bechtle

Successfully closing gaps in IT security.

Don’t give cyber attacks a chance with effective threat detection, immediate protection and preventive measures.

bechtle.com

The fear of cyber attacks *such as industrial espionage, data theft or sabotage* **is growing.**

Recent studies conclude that 7 out of 10 companies feel severely threatened by analogue and digital attacks. This figure is worrying and, unfortunately, justified: in 2024 alone, 81% of companies were already affected by an attack.

A decisive factor in the ever-increasing threat situation is the rapid digital transformation of the economy. The resulting global networking and automation of processes opens up numerous opportunities on the one hand, but also offers cyber criminals greater scope for attack on the other.

Companies should act and take appropriate measures, because the consequences for the economy are fatal: 65% of companies feel that their existence is threatened by cyber attacks.

Not only large corporations are affected, but increasingly also medium-sized companies. They often do not have sufficient resources and expertise to protect themselves against the increasingly complex threat.

Are medium-sized companies more vulnerable to cyber threats? What are the risks of cyber attacks? What does the NIS2 directive mean and who does it affect? Find answers to these and other pressing questions about IT security in this e-book.

Challenges
of IT security.

The digital world with its new technologies offers companies many advantages. At the same time, however, it also opens up new opportunities for cyber criminals, who are launching ever more sophisticated attacks.

Gateway for cyber attacks.

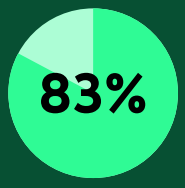
Increasing **remote and hybrid working** as well as company-specific IT guidelines (bring-your-own-device, BYOD) for the use of employees' own laptops, smartphones and other personal devices by employees and authorised third parties such as suppliers drastically increase complexity. As a result, security teams have to protect more and more devices, applications, data and connections.

Networking in the cloud simplifies the world of communication and work by providing employees and the ecosystem of customers, suppliers and partners with easy access to systems and services. At the same time, the risk of unauthorised access to data increases as all information is accessible via the internet.

The **Internet of Things (IoT)** is the driving force behind industrial applications and a central component of future value creation. However, the devices connected to the IoT are often inadequately secured or not secured at all by default and can therefore be compromised remotely by attackers.

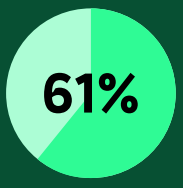
Artificial intelligence (AI) as a new technology offers companies and cyber criminals alike significant productivity gains. The latter can increase the scope, speed and impact of their attacks, particularly through the use of generative AI in social engineering and malware development.

AI - threat or opportunity for IT security?



Artificial intelligence exacerbates the **threat to the economy.**

Artificial intelligence **makes cyber attacks easier.**



The use of artificial intelligence can significantly **improve IT security.**

(Quelle: Bitkom Research 2024)

The middle class as easy prey. Is that true?

Cyber criminals are increasingly targeting critical infrastructures, governments and companies. Small and medium-sized enterprises in particular are easy prey. Many companies underestimate the risk of a cyber attack and implement the necessary protective measures only hesitantly or selectively. However, there is often a lack of dedicated resources to raise an organisation's IT security to the necessary level.

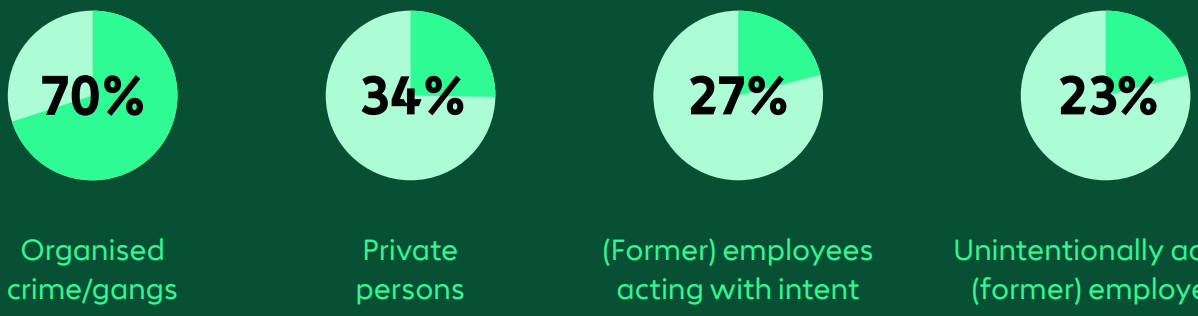
A situation that makes SMEs the weakest link in the supply chain and therefore a gateway for cyber attacks on larger, better-protected companies. Companies of all sizes should therefore not only take IT security measures within their own organisation, but across the entire digital ecosystem in which they operate. In this way, cascading effects can be avoided.

