Cyber Security in Austria

As the year 2020 proves to be „the year of contradictions", the field of cyber security is experiencing a wide gap between perception and reality. Although our cyber security study shows that Austrian companies are better prepared against cyber attacks, there is yet much to be done, as digitalization requires new ways of thinking, new actions and new strategies from everyone.

False sense of security

Companies believe to be ahead of the attackers, however, it has been proven that the dwell time of cyber criminals in corporate networks is getting longer and longer (100 to 170 days). Austrian companies are lulling themselves into a false sense of security: one third of companies believe that it takes one to four weeks to safely remove invader. Another 25 percent are even convinced that it would only take two to six days to do so. These assumptions may be quite accurate for commodity attacks but with the increasing complexity of attacks, they are entirely incorrect.

Doomsaying

Companies believe in their tactics but consider cyber criminals "invincible". On the one hand, companies are convinced that they can quickly detect cyber attacks and ward them off. At the same time, 85 percent trust their security measures. But on the other hand, the majority also believe that it only takes minutes (23 percent), hours (31 percent) or days (24 percent) for a cyber attack to be successful. The reason for this scepticism could be a lack of transparency about the actual security situation, but also deficiencies in communication that need to be improved.

Out of sight, out of mind

Companies outsource, but do not trust their cloud suppliers. Only eight percent of companies trust the security measures of their suppliers and cloud service providers. What is particularly striking is that this concern is not reflected on the expense side: only 19 percent of the survey participants invest in measures aimed at reducing third party risk.

Another interesting fact: companies have learned to deal with standard threats from cyberspace. They invest and train. But when it comes to more complex cyber security challenges, many companies avoid the subject and prefer to carry on without further ado.

Island of the blessed

Companies invest in defense, but neglect damage control. A successful cyber security strategy rarely means not having been attacked. The demand for cyber insurance is slowly increasing. However, not even a fourth of the companies (23 percent) are insured against cyber attacks. This is mainly due to differing expectations: what insurance companies offer still differs too much from what companies expect. Nevertheless, some companies also cite as a reason that their preference to invest in cyber defense and corresponding technologies believing that, therefore, they do not need insurance. A contradiction that can have far-reaching consequences.

Ignorance does not protect against attacks

In many cases, companies act without knowing the exact situation. Ignorance continues to dominate the picture. For example, 18 percent of companies cannot say whether they have become victims of a cyber attack. Even the effects often remain in the dark: one in three of the companies surveyed (36 percent) that had been attacked in the past year were unable to quantify the financial damage. 37 percent cannot give a clear indication of the annual cyber security budget of the company. A quarter of the companies (24 percent) are unsure if they have cyber insurance. These and other figures reveal that even those who have a clear view of cyber security often lack crucial information.

Key Findings

Face-to-face with danger

36% cannot quantify the financial damage after an attack

64% of companies report having identified attacks in less than 48 hours

60% look for vulnerabilities in their systems after an attack

27% have great confidence in their security measures

18% say they do not know if they were attacked

44% say that attacks by state actors have become more important

74% of cyber attacks fall into the „phishing“ category

Attack out of nowhere

57% of companies have been victims of a cyber attack in the last 12 months

KPMG

With the current

20%

would partially reverse digitalization

77%

want more support from the State

64%

expect information and exchange from government agencies

26%

are influenced by cyber crime to invest in digitalization

Broad-based

25%

prepare for possible damage through cyber insurance

27%

have no dedicated budget for cyber security

69%

invest in awareness and security monitoring to protect against attacks

8%

trust the security measures of their suppliers and service providers

In cooperation with

KURATORIUM SICHERES ÖSTERREICH

Sicherheitsforum Digitale Wirtschaft Österreich

Silence is golden

Companies are demanding more cooperation, but remain silent. Although cooperation and networks are supported by companies, open communication is still a long way off when it comes to cyber crime. For example, only three percent of companies clearly comment on statements concerning loss of reputation. The survey shows: reporting anomalies in cyber space is a great question of trust, so a trustworthy exchange of information must be further promoted, since the fight against cyber crime can only be won in a joint effort.

Good cop, bad cop

Governments are supposed to act as guards, but often pose a threat themselves. This is because governmental or State-supported cyber attacks are increasing, and institutionalized crime by government agencies has become a reality worldwide. Many domestic companies misjudge the danger: they are world market or industry leaders or have valuable, innovative ideas. Nevertheless, with too many of them assuming that they are not a potential target for cyber criminals. It is also paradoxical in this context that trust has been lost in precisely those government institutions on which companies actually rely for security.

Boon and bane

Companies are seizing the opportunities of digitalization and cursing the challenge sat the same time, as it demands new ways of thinking, new actions and new strategies from Austrian companies. Cyber security must therefore be thought of as an integral part of digitalization initiatives. In everyday life, companies are faced with the Herculean effort of containing the risk of digital transformation without losing the opportunities. Integrated security solutions that take into account the entire corporate cycle must be found. More and more companies are realizing this: cyber security is not a "spoilsport", but can become a decisive competitive advantage.

Conclusion: the acceptance of the unavoidable

An important fact must be made common knowledge in Austrian companies: cyber security cannot guarantee absolute security. Rather, the role of cyber security must be redefined: as a synergy-creating element in creating, maintaining and guaranteeing the actual function of the company, even when the unexpected happens. Companies must therefore become more resistant to cyber attacks through and through. On the one hand, they must protect themselves against attacks, and on the other hand, they must remain operational and functional in case of an attack. Companies need the ability of cyber resilience: to deliver continuous performance despite adverse conditions.

Michael Schirmbrand
Partner, Advisory
T +43 664 816 09 69
E mschirmbrand@kpmg.at

Andreas Tomek
Partner, Advisory
T +43 664 816 09 95
E atomek@kpmg.at

Gert Weidinger
Partner, Advisory
T +43 664 304 60 11
E gweidinger@kpmg.at

Robert Lamprecht
Director, Advisory
T +43 664 816 12 32
E rlamprecht@kpmg.at

kpmg.at/cyber

Emergency-Hotline: 0800 07 10 30/cyber@kpmg.at