Security.

Cyber risks in Switzerland.

#zukunftsstark

Your strong IT partner.
Today and tomorrow.

BECHTLE

Contents

The threat is real.

Digitalisation is here to stay, in virtually all industries. With the growing importance of IT and cloud computing for business processes on the one hand, and the proliferation of connected systems on the other, companies are increasingly exposed to cyber threats: Hackers and other cyber criminals, secret services, and other state and private players use the internet to drive their very own agendas and cause considerable damage in their wake – from siphoning financial and personal data to industrial espionage to crippling entire operations. The methods attackers use are multiplying while becoming more refined and automated.

- The KPMG study Clarity on Cyber Security[1] from mid 2018 showed that 42% of the Swiss companies surveyed had suffered financial damage due to a cyberattack, 42% had experienced a breakdown of critical business processes and 25% had suffered significant damage to their reputation.

- Regarding the evolution of malware such as viruses, worms and trojans, Cisco's Threat Report February 2019[2] established that malware such as Emotet continues to dominate the threat landscape and still mostly spreads via e-mail.

- It's no wonder then that even the World Economic Forum has recognised the significance of cyber threats. Their Global Risks Report 2018[3] ranked cyberattacks as one of the top 5 risks for the first time. In the WEF's Global Risks Report 2020[4], they still made the top 10alongside data theft and data fraud and are in the same category as natural disasters and climate change. The World Economic Forum believes cyber threats will continue to pose a significant threat for the next decade.

The KMPG study also indicates, however, that Swiss companies are not yet sufficiently prepared to stymie attacks. Although 82% of companies surveyed have an action plan to defend against cyberattacks, they haven't considered attacks on their supply chain or business partners. The problem is very real and doesn't only affect the private, but also the public sector. At the beginning of 2020, the Swiss car importer, AMAG, fell victim to a cyberattack[5] which affected the supply of spare parts to downstream operations.

With the number and complexity of attacks on the rise, one thing is clear – a mere firewall is not enough to protect against cyber risks. IT security has become a strategic area that companies need to make one of their key pillars. A carefully planned security concept based on an incoming risk analysis, however, allows problems to be limited and overcome. In addition to modern security solutions and cloud-based security platforms, an up-to-date information security management system (ISMS) and awareness training for employees are also helpful.

[1] https://assets.kpmg/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf
[2] https://www.cisco.com/c/de_ch/products/security/security-reports.html
[3] https://www.weforum.org/reports/the-global-risks-report-2018
[4] https://www.weforum.org/reports/the-global-risks-report-2020
[5] https://www.luzernerzeitung.ch/news-service/wirtschaft/amag-von-hackern-angegriffen-ld.1190701

Current top threats for Switzerland.

In Switzerland, MELANI (Reporting and Analysis Centre for Information Assurance) continuously analyses the cyber threat landscape. The most recent bi-annual report – 2019/II[6] highlights the most significant concrete threats for July to December 2019:

- Cyber espionage
- Attacks on IoT devices and industrial control systems
- DDoS attacks
- Social engineering and phishing
- Data leaks
- Ransomware

In their first report on the threat situation according to the new Intelligence Service Act[7] the Federal Council advised at the beginning of May 2019 that espionage often employs modern cybercrime tools in addition to more traditional methods. They specify that the focus is on public bodies, international organisations in Geneva, diplomats and diplomatic representatives, companies from the technology, arms, finance, and trade industries as well as universities.

The report also attaches great significance to attacks on critical infrastructures. Several federal agencies and private companies have already fallen victim to foreign cyberattacks, having to bear high damages. The energy sector is currently increasingly the focus of espionage and awareness raising campaigns. In other countries, there have been targeted sabotage actions on the power supply (Ukraine 2016), and the ransomware WannaCry drastically affected the emergency systems of hospitals in the United Kingdom. The bottom line of the report: "The more common cyberattacks become, the larger the risk that Switzerland and its critical structures will at least suffer collateral damage."

[6] https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-2.html

[7] https://www.vbs.admin.ch/content/vbs-internet/de/ueber-das-vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.detail.nsb.html/74905.html

Cyber espionage.

