Whitepaper

InfoGuard Threat Intelligence Insights 2025

An Analysis of the Threat Landscape – Including Forecast and Recommended Actions

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

As of May 2026

Executive Summary

Cyber attacks are not becoming more sophisticated, but more efficient. The comprehensive analysis for the year 2025 shows that attacks are increasingly following a scalable, automated and division-of-labour model. The decisive moment in this remains initial access. Phishing, compromised identities and insufficiently secured remote access points continue to be among the most common and at the same time most effective initial vectors.

At the same time, attackers' focus is clearly shifting towards identities. Even a single set of compromised credentials is sufficient to obtain extensive control over systems and data. It is also striking that security incidents rarely arise due to a lack of protective mechanisms, but rather due to insufficient visibility and delayed response. Organisations with mature monitoring and tested incident response significantly limit damage.

Clear sector-specific differences can be seen: while some sectors detect attacks at an early stage and respond accordingly, others often only intervene once the impact has already occurred. Against this backdrop, the key to cyber resilience does not lie in investing in additional monitoring and detection tools, but in the ability to detect attacks at an early stage and to manage them in a targeted manner.

From this, the report derives seven central action areas for 2026: from consistent protection of identities ("identity first"), through shortened patch cycles and an extended zero-trust architecture, to enhanced visibility across identities, cloud and APIs. This is supplemented by systematic preparation for emergencies – for example through tested incident response processes, robust backup strategies and a targeted reduction of risks in the supply chain. These action areas form the basis not only for reducing cyber risks, but also for maintaining controlled command of the situation in the event of an incident.

Securing Your Digital World

InfoGuard SWISS CYBER SECURITY

Table of Contents

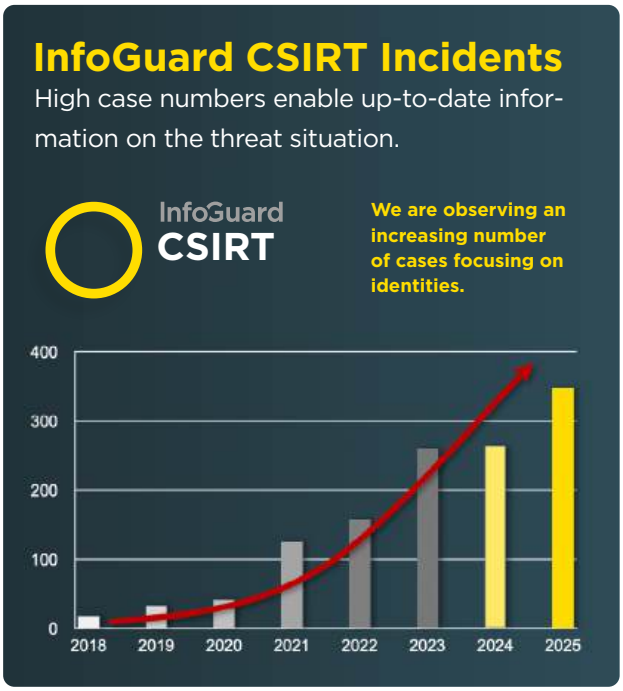
1. Review 2025

The current threat landscape continues to deteriorate. This is particularly evident in the operational reality of incident response. In 2025, the InfoGuard CSIRT handled more than 350 cyber incidents, representing a substantial increase of around 20 percent compared to the previous year. This trend was already apparent in the first half of the year: complex attacks rose by an impressive 115 percent compared with the previous period.

This development is not a statistical outlier, but rather an expression of a structural shift. The rising number of cases reflects an increasingly dynamic and robust situational picture. It is striking that 2025 produced hardly any new attack methods.

Instead, the industrialisation of cyber attacks accelerated significantly. Attackers are operating more efficiently and faster, within highly scalable, division-of-labour structures.

Automation, the trade in compromised access via initial access brokers, AI-supported attack tools and professionalised ransomware ecosystems are further lowering the barriers to entry – and are leading to cyber attacks increasingly being organised along the lines of a service model.



Source InfoGuard Intelligence

2. Initial Access Vectors

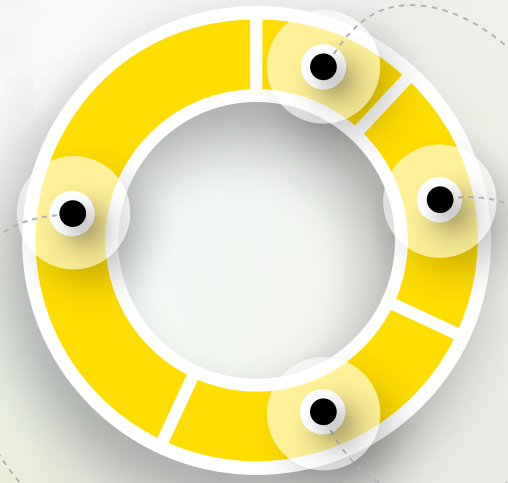
Initial access remained the most critical phase of every attack chain. Once attackers succeed in gaining access to the corporate network, the focus inevitably shifts from prevention to damage limitation.

In 43 per cent of the security incidents handled by the InfoGuard CSIRT, initial access occurred via phishing. Over the past five years, this share has more than doubled and has become established as the dominant attack vector. This is likely due in particular to the increasing use of LLMs by attackers, enabling personalised and contextually convincing attacks.

An opposite trend can be seen in the exploitation of vulnerabilities: while phishing is increasing sharply, the proportion of incidents caused by vulnerabilities has fallen to just 20 per cent over five years. One possible reason for this is a more deliberate exposure of services to the internet.

Organisations have learned from past security incidents and no longer expose workloads directly to the internet, but instead protect them via upstream authentication portals. However, the high number of security incidents in which exposed services are still protected solely by simple username–password combinations remains worrying. This is a level of security that no longer withstands today's attack realities.

Compared with previous years, the number of incidents occurring via the supply chain has continued to rise. Many companies are still not sufficiently aware of this risk and underestimate the associated dangers.