People as a **safety factor.**

People are often overlooked as a risk factor by companies. Lack of caution, lack of knowledge or deliberate behaviour - people are one of the key weak points when it comes to IT security. It is therefore important to recognise people as a security factor and to train employees. This is the only way they can quickly recognise and prevent a cyber attack using social engineering, for example. Companies should clearly communicate which relevant threats are prevalent and how IT security is ensured within the company. This is the only way that employees can become part of the security solution and defence.

Did you know that your IT security is not only threatened by organised crime and gangs?

Cyber threats originate from the following groups of perpetrators:



(Quelle: Bitkom Research 2024)

The complex why of a cyberattack.

Financial interest, political or ideological reasons, revenge, competitive advantage or simply for fun or opportunity. The motives for a cyber attack are many and varied. Regardless of the reasons, they can have serious consequences for the company, and the complexity of cyber attacks ranges from simply developed virus software to advanced espionage or sabotage software.
The goal remains the same: an attack on hardware, software or networks to cause damage, steal data or otherwise influence IT systems.

The five most serious consequences of a cyberattack:

1 **Data loss.**
Theft of secret, confidential or sensitive information such as intellectual property.

2 **Financial losses.**
Costs caused by blackmail, theft of bank data, business interruptions, fines or counterfeiting or plagiarism.

3 **Reputational risks.**
Loss of trust from customers and partners can cause long-term damage to image and business relationships.

4 **Legal consequences.**
Violations of data protection laws or regulatory requirements can be sanctioned and subject to high fines.

5 **Business disruptions.**
Disruptions to business processes, be it a brief interruption or a complete shutdown, always cause productivity losses.

Companies are well advised not to leave the security of their digital infrastructure and data to chance. Even if antivirus programmes and a firewall are essential protection components, they are not enough against the increasingly sophisticated cyber threats. Companies should think big and focus on a holistic security strategy, with the decision-making power lying at management level. It is important to choose the right solutions from the multitude of potential applications and measures in order to harmonise processes, people and technologies, secure business operations and at the same time stay within budget.

IT security:
An investment that pays off.

There is a lot at stake for companies, but there is also a lot to gain. After all, protection against material and immaterial losses is the best risk provision for the future. Even if the return on investment (ROI) is not immediately demonstrable.

What is cyber security?

The aim of cyber security or IT security is to protect a company's systems, networks, digital infrastructure, devices, applications, data and people from digital attacks, unauthorised access and potential damage. Various technologies, policies and procedures are used to either prevent cyber attacks or mitigate their effects.

A cyber security concept includes the following aspects:

- AI security
- Critical infrastructure security
- Network security
- Endpoint security
- Application security
- Cloud security
- Data security
- Mobile Security

If companies have recognised the importance of cybersecurity, this demonstrates, on the one hand, a responsible approach to advancing digitalisation and the associated dynamic threat situation and, on the other, an obligation to comply with regulatory guidelines.

Managing directors and board members are personally liable for violations of data protection laws and regulatory requirements. This once again makes it clear that the task of IT security must be a mandate for management. The fact that companies are aware of the dangers is shown by the increasing global expenditure on information security.

According to a forecast by Gartner, this is expected to rise by 15% to USD 212 billion in 2025.

Total expenditure for the current year 2024 is estimated at USD 184 billion. This corresponds to an average increase of 13.4% compared to the previous year.

In 2023, a total of USD 162 billion was invested in IT security worldwide, which corresponds to an average increase of 12.7% compared to 2022.

	2023	2024	2025
Segment	**Expenditure**	**Expenditure**	**Expenditure**
Security software	76.574	87.481	100.692
Security services	65.556	74.478	86.073
Network security	19.985	21.912	24.787
Total expenditure	**162.115**	**183.872**	**211.552**

Global spending on information security by segment from 2023-2025 in USD millions
(Source: Gartner, August 2024)

The most common cyber threats *in Europe according to the ENISA Threat Landscape (ETL) Report 2023:*

Ransomware.
In a ransomware attack, the data on an IT system is encrypted, restricting access to these resources. The data is only released or decrypted against payment of a ransom. Ransomware is a form of malware.

