swisscom

Cyber Security Threat Radar
2020/2021

Business resilience and agility are required

Contents

Imprint

Publisher	Swisscom Ltd, Group Security
Concept / Realisation	Agentur Nordjungs, Zurich
Editorial	Swisscom Ltd, Group Security
Copyright	© April 2021 by Swisscom (Switzerland) Ltd, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Print	OK DIGITALDRUCK AG, Zurich
Edition	125 copies

“Special situations call for special measures in terms of security, protection and risk awareness.”

Philippe Vuilleumier
Head of Group Security
Swisscom (Switzerland) Ltd

Introducing the Cyber Security Threat Radar

It is precisely in a special, disruptive situation – such as the one we are currently in – that retaining an overview is so important. Many people are wondering whether the coronavirus pandemic has given rise to more cyber activity. Have homeworking, social distancing and a degree of uncertainty made us more vulnerable to attack? Our answer would be **yes ... and no.**

Special situations call for special measures in terms of security, protection and risk awareness. And yes, outsourcing the entire IT infrastructure to the home-based offices of employees has presented some difficult challenges for many companies and organisations.

But is the current situation leading to more attacks? Is there an increased potential for attack vectors? That is something we are unable to confirm. Our experts in the various Security Operation Centers at Swisscom monitor Switzerland's entire network and have been unable to establish either intensified attack behaviour, or increased surges in phishing or ransomware.

Yet what about the reports that Swiss hospitals are increasingly coming under attack? And the cyberattacks on several Swiss companies, which have been reported in the media? These things did happen in 2020, but are they corona-related? Of course not. Organisational, procedural or technical vulnerabilities existed in those areas even before this particular situation arose. And yes, even Swisscom was not spared from network faults in 2020. The faults were able to be quickly remedied – but they left a nasty taste. For many companies and organisations, it's now a matter of eradicating vulnerabilities, transforming them into strengths and building up a security culture that makes technical, organisational and procedural changes, so that they can look resiliently into the future.

The current Cyber Security Threat Radar 2020/2021 determines the current threat situation, in order thus to obtain an overview of impending cyber risks and the potential hazards that result from these. It observes and monitors trends as well as challenges, evaluates them, and – through the pooling of expert knowledge – provides an overview of the threat situation and its development in Switzerland. It describes the attackers' motivation and means.

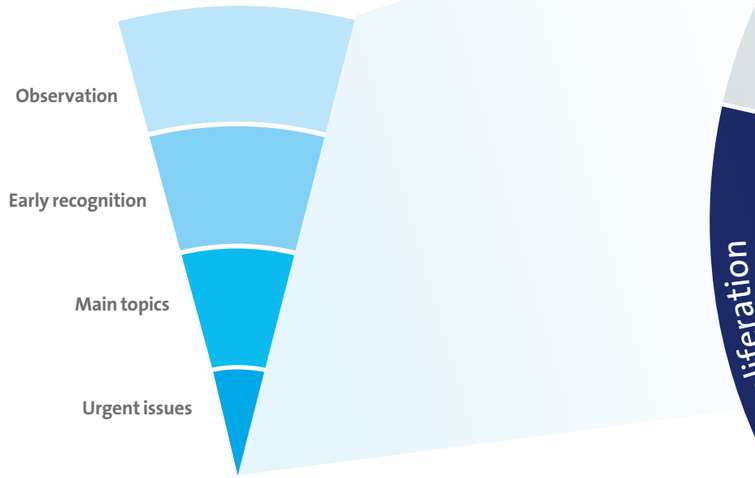
Based on the data collected and analysed by Swisscom, it indicates the methods and tools that attackers use most frequently. It also explains which countermeasures are particularly effective for enabling an attack to be recognised as quickly as possible.