Top Initial Access Vectors 2025

- **12%** Supply Chain
- **20%** Vulnerability
- **25%** Unsecure Service Exposed
- **43%** Phishing

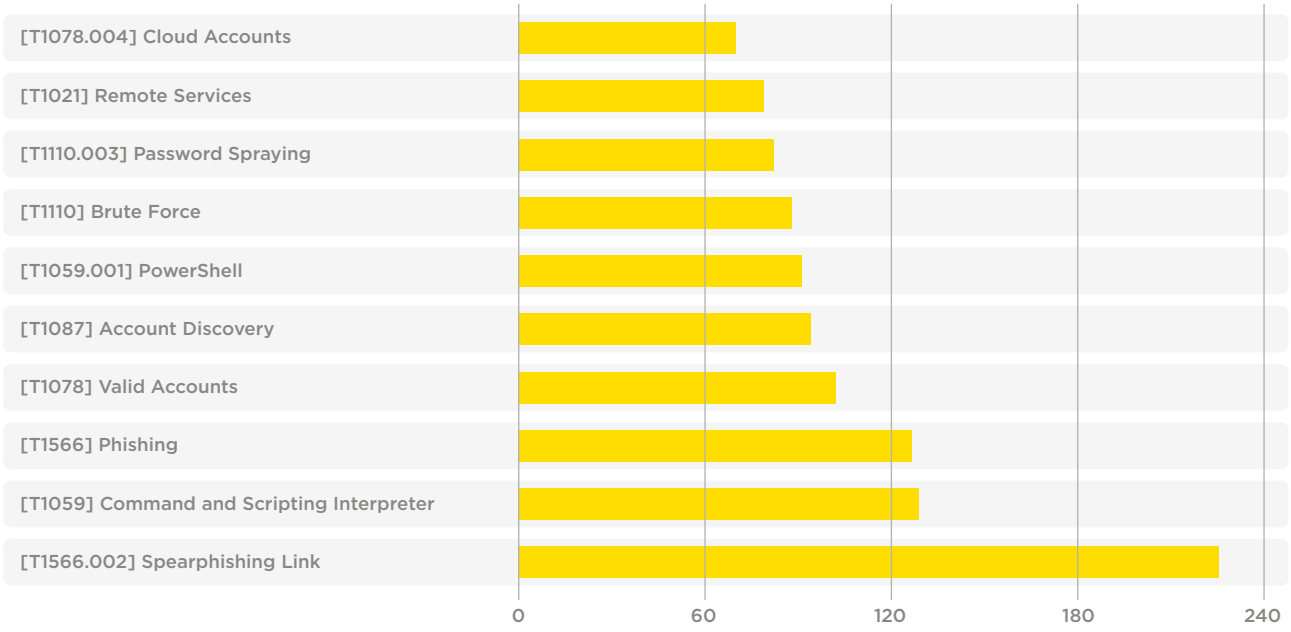
2.1 Phishing

During the reporting period, phishing remained the dominant initial access vector for cyber attacks. At the same time, the quality of attacks reached a new level of escalation: personalised content, AI-generated texts, deepfake voice messages and the precise imitation of internal communication styles.

Credential harvesting increasingly shifted to cloud services such as Microsoft 365 (M365) and Google Workspace. MFA bypass techniques such as the theft of session tokens or adversary-in-the-middle kits were no longer observed as exceptions, but as established standard methods. Phishing is less an awareness issue and more a question of identity security. It is therefore not surprising that a considerable proportion of the true positive security incidents detected by the InfoGuard MDR service in 2025 was specifically directed at identities. Typical attack methods include spear-phishing, phishing, brute force and password spraying, which attackers use to systematically gain control over on-premises and cloud-based accounts.

The consequences of successful phishing attacks were usually not isolated, but cascading in nature: further phishing campaigns, data exfiltration from SharePoint and OneDrive environments, the sending of fraudulent invoices, or the targeted theft of sensitive e-mail threads.

Most Frequent True Positive Detections in the Security Operations Centre (SOC)



2.2 Unsecured Remote Access

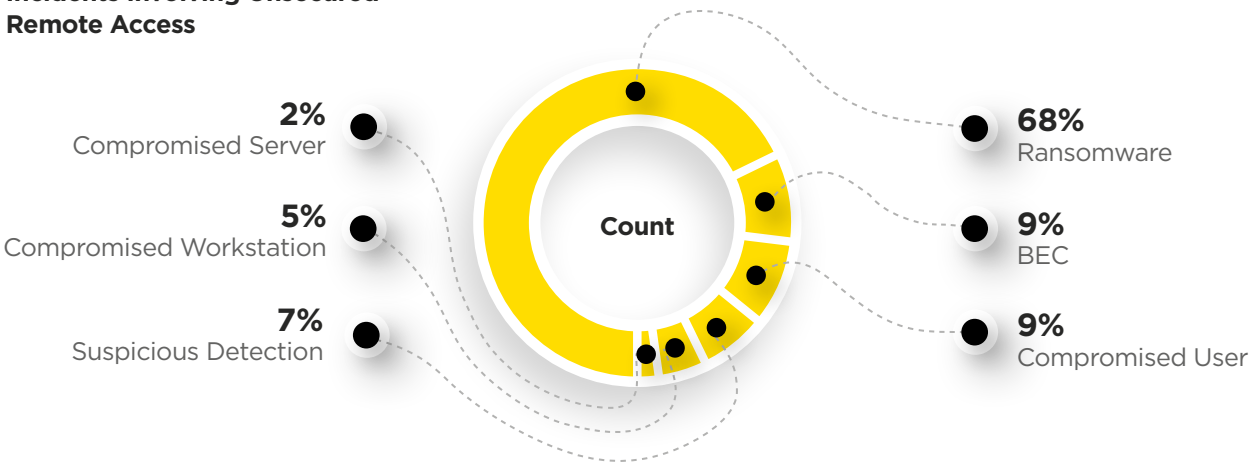
Open or poorly secured VPN, RDP and remote management access points remained a preferred entry vector for ransomware actors, with particularly severe consequences: in 68 per cent of observed incidents, access via such entry points led directly to a ransomware compromise.

The greatest security lapse continued to be the absence of multi-factor authentication. This enables attackers to penetrate corporate networks with minimal effort and maximum impact. Weak, reused or only temporarily set passwords further increase this attack surface and make it easier to compromise user accounts through brute force attacks.

InfoGuard observed in numerous companies a lack of restrictions on which user accounts were permitted to use remote access. In some cases, the entry point could be traced back to technical or temporary user accounts. These were protected with weak passwords and, in some instances, were compromised via exposed legacy protocols that offer little or no protection mechanisms.

Initial access brokers further professionalised the trade in compromised access. Companies were increasingly no longer attacked directly, but traded and resold as ready-made entry points.

Incidents Involving Unsecured Remote Access



2.3 Vulnerabilities

The year 2025 was characterised by a massively accelerated exploitation of newly published RCE vulnerabilities. The time window between the publication of a CVE and active exploit use shrank in many cases from weeks to just a few days or even hours. The increasing use of agentic AI by attackers is likely to intensify this development further in future and structurally overwhelm classic, often sluggish patch processes.

