EXPLORE NEW HORIZONS: Modern security approaches in the age of digitalisation.

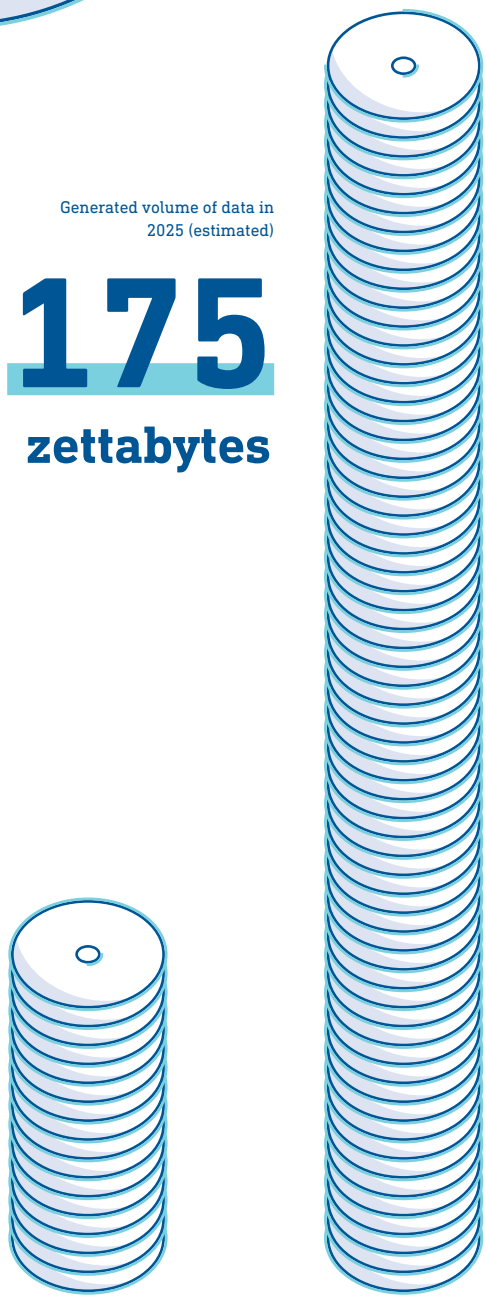
WHY YOU SHOULD ACT NOW
TO PROTECT YOUR COMPANY.

Data flood and new security approach.

Generated volume of data in 2025 (estimated)

175

zettabytes



2019 2025

As a result of digitalisation, machines are increasingly networked and data volumes have rocketed: By 2025, the market research company, IDC, believes that over 175 zettabytes of data will be generated. That's nearly three-quarters more data than in 2019. If we saved this data on standard DVDs, we'd have enough to stretch between the Earth and the moon 23 times.

These developments are proving challenging for companies as it's not only becoming increasingly difficult to manage this data, but it also needs to be comprehensively protected. Cloud use is on the rise and this is being accompanied by hybrid infrastructures. This is on top of confusing legal provisions of the GDPR and increasingly restrictive industry-specific regulations on data protection and IT security, particularly for Swiss companies with European or European-located users. Changes made to the Swiss Data Protection Regulation, which is based on the GDPR, will be keeping us busy in the near future. In these times of change, it's clear that digital transformation is only possible when enterprise IT security is rethought. A digital strategy must also include a security strategy. IT security is no longer optional, it's an absolute must for Swiss SMEs. A strategic approach that not only concerns IT and data protection, but also risk management and overall management has to be taken. In our digital world, the success of digital business models and processes is closely entwined with IT security. The research and advisory company Gartner says the following: "[...] traditional security concepts have no place in an era characterised by digital innovation."

?

But how are things looking on the ground? What challenges are you facing and how can you create a security strategy that meets your needs? This whitepaper explains why a holistic security approach is so essential today.

The status quo in IT security.

What's the situation at your company today?

