Press release

swisscom

Cyber crime: where the threat comes from

The current Cyber Security Threat Radar from Swisscom shows how cyber criminals are adapting their attack methods as a result of the pandemic, by targeting home-workers and deploying the latest AI technology

The flood of cyber threats is unwaveringly high. Large companies and SMEs are still the focus of attention for hackers. The switch to home-working by many employees as a result of the pandemic has provided a welcome new target for cyber criminals as they adapt their attack methods to the new landscape.

The latest Cyber Security Threat Radar shows that the number of attacks is continuing at a constantly high level. While some – more traditional – attack methods are declining, the use of intelligent and often AI-controlled processes is on the rise. The challenge for companies and organisations – staying on top of the situation in the face of constantly evolving attack methods.

New requirements, new methods of attack

Workplace heterogeneity, for example, is now one of the biggest challenges in IT security
The immediate dispatch of employees to work from home was one of the greatest demands placed on IT and security departments in recent years. Working from home (WFH), together with mobile and agile working models including "bring your own device", offer great opportunities – but they also open up new areas of attack. Attackers are skilfully exploiting this development to their advantage.

Attacks based on AI (artificial intelligence) are also increasingly coming to the fore and regarded as a growing threat in the Cyber Security Threat Radar. They are used for targeted disinformation, as in the case of deepfakes, for instance. A recent example is the Tiktok channel "Deeptomcruise", which caused a furore with videos showing Tom Cruise doing magic tricks and playing golf. The real magic trick, however, was the video itself. For once the Hollywood star was not standing in front of the camera and knew nothing about it. It is an almost perfect fake, created using AI. This enables cyber criminals to use a range of different information to automatically fabricate an artificial profile,

which is extremely difficult to spot as a fake. The measures that companies can take against these and other challenges are explained in the report.

A compass in the cyber world

Using the Cyber Security Threat Radar, Swisscom specialists have identified the current threat status in Switzerland. The report explains the motivations of cyber criminals and reveals their methods. It takes account of and observes trends and challenges, evaluates them and – through the pooling of expert knowledge – provides an overview of the threat situation and how it is developing in Switzerland. It also shows which countermeasures are particularly effective for enabling attacks to be detected as quickly and efficiently as possible. The Cyber Security Threat Radar serves as a guide and compass for navigating safely through the cyber world.

Berne, 16 April 2021

More information:

www.swisscom.ch/security