Malware.
Malware is derived from the words 'malicious' and 'software' and is an umbrella term for many types of cyber threats, such as viruses and Trojans. It refers to malicious software that executes unwanted and usually dangerous functions on an IT system. These include damaging systems, stealing data or disrupting or preventing access to IT infrastructures.

Social Engineering.
Social engineering is one of the most common 'door-opening methods' for obtaining sensitive information. Attackers use fraud or social manipulation to try to influence people into disclosing confidential information. Types of social engineering attacks include phishing, pretexting and deepfake.

Threat to data security.
Data security is jeopardised by attacks aimed at stealing, manipulating or destroying data. Data security can be threatened by people within a company ('insider threat') as well as, for example, by malware, botnets, phishing or advanced persistent threats (APTs).

Threat to availability - Denial of Service (DoS) & Distribute Denial of Service (DDoS). In a DoS attack, so many requests are sent to a server until it can no longer cope with this volume and refuses to provide the service or fails completely. In a DDoS attack, instead of a single system, many different systems are used to strike in a coordinated manner over a large area.

Desinformation.
The targeted dissemination of false or misleading information is intended to manipulate people. In contrast to misinformation, which has no intention to deceive, disinformation deliberately deceives people, for example through deep fakes, fake images or replicated websites.

Attacks on supply chains.
Cyber attacks aimed at supply chains either cause direct damage or use the gap as a springboard to other targets. As no company today operates independently, it is not a supply chain, but a digitally networked ecosystem with a large number of companies.

Increase defence capability.

The importance of increasing cyber resilience is confirmed by the results of the Microsoft Digital Defence Report 2024, for which the Group analysed more than 78 trillion cyber signals every day.

The results show a significant increase in the global threat of cyber attacks. For example, the number of ransomware attacks has increased 2.75-fold year-on-year. At the same time, however, the number of attacks that led to encryption has decreased threefold. The report lists social engineering, identity theft and vulnerabilities in software or unpatched operating systems as remaining critical.

At a time when cyber attacks are the order of the day, companies need to develop effective security concepts, *implement comprehensive solutions and sensitise their employees.*

Cybersecurity - three elements lead to success.

Security concept.

In addition to a comprehensive analysis of the current situation, an optimal strategy for holistic IT security includes three key pillars: prevention, detection and response.

- **Prevention.** The deep integration of modern security technologies into existing infrastructures can effectively prevent cyber attacks.
- **Detection.** The early identification of unusual events and the detection of threats supports the proactive recognition and defence against cyber attacks.
- **Reaction.** Coordinated crisis management, including action and recovery plans, enables a fast and effective response to cyber attacks.

As a security concept should fulfil both the company's security objectives and the legal requirements and guidelines, meaningful documentation and effective processes are essential for implementation.

Sensitisation and training of employees.

People are increasingly becoming the target of cyber criminals. Ongoing training can counteract this by informing employees about potential dangers and teaching them how to recognise and respond to threats such as phishing attempts at an early stage. It is also important to make the company's expectations regarding IT security clear and to create a security culture that permeates all levels of the organisation.

Digital hygiene.

Digital hygiene includes best practices that should be jointly implemented by an organisation's security experts, administrators and employees to protect against digital threats such as viruses, malware or identity theft. These should be based on an IT or governance policy on digital hygiene that facilitates the introduction and implementation of principles and procedures in the organisation and ecosystem. Measures for optimal IT hygiene include the following:

- Password protection for secure authentication and secure access authorisations, e.g. through multi-factor authentication
- Security of emails and devices, e.g. through the exclusive use of devices for business purposes
- Automatic backups & encryption of sensitive data
- Regular software updates & formal patch management
- Continuous monitoring and control of IT systems
- Installation of cyber security solutions
- VPN usage & network security, e.g. to protect data over insecure Wi-Fi networks, endpoint protection, network monitoring and data backup solutions

The hurdles *in the SME sector.*

Particularly in SMEs, the project of holistic cyber security often fails due to financial and operational hurdles. There is a lack of trained IT security officers whose job it is to uncover weaknesses, identify potential for optimisation and develop appropriate IT security concepts as a result, SMEs are also unable to use certifications such as the TISAX certification for secure work in the automotive industry to strengthen their international competitiveness. Without a security team, compliance with legal guidelines such as NIS2 will also be a challenge. Numerous initiatives have already been launched by the government to provide support, training and resources to help small businesses in particular to cope with the complexity of cyber security.