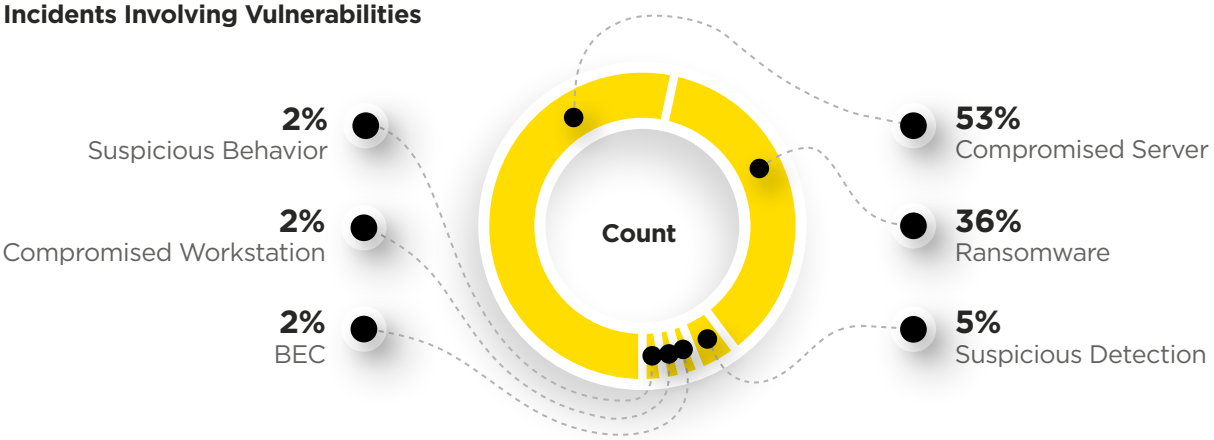
Edge devices and remotely exposed services were particularly affected, such as:

- Ivanti
- SonicWall
- SAP
- Microsoft SharePoint
- WordPress plug-ins

Exploit kits were often available shortly after a vulnerability was published – in some cases faster than organisations were able to complete their risk analysis. Late patching gave many companies a false sense of security, as systems had often already been compromised by the time the patches were applied. This allowed attackers to continue their activities undetected and operationalise them with a time delay.

In 53 per cent of incidents in which a vulnerability was used as the initial access point, this led to a compromised server. Rapid detection and response were decisive for how events unfolded: in many cases, swift intervention prevented lateral movement. Nevertheless, 36 per cent of these incidents resulted in a successful ransomware attack, in some cases with considerable operational and financial impact on business operations.

Incidents Involving Vulnerabilities



2.4 Supply Chain

Instead of attacking their targets directly, attackers increasingly used access via the supply chain and deliberately exploited existing trust relationships as an entry point.

Among other things, the following were observed: the exploitation of unsecured remote maintenance accesses, malicious software updates, and business software advertised via Google Ads that was delivered bundled with remote maintenance software or trojans. In addition, insufficiently restricted and monitored site to site (S2S) VPN connections to partners increasingly developed into a structural risk factor.

Supply chains continue to represent a structural risk, as they give attackers direct access to internal networks. Companies in the financial and insurance sector as well as in the information and communication sector were particularly at risk from targeted supply chain attacks.

These organisations often have strong security set-ups to fend off and detect attacks. This creates a strategic advantage for attackers: the route via the supply chain is often less visible, less protected and operationally more efficient than a direct attack on the actual target.

Supply chain incidents per sector

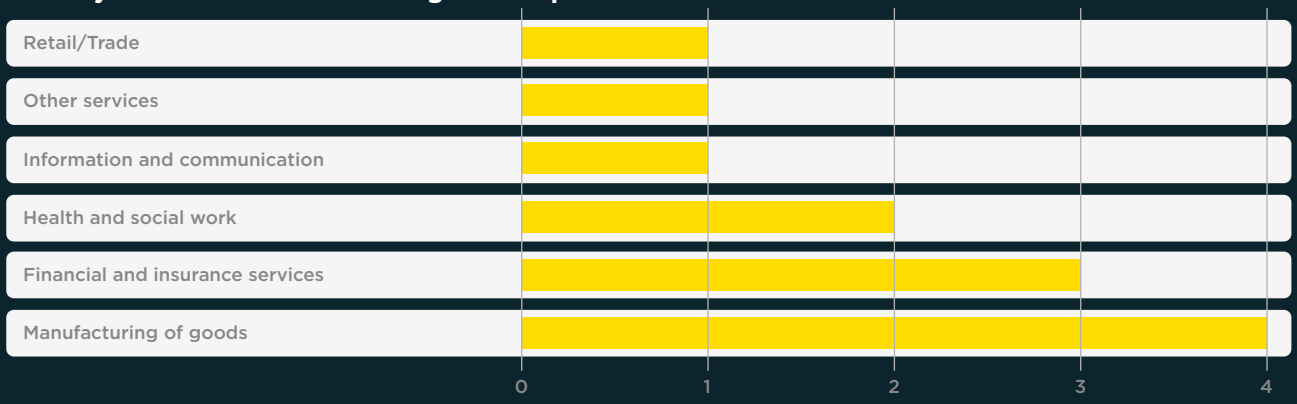
2.5 Misconfiguration

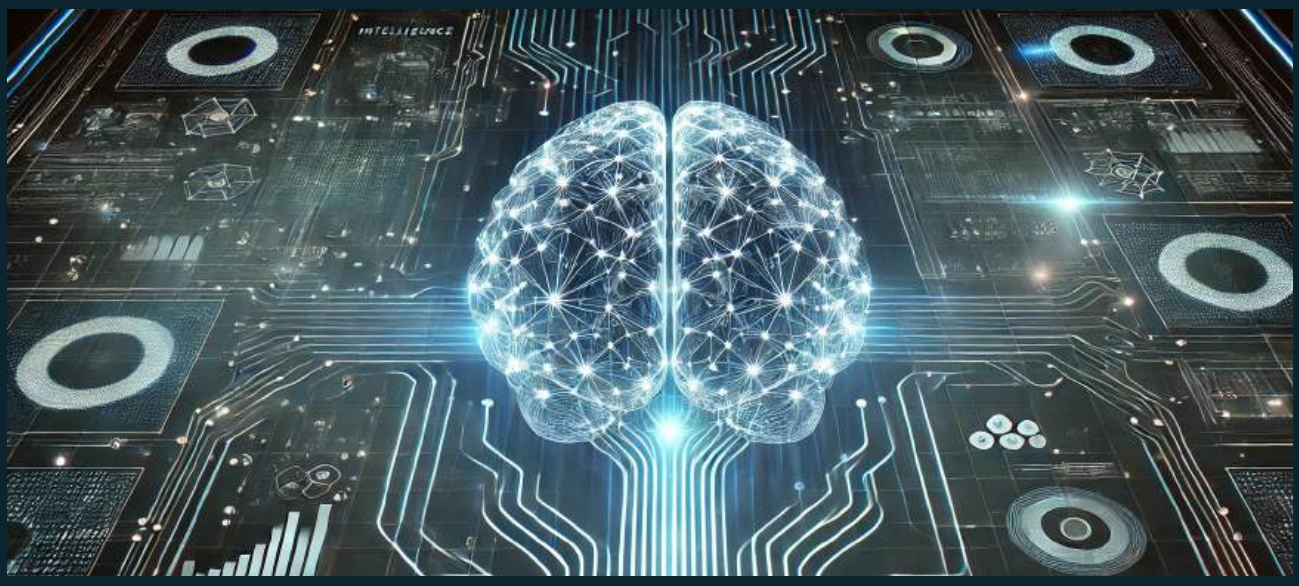
Misconfigurations remained an often underestimated attack vector. They rarely arise from individual serious mistakes, but rather from a multitude of small, everyday omissions. The causes range from a lack of know how, to time pressure and distraction in day to day work, through to insufficient engagement with security relevant changes, such as patch notes or system updates. Added to this are missing quality assurance processes that would ensure that changes are checked and documented consistently.