Whether from governments or companies, espionage – the systematic interception or tapping of information for power political reasons or to gain business secrets – is playing an increasingly large role in cyber space. Attackers exploit technical vulnerabilities in IT systems and networks and try to gain the login details of authorised users by means of social engineering such as phishing and spear phishing and use these to enter information systems. And while technical security is indeed the basic premise for defence against espionage attacks, the human factor still plays at least as important a role.

RECOMMENDATION:

- Know what's valuable. Classify the information stored in your IT systems and protect especially valuable data with measures such as encryption.
- Make sure all employees involved receive thorough security training – especially in the area of social engineering such as phishing, and how to handle confidential data such as login credentials, personal information, etc.

EXAMPLE:

Attackers sent targeted phishing e-mails that launched the Olympic Destroyer malware when the attached documents were opened. Those affected were financial organisations in Russia and defence laboratories. One variant of these e-mails was in the form of a forged invitation to an international conference, purporting to be from the Federal Office for Civil Protection and the Spiez Laboratory. The Laboratory itself was not attacked, but its name was used to lend the invitations a degree of authenticity.

Attacks on IoT devices and industrial control systems.

Both MELANI and the intelligence service see the Internet of Things (IoT) as the new focus of cyber security, as many devices connected to the internet offer little to no protection against cyberattacks and can very easily be tracked, sabotaged, or manipulated to provide false data. And they can be hijacked, consolidated into a bot net and used to conduct DDoS attacks, for example, to incapacitate other systems. This also applies to industrial control systems that were not originally designed for networking and only subsequently integrated into the IoT.

The IoT poses many challenges for IT security, and some IoT devices have no option to incorporate security functions into them. Plus, vendors either do nothing at all to rectify vulnerabilities or do so very reluctantly. A multitude of IoT devices developed for private used are also being used in companies, despite not having the necessary level of security. And on top of that, existing IT security solutions are often not able to detect IoT devices. Many companies therefore have only a very general idea of which IoT devices are installed where.

RECOMMENDATION:

- Visibility is essential. Create an inventory of all linked systems – right down to individual IoT devices.
- Private devices employees use in the company network should also be considered.
- Use an IT security solution that can also protect IoT devices.
- Make use of the Minimum ICT standard[8] published by the Federal Office for National Economic Supply (FONES).
- The measures for the protection of industrial control systems (ICSs)[9] are also very useful.

EXAMPLE:

One day, the municipality of Ebikon discovered that attackers had made several thousand attempts to penetrate into the water supply's network used for autonomous operations. Fortunately, none of the attempts was successful, and Ebikon was able to fine-tune existing security measures to ensure better protection in the future.

[8] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
[9] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

DDoS attacks.

DDoS attacks (distributed denial of service) aim to limit the capacity of IT systems or even cause complete failure by flooding them with requests. Attack targets are often websites or online shops meaning that DDoS attacks can cause direct losses in revenues or have a negative impact on companies' reputations because their web presence is down.

Attacks of this type use bot nets, where IT systems or IoT devices of a large number of users and companies are hijacked and used to send huge amount of requests. The account owners aren't usually aware anything has happened. Attacks on the target systems generally take place on many layers. While the focus used to be on classic network and system resources (layers 3 and 4), attackers increasingly also target the application layer (7) and directly overwhelm applications running on systems.

RECOMMENDATION:

- Continuously monitor network traffic with an IDS (intrusion detection) system to detect anomalies that occur during a DDoS attack immediately.
- Employ a web application firewall to minimise the risk of your web-based services being attacked.
- Configure your firewall in a way that allows only the protocols that are really necessary to access each system.
- More recommendations on how to defend yourself against DDoS attacks can be found in MELANI's Measures to Counter DDoS attacks[10].

EXAMPLE:

The hacker group Apophis Squad claimed responsibility for many DDoS attacks including one on the Swiss secure e-mail provider Protonmail with the aim to demand ransom, resulting in many days of limited service. In the end, the members of the hacker group were arrested. After this, however, there were further attempted ransom attacks under the name of Apophis Squad, but these came from copy cats who used the Protonmail case to threaten recipients with sweeping DDoS attacks. When the ultimatum dates rolled around, however, nothing happened.

[10] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

Social engineering and phishing.

