Cyber Security in Austria 2021

The probability of being attacked digitally has never been higher than in 2021 as the world is witnessing a dramatic growth in cyber crime. The Corona pandemic and the digitalization that increased during this unusual year have led to sleepless nights - just a few years ago companies were wondering whether they would be attacked at all, today they are asking themselves only one question: when is cyber crime going to hit? But even if all the odds are against you – the best strat-egy is to act and face the challenges proactively.

From A to Z

To avoid being thrown in at the deep end yourself, neither paranoia nor the current fashion item "tinfoil hat" are good advisors. Cyber Security requires leadership action and innovative cyber security thinking. Steady but certain steps toward cyber security are the best bet. Austria's companies are currently better prepared for cyber crime than they were in our first survey in 2015, but increasing complexity, speed and interdependence mean that many of the current protective measures are no longer efficient and effective enough. Comprehensive technical and organizational solutions are needed: security models for the complete lifecycle of a product - including analysis, planning, design, implementation, and monitoring - as well as the entire digitalization process. From prevention to detection to response - all pillars must be handled strategically. This is the only way Austria's companies can protect themselves against cyber crime in this challenging environment.

Dynamics of cyberspace

But how do you regulate the raging threat if you are unaware of the leak? Building cyber resilience means being aware of your risks. In addition, there are new technologies that will massively change the digital landscape in the coming years - most notably artificial intelligence (AI) and quantum computing. But the problem is also part of the solution: AI will play a central role in the fight against cyber crime - both in the detection of attacks, the analysis of attack behavior, risk assessment and malware detection. Another "secret weapon" is to build up security right from the beginning instead of patching up here and there afterwards.

Increased demands on IT security and adherence to compliance guidelines are among the most important challenges.

Professionals at work

The cybercriminals are up to all kinds of tricks: We are dealing with a professionalization of criminal organizations. One particularly lucrative business model is the illegal offer of "Cybercrime as a Service": the criminals rely on division of labor and provide various tools. At the same time, state actors are on the rise - often difficult to distinguish from criminal organizations. Monetary motives are naturally at the forefront of the attackers' minds, but ideological and political motives also play a significant role. The motives range from aimless fundraising to a "big game hunt" for particularly valuable companies to retaliation for economic sanctions and social as well as political destabilization - hybrid threats are on the rise.

Crime scene Europe

Where are most companies up to their necks in terms of cyber crime? Estimates suggest that around one-third of all cyberattacks are against European companies. Already, two-thirds of companies have experienced an attack of some sort. It is predicted that the number of cyberattacks will continue to increase, with SMEs becoming targets for cyber criminals more often in 2021. Many companies still have the misconception that they are not interesting enough for the attackers. As a result, they are not adequately protected, which is an ideal gateway for cyber criminals.