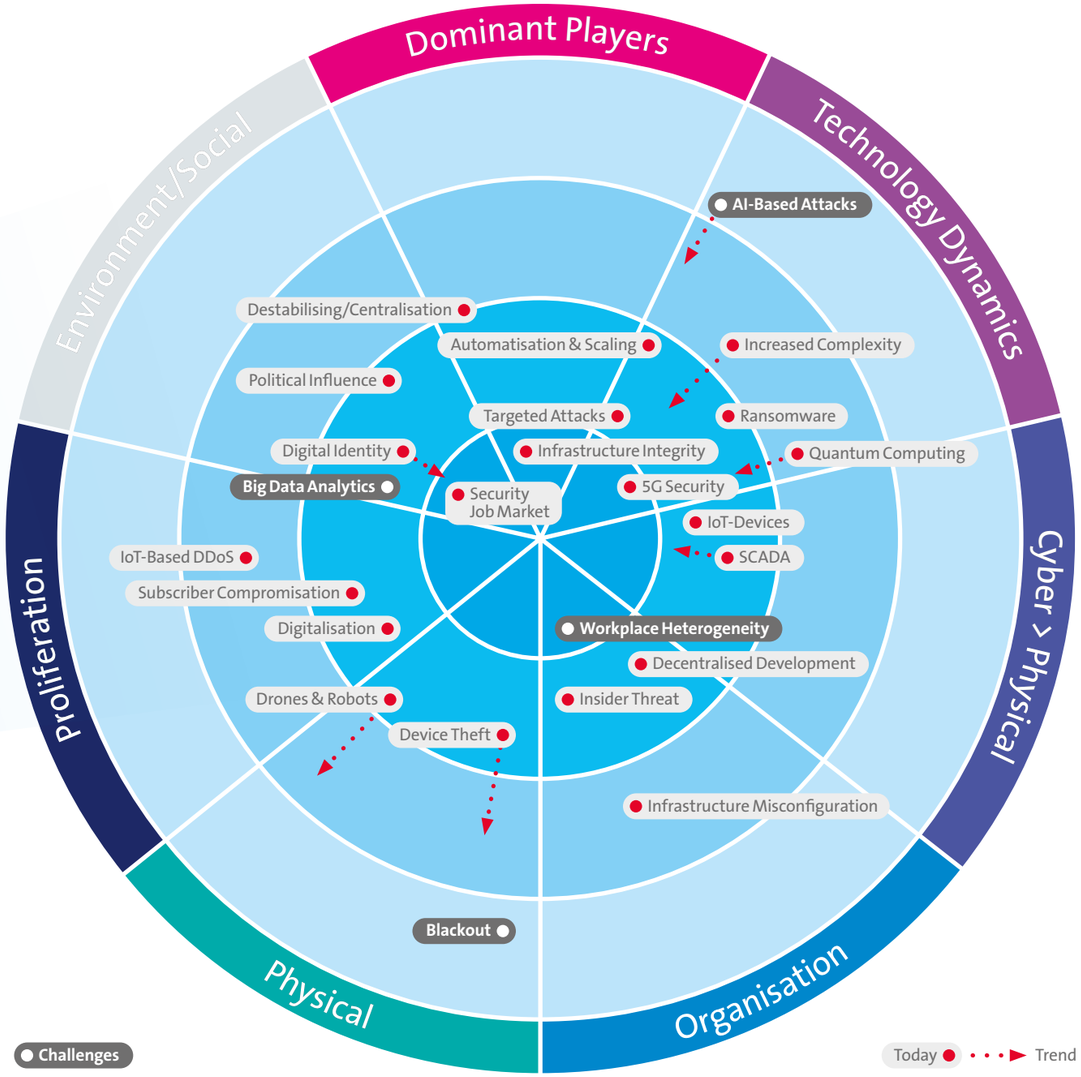
The Cyber Security Threat Radar 2020/2021 serves as a guide and compass for navigating safely through the cyberworld.

Current situation – introducing the threat radar

Being able to fall back on tried and tested security strategies and procedures at the right moment helps us to deal with unpredictable events – so-called "black swans". Combined with a consistent security culture, error transparency and properly trained staff, they create the basis for organisational resilience.

This requires potential threats to be recognised at an early stage and systematically recorded. To depict the threat status and its evolution, we use the well-known Cyber Security Threat Radar, which we have already referred to in previous editions of the Swisscom Security Report.