Social engineering targets the human factor. Attackers attempt to gain access to confidential personal and corporate data or infect the systems with malware by using methods ranging from fake calls to e-mails requesting passwords or account and credit card details supposedly for verification purposes – often via a forged online form. These are known as phishing e-mails. If you still rely on recognising phishing e-mails by their poor grammar, spelling, or amateur graphics, the attackers will easily fool you with their fakes that are getting more credible and realistic by the day.

A special, widespread variation is spear phishing, where attackers don't randomly throw a net at a wide range of addresses, but target specific organisations and people. Recipients are carefully researched beforehand, on social media, for example, and attackers pretend to be business partners, executives, or other persons of trust. The e-mail content can be tailored to the target based on their research.

RECOMMENDATION:

- Never disclose personal login data over the phone, in an e-mail, or via a web contact form.
- Never install software or follow a link when requested to on the phone or in an e-mail.
- Be wary in cases of unusual contact and seek advice.
- Clearly and precisely govern all processes related to payment transactions and ensure that your employees adhere to the rules.
- Make sure all employees involved receive thorough security training – especially in the area of social engineering, phishing e-mails and how to handle login credentials.

EXAMPLES:

A series of calls were reported to MELANI in which the caller posed as a bank employee and asked the victims to update their online banking. They were instructed to install remote access software such as TeamViewer and then enter their online banking details so that the company could run a test payment. The attackers then have remote access to the system, can intercept credentials and make their own payments.

Office 365 is also a target of cyber criminals. Phishing e-mails try to convince recipients to enter their Office 365 login details. Typically, Office 365 access is only secured with a user ID in the form of an e-mail address and a password. The attacker can then commit wire fraud. They look in the Office 365 accounts for electronic invoices and resend them with a different IBAN. These sort of attacks principally target companies that send large invoices to foreign companies. Attackers in possession of a CEO's login data were able to persuade the CFO to make an urgent payment of one million US dollars – he couldn't do it himself since he was in a meeting. This was actually the case as the hacker had access to the CEO's calendar and therefore his schedule.

E-banking trojans.

Crimeware is the term used to refer to malware that serves a specific criminal purpose such as sabotaging IT systems, manipulating data, espionage, or sending spam e-mails in bulk. Another target of crimeware is the finance sector, especially payment transactions in online or offline e-banking. In 2018, Retefe was one of the most prevalent e-banking trojans in Switzerland, targeting Windows and MacOS systems of private individuals and accessing its victims' systems via corrupt Word documents. Once the system is infected, attackers can hook up to the e-banking process and divert transfers.

Another virulent e-banking trojan called Gozi also sets its sights on offline payment systems and therefore companies that tend to use such systems as an alternative to direct online e-banking. Trojans are, however, no longer the only mechanism that criminals use to collect their victims' banking details. Official and unofficial app stores are more and more frequently featuring fakes apps purporting to be from banks that require credit card or login information to increase credit limits, for example.

RECOMMENDATION:

- Use dedicated devices for payments with limited internet access. These devices should not be used for other internet activities such as checking e-mails or browsing and their security kept up-to-date.
- Make it so that payments have to be approved by two people, and make the sure the approval is carried out on a second device.
- Be cautious with attachments, especially those in Word format, and only open them if there is no doubt as to the identity of the sender and they are trustworthy.

EXAMPLE:

PostFinance was affected by a fake app. The app, posing as an official PostFinance release, asked users to provide their credit card details. Once the user supplied these, a Thank You page appeared and the app terminated – at which point the only thing to do was call your credit card company and block the card.

Ransomware.

Ransomware – also known as CryptoLocker – is a category of crimeware that has had some direct hits on companies, from one-man companies to regional hospitals. According to media reports, ransomware attacks have been on the increase since the start of 2019. Ransomware encrypts the victims' data, making it unreadable. This can bring business to a standstill. Only once a certain sum has been paid in crypto currency such as Bitcoin will the data unencrypted – or so the attackers say, because when you're dealing with blackmail, there is no guarantee.