InfoGuard observed a wide variety of misconfigurations during the reporting period. These included, among other things, orphaned DNS pointers to cloud resources that could be taken over by attackers, as well as unintentional deactivation of authentication mechanisms. Management interfaces exposed to the internet and the unintentional exposure of internal data repositories were also identified.

Misconfigurations cannot be clearly attributed to any particular sector. However, it was noticeable that affected companies often had complex, hybrid infrastructures with numerous interfaces and external service providers. In many cases, the root cause could be traced back to a structural governance deficit, as clear responsibilities for implementation, control mechanisms and adequate documentation of changes were lacking.

Security incidents due to misconfigurations per sector





3. Sector Trends

3.1 Monitoring

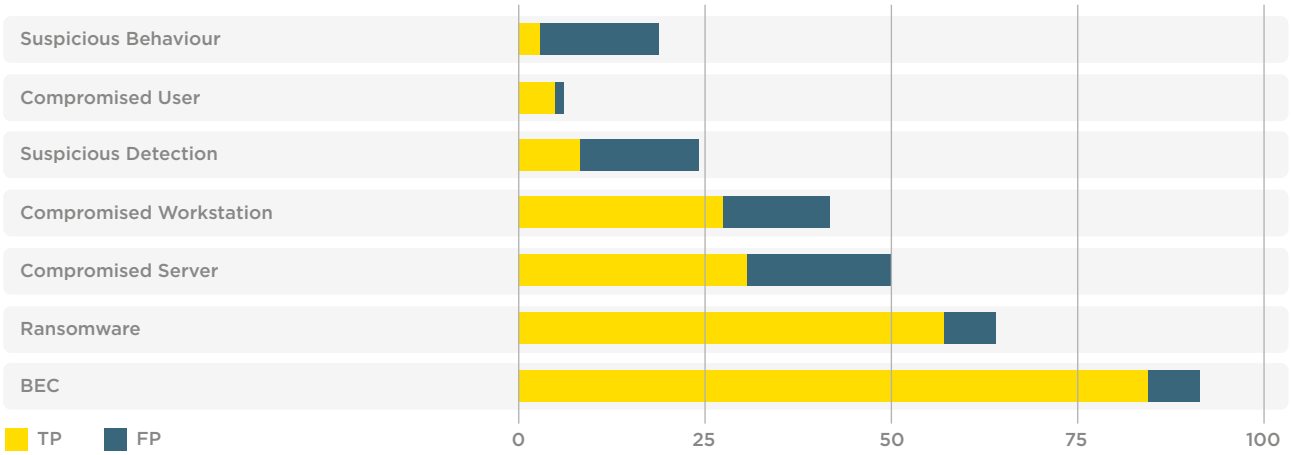
Over the past year, InfoGuard observed that organisations increasingly engaged external expertise earlier and in a more targeted way when there was suspicion or indications of a compromise – a clear sign of growing awareness of cyber risks.

Organisations with mature monitoring and established response processes demonstrably and significantly reduce the impact of an attack. The difference lies less in preventing an attack and more in the speed and quality of detection and the subsequent response.

Among the false positive alerts handled by the InfoGuard CSIRT were, for example:

- Checks of vulnerable, exposed systems to rule out that a system had already been compromised before patching.
- Support in analysing unknown detections from deployed monitoring technology.
- Insufficient context in the monitoring technology for a conclusive and reliable assessment.
- Second opinions or validation of analyses carried out in-house.
- Support in analysing possible lateral movements from a compromised partner network.

False-positive rate per incident type



Notable is the sectoral distribution: the InfoGuard CSIRT was particularly often called in to assist with false positive alerts in the energy and water, financial and insurance services, health and social work, IT and communications sectors, as well as in public administration, defence and social security. This clustering is no coincidence, but an indicator of existing and functioning monitoring structures that make attacks visible at an early stage.

By contrast, organisations in manufacturing, retail, transport and the construction industry still tend to get in touch at a later stage – namely when attackers have already achieved their objectives and the damage is beginning to become apparent. In these areas, monitoring is still understood less as a continuous capability and more as a reactive measure in the event of an incident.

For the early detection of attackers, the following factors are particularly crucial:

- Use of Endpoint Detection and Response (EDR) technology instead of purely signature based antivirus solutions
- Supplementing with Identity Detection and Response (IDR) technology
- Log correlation across multiple sources, especially firewall, proxy, VPN and VDI logs

At the same time, we identified clear visibility gaps:

- Missing or too short retained firewall and (VPN) authentication logs
- Limited transparency in SaaS and PaaS services without SSO integration
- Third party systems and appliances without integrated security monitoring
- Shadow IT and temporary cloud workloads at cloud providers

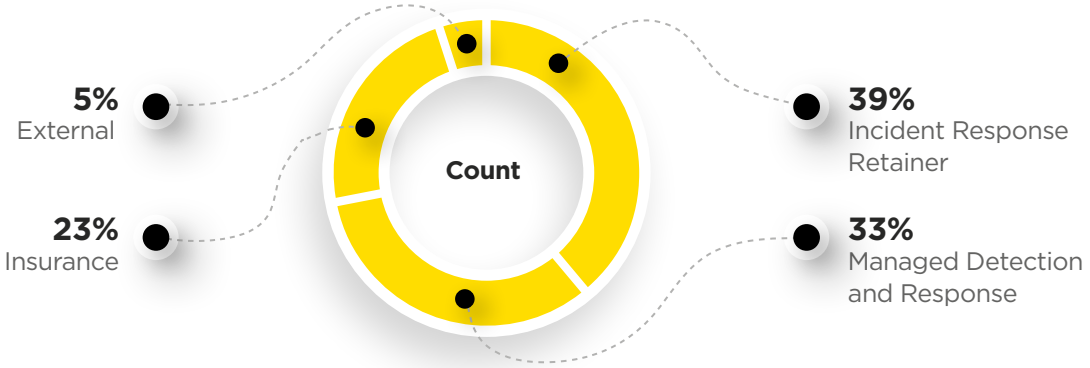
The central pattern is clearly recognisable: in the reporting period, attacks rarely failed due to missing protective mechanisms, but rather because they were detected too late or drowned in the noise of the systems.

