KPMG

Cyber security in Austria

Cybercrime is a global billion-Euro business, whose victims also include Austrians. When it comes to cyber attacks and security, facts and figures are important elements for maintaining an overview of the 'state of the nation'. To this end, KPMG conducted its third survey in Austria.

The numbers reveal trends and changes, the fact that Austria is already well positioned and also shows areas requiring improvement. These numbers provide a crucial basis for discussion and further activities.

Next level: the digital economy hub

These figures now require action. As a country, our highest priority should be to develop an effective strategy to fight cyber risks. This requires creating the basis for a successful digital hub. We have outstanding and equivalent qualities, such as legal certainty and stability. These qualities now require digital adaptation, in order to secure Austria's viability as an economic hub.

Meaningful and strategic measures need to be developed to achieve this, by both individual as well as governmental organisations. Why?

When it comes to cyber activities, all players are at risk and everyone should play their part. A common strategy requires collaboration as well as sharing ideas and information. Only united can we win the fight against cybercrime.

This awareness has already been partly established, as seen by the multiple existing joint undertakings.

Wrong perspectives: the biggest misconceptions

There are still many misconceptions about cyber security. And these lead companies to make strategically unwise decisions. One of the biggest misconceptions is to strive for 100 percent cyber security. Such a cybercrime goal is neither feasible nor appropriate. Instead, the goal should be to focus on particularly valuable information, given the sheer magnitude of the data flow in a corporate environment.

Another misconception is assuming that the key to cyber security is implementing the best security tools available. Technical tools are indispensable for basic security.

Unfortunately, it is often assumed that cyber security is simply a technical matter. IT tools are just a part of an integrated cyber security policy and do not form the basis thereof. Companies need to implement a strategic mix of measures that considers technology, people and processes equally.

Important to this is that cyber security be discussed and steered from the executive level. This is not an easy task given the complexity of technology and the speed with which it changes.

Some companies erroneously believe: "We employ the best experts to protect us from cybercrime." Naturally, it would be important to employ experts. The real challenge, however, is mainstreaming cyber security within companies.

Cyber security needs to be included in organisation-wide policies and guidelines as well as be completely integrated into the organisation's objectives.

Cyber security in Austria

Key findings 2018

Internet crime

Austria's enterprises targeted

60% of attacks are aimed at the weakness: people

61% of companies have been victims of a cyber attack

73% feel confident about cyber security matters

91% have improved their understanding of cyber risks

Between attack and defence

company action & reaction

52% predict an increase in their cyber security budget

45% do not report cybercrime incidents

Success strategy

cyber security is a matter for the CEO

45% analyse cyber security risks using key performance indicators

79% discuss cyber security topics at the topmost company level

Effective defence

artificial intelligence offers innovative options

26% have indicated that digital labs already play an important role

32% are informed about cyber security challenges by artificial intelligence

New security rules

the internet is not a lawless space

15% see data deletion as the biggest problem in GDPR implementation

74% are expecting an increase in customer inquiries regarding data protection

A new path

the future of cyber security in companies

67% of companies complain of a lack of cyber security experts

49% believe that cloud applications reduce infrastructure expenses

* In March and April 2018, KPMG surveyed 269 Austrian companies about how they meet the challenges of cybercrime and what cyber security measures they take. The survey was conducted with the cooperation of the Kuratorium Sicheres Österreich (Austrian Security Board, KSÖ). A copy can be requested via email to publikationen@kpmg.at.

PREVENTION AND SECURITY

It's the CEO's move: cyber security within companies

Cyber risks pose a big challenge for management. Delegating responsibilities to experts is no longer acceptable. It is essential that management leads the company and takes responsibility, in the following areas:

- Granting resources to maintain cyber security.
- Company-wide governance that allows for risk-based decision-making.
- A corporate culture in which everyone knows what their responsibilities are.

Companies can reduce their risks by increasing capacity in the following three critical areas:

- Prevention: strategic, tactical and technical measures; awareness-raising measures
- Detection: monitoring critical incidents and security issues
- Reaction: after a cyber attack, setting up a structured action plan (including a recovery scheme)

For all measures to strengthen both security with companies and within the Austrian hub: cyber security must be handled both at the corporate and political level, with the importance it is due.

Austria is on the right path when it comes to cyber security. However, there is no time to relax. More challenges are expected.

Because cyber security is, above all, distinguished by two characteristics: change and speed.

Writing the future together

With KPMG, you can find the right strategy to optimally implement your cyber security approach.

Our excellent know-how and many years of experience allow us to develop optimal solutions for cyber security that you can rely on.

You can make it a true strategic advantage.

Contact

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

© 2018 KPMG Security Services GmbH, Austrian member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative („KPMG International"), a Swiss entity. All rights reserved. Printed in Austria. KPMG and the KPMG logo are registered trademarks of KPMG International.

The information contained herein is of general nature and is not intended to adress the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.