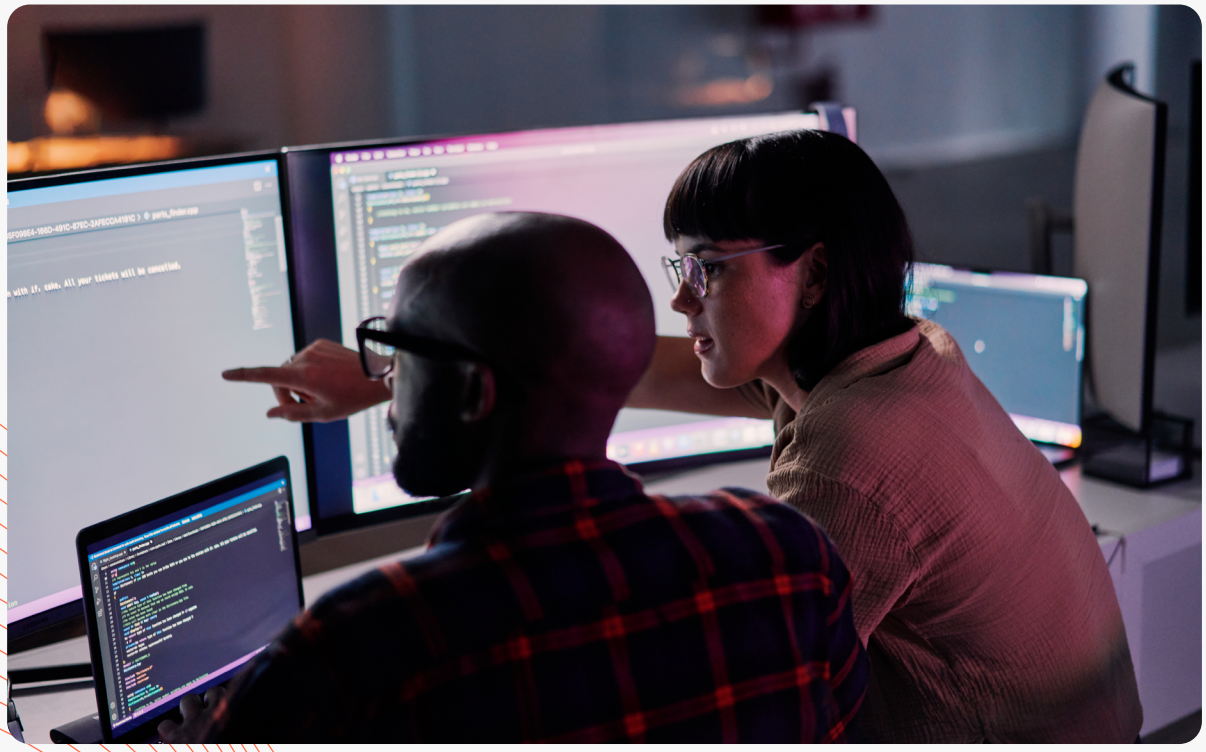
valantic

WHEN EVERY SECOND COUNTS

Disaster
Cyber Attack

What to do when a disaster strikes...



Inhalt

Foreword

valantic Management Consulting is a 100% percent valantic group company that advises customers needing advice where IT and business expertise overlap. Covering everything from A as in Application use case to Z as in Zero day exploit, data protection also plays a central role, with over one hundred companies currently employing us as their external data protection officer.

In this Whitepaper, we would like to give you the opportunity to learn from the experiences of others, using the example of an actual cyber compromise of a typical – but unnamed – German hidden champion that fell victim to a ransomware attack. In the case concerned, ransomware (also known as an extortion Trojan, extortion software or encryption Trojan) encrypted the IT systems, thereby rendering them unusable.

It quickly became clear that an experienced partner was needed to analyze the attack and get the systems up and running again. Unfortunately, this is not a rare occurrence. The total amount of damage to German companies caused by cybercrime reached a record value of over 266 billion euros in 2024. Of this, 13.4 billion euros were attributable to the costs of extortion with stolen or encrypted data (Statista, 2024).

This is because well-known companies and many public authorities are now also affected by cybercrime and IT attacks. "Authorities warn of mass ransomware attacks", headlined the SZ (Muth, 2023). The APT28 group, which is attributed to the Russian secret service, is considered responsible for the hacker attack on the SPD party headquarters in May 2024. The CDU network was also affected this year by the "most serious attack on an IT structure that a political party in Germany has ever experienced" (Brecht, 2024).

