valantic

PROTECTION OF TRADE SECRETS

Sensitive Data in Focus: Prevention and Protection in the Digital Era

Table of Contents

Dear reader,

In the digital age, companies are faced with the constant challenge of effectively protecting their sensitive information and trade secrets against the growing number of cyberattacks. A recent survey by the digital association Bitkom shows that two thirds of German companies see their existence jeopardized by such threats. Ransomware attacks and the theft of confidential information in particular represent current and serious risks.

This white paper provides you with a comprehensive overview of the latest technologies and strategies for defending against cyber threats. From authentication methods and procedures to data loss prevention and network monitoring, we look at the measures that can help you protect your business assets.

We aim to provide you with practical and effective approaches to secure your trade secrets in an insecure and rapidly changing digital landscape. Use this white paper to learn about the latest developments and adapt your security strategy accordingly.

We wish you an informative read.

Yours sincerely, the authors,
Dr. Werner Gutau and Thomas Lang

Dr. Werner Gutau

consulting@gutau.de

For more than 25 years, Dr. Werner Gutau has reconciled security requirements with operational concerns as CISO and divisional CSO. His focus has been on the high-tech industry, where high security requirements, IP protection and complex, global supply chains are part of day-to-day business. With risk-based approaches and pragmatism, he satisfies customers as well as regulators and certifiers. He has also successfully contributed his experience to committee work and shaped security standards in the process. Since retiring from "regular" professional life, he has passed on his experience as a consultant.

Thomas Lang

thomas.lang@mc.valantic com

After more than 20 years as a consultant and entrepreneur, Thomas Lang's ability to get to grips quickly with critical situations has become second nature. He remains calm, whatever the circumstances, and understands how to separate the important from the unimportant, and bring structure into the unstructured. This helps him maintain a clear overview in complex situations. Additionally to IT security & compliance, his consulting expertise focuses on, among other things, IT strategy, project governance and controlling, crisis management, and IT infrastructure & operations.

Protecting trade secrets securely against cyberattacks

Two thirds of all German companies see their existence threatened by cyberattacks, according to a 2024 survey of more than 1,000 managers conducted by the digital association Bitkom. This is a worryingly high figure. 80% of survey participants report that the number of cyberattacks on their company has increased in the past twelve months (Bitkom Research, 2024).

Ransomware 2024/25: encryption plus data theft

According to Bitkom (2024), dangerous ransomware attacks, which encrypt systems and data and only release them again after a ransom has been paid, have reached a new all-time high. Ransomware has caused enormous damage to 31% of survey participants in the past twelve months. Ransomware will remain one of the biggest threats in 2025 and is often combined with the theft of business secrets.

Cyber criminals use a tried-and-tested but always successful attack pattern. **Seductive phishing emails** are the gateway for most ransomware attacks, with AI-generated emails and deepfake imitations looking increasingly convincing. Employee training and phishing detection systems can help prevent ransomware attacks and stay one step ahead of cybercriminals. However, this next generation of phishing attacks will **take advantage of AI's ability to learn from real-time data and adapt to advanced security measures.**

Consequently, even the hype technology of artificial intelligence is rated rather critically as a risk factor by 83% of the managers surveyed because it exacerbates the threat situation (Bitkom Research, 2024). Generative AI will enable operations on a much larger scale. For example, cybercriminals can use AI to launch thousands of targeted phishing attacks simultaneously and customize each one for maximum impact.

This leads to only one conclusion: **no company, from SMEs to large corporations, can feel safe.** The world is tending to become a very insecure place, partly due to AI. What can companies do to protect themselves against a growing threat situation?

Trade secrets are target #1

Attackers often aim not only to encrypt data, but above all to steal trade secrets such as strategy papers, financial data, blueprints of future products or customer data, which are then auctioned off to the highest bidder on the darknet and turned into money. The damage that affected companies face can hardly be realistically estimated and ranges from loss of sales in the millions to a threat to their entire existence. Often unnoticed: attackers are on average in the company network for over 200 days and read along before they are even discovered.

A popular example is the theft of access data and passwords, which are used to prepare for larger attacks in the future. Accounts of managers with very far-reaching access rights are particularly targeted by attackers.

83%

of managers surveyed say that AI is exacerbating the threat to the economy (Bitkom Research, 2024).

Which company information is worth protecting?