Waiting is not the solution. Medium-sized companies that do not have a security team should hire a service provider for security reasons or at least research them so that they can be contacted quickly in the event of a cyber attack.

Do you have insurance that covers cyber risks?

Insurers are increasingly offering products that protect companies against various types of cyber attacks. Whether it's identity theft, guarantees against business interruption, legal advice when reporting a personal data breach or technical support for the recovery of IT systems after a cyber attack, the insurance must cover the most significant risks and secure the future of the company.

Checklist: What to do in the event of a cyber attack?

- Evaluate the incident to rule out a technical defect and confirm a cyber attack.
- In the event of a proven incident, isolate all affected devices and systems, disconnect them from the Internet and prevent all unauthorised access.
- Do not switch off or modify the devices affected by the attack, as this will hinder the work of the IT forensic experts or investigators.
- Stop all backups to protect them from further impact.
- In the event of a proven incident, notify the police or relevant authorities and, if possible, press charges.
- Inform your employees and your ecosystem of partners, suppliers and customers.
- Create a logbook with all the information about this incident to document all events and actions.

Interview with *Marc Bothorel.*

CEO of Porter Consulting Europe and cyber security speaker for the CPME.

Can you identify any differences in how large enterprises and small to medium-sized enterprises (SMEs) manage IT security?
Yes, there are many differences. First and foremost, large companies have an IT department. Very often with cybersecurity specialists, a CSIO, and the means to implement appropriate security. Most SMEs simply have no dedicated IT staff, and the responsibility lies with the managing director.

Secondly, large companies are much more aware of cybersecurity issues than SMEs, because many of them have already been the victims of cyber attacks, which has led them to take appropriate measures to protect themselves. SMBs have not yet fully grasped the extent of cybercrime that exists today. Probably because the press often reports cyber attacks on large corporations, SMEs don't see themselves as targets. This is completely untrue. Today, we are witnessing cybercrime affecting all sectors of industry and all sizes of company, what we call trawling.

This lack of awareness among SMEs ultimately means that their investments in cyber security are completely inadequate in the face of the current cyber threat. I'd like to quote a phrase coined by the Director General of ANSSI six months ago, who said that today you don't need to be a target to be a victim.

ANSSI is the French equivalent of BSI in Germany, is that correct?
Exactly, and the ANSSI (Agence Nationale de la Sécurité des Systèmes Informatiques) also drives the third aspect of why large companies deal with IT security differently. Because many of them are operators of critical infrastructures and essential services and are regularly monitored by the ANSSI. As equivalent of the BSI (Bundesamt für Sicherheit in der Informationstechnik), the ANSSI presented its work on transposing NIS2 into French law.

Is the lack of awareness regarding cyber-security a national problem or do you see it as a European task to tackle this?
There are many studies on this among SMEs, including a recent one in France. The results are alarming, here are some important findings: IT management is the responsibility of the company manager for 82 % of them. In 53% of these companies, employees use personal equipment for work purposes, 95% of which is their cell phone, 34% their computer and 28% their personal e-mail.

When questioned about cybersecurity, 6 in 10 organisations say they are poorly protected, especially those with more than 10 employees. Another finding, which underlines my previous answer, is that two-thirds of companies surveyed believe they are only slightly exposed to the risk of cyber attacks or are unaware of this risk.

If I compare this with other European studies, I can say that it is not a national problem. With NIS2, the EU is taking exactly the right step.

Is NIS2 really necessary or will this guideline be another hurdle for the global economy?
As cybersecurity referent for France's leading employers' association CPME, I was involved in the transposition of the NIS2 directive as early as 2021, when it was still only in draft form. We, the employers' association, believe that NIS2 is absolutely necessary to lay the foundations for

economic security in our digital world in the face of exponential cybercrime.

Organisations should therefore see NIS2 not as a hindrance, but as an advantage. In fact, it is a real economic advantage for a company to show its ecosystem and especially its customers that it has taken measures to protect its data, its know-how, and its business, as well as that of its customers.

This directive is therefore an important step in protecting the European economy. In this context, each European country must ensure that the transposition of NIS2 into the local law of each country is harmonised at European level. So that companies operating in different European countries only have to comply with one set of standards.