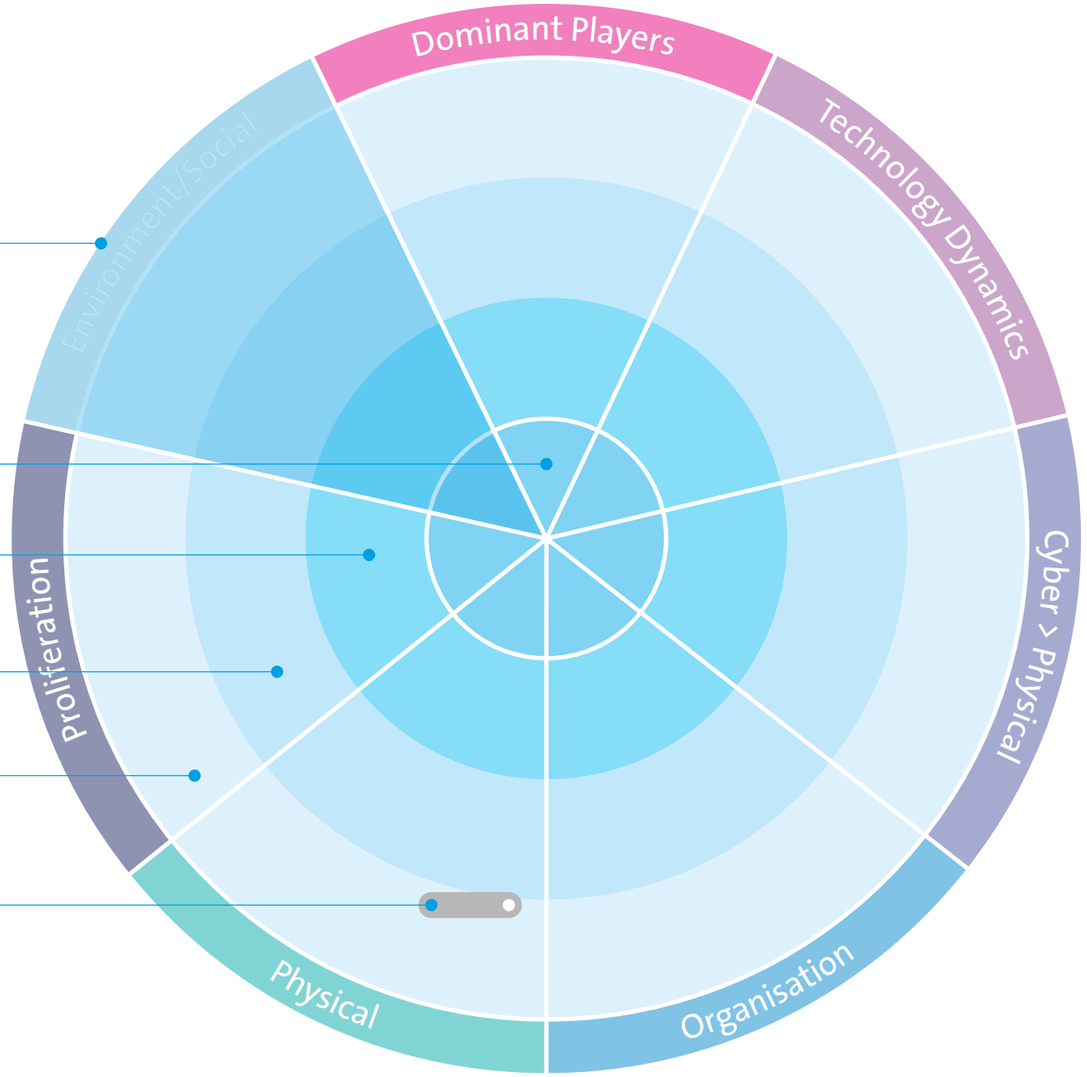
Methodology

The threat radar is broken down into seven **segments,** which demarcate the different threat domains. The threats belonging to each of these **segments** can be assigned to one of four concentric circles. The circles indicate a threat's urgency and thus also the vagueness inherent in assessing such threats. The closer the threat is to the centre of the circle, the more concrete it is and the more important it is to take appropriate countermeasures.