3.2 Readiness

The InfoGuard CSIRT supports companies in any initial situation. For existing customers – for example with an Incident Response Retainer or Managed Detection and Response – structured onboarding already creates operational readiness before a potential incident, so that action can be taken without delay in an emergency. The situation is different for companies that make contact via insurance or as new customers: here the maturity of incident response readiness varies considerably, with direct impact on reaction speed and the extent of damage.

In practice, the InfoGuard CSIRT identified recurring gaps in incident readiness at many organisations. Remarkable here is less the absence of concepts and more their lack of practical applicability in an emergency. Closing the identified gaps would, in numerous cases, enable a faster and more effective response and significantly reduce the damage incurred.

Customer relationship



Typical gaps in practice:

- **Validation of ransomware secure backup retention:**
  In some cases, it became apparent that business critical backups were stored exclusively on a NAS and were therefore directly accessible and deletable by attackers. Without additional protection mechanisms such as air gapping or immutable storage, the supposed safety copy itself becomes a risk.

- **Missing or unpractised incident response, business continuity and backup recovery plans:**
  Although many organisations invest time in incident response, business continuity and recovery plans, in practice it often became apparent that these plans had never been tested under realistic conditions. Without regular exercises – for example in the form of Tabletop Exercises (TTX) – their effectiveness in an emergency remains uncertain.

- **Non available emergency documentation in an incident:**
  Ransomware attacks in particular reveal a recurring pattern: central information such as emergency contact lists, access data, licences or recovery plans are not available at the decisive moment because they themselves have been encrypted. Critical documents must therefore be deliberately stored offline and independently of the productive infrastructure.

- **Insufficient log retention and forensic visibility:**
  For the forensic analysis of an incident, logs such as endpoint logs, firewall logs or antivirus logs are often the only reliable information source. If this data is missing or not retained long term, a sound forensic review is hardly possible. This not only makes root cause analysis more difficult, it also delays secure recovery. Central, tamper proof and, as far as possible, ransomware resistant storage of relevant logs is therefore essential. Modern EDR and XDR solutions already offer integrated options for extended and secure log retention. The central pattern is clear: it is not the mere existence of security measures that determines success in an emergency – but their availability, practical usability and immediate applicability under stress.

The central pattern is clear: It is not the mere existence of security measures that determines success in an emergency – but their availability, practical usability and immediate applicability under stress.

4. Threats

4.1 Ransomware

Measured by potential impact, ransomware was among the most significant cyber threats to companies during the reporting period, and this will not change in the near future. A successful attack rarely leads to short term disruptions; instead it often drags on for weeks or months until normal operations are restored.

Compared with previous years, however, a significant development became apparent: attackers increasingly dispensed with encryption and limited themselves to exfiltrating sensitive data. Such attacks often remain undetected until attackers threaten to publish the exfiltrated data in order to maximise pressure.

Ransomware attacks are generally opportunistic and rarely targeted. The focus is not on the individual company, but on its vulnerability. This dynamic is also reflected in the cross sector distribution of incidents.

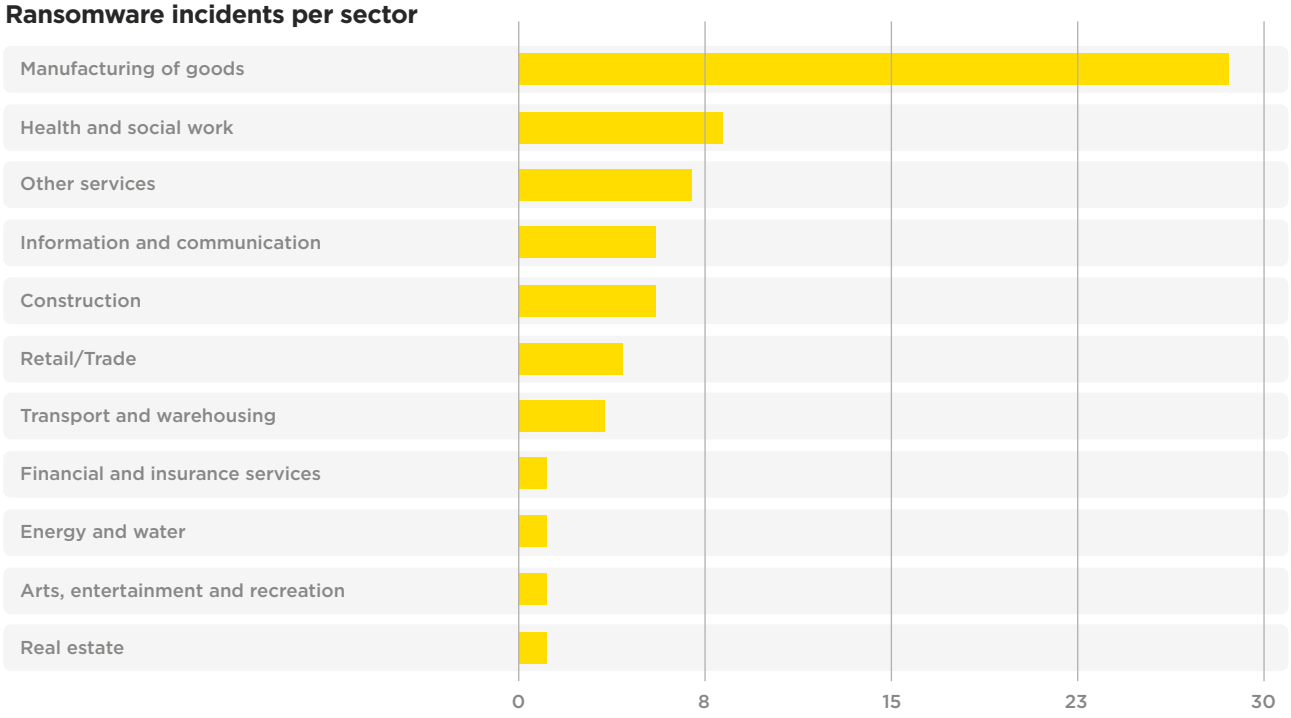
The majority of incidents recorded by the InfoGuard CSIRT occurred in the manufacturing sector. Compared with more heavily regulated industries, this sector is subject to fewer binding requirements on cyber resilience, which is directly reflected in its attack surface.