Is NIS2 just the beginning?
NIS2 is not the beginning, but it is part of a set of other European regulations such as the General Data Protection Regulation (GDPR), DORA (Digital Operational Resilience Act) the CRA (Cyber Resilient Act), the IA Act etc., all aiming to strengthen and protect our European digital economy.

And all these European directives are closely linked. For example, the Cyber Resilient Act aims to require solution providers to ensure a level of cyber security for their products and solutions for up to five years after the end of life of those products. This is crucial to ensure that the IT infrastructures of companies subject to NIS2 have a solid, protected foundation for their IT.

It is therefore the implementation of all these European regulations, and not just NIS2, that will enable us to achieve the right level of protection for businesses and therefore for the economies of EU member states.

Are the costs of adequate IT security ultimately lower than the impact of cyber attacks?
A 2022 study by Wavestone, a leading global cyber security consultancy, shows that the effects of a cyber attack last an average of 3 to 7 weeks. And that's just an average.

And from the Gendarmerie Nationale it's estimated that following a successful attack, an SME suffers around 50,000 Euro in operating losses on average. But more importantly, the loss of reputation and customer confidence as a result of the attack costs an average of 150,000 euro. Not to mention the risk of the company filing for bankruptcy.

In this respect, the estimates of the Fédération Française des Assurances are very revealing: Cyber risk has been the number one risk for companies for the past five years and will be for at least the next five years, far ahead of other potential losses. And the risk of a cyber attack is over 80 %, with an impact of over 80 % on the company's business.

It therefore seems obvious to me that the anticipation and prevention of cyber threats and the measures to protect a business, are far less important than both the probability of being attacked and the disastrous consequences, both psychological and financial, of a successful cyber attack.

What is your personal advice for SMEs to address IT security?
Don't underestimate the risk of cyber attacks. It's the number one risk to your business, far ahead of all other risks, and insurers say so.

You don't have to be a target to be a victim. Cybercriminals already have enough stolen data to launch massive attack campaigns, regardless of a company's size or industry. The question is not whether they will become a cyber victim, but when they will, if they are not already.

The cost of a cyber attack in terms of lost business, reputational damage, medium and long-term customer loss, and psychological impact far outweighs the cost of protecting your IT infrastructure. This is an absolute necessity to protect your business, but also an undeniable selling point to reassure your customers.

IT in general, and cybersecurity in particular, is not your core business, nor perhaps that of your current IT service provider. Call in a specialist who can implement and maintain the solutions you need to protect your business.

There is no such thing as zero risk, especially when it comes to cyber security. That's why you need cyber insurance that covers the residual risk and, in the event of a successful attack, covers business interruption, IT recovery and any costly administrative procedures.

Marc Bothorel began his career as a systems & network engineer at Schneider Electric in 1985. Joining HP in 1988, he pursued a career in consulting, marketing and sales development in France, then for the EMEA region. In 2007, he left HP to set up his own IT services company, Starware Micro Services, which was awarded the ExpertCyber AFNOR label in September 2021. In 2022, he sold Starware Micro Services and bought Porter Consulting Europe, an IT and cybersecurity consulting and training company. In the same year, he co-founded Qorum Secur 'Num. Marc is also the national cybersecurity referent for the CPME and a member of the Board of Directors of cybermalveillance.gouv.fr.

Things to know *about NIS2.*

NIS2 is a Europe-wide cyber security directive that came into force on 16 January 2023. It follows on from the NIS Directive or NIS1 Directive introduced in 2016. The abbreviation NIS stands for "Network and Information Security".

The EU member states must transpose the NIS2 Directive into national law by 17 October 2024. Based on current knowledge (25 September 2024), implementation in Germany is likely to be delayed until March 2025.

Like NIS1, NIS2 is intended to protect important institutions in the EU Member States from cyber attacks and create a standardised level of security throughout Europe.

It is estimated that around 25,000 companies in Germany will be affected by the requirements of the NIS2 directive. These are divided into two categories:

The *main* facilities include companies from the following sectors:

- Energy
- Transport
- Banking
- Financial markets
- Healthcare
- Drinking water
- Waste water
- Digital infrastructure
- IT & Telecommunications
- Public administration
- Space

Among the *important* facilities include companies from the following sectors:

- Waste management
- Postal and courier services
- Food production, processing and distribution
- Production: Manufacture and trade in chemical substances
- Production: manufacture and processing of medical devices, machines, vehicles and electrical and digital devices
- Providers of digital services (search engines, online marketplaces)
- Research

Companies must check independently whether they are subject to the NIS2 Directive. They are not automatically informed of this.