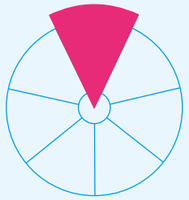
We refer to the circles as follows:

- **Urgent issues** in the case of threats that are already a reality and are being managed with a relatively large deployment of resources.
- **Main topics** in the case of threats that have already materialised on occasion and are managed with a normal deployment of resources. Defined processes often exist to efficiently counter threats of this nature.
- **Early recognition** for threats that have not yet materialised or are currently having only a very minor impact. Projects have been launched with the goal of addressing imminent growth in importance of these threats at an early stage.
- **Observation** for threats that are only expected to arise in a few years' time. No specific measures have been defined for handling these threats.

Moreover, the individual **threats** indicated by the points mentioned display a **trend,** which may be increasing, decreasing or stable in terms of its criticality. The length of the trend beam indicates how swiftly the criticality of the threat is expected to change.

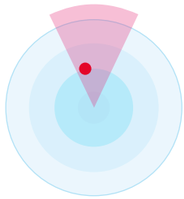


Details incl. trend and comparison with the previous year



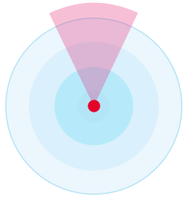
Dominant Players

This section summarises threats arising through dependencies on dominant manufacturers, services or protocols.



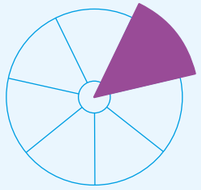
Destabilising/Centralisation
Strong centralisation in the structure of the Internet leads to cluster risks. The outage of one service, such as Amazon Web Services (AWS), can have a global impact. Outage of central services such as DynDNS, AWS, etc.

► Unchanged



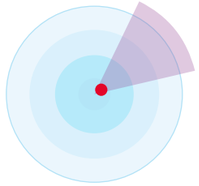
Infrastructure Integrity
Key components of critical infrastructures can have vulnerabilities incorporated, either through negligence or deliberately, which endanger the security of the system.

► Unchanged



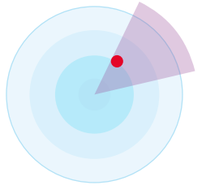
Technology Dynamics

This is the term used to describe threats arising from the swift pace of technological innovation, which not only offers attackers new opportunities to launch attacks but also enables them to develop new threats themselves.



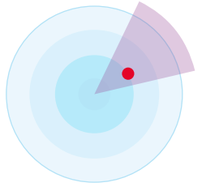
5G Security
5G is still a recent mobile telecommunications technology. Its launch not only offers up a large number of opportunities, but also opens the door to unknown threats.

▲ Increasing threat



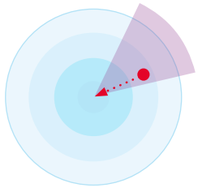
Automatisation & Scaling
The greater automation of technical operating processes will have a greater impact in the event of successful attacks or misconfigurations.

▲ Increasing threat



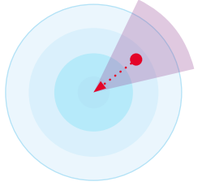
Ransomware
Large amounts of critical data are encrypted and only (possibly) decrypted in exchange for the payment of a ransom.

▼ Decreasing threat



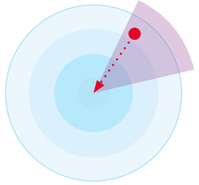
Quantum Computing
Quantum computers can make existing cryptographic processes unusable, since they are able to crack them in next to no time.

► Unchanged



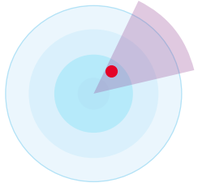
Increased Complexity
The complexity of systems is constantly increasing, particularly beyond technological and corporate boundaries. This increases exposure to risk and makes locating errors more difficult.