Manufacturing companies also frequently operate heterogeneous, historically grown IT landscapes with long life cycles, in which applications and systems are kept running even though they are already critical from a security perspective.

Particularly relevant is the close interlinking of IT and OT infrastructures. Production environments are often connected via vendor specific maintenance accesses that are not consistently segmented or monitored. A successful attack on IT can therefore have a direct and immediate impact on operational production – with correspondingly serious consequences.

The key insight: ransomware is no longer just an IT security problem. It is increasingly developing into a business critical risk with direct impacts on supply chains, production and market availability.

Ransomware incidents per sector



4.2 Business E-Mail Compromise (BEC)

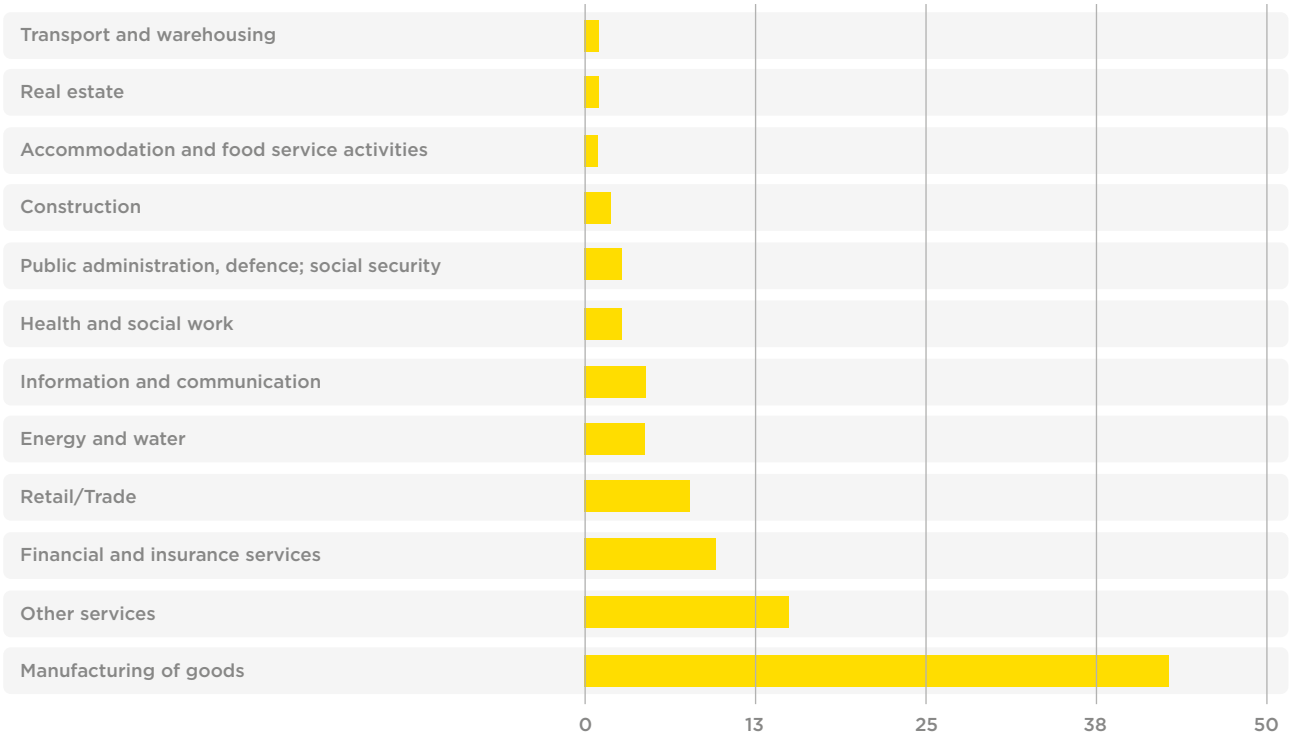
Against the backdrop of LLMs, info stealers and increasing credential leaks, the number of Business E-mail Compromise cases continues to rise measurably. The majority of compromised e-mail accounts are linked to phishing attacks. Attackers most frequently used “adversary in the middle” attacks to specifically and systematically bypass multi factor authentication (MFA). To technically prevent such attack tactics in future, phishing resistant methods such as passkeys or FIDO2 should be implemented consistently and across the board.

In most cases, the immediate damage from Business E mail Compromise remains manageable. Often, hijacked accounts are merely equipped with a forwarding rule to conceal the compromise and then used to compromise further business partners via targeted phishing campaigns.

However, the InfoGuard CSIRT also recorded several cases in which attackers succeeded in manipulating invoices, causing some companies to suffer significant and immediately effective financial losses. In individual cases, the financial damage even exceeded typical ransomware payments. In addition to payment fraud, the InfoGuard CSIRT also observed threat actors who used compromised M365 accounts to exfiltrate company data from OneDrive and SharePoint and then put pressure on companies by threatening to publish this data.

Most BEC incidents were recorded in the manufacturing sector. This is likely due, among other things, to the numerous supplier relationships and the fact that invoices in this sector are frequently processed by e mail. At the same time, typical structural weaknesses become apparent here: lack of multi factor authentication, insufficient identity monitoring, and a lack of transparency over communication processes – factors that not only facilitate such attacks but also often lead to late detection.

Business E-Mail Compromise per sector



The time between compromise and discovery of payment fraud is often longer than the retention period of logs relevant for forensic investigation.

In some cases, the InfoGuard CSIRT could no longer determine the exact time of compromise.

4.3 Identity Theft

During the reporting period, the InfoGuard SOC and CSIRT observed that the majority of attacks targeted identities directly. Accordingly, most true positive detections in the Security Operations Center (SOC) related to TTPs associated with identities, such as spear phishing links, phishing, valid accounts, account discovery, brute force, password spraying, remote services and cloud accounts.

To detect such attacks efficiently and at an early stage, monitoring should be extended to include IDR (Identity Detection and Response), and identities should be systematically monitored as an independent protection domain.