MELANI has always classed ransomware as one of the types of attack with the most devastating effects for SMEs and critical infrastructures. The most well-known ransomware is currently Ryuk, GandCrab, Dharma, and Locky. Ryuk, in particular, stands out. Ransomware first collects data and then uses it as a basis to target and encrypt wealthy victims' systems. Ryuk uses the trojan Emotet to spread itself via social engineering and infiltrates via faked e-mails with Word documents attached. Emotet was originally designed as a banking trojan, but today is used chiefly to send spam and download subsequent malware. In the case of Ryuk, Emotet first downloads the malware Trickbot that searches the entire network and spreads itself. The actual ransomware is only downloaded if a sufficiently large network is detected – otherwise the attacks wouldn't be profitable.

RECOMMENDATION:

- In order that encryption doesn't become an issue, perform regular backups of your data and store these on external media that you then disconnect from your system, or in a cloud that is not automatically synced. In this way you ensure that there is no way any ransomware can encrypt your backup.
- Employ security solutions that only permit approved applications to access your data.
- Segment your network, isolating vulnerable departments that often have to open e-mails from unknown senders so that ransomware can't spread to other areas.

IT security with Bechtle Schweiz AG.

Bechtle understands the challenges facing IT security – from technical and information security to data protection. Our experience with security problems and solutions led to us to create 360 degree Bechtle Security that covers all aspects of IT security, end-to-end. It consists of various security operation centre modules and ensures that threats are detected early and dealt with before they can have consequences for your company.

Bechtle Security offers the following components and benefits:

- Planning, implementation, analysis and operation – all from a single source.
- Comprehensive security concept
- On-site operational support
- Security monitoring, log analyses, cyber defence and threat intelligence
- Remote operation of (parts of) security infrastructures
- Security incident management or as an integrated service as part of IT incident management
- Collaborations and partner certifications with all big-name security vendors
- Highest consultation expertise thanks the Bechtle Internet Security & Services (BISS) Competence Centre in Neckarsulm with over 150 security engineers and consultants

IT security begins with consulting We provide comprehensive consulting on all IT security topics:

- Application security
- Cloud security
- Cyber Crime & Defence
- Data centre security
- Data protection and information security
- Security Awareness Training
- Infrastructure and perimeter security
- Workplace security

To make sure you get security that's perfectly tailored to your company, we develop everything from scratch and thoroughly support you in the implementation of your individual solution:

- Analysis of security requirements
- Design and creation of a proof of concept
- Implementation of security solutions into your infrastructure by our certified security experts
- Expertise and knowledge transfer thanks to our Bechtle Internet Security & Services (BISS) Competence Centre
- Cyber Crime & Defence

© 2020 · Bechtle Schweiz AG · 09/20

BECHTLE SCHWEIZ AG.

A leading IT service provider in Switzerland, Bechtle Schweiz AG is your go-to partner for all things IT—from consulting to infrastructure, from services to software, on the ground and in the cloud. Trusted by small to large enterprises and public institutions, our offering spans the entire plan-build-run lifecycle of corporate IT backed by top-level vendor certifications. Our 600 employees across nine sites give you the reliability and experience you need to turn your IT into a true asset for your business.

10 LOCATIONS.

- Baar
- Bsel
- Bern
- Carouge
- Mägenwil
- Morges
- Pratteln
- Regensdorf
- Rotkreuz
- St.Gallen

BECHTLE GROUP CH.

- Abissa, abissa.ch
- Acommit, acommit.ch
- Alpha Solutions, alphasolutions.ch
- ARP, arp.ch
- Bechtle Schweiz, bechtle.ch
- Bechtle direct, bechtle.ch
- Codalis, codalis.ch
- Solid Solutions, solidsolutions.ch

BECHTLE INTERNATIONAL.

- Founded in 1983 in Neckarsulm (DE)
- 75 IT systems integrators in Germany, Austria and Switzerland
- 24 e-commerce subsidiaries in 14 countries
- Over 11,000 employees
- Over 70,000 satisfied customers
- Bechtle is listed on the MDAX and TecDAX indexes
- In 2018, the group generated revenues of around 4.3 billion euros

Further information: bechtle.ch

Bechtle Schweiz AG
Phone +41 848 820 420
info.ch@bechtle.com | bechtle.ch

Baar | Basel | Bern | Carouge | Mägenwil | Morges | Pratteln | Regensdorf | Rotkreuz | St.Gallen

Your strong IT partner.
Today and tomorrow.

BECHTLE