The security market is extremely fragmented with some 1,000 enterprise IT security solution providers – and this figure is increasing. The challenges are obvious: the various offers lead to increased complexity and the question of who is the right provider for which problem is never far away. In addition, the IT infrastructure has grown organically over years while security was considered with a silo mentality resulting in standalone solutions that don't mesh. Managing these structures is rapidly becoming confusing and complex and security breaches are a given. The situation in Switzerland is similar to that in Germany, which in its "IT Security in Germany 2018" study, IDG describes as follows:

Classic security silos, endpoint, messaging, network and web security can no longer provide sufficient protection. It's not uncommon for them to be spread between 50 to 80 security solutions, ranging from on premise software solutions, appliance, Security-as-a-Service and Managed Security Services.

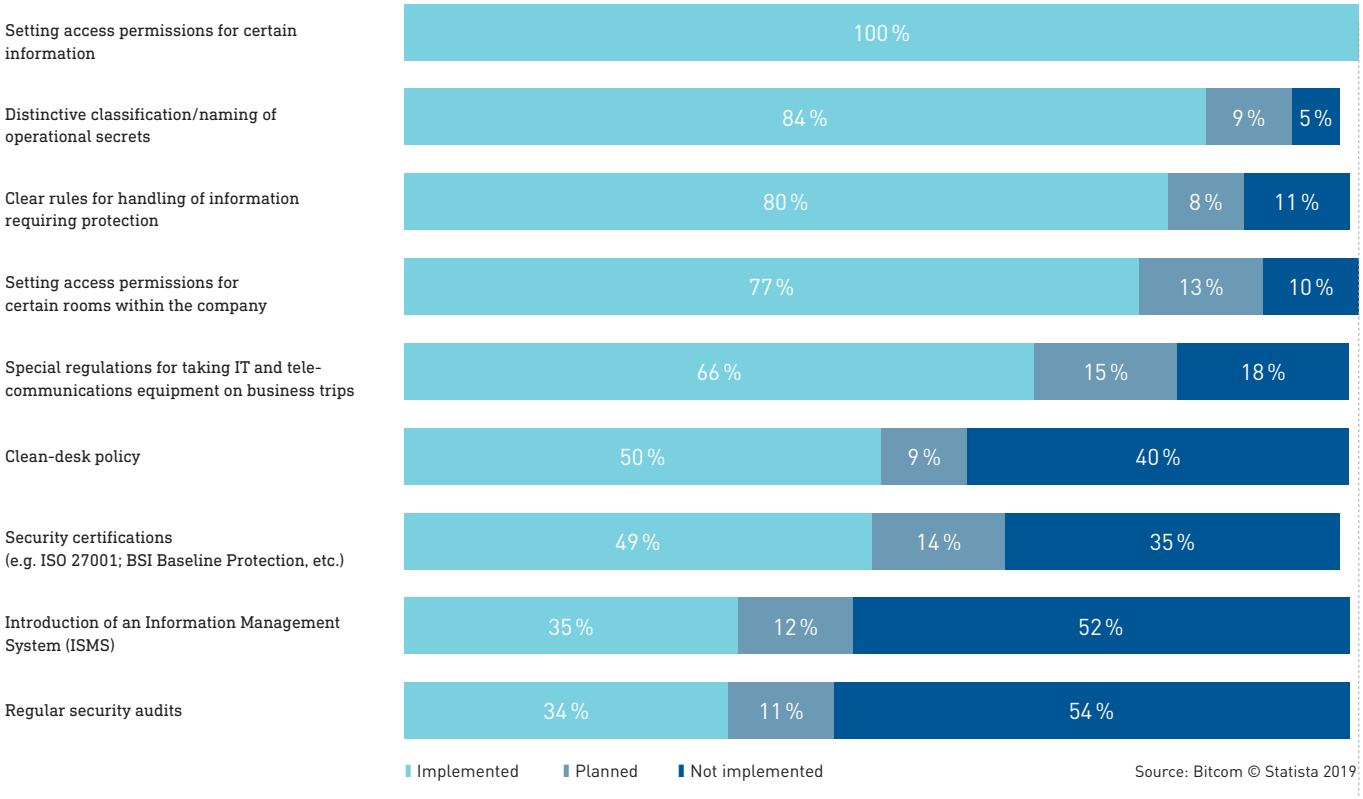
Most German companies have firewalls, malware protection and content filters to combat well-known threat scenarios. The latest IDC study shows that, in the past few years, they have also invested in solutions to detect and deal with non-signature based malware, ransomware, targeted attacks, zero-day exploits and BEC (Business E-Mail Compromise) attacks.