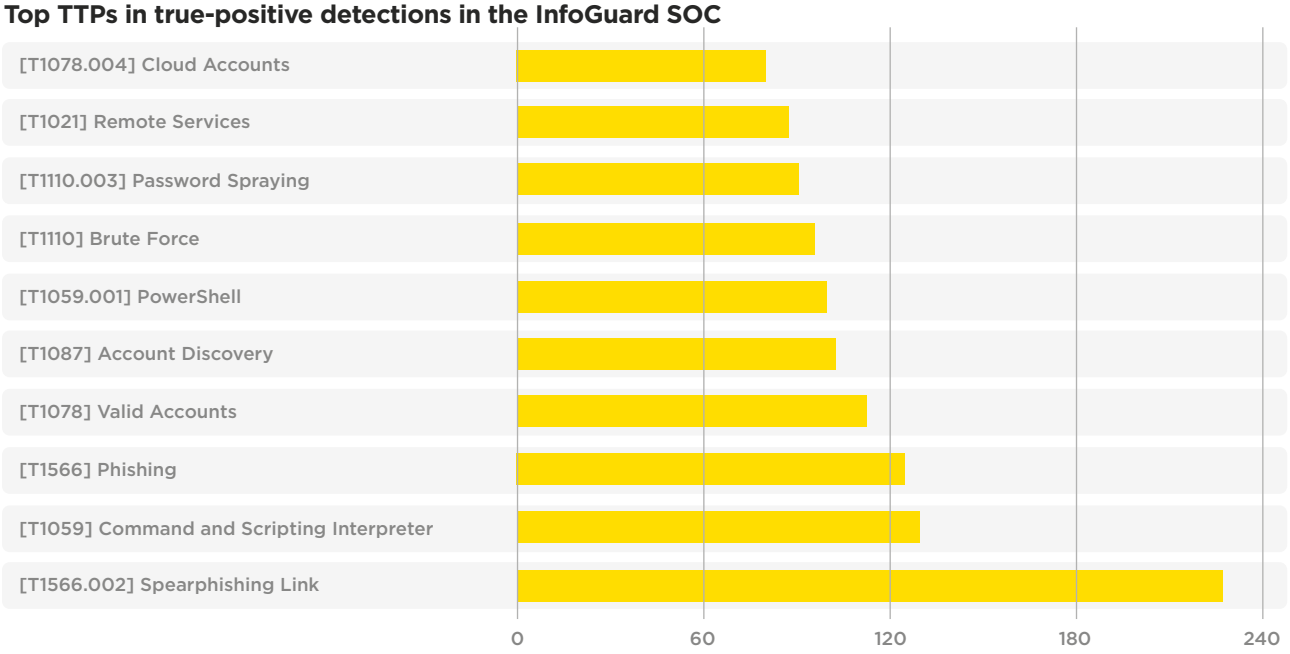
At the same time, it is crucial to manage as many corporate accounts as possible via a central SSO solution in order to increase transparency, control and enforceability of security policies. The InfoGuard SOC also observed various attack paths that attackers can use to take over identities.

The following attack patterns were particularly common:

- ClickFix info stealers; social engineering using familiar captcha dialogs
- Company software advertised via search engines with built in info stealers
- Social engineering targeting decision makers via manipulated online meeting executables with malicious code
- Social engineering targeting developers who unknowingly execute malicious code on corporate systems
- LLM-optimised phishing e mails with high linguistic and contextual credibility

The InfoGuard CSIRT increasingly observed passwords and tokens being stolen on private end devices and subsequently used by attackers against companies. This development is shifting the attack surface into the uncontrollable area outside the corporate infrastructure. For organisations, this leads to a clear consequence: the validity of access tokens on non corporate devices should be kept as short as possible or completely prevented as long as phishing resistant MFA mechanisms are not in use across the board. Otherwise, a persistent access path emerges that largely eludes classic protection mechanisms.

Top TTPs in true-positive detections in the InfoGuard SOC



4.4 State sponsored Actors

In 2025, the InfoGuard CSIRT observed several successful attacks carried out by state sponsored actors. As analysed in the InfoGuard Threat Intelligence Report Q1/2026, these espionage activities are increasingly taking place in the context of geopolitical tensions and are aimed at long term positioning within critical infrastructures and strategically relevant industries. Particular targets included public authorities, the defence industry, energy providers and telecommunications.

Financially motivated state sponsored actors focused primarily on financial institutions, especially crypto banks. State sponsored actors are known to have "unlimited" resources to gain access to corporate networks, as well as the ability to develop highly specialised, tailor made malware that often remains completely undetected in the victim's network. Nevertheless, practice shows that these actors also frequently use known vulnerabilities for initial access – but faster, more targeted and more consistently than typical attack groups.

Within compromised networks, state sponsored actors repeatedly used malware and attack vectors that were not reliably detected by modern EDR solutions or could be specifically bypassed. It can be assumed that these actors are familiar with common monitoring solutions, know how they work and adapt their attacks accordingly.

For affected organisations, this leads to a clear consequence: standardised security architectures alone do not provide sufficient protection against highly sophisticated attackers. Instead, a combination of different XDR technologies is required – such as Endpoint, Network, Identity and Cloud Detection and Response – supplemented by individually developed, organisation specific detection mechanisms that state sponsored actors cannot easily anticipate when testing with off the shelf technologies.

4.5 AI supported Attacks

During the reporting period, AI was still not a magical game changer for attackers, but clearly a measurable efficiency and scaling booster.
From a cyber defence perspective, the use of AI on the attacker side remains difficult to prove directly. Nevertheless, various developments point to a significantly increased use: the rising success rate of phishing attacks as well as the accelerated compromise of edge devices suggest that attackers are deliberately using LLMs to create flawless, context specific phishing e mails which, compared with previous years, have reached a new level of quality. In the exploitation of edge devices, AI supports both the creation of exploits, FUD malware and web shells, and the scaling and automation of attacks through agentic AI.

The peak of what attackers can achieve with AI is still far from reached. For defenders, this means that new attack methods must be identified at an early stage and that both organisational and technical defence mechanisms must be continuously adapted.

The change is particularly evident in the area of social engineering: deepfake voice and video calls are forcing organisations to fundamentally question traditional trust mechanisms. Voices and faces are losing their function as reliable identity characteristics. In virtual interactions, the authenticity of the counterpart should therefore be systematically verified. This can be done, for example, through additional, independent authentication factors or clearly defined verification processes.

5. The seven Key Recommendations for Action for 2026

The analysis of incidents by the InfoGuard CSIRT and the InfoGuard SOC clearly shows in which areas companies need to strengthen their cyber resilience in a targeted and prioritised manner. The focus should be on the following seven areas of action:

1. Identity First

Identities are the central and most frequently exploited attack vector in modern cyber attacks. Companies should therefore consistently use multi factor authentication for all external and sensitive internal services. Phishing resistant MFA methods such as passkeys or FIDO2, strict conditional access policies and monitoring of access tokens help to detect and effectively prevent account takeovers at an early stage.