No company wants its trade secrets to fall into the wrong hands. The first step is therefore to gain an overview and identify sensitive trade secrets and the processes in which they are needed. A business impact analysis helps to determine the level of protection required and to prioritize budgets and measures. Information worthy of protection includes strategy papers, know-how, calculation bases and access data to accounts and financial systems.
Everything you would like to know about your competitors and customers is also of interest to third parties about your company. Confidential and strictly confidential information in particular, the disclosure of which could jeopardize the achievement of business objectives, requires special protection.

Trade secrets according to law

There is also a legal aspect: a trade secret is information according to Section 2 (1) of the GeschGehG,

a) which is not generally known or readily accessible, either as a whole or in the precise arrangement and composition of its components, to persons within the circles that normally deal with this type of information and is therefore of **commercial value** and

b) which is the subject of confidentiality measures that are **reasonable in the circumstances** by its legitimate owner and

c) for which there is a **legitimate interest** in confidentiality.

Information and data that are not adequately protected are therefore not trade secrets under German law and any damage cannot be claimed.

Corresponding laws exist in most Western countries, but also in China, for example.

The most important security measures

Physical theft in company buildings on site is often forgotten. Physical protection measures therefore also include access controls to the building, the storage of critical documents in safes, appropriate key management and the complete destruction of paper documents by a shredder once the retention period has expired.

In contrast, digital cyberattacks, including the aforementioned ransomware, are largely prevented by cybersecurity measures. The most important measures include the following:

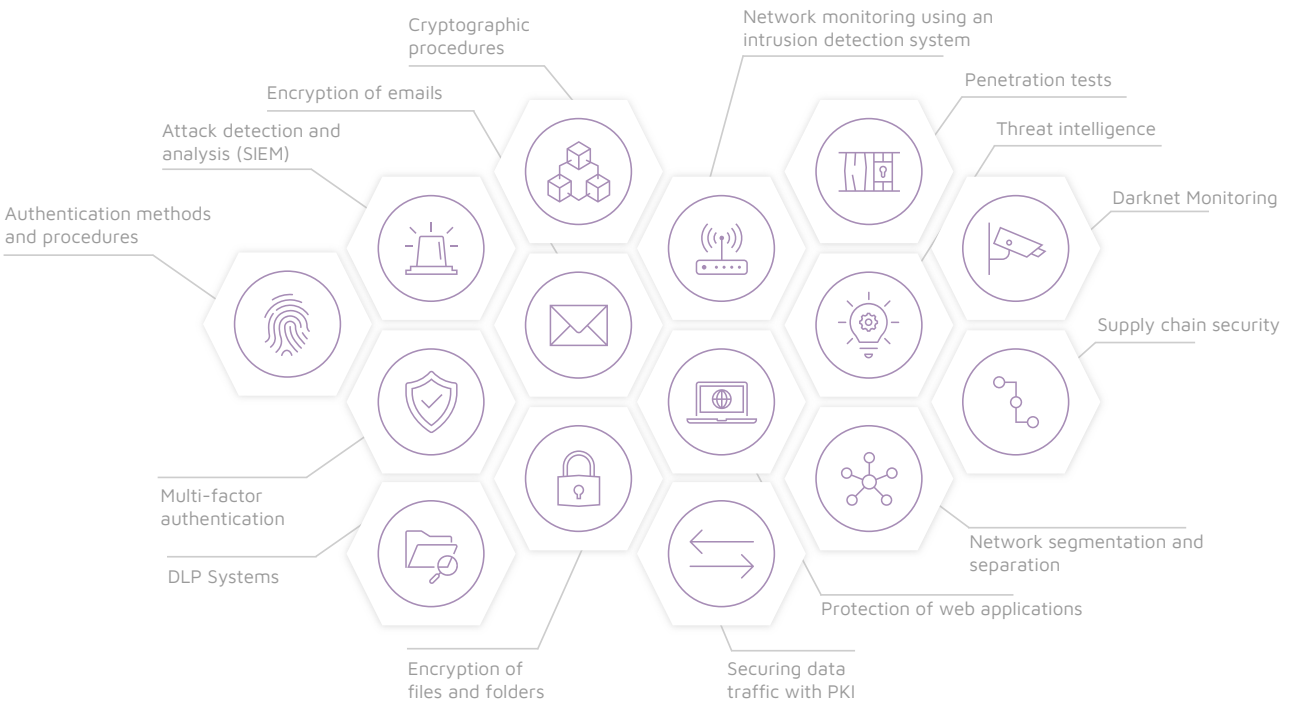


Fig. 1: Overview of cyber security measures to reduce the vulnerability of companies
Source: valantic

Authentication methods and procedures

There are various procedures and factors for authentication and fulfillment of IT security objectives. These methods can be divided into three categories - knowledge-based, possession-based and biometric factors. Depending on the area of application, the procedures are suitable individually or in combination.