Monitoring, managing and maintaining such a complex security landscape is becoming more difficult and is now one of the biggest IT challenges.[1]

1 https://www.idc.com/de/research/multi-client-project/detail?id=5f687ba8ec8598b86913 – Abgerufen am 29. Juli 2019

The wide range of measures used is underlined by a Bitkom study on organisational and process-technical security precautions already in place in companies. It's clear that there is room for improvement in the areas of security certification and regular audits.

Which of the following organisational or process-technical security precautions do you take in your company or are you planning on implementing in the future?



5,2 billion

Estimated lost revenues due to cyberattacks between 2019 and 2023.

In this challenging environment, companies are often faced with the questions of whether they are suitably protected and if undetected gaps in security could be exploited. A lack of an overview and transparency caused by silos and confusing structures are additional pain points for businesses. On top of this, a lot of companies are unclear about what they really need to do, both in terms of a strategic alignment of IT security and operative measures. In addition to these technical challenges, there is another factor to consider—the increasing lack of a skilled workforce. Key positions in the fields of IT and IT security are often difficult to fill and this is having serious effects: The loss in revenue caused by cyberattacks between 2019 and 2023 is estimated to be $5.2 bn[2].

Companies around the world are upgrading their IT security: Bitkom estimates the value of the German IT security market as €4.4 m in 2019—an increase of 7.3% yoy[3]. This growth is first and foremost down to the increasing demand for integrated offers that are individually tailored to customers' needs. Companies have come to realise it is time to act. But what should you do now?

2 https://www.computerwoche.de/a/cyber-kriminalitaet-kostet-unternehmen-5-2-billionen-dollar,3546489 – Abgerufen am 29. Juli 2019
3 https://www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-erstmals-ueber-4-Milliarden-Euro.html. – Abgerufen am 25. Juli 2019

Traditional IT security has had its day:

From perceived security to a holistic strategy.

Traditional, tactical security solutions are based on the principal of shielding. This means that everything that happens within the company is regarded as safe, whilst everything outside is potentially dangerous. These days however, security needs to be reconsidered. IT security has to be effective wherever there are data and users. Classic company shielding whereby the enterprise is like a castle, protected by thick walls and surrounded by a moat, falls short. Implementing different partial solutions causes latencies. Studies also show that a quarter of all cyberattacks in 2018 took place from within the infrastructure[4]. Usage habits have also changed. Employees want to be able to work as quickly and flexibly outside of the company as they can inside, as in the modern world of work, we have to be constantly connected via the internet no matter where we are in the world. Alongside toughening up clients, file encryption and standardised operating system interfaces, the following points need to be taken into consideration in order to enhance security standards:

1. Identity and Access Management.

It is increasingly important to control who has access to which data. Identity is the new perimeter. Login data remains the main point of attack for hackers, which is why companies need to reconsider only using passwords as these very quickly present a security vulnerability. The modern alternative: multi-factor authentication including a centralised access-control level – the modern, digitalised company needs modern identity and access management.

4 https://www.securitymagazine.com/articles/88907-verizon-2018-data-breach-investigations-report-ransomware-still-a-top-cybersecurity-threat – Abgerufen am 29. Juli 2019

2. Vendor consolidation and end-to-end security.

Using many vendors according to the best of breed approach makes no sense, especially for SMEs as it becomes impossible to keep track. Businesses can't operate multiple vendors as they simply don't have the staff to do so and attacks are difficult to detect and analyse. Companies should instead put their faith in end-to-end security approaches to develop a holistic security strategy. Companies have to align people, processes and technologies, but that's only possible if overarching monitoring of the infrastructure has been established along with corresponding internal and external processes for taking action in the event of incidents as part of the reporting obligations.

3. Single-sign on (SSO), passwordless.

Using a single authentication process, users can access all resources, applications and services assigned to them. Instead of having to log in to each service individually, users only need to log in once to be able to access everything. The technology used can differ depending on each use case: For media solutions, users have an electronic token while with a portal solution, first authentication takes place, for example, on a website by entering a user name and password or with two-factor authentication when the browser stores an http cookie which uniquely identifies the user. This cookie enables users to access other applications. A ticketing system works in a similar way in that a circle of trust is created between several devices. Each user receives a unique identifier which is exchanged between those in the circle of trust. This means that the user is authenticated for all other devices within the circle. Most companies use a local solution. Software is installed on the user's end device which fills in input boxes with information, completing the login process for the respective services. The advantage of this solution is that it can be run on a variety of systems. The downside is that fake input forms can intercept user data.