In principle, NIS2 applies to a large number of new sectors and companies with 50 or more mployees. It also applies to companies with a high level of importance for the public and economic processes.

Companies affected by the NIS2 Directive must register with the Federal Office for Information Security (BSI) as an affected organisation no later than three months after publication of the national implementation.

If your own assessment of the situation is unclear, it is advisable to seek legal advice from a specialised IT lawyer or an IT consultancy. IT specialist lawyer in order to be legally burdened

The aim is to obtain a clear statement of the consequences of being affected by NIS2 as a basis for decision-making.

If the result of the required self-assessment of affectedness is positive, the second step is to examine what action an organisation needs to take as a result.

The NIS2 directive requires the establishment of comprehensive management measures for risk handling, information security and emergency and cyber security processes. These must be implemented holistically within the affected organisations.

The need for action is based on which organisational and technical measures have already been implemented.

NIS2 (Art. 21) and the new version of the BSI Act (BSIG, §30 and 31) stipulate the following requirements on the subject of risk management:

Risk management and information security.
What is required is the holistic and systematic handling of risks (identification to management) for the operation and the security of the company's assets. This can be ensured by establishing management systems for risk management, information security (ISMS) and governance processes (GRC).

Business Continuity Management.
The implementation of emergency measures including backup management, disaster recovery and crisis management is required to ensure business continuity in all situations.

Security in procurement and development.
Security measures must be in place for the acquisition, development and maintenance of IT systems, components and processes. In accordance with the NIS2 directive, it is necessary to establish clear security requirements for this and implement them consistently. They must fulfil the The company's risk management system must comply with current technological standards and include regular risk assessments and the management of vulnerabilities.

Identity management.
Among other things, concepts and solutions for the use of multi-factor authentication and secure communication connections are required. The foundations for this are created by establishing identity management systems in the company.

Incident Management.
Concepts for dealing with security incidents are required. Time-critical reporting obligations within 24 hours apply to serious incidents.

Cryptography.
Concepts and procedures for the use of state-of-the-art cryptography and encryption and their application in all communication connections are required.

Personal security.
This includes concepts for access control and the centralized management of access protection to facilities and IT systems in order to prevent the misuse of access through identity theft.

Training and awareness.
The implementation of cyber security training is required. Security-oriented ways of thinking and behaviour must be taught, which employees should internalise in order to help protect against cyber attacks.

Supply chain.
This includes the security of the supply chain with the contractual requirements with suppliers and service providers. Organisations must impose higher security requirements on their suppliers and service providers that are part of the supply chain.

Effectiveness tests and verification.
Procedures are required to continuously assess and improve the effectiveness of all measures in the area of cyber security and the operation of management systems. Special focus must be placed on the verifiability of all necessary measures through appropriate documentation.

Another new feature of NIS2 is closer monitoring by the supervisory authorities and stricter sanction mechanisms. These include significantly higher fines as well as a clear reference to the personal liability of the management.

What does Bechtle SMART Business Security 365 offer your company?

- **Reliable protection** for computers and mobile devices against cyber threats.
- **Secure access management** and authentication procedures such as multi-factor authentication.
- **Continuous education** of employees about cyber threats to increase security awareness and resilience in the organisation.
- **Constant monitoring** of invasion risks for early detection and combating of threats.
- Support with **compliance with guidelines** such as NIS2 and reduction of the risk of penalties and fines.

Create the basis for stable, secure, and scalable growth with Microsoft and Bechtle. Boost productivity and innovation in your company with Bechtle SMART Business Security 365.

About **Bechtle.**

Bechtle is one of the leading security integrators in Germany, with more than 550 experts and over 1,400 individually active certifications in the field of IT security.

Bechtle operates around 20 security competence centres with more than 30 central and decentralised security units in Germany, Austria and Switzerland. With our managed services, customers are covered 24 hours a day, 7 days a week, 365 days a year.

Contact us to find out more about our security awareness services and many other IT services and solutions:

microsoft-security@bechtle.com

Sources:
Economic Protection 2024, Bitkom Research 2024.
Press release, Gartner, August 2024.
Microsoft Digital Defense Report 2024, October 2024.
European Union Agency for Cybersecurity (ENISA), 2023.