Key Findings

19%

trust in the security of their suppliers and cloud service providers

35%

of large companies proactively go public in the event of a cyberattack

38%

have noticed an increase in cyberattacks during the pandemic

49%

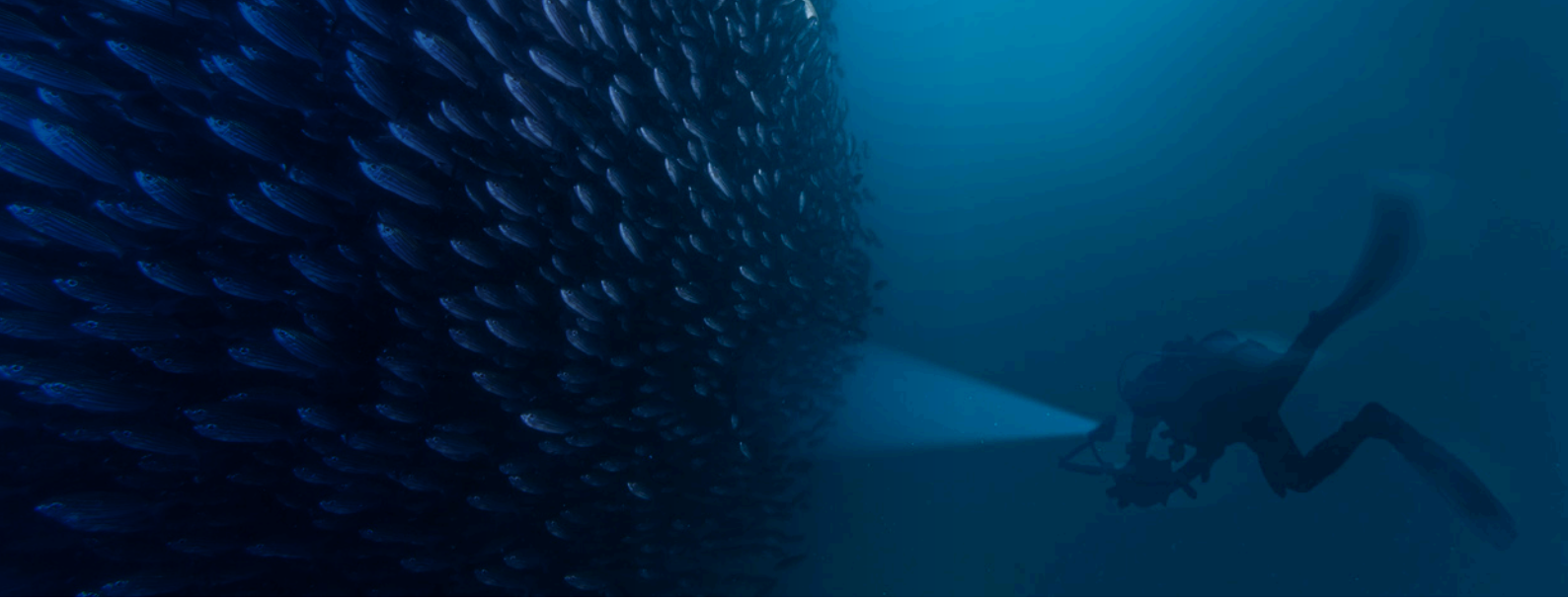
would invest in protection against Cryptolocker and Ransomware if money was not an issue

60%

of companies surveyed had been victim of a cyberattack in the last 12 months

78%

want to be supported more by the government



Various construction sites

Digitalization cannot be successful without cyber security: The Corona pandemic has proven to be a strong driver for digital transformation, while at the same time overhasty flexibilization and decentralization of workplaces create an optimal breeding ground for cyberattacks. Austria's companies must prevent the creek from turning into a raging river. They are in danger of missing the point at which digitalization moves too fast and they are no longer able to handle it. A worrying realization: we have entrusted control to the USA and Asia when it comes to digitalization. In addition, the shortage of security professionals is alarming. In Austria we will only be able to solve this problem in the long run, with the challenge to encourage people to take an interest in this subject. After all, security is no longer just an IT speciality but has become an interdisciplinary topic for education, science, and research. At the same time, cyber security budgets in Austrian companies are increasing, although not always in a problem-oriented manner: companies recognize a challenge, but often invest ineffectively. The consequences are security concepts that are not thought through to the end, carelessness driven by digitalization, features instead of security, and the omnipresent lack of experts able to handle these technologies.

A strong hand

The emerging dynamics of cyberspace are increasing digital dependency. The solution is cooperation because action at the individual company level will no longer be enough. Policies are needed that incentivize higher standards of care in the provision of technologies and services, but also encourage collaboration. Clear rules are required in cyberspace, because many incidents are caused by a manageable number of cyber crime groups: the currently known 26 ransomware groups have harmed and released data from more than 1,600 companies. The groups themselves face limited global consequences for their actions and credible deterrence is still missing. National and international cooperation is therefore more important than ever. Because against the storm tide of "cyber crime", protective dams can only be built together.

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