► Unchanged



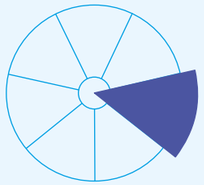
AI-Based Attacks
Artificial intelligence (AI) attacks are more targeted and therefore harder to detect. With AI, attacks can be carried out more efficiently on classic attack vectors such as ransomware, phishing, spear phishing and also occasionally on new scenarios like deepfakes and disinformation.

▲ Increasing threat



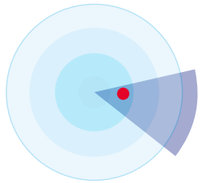
Targeted Attacks (APTs)
Targeted and complex attacks intended to achieve a specific objective. Key individuals are identified and attacked in a targeted manner directly or indirectly (lateral movement) in order to obtain relevant information or maximise the amount of damage inflicted. A key aspect is persistence, i.e. the attacker acting undetected for as long as possible.

► Unchanged



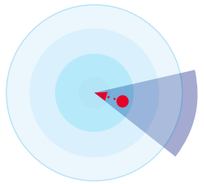
Cyber > Physical

This heading includes attacks via the cyberspace infrastructure, which will increasingly be causing damage in the physical world.



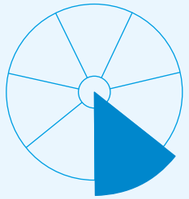
IoT-Devices
Poorly protected devices may be compromised and sabotaged. Such acts could limit the devices' integral functions, such as availability or data integrity.

- Unchanged



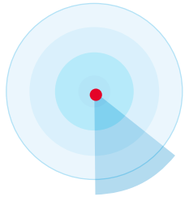
SCADA
Many control systems for critical infrastructure installations still exist, which are protected either poorly or not at all.

- Unchanged



Organisation

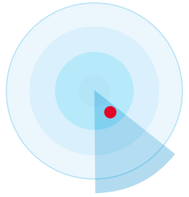
Organisation means threats that arise through changes in an organisation or exploit weaknesses in the organisation.



Workplace Heterogeneity

Alongside the many opportunities associated with new working models, the uncontrolled use of such models, such as “Bring your own Device” (BYOD) or increased use of remote workplaces, exposes companies to greater risks.

▲ Increasing threat



Decentralised Development

Traditional development departments are dying out and application development is moving more closely towards the business units, while at the same time release cycles are getting shorter.

► Unchanged

Insider Threat

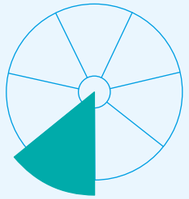
Partners or employees manipulate, misuse or sell information, whether through negligence or intentionally.

▲ Increasing threat

Infrastructure Misconfiguration

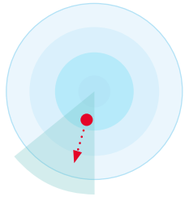
Exploitation of misconfigured infrastructure components and/or vulnerabilities, which are identified and rectified at a late stage.

▼ Decreasing threat



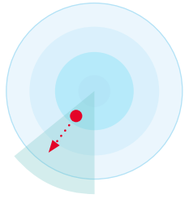
Physical

Threats that arise from the physical environment and are generally more focused on physical targets.



Device Theft
The theft of critical infrastructure components, in particular, or in future increasingly of IoT-Devices, can lead to a loss of data or impair service availability.

► Unchanged

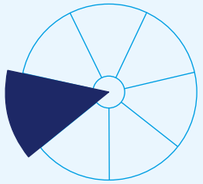


Drones & Robots
Reconnaissance or attacks over long distances are becoming easier and cheaper. Miniaturisation is making attackers more difficult to identify.

► Unchanged

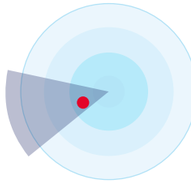
Blackout
Attacks on critical infrastructures such as electricity grid operators. Protection against outages is a key element and business continuity is also increasingly becoming part of the debate on cyber resilience.

▲ Increasing threat



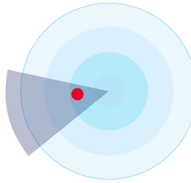
Proliferation

Threats that take advantage of the increasingly easier and cheaper accessibility to IT media and expertise, come under the heading of proliferation. Not only does proliferation open up new potential areas of attack, it also increases the availability of tools that can be used for attacks.



