STRONG TIES TO SUCCESSFULLY COMBAT CYBERCRIME

Intelligent and networked devices and applications are now an indispensable part of our professional and private lives. The drawback to this is that cybercrime has become an extremely lucrative business. In future, we can only successfully defend against this if local security competence centres such as SWITCH-CERT work closely together with a high degree of trust, both nationally and internationally.

There is one issue on which users, companies and cybercriminals agree: increasing digitalisation offers unforeseen opportunities. In addition to all the benefits of limitless access to information, we are also experiencing the unwanted consequences to an ever greater extent. Low-quality hardware and software leads to an increasing stream of vulnerabilities that are difficult or impossible to remedy. Sophisticated, targeted and regionally focused attacks culminate in vast amounts of stolen data and billions in losses for those affected.

Asymmetry favouring the attackers

Meanwhile, the estimated damage caused by cybercriminals in the Western world has outstripped that of crime in the physical world. The more added value is shifted to the internet, the more lucrative their criminal business model becomes. In addition, the attackers enjoy great advantages over their victims and law enforcement in the virtual world:

- In a highly complex world, there will always be inattentive people and technical vulnerabilities
- Attackers operate globally without having to be present locally
- Attack models can be multiplied billions of times with minimal effort, while each attack must be fought off individually
- Attackers do not care about jurisdictions, but work together in dynamic value creation chains worldwide. Law enforcement across jurisdictions, on the other hand, is very complex, slow and expensive
- If a perpetrator is caught, judges often don't pass sentence due to outmoded legal bases and a lack of specialist knowledge

Only collaboration leads to success

If you analyse the challenges in IT security, you inevitably come to the conclusion that the key to sustainable success lies in inter-institutional collaboration. No IT department in the world will ever be able to go it alone against the risks of cyberspace. In addition to the implementation of preventative measures, which has long been practised, reactive skills such as the detection of attacks, incident response and the associated acquisition of relevant threat intelligence are becoming increasingly important. There are two basic requirements for well-coordinated national and international collaboration: personal trust and close relationships. These can't be bought: they have to be built up and maintained over many years. A CERT is thus not only a committed team in itself; the various CERTs and professional organisations worldwide work together in the same way.

With over 20 years of systematic work and active participation in international organisations such as TF-CSIRT, FIRST, CENTR and GÉANT, SWITCH-CERT has built a unique international contact network for Switzerland with a high degree of trust, one which creates huge added value for all customer groups. Together with national competence centres such as MELANI and fedpol, we continually optimise this collaboration and accelerate information flows. We have thereby succeeded in utilising Switzerland's limited resources to their fullest extent, true to our conviction that close national and international collaboration with a high degree of trust is an essential prerequisite for successfully combating cybercrime.

Global relationships provide local benefits

SWITCH-CERT is part of a worldwide knowledge and alert exchange network. Relationships with international CERT communities have been systematically built and deepened over the course of 20 years. This global relationship network cannot be readily copied. The same is true for collaborations on a national level in the interests of national IT security.

For example:

- Longstanding collaboration with OFCOM and law enforcement authorities as part of our registry activities. This shows that even in a small country with limited resources, it is possible to operate a critical infrastructure on an internationally leading level
- Close coordination and collaboration with the Reporting and Analysis Centre for Information Assurance MELANI (GovCERT for Switzerland)
- Involvement in the implementation of the national strategy for Switzerland's protection against cyber risks, adopted by the Federal Council in 2012. SWITCH supports the federal government in the sphere of action 5, 'International relations and initiatives', for measure 11, 'Coordination of all those involved in initiatives and best practices in the area of safety and security processes'
- Involvement in the Swiss Security Network (SSN), a joint platform from the federal government and cantons for collaboration in the area of security
- Involvement in a working group for the federal expert group 'Future of data processing and data security'
- Involvement in the cybersecurity platform of the Swiss Academy of Engineering Sciences (SATW)
- Founding member of the Swiss Internet Security Alliance (SISA)

For many years, SWITCH-CERT has been using its security expertise and experience in the management and moderation of trusted communities for the benefit of the university community, internet users and the Swiss economy, with considerable success. Collaboration with SWITCH-CERT opens up a high-calibre network of relationships for its customers, providing invaluable services in the fight against cybercrime.

Words
Martin Leuthold, SWITCH