Knowledge-based factors include, for example, passwords, PINs and passphrases. The password is the most widely used authentication method and ideally consists of a random sequence of numbers, letters and special characters. In contrast, the personal identification number (PIN) usually consists of a 4- or 6-digit sequence of numbers with which the user identifies themselves on their device.

Possession-based factors include FIDO and OTP security tokens as well as smartphones and classic smartcards. Security tokens are usually used to provide additional security for user accounts. They act as a second factor, often in the form of a USB stick, and can be uniquely assigned to a user and thus personalized. Security tokens generate a one-time password (OTP). The smartphone serves as a common authentication medium.

Biometric factors form the third category of authentication methods. These include, for example, fingerprint and iris scanners as well as vein or facial recognition, typing behavior and voice recognition. Of these, fingerprint and facial recognition have established themselves.

Multi-factor authentication

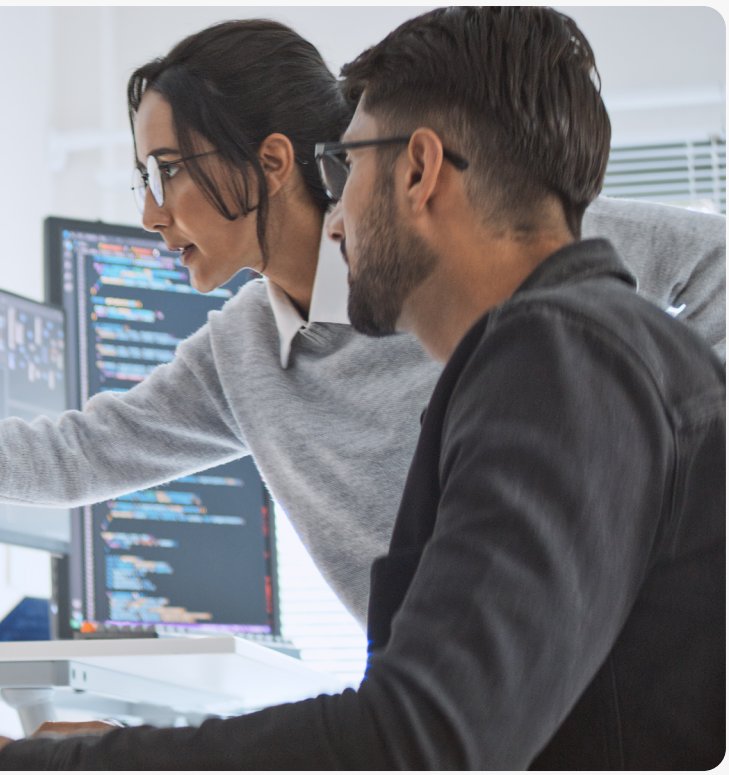
Multi-factor authentication (MFA) is the process of proving a user's identity using more than one factor (e.g. password + one-time password (OTP) or password + fingerprint + security token). Multifactor authentication is considered to be particularly secure.

DLP Systems

Data loss prevention (DLP) is a strategic security measure that ensures that sensitive or critical information is not transferred outside the company network. However, the administration and training costs are relatively high.

Cryptographic procedures

Cryptographic procedures are encryption methods that protect particularly sensitive content. The quality of cryptographic methods depends in particular on the encryption method used and the selected key length (e.g. 512 bits). As the key length increases, so does the number of possibilities that need to be tried in order to decrypt an encrypted message. The longer the key, the better the encrypted information is protected.



Encryption of files and folders

File and folder encryption involves the encryption of individual objects, such as containers, folders or individual files. This type of encryption is therefore also known as object encryption. Object encryption makes it possible to transport files and folders securely from one location to another and prevent unauthorized access.

Encryption of emails

Business emails often contain important and sensitive information. The protection objectives can generally be achieved by encrypting the transport route or the email content.

Securing data traffic with PKI

In digital data traffic, it is important to guarantee the identity of the communication partners and the authenticity of the transmitted content. Proof of digital identities for individuals and organizations can be ensured by using certificates. Electronic signatures are suitable for proving the authenticity of transmitted documents and messages. Certificate-based solutions are also used for encrypted data transport.