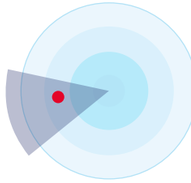
Digitalisation
Increasing levels of networking between the real and virtual world of people's private and work lives open up more avenues of attack.

► Unchanged



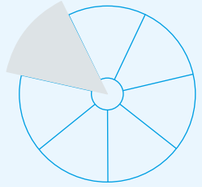
Subscriber Compromisation
Malware attacks mobile users' private data or is used to attack telecommunication and/or IT infrastructures.

► Unchanged



IoT-Based DDoS
Strong growth in the number of IoT-Devices coupled with low-level protection produces more "takeover candidates" for botnets.

► Unchanged

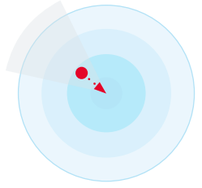


Environment/Social

This means threats arising as a result of socio-political changes, or which are facilitated or become more valuable to attackers as a result of such changes.

Security Job Market
Difficulties meeting demand for security professionals mean that less expertise is being deployed against attacks, which are becoming increasingly complex and intelligent.

► Unchanged



Digital Identity
Authenticated, personal digital identities may be misused or stolen, e.g. to conclude a contract under another person's name.

► Unchanged

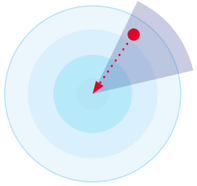
Big Data Analytics
More data and better analysis models can be misused in order to influence human behaviour. Decisions are increasingly left to autonomous systems. Data from "big data lakes" is subject to systematic misuse for the purposes of disinformation, fake news, social and psychosocial analyses and for establishing movement patterns. This is accompanied by invasion of privacy.

▲ Increasing threat

Political Influence
Political currents may influence technological or economic decisions, e.g. in the selection of technology suppliers. This may give rise to new risks.

► Unchanged

Challenges and trends



AI-Based Attacks

What's it all about?

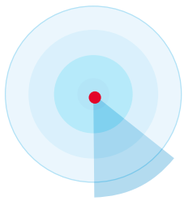
The last few years have been increasingly overshadowed by data protection and security breaches, with "deepfakes" or "disinformation in general" also featuring strongly.

How will things develop?

Artificial intelligence is growing stronger by the day, expanding its own capabilities and constantly learning. And the advantages and disadvantages of this technology have been increasingly coming under the spotlight – and remaining there.

How can we deal with the challenge/ trend effectively?

- Training and raising awareness among staff have utmost priority here
- Technical precautions via SOC for analysis and identification of such attacks



Workplace Heterogeneity

Alongside the many opportunities associated with new working models, the uncontrolled use of such models, such as "Bring your own Device" (BYOD) or – as currently driven by the pandemic – the increased use of remote workplaces, exposes companies to greater risk.

It's the strongest change in the radar since 2020, and has moved into the spotlight – almost disruptively driven, of course – by the global pandemic situation. The "new work" and working from home (WFH) will certainly be more firmly anchored within companies after the pandemic, and will become an accepted working model.

- Adaptation of existing policies and instructions; away from "teleworking" and towards mobile working
- Integrate security standards like Privileged Access Management
- Extend risk management to the mobile workplace and promote agile risk management
- Strengthen multifactor authentication and integrate it into the system landscape
- Establish a consistent security culture involving employees (human-centred approach)

Blackout

What's it all about?

Attacks on critical infrastructures such as electricity grid operators. Media reports indicate that the vulnerability of critical infrastructures to cyberattacks has massively increased. Protection against outages is becoming a key element and business continuity is also increasingly becoming part of the debate on cyber resilience.

How will things develop?

The attacks on critical infrastructures will definitely continue to increase and intensify. We are also sensing here a high level of risk caused by key persons in the operation of SCADA systems leaving due to retirement, and an increasing complexity of IoT-Devices on the operating platforms.