SSO is only really secure, convenient and user-friendly when used in combination with passwordless authentication technology. Using a fingerprint scanner, face detection software, magic link via e-mail or confirmation code via SMS, the user's identity is typically confirmed based on three factors. Security questions and additional information can also be added. Once the identity has been confirmed, the user can access all applications and services. The benefits are obvious: the user has the simplest-possible, yet very secure access, and so can work productively. As the authentication only needs to be transmitted once, security is increased plus the user doesn't have to remember several passwords that would probably be far too weak anyway.

4. Container isolation.

Standardisation is a necessary requirement to boost the security level of modern cloud-based workstations. To achieve this standardisation and stable, reliable procedures, isolation containers (for applications, operating systems or processes, for example) are necessary.

5. Holistic cyber defence concept.

Companies are quickly faced with some challenges: How can I guarantee detection and monitoring in terms of cybersecurity? How can I structure a concept that involves an increasing number of people and departments? A holistic cyber defence concept takes into account these points: fundamentally, a company's infrastructure is protected by suitable preventative measures. Constant monitoring must always be ensured and that requires a security operations centre, managed with either external or internal resources. However, companies should also be equipped to deal with attacks and be able to react quickly when they occur. This starts with defence, affects how an incident is investigated and can also affect internal and external communication in the event of infection. An emergency plan for such a situation is critical these days. The following image shows the individual components of a technological and organisational cyber defence concept. See figure below.

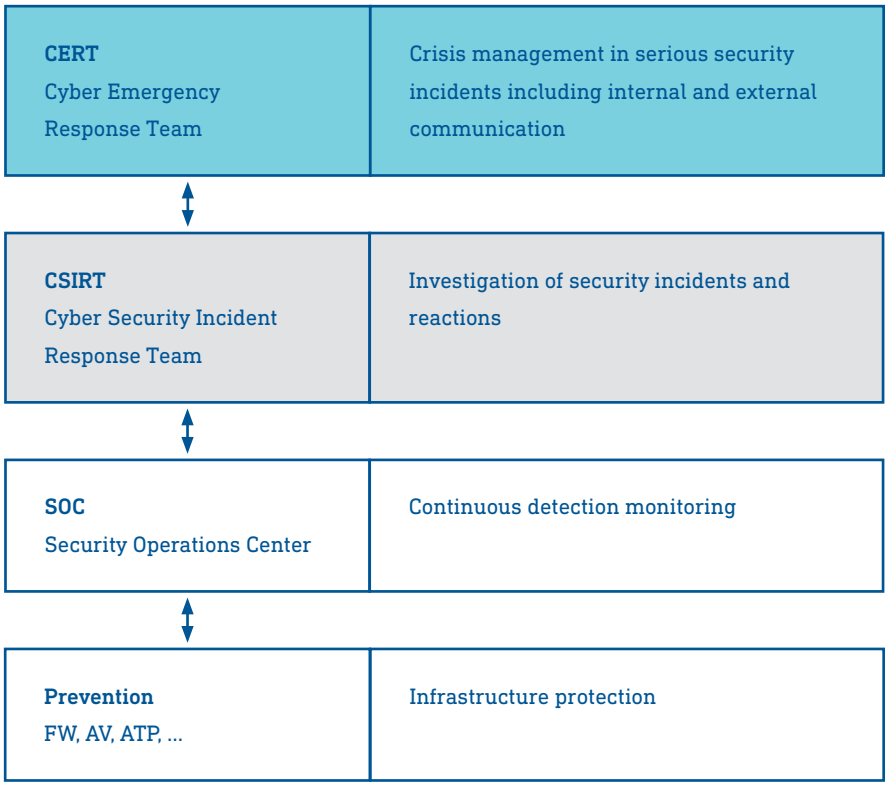
6. Security awareness and organisational security.