However, all of these scenarios require one component: a public key infrastructure (PKI).

Network monitoring using an intrusion detection system

An intrusion detection system (IDS) or intrusion prevention system (IPS) detects and logs anomalies in the company network. The aim of both systems is to detect the intrusion and distribution of malware before the damage occurs.

In contrast to the IDS, which only displays anomalous behavior and generates alarms, an IPS can also intervene automatically. This is intended to prevent the further spread of malware via the company network. It should be noted that direct intervention by an IPS has a direct impact on the availability of systems, for example in industrial and production facilities or fully automated ordering/delivery processes as well as reporting and security processes (e.g. fire protection).

Protection of web applications

A web application firewall (WAF) protects web applications such as websites, online stores and home banking portals from attacks. The WAF examines the communication between the user and the web application at application level and blocks potentially harmful data traffic such as SQL injections or cross-site scripting. The term Web Service Firewall (WSF) is also commonly used for machine-to-machine communication.

Attack detection and analysis (SIEM)

Security information and event management systems (SIEM for short) are used to analyze anomalies and detect attacks on the company infrastructure. They enable the holistic detection of security-critical events in the IT infrastructure in real time and the implementation of suitable defensive measures, some of which are automated.

SIEM can provide support against the following threats: attack activities by external parties (hacker attacks), threats by insiders (e.g. unauthorized file access from other departments, computer sabotage) and compliance violations.

Network segmentation and separation

The division of networks through network segmentation and separation is an effective measure to prevent the spread of malware. With network segmentation, a network is divided into several segments, each of which acts as its own sub-network. Communication between these segments is restricted via defined zone boundaries (boundary protections). This protects segments in the network from attacks from other, already affected segments.

Penetration tests

Regular penetration tests are simulated attacks on your networks that can uncover gaps and configuration errors before any damage occurs. This often makes sense before new applications or systems are released.

Darknet Monitoring

The loss of business-critical information can have serious consequences. If you know about the loss, you can react. Just as in the real world, where stolen goods are traded on the black market, stolen company information such as stolen login details or payment transaction information is traded on the internet on what is known as the dark web. This refers to a large number of separate, non-publicly accessible networks (darknets) within the internet.

If, for example, login information for company accounts appears on the darknet, this allows conclusions to be drawn about an imminent attack on the compromised company.

Threat Intelligence

Threat Intelligence (cyber risk intelligence) collects, analyses and prioritizes potential and current threats to IT systems, networks and organizations. Threat Intelligence draws on internal data (e.g. log protocols) and external sources (e.g. darknet/dark web). The aim is to detect threats earlier, shorten response times and reduce risks through preventive measures.

Supply chain security

In principle, partners should achieve the same level of protection as the client. This must be specified in contracts and compliance must be monitored. Well-known third-party risk management service providers include Bitsight, Panorays, SecurityScorecard and others.

Top risk: ill-considered use of AI tools

As AI becomes increasingly ubiquitous in both private and professional environments, the risk of inappropriate use of AI tools is growing. One of the biggest risks in 2025/26 will be data breaches caused by employees inadvertently sharing sensitive information with AI platforms such as ChatGPT or Google Gemini. AI systems can process huge amounts of data and when this data is fed into external AI tools, the risk increases dramatically.

For example, employees could enter sensitive financial data into an AI tool to create a report or analysis without realizing that their data could be stored and accessed by external, unauthorized users.

AI-generated malware and multi-agent systems

Attackers will increasingly use advanced AI tools beyond code completion tools like GitHub Copilot to generate code. AI platforms will be able to program a complete code for malware with a single command prompt.

This trend encourages the rapid creation of sophisticated and highly targeted cyberthreats. The barrier to entry for malicious actors is dropping dramatically and the world is becoming a far less safe place. This is because the tools are easily accessible, difficult to detect and evolving faster than traditional security defenses can adapt.

Multi-agent AI systems will emerge, with multiple AI models working together to solve complex problems. Attackers will use these systems to carry out coordinated, distributed attacks that are more difficult to detect and defend against. At the same time, defenders will use similar systems to detect threats in real time and respond across networks and devices.

Management Summary

In the digital age, companies are faced with the perpetual challenge of protecting their trade secrets from growing threats. Cyberattacks are just one scenario, albeit a relevant one, as the alarming results of the Bitkom 2024 survey show. The loss of sensitive information in particular is increasingly coming into focus. While artificial intelligence is also perceived as a risk factor, **essential security strategies and technologies, such as threat intelligence, authentication methods and procedures, data loss prevention and network monitoring, offer ways to counter this risk.**

About valantic

valantic has been advising companies competently and comprehensively in the area of cyber security for many years – from information security management and regulatory compliance to preventive measures such as threat intelligence analyses and darknet monitoring. In this way, we ensure that our clients are one step ahead of threats in the digital age. After all, security starts before the crisis.

