hacking in general. However, this world has completely changed in the past 36 months. In addition to ransomware, AI-generated viruses are now freely available to everyone on the dark web. Furthermore, the email addresses of real employees of German companies can also be easily purchased by anyone for bitcoins.

Since then, hacking has become possible in a professional form for both amateurs and criminals. Therefore, we have witnessed a gigantic increase in the number of hacking attacks internationally over the past three years, which, like a biological virus, will never disappear again.

Myth 2

„My IT department and my IT consultants can protect us effectively.“

This is impossible in 99.999% of all companies. The reason is as simple as it is compelling: your IT people and the employees of your external support companies all lack specialized training in cybersecurity, which would also need to be less than 24 months old (as of 2024).

Indeed, one can still complete a master’s degree in computer science in 2024 without having studied cybersecurity for even a single semester.

A non-specialized IT staff member cannot possibly be on par with a hacker whose work is further enhanced by the use of cutting-edge AI. As such, it is extremely unlikely that the IT experts currently supervising in Germany, whether internal or external, can provide cybersecurity at the necessary level. Conclusion: Every company needs software from a cybersecurity specialist!

Myth 3

„Cybercrime is not yet a threat to me today. I can still wait and observe.“

That is completely wrong. We tend to overestimate what we can see with our eyes and underestimate everything that lies beyond our visual perception. This human cognitive bias has its roots in evolution and might have been useful about 100,000 years ago.

The initial use of cybersecurity software is therefore a new, permanent, and indispensable task for your company.

Responsible Decisions: Act Now for IT Security

As a responsible managing director, you must make these decisions now and implement effective protective measures. It should be noted that the employees who have been responsible for IT technology in your company so far are most likely not qualified to develop the first cybersecurity strategy for your company.

Therefore, make this issue a top priority today! The maximum risk is the permanent loss of all company data, which directly affects you as the managing director.

Smart Cyber Security GmbH
Südportal 3
22848 Norderstedt

+49 40 604 29 83 0
kontakt@smart-cybersecurity.de
www.smart-cybersecurity.de

Smart Cyber Security