2. Shorten patch cycles

Companies should keep their patch cycles short and implement security critical updates at the perimeter without delay. After each patch, systems should be specifically checked for any prior compromise in order to avoid a false sense of security created by supposedly closed vulnerabilities.

3. Push zero trust

Zero trust does not end at the perimeter. Even when MFA or ZTNA is used, attackers must not be able to move freely within the network after a compromise. Consistent network segmentation, monitored zone transitions and regular re authentication of user identities are central to containing lateral movement.

4. Extend monitoring

Where the focus in recent years was mainly on monitoring endpoints (EDR) and networks (NDR), monitoring today must also cover identities, cloud resources and exposed APIs. Only a holistic view of all relevant attack surfaces prevents blind spots and significantly shortens the time to detection.

5. Test incident response

Companies should regularly train their incident response capabilities using Tabletop Exercises (TTX). In realistic attack scenarios, teams can rehearse emergencies under seemingly real world conditions, identify technical and organisational weaknesses and derive targeted measures to strengthen cyber resilience, thereby ensuring their ability to act in a crisis.

6. Validate backup strategy

Backups must also withstand a ransomware attack. Companies should therefore check whether attackers are able to delete or manipulate backups. If complete protection is not guaranteed, immutable or physically separated offline backups are essential. At the same time, functioning disaster recovery processes must be tested and verified regularly.

7. Minimise supply chain risk

Software updates, maintenance and supplier accesses should be consistently monitored and restricted. At the same time, the use of non corporate software should be technically controlled, validated or systematically prohibited in order to reduce indirect attack paths via trusted third parties.

6. Conclusion

Cyber attacks in 2026 do not follow a new logic – but a new level of ruthlessness. It is not the sophistication of the attacks that has fundamentally changed, but their speed, scale and precision in exploiting existing weaknesses. The analysis clearly shows: attackers do not primarily use exotic zero days for initial access, but systematically exploit identities, misconfigurations, insufficiently secured remote accesses and blind spots in monitoring. At the same time, attacks are increasingly shifting into areas that lie outside organisations' direct control – such as supply chains, cloud services or private end devices.

The real challenge therefore does not lie in preventing attacks, but in the ability to detect compromises early, interpret them correctly and act decisively.

Organisations that possess these capabilities significantly reduce damage, regardless of whether an attack was successful or not. Companies that lack this visibility, on the other hand, often only detect attacks once operations have already been impaired or data has been exfiltrated.

The central guiding thesis is therefore:

Cyber resilience does not arise from more cyber defence tools, but from consistent visibility, context based analysis and operational ability to act at the decisive moment.

6.1 From reactive Security to proactive Cyber Resilience

To detect attacks at an early stage and to steer them in a targeted manner, organisations need a continuous, up to date view of their own threat situation – tailored to their infrastructure, sector and individual risks. This is precisely where modern threat intelligence comes in: it makes hidden attackers visible, identifies new attack patterns and translates global insights into concrete measures for your own environment.

With InfoGuard's threat intelligence services, you can specifically check whether a compromise has already occurred, identify hidden threats through proactive threat hunting and gain well founded insights into current attacks, actors and tactics.

Detect attackers before they cause damage – and create the basis for sound, proactive security decisions. We look forward to an informal, non binding discussion with you.

Learn more about Threat Intelligence.

The five Key Takeaways

1. Identity is the new perimeter

Attacks today no longer start at the network, but with identities. Prioritise the protection of accounts, tokens and accesses – with phishing resistant MFA, SSO and active identity monitoring. A single set of compromised credentials is enough to cause extensive damage.

2. Speed beats prevention

Attackers are faster than traditional security processes. Consistently shorten patch cycles and actively check systems for existing compromises – even after patching. Reactive security creates a false sense of security.

3. Visibility determines the extent of damage

Attacks rarely fail due to a lack of protective mechanisms, but because they are detected too late. Extend your monitoring to identities, cloud and logs, and ensure sufficient data retention for analysis. Those who see early can act.

4. Incident readiness is a business issue

In an emergency, it does not matter whether plans exist, but whether they are accessible and functional when needed. Test incident response, backup and recovery regularly under realistic conditions. Untested concepts fail under stress.

5. Cyber risks are increasingly arising outside your own control

Supply chains, cloud services and private end devices massively expand the attack surface. Reduce dependencies, control access and consistently monitor external connections. Trust is not a security concept.

Cyber attacks are among the greatest operational risks for businesses.

Take precautions and protect your company around the clock against cyber attacks – fast, professional and reliable. Contact us now for a non binding consultation.

Learn everything about effective Cyber Defence

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Your cyber security
our passion and expertise

Cyber defence and incident response are crucial, but only two aspects of comprehensive and successful cyber security. Our 360° cyber security approach also includes cloud security, managed security & network solutions for IT, OT and cloud infrastructures, penetration testing & red teaming as well as security consulting services. The SOC services are provided from the ISO 27001 certified and ISAE 3000 Type 2 audited Cyber Defence Center (CDC) in Switzerland and from Germany – with 24/7 operation and continuous staffing.

2001
Over 25 Years of Experience and Expertise

100%
Independent

350+
Security Experts

6
Locations in Baar, Bern, Frankfurt, Munich, Düsseldorf and Vienna

24/7
Real time monitoring and emergency intervention

2x SOC in CH & DE
24/7 Security Operations Center in Switzerland and Germany

CSIRT Computer Security Incident Response Team
BSI-qualified APT response service provider and FIRST member

ISO 27001
ISO 14001
ISAE 3000 Type 2

Do you have a security incident?
We support you at any time – quickly, competently and with extensive experience.

+41 41 749 24 24

DE +49 896 142 9677

AT +43 1 442 0177

investigations@infoguard.ch

Baar (Head Office)
InfoGuard AG, Lindenstrasse 10, 6340 Baar, Switzerland, +41 41 749 19 00, info@infoguard.ch, infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Switzerland
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

Frankfurt
InfoGuard Deutschland GmbH
Frankfurter Straße 233
63263 Neu-Isenburg
Germany
+49 6102 7840 0
info@infoguard.de
infoguard.de

Munich
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 Munich
Germany
+49 896 142 9660
info@infoguard.de
infoguard.de

Düsseldorf
InfoGuard Deutschland GmbH
Am Gierath 20A
40885 Ratingen
Germany
+49 2102 5789 800
info@infoguard.de
infoguard.de

Vienna
InfoGuard GmbH
Kohlmarkt 8-10
1010 Vienna
Austria
+43 1 442 0170
info@infoguard.at
infoguard.at