The human factor needs to be taken into account when considering security. Companies should try to minimise the risks employees pose to their IT security. Secure awareness training for employees is therefore an essential pillar of a holistic security concept. Furthermore, companies must constantly review their security level and check both their organisational security and technical security analyses. Within the framework of organisational vulnerability analyses, existing information security and data protection measures are checked helping companies plug any gaps.

Components of a cybersecurity concept
Technological and organisational

Components regardless whether the solution is based on:

- SIEM architecture
- Next generation cyber-defence architecture
- User device behaviour from the edge of the infrastructure



What steps do businesses need to take?

First of all, it is imperative to check the current status and ask what protection is required. This means considering the big picture instead of purchasing isolated solutions for single departments. In the future, security can longer only be considered from a technical point of view, but should also include legal requirements, employee awareness, infrastructure planning, the existing (cloud) architecture plus those responsible for operative performance. This change in perspective also supports standalone solutions and moves away from a silo mentality.

There are two ways to create a modern, holistic security approach, but it is important to first think about which one better suits the initial situation and to exactly consider and describe the target scenario:

1

Reduce infrastructure security solutions to a few or even one single vendor. The focus is on user behaviour and the targeted increase in infrastructure security level. With the user behaviour approach, data that the network collects about events, actions, files and users is analysed. Using modern technologies (machine learning and AI), anomalies can be detected in real-time and reacted to appropriately. This enables IT departments to establish suitable processes to be able to react as quickly as possible in the event of an attack.

2

The existing infrastructure must remain with multiple security solutions continuing to be used. This approach is more difficult because implementation and operation are very complex, but, for many companies, it is a necessity. An overarching security strategy is therefore essential. As a rule, a SIEM architecture is used to correctly detect and efficiently manage attacks and incidents. For this purpose, Log Sources are analysed and a rulebook written based on the results that prescribes reactions to a recognised attack pattern. If unusual activities are detected in the network that are covered by the rulebook, an alarm is triggered and the activity is generally blocked. It is very time-consuming to create and maintain this rulebook. Unknown incidents are generally not detected or reported.

Both solutions take a holistic view of security. A serious strategic security approach is only possible when both attack prevention and detection are possible and a process (reaction) in the event of an incident has been defined. Companies with a developed, holistic security approach will be much less susceptible to cyberattacks in the future. However, introducing such a strategy takes a lot of time and effort. Few companies are able to pull this off on their own without neglecting their day-to-day operations. Our recommendation is clear: take the opportunity to request external consultation and consider handing over responsibility for detection and reaction.

Integrated security

Play it safe:
IT Security. By Bechtle.

36 years' experience

>300 certifications

>200 experts

8 competence centres

>40 vendor partners

Bechtle Security can be summed up as follows:

36 years of experience, 8 competence centres, over 200 IT security experts. Collaboration with over 40 vendor partners and more than 300 certifications. Our holistic approach, along with our experience and our extensive network are what really count: we want to ensure that our customers can work securely and efficiently. For this reason, we have developed issue-specific expertise for all IT security-relevant practices and offer diverse tests, workshops, analyses and comprehensive managed services—from initial consultation and design of a holistic security solution to incident management, we are exactly the right partner for our customers.

IN A CHANGING WORLD WHERE DIGITALISATION CONTINUES TO MAKE STRIDES, WE ARE AT THE CUTTING EDGE. WE TAKE SECURITY PERSONALLY AND TAKE A STEP-BY-STEP APPROACH TO CREATE A SECURITY SOLUTION TAILORED TO OUR CUSTOMERS' NEEDS:

- If required, our business architects will work together with you to examine the current situation at your business. We consider the challenges you face so that we can create independent solutions and see if there is any potential for improvement.

- In co-operation with our solution architects and security experts, we work with you to create a suitable solutions concept, ensuring that you are comprehensively protected.

- We put together the best applications from our extensive range of vendor partners and are by your side from implementation to detection and reaction.

- On request, we can also manage individual services.

We take care of your IT security so that you can take care of business.
We'll help you work securely.

IT security. By Bechtle.

!

If you'd like to find out more about IT security or would like a no-obligation consultation, e-mail us at:
info.ch@bechtle.com

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