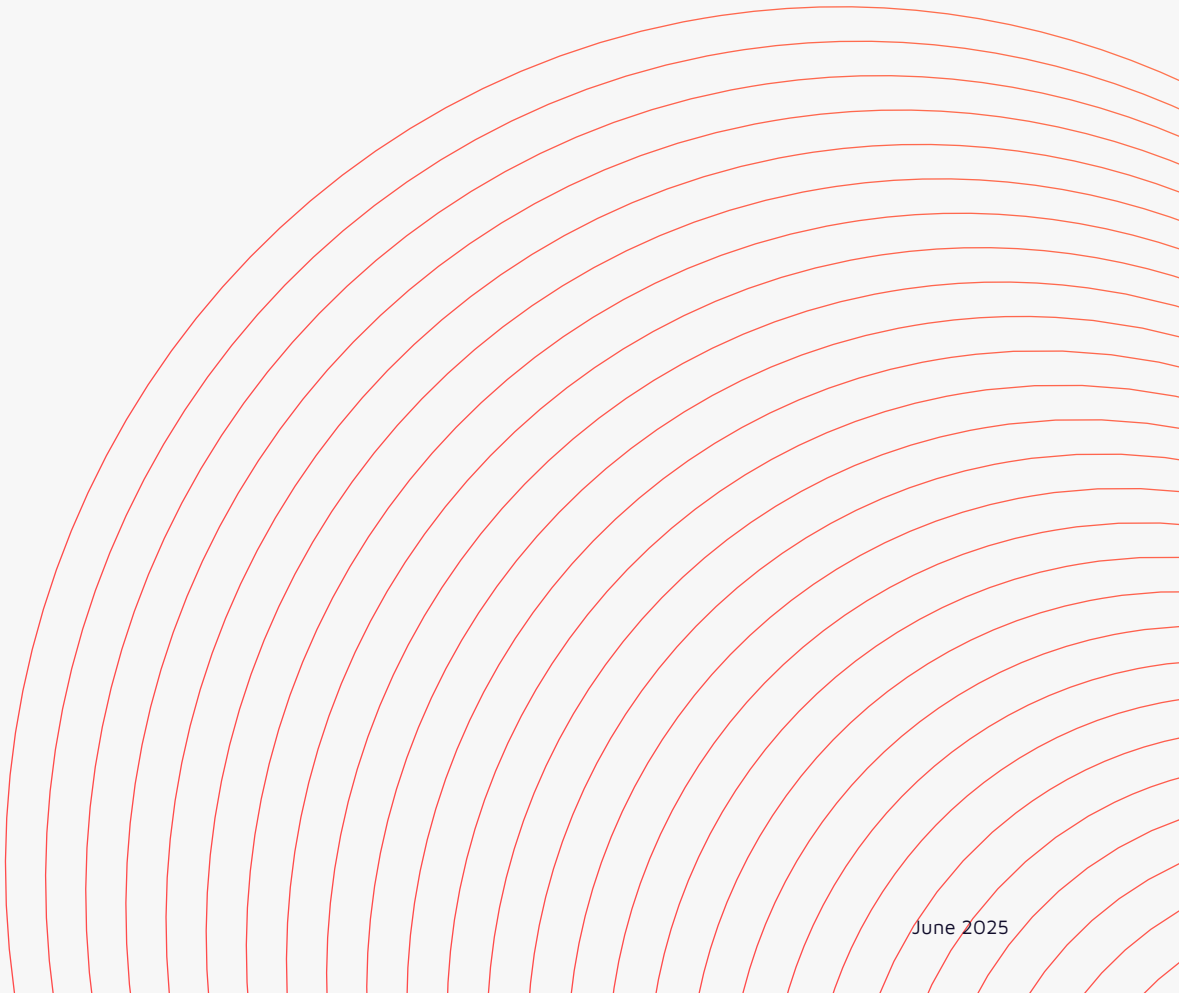
valantic

Contact

Dreieich Plaza 2A
63303 Dreieich
Germany

Phone +49 6103 5086 0
info@mc.valantic.com

www.valantic.com



June 2025