How can we deal with the challenge/ trend effectively?

- Business continuity management is to be given greater consideration in the planning of cybersecurity strategies
- Collaborative and interdisciplinary action in companies and organisations
- DevSecOps – set up and actively support frameworks in agile settings
- Strengthen responsibility in the "first line of defence"

Big Data Analytics

More data and better analysis models can be misused in order to influence how people behave with regard to data and IT systems. Decisions are increasingly left to autonomous systems. Data from "big data lakes" is subject to systematic misuse for the purposes of disinformation and fake news, and for social and psychosocial analyses. This is accompanied by invasion of privacy, which may have social consequences.

Data is the new gold – at least that is the term used so frequently to describe it in science and the trade press. On the other hand, there is the benefit for evaluating complex social systems and the availability of data for analysis purposes, for example in the health sector. This offers a lot of scope for new developments, but also the risk of the "transparent citizen" and/or large-scale loss of sensitive (corporate) data. The correlation of available and searchable data, e.g. via OSINT, also opens the floodgates for cybercriminals and social engineers.

- Ethical guiding principles are particularly important here – including in the use of data that has been entrusted to us
- It is necessary to place technical and organisational restrictions on access to the data
- Develop sensitivity: Which cloud services do we use, and how do we use them? Which data are stored, and where?

Conclusion

2020 was a disruptive and challenging year for organisations and companies, for employees and for Swiss security departments. Alongside all the obstacles and restrictions, it was a year that also allowed the opportunity for new developments and perspectives.

It's no wonder, therefore, that the issue of workplace heterogeneity has become a focal point of this year's Cyber Security Threat Radar – certainly one of the greatest changes in a threat vector in recent years. The immediate sending of all employees to work from home was one of the greatest challenges that IT and security departments have had to manage in recent years. And it worked – sometimes well, sometimes less so. But things turned out well overall. And this clearly shows how agile companies and organisations must be in today's world in order to keep pace with the competition, the market and social demands.

Digital transformation has been given a forceful boost in many companies and organisations. Yet there have been no major innovations; nothing really new has been developed, though existing work tools have become more firmly incorporated into the "new way of working". The security efforts involved in Zoom (from Zoombombing to end-to-end-encrypted communication) and the further development of Microsoft Office 365 as a collaborative tool are tangible and visible. The digital transformation continues to develop at a rapid pace – often also at the expense of security or of privacy and data protection, as demonstrated strikingly by the hyped audio chat app Clubhouse.

« The digital transformation continues to develop at a rapid pace – often also at the expense of security or of privacy and data protection, as demonstrated strikingly by the hyped audio chat app Clubhouse. »

Big Data also continues to play a major role in social media, new collaborative services and in the marketing machinery. Artificial intelligence (AI) is taking on a new importance in connection with AI-based attacks such as disinformation (deepfakes, fake news). The methods of attack used by cybercriminals will grow increasingly sophisticated and may reach new dimensions, for which we need to be prepared.

Maintaining a consistent security culture will have a crucial role in this. The theme of the RSA Conference 2020 was "The Human Element" – almost a premonition of the special situation in which we now find ourselves. Placing the human factor at the centre, specifically addressing its needs, requirements and problems, protecting it and supporting it in the security processes to be accomplished: this was all definitely brought into focus in 2020 – and will stay with us in 2021 and beyond. Dynamically adapting the organisation, the culture and the processes will become increasingly important in view of the new attack vectors.

This much is clear: the hazards in the digital world have not got any smaller. Yet our experts at the Swisscom Security Operation Center were not able to detect any significant increases in them. They were simply different here and there, tailored to situational issues and often focused on humans as the entry vector. The employee as the "first line of defence" is and remains the most important element in the security chain, and should be regarded accordingly.

For a safer networked world

Swisscom places the needs of employees, customers and partners at the heart of all our security considerations.

We develop **secure solutions**, **products and services** for our customers and partners. To protect them, we use the **latest technology** and our **comprehensive infrastructure**, and we consistently practise a **culture of security**.

#talkingaboutsecurity

swisscom.ch/security