If your company would like to take precautions to avoid a scenario such as the one described in this Whitepaper, or you have perhaps even just been targeted by a cyber attack, we can help you at once with our expertise and experience. Please do not hesitate to contact us.

Stay alert!

Yours Thomas Lang

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.

Just another morning...

It often starts with the IT department noticing irregularities early in the morning. At this point, no one really believes that something like this could happen to them. Until the bitter realization sets in and the first "oh-oh" moment occurs: We're the target of a cyber attack. Network connections soon disconnect, systems shut down, and superiors and top-level management are informed.

As staff begin to come to terms with what has happened, valantic consultants' phones start to ring with requests for concrete courses of action, contacts to forensic experts and active crisis management. When such calls are received, one thing is clear: Everything must happen in a flash, and a consultant generally needs to be dispatched to the customer's premises ASAP.

After the initial shock

Documenting evidence and the course of events

At the scene of the incident, you can literally cut the air with a knife. On the way to the meeting room, which is converted into a **„cyber war room"** over the next few days, you pass abandoned workstations, and doors, some of which cannot be locked, others which cannot be released – since most of the access control systems have failed. Your first impression is that absolutely nothing is working here at the moment.

After that, things get going as systematically as possible:

- Names and roles are documented
- What happened – sequence, chronology?
- Has an extortion note been received?
- Who was informed how, when, by whom and with what content (customers, business partners, public authorities)?
- What backup modalities are available?
- When was the last "clean" backup made, for example, by removing tapes to a remote location?

These and other questions are asked and worked through urgently, but methodically, since one thing is clear: every minute costs money.

Blue Yonder (USA) – Impact on Starbucks and other retailers

In November 2024, the US software provider Blue Yonder was the victim of a ransomware attack. As Blue Yonder acts as a supply chain management service provider for companies such as Starbucks, Morrisons and Sainsbury's, the attack caused significant operational disruption for these retailers. Starbucks, for example, had to manually track the working hours of its employees.

Source: The Associated Press, 2024

Important measures?

Almost all the essential systems were encrypted in the abovementioned cases, resulting in business operations grinding to a complete halt. Hundreds to thousands of employees had to be sent home and customer orders could no longer be processed. Not only the clock, but above all the "money meter", was ticking. At that moment, every minute was costing money – and lots of it – with "money" being the operative word here: For the black-mailers were demanding a ransom – only then would the systems be decrypted and become usable again.

Other questions to bear in mind:

- Has your company already addressed the question of how to respond to extortion?
- Do response plans exist if members of the owning family are affected or, even more perfidiously, threats are made to contaminate products?
- Are management and board members aware that they will be listed as a "paying victim" on the Darknet after yielding to a ransom demand?
- Does your company have a Bitcoin account?
- Do you want to involve the public authorities (criminal police, the state office of criminal investigation or even the Office for the Protection of the Constitution)?

It takes some time for the responsible persons to realize the extent and potential threat. In addition, valantic's consultants must point out the 72-hour deadline within which a report must be made to the data protection authority after a data breach becomes known.

Südwestfalen-IT – Attack by Akira

At the end of October 2024, the Akira ransomware group paralyzed over 70 municipalities in North Rhine-Westphalia by attacking the IT service provider Südwestfalen-IT. Administrative activities in the affected municipalities largely came to a standstill and many citizen services had to be closed. The recovery work is still ongoing today. The threat actors behind the new name appear to be old acquaintances from the scene. Process analyses of the malicious code circulating since March 2023 point to the former Conti masterminds.

Source: B2B Cyber Security, 2023

To pay or not to pay?

Whenever a ransomware attack occurs, the one decisive question always arises: To pay or not to pay the ransom? The answer will ultimately lie in whether the company's IT can be fully reinstated without paying a ransom, leaving the affected companies with two options to choose from:

The "No-Pay" scenario – Advantages and disadvantages

The No-Pay scenario assumes that the company can restart its IT systems itself by purging the infected systems and importing existing backups. An extremely methodical and meticulous approach is critical here. Even if all the systems can be restored from back-ups, the risk remains that the attackers have concealed a key somewhere deep down in the system – buzzword: **Golden Ticket**. Since no company wishes to expose itself to this risk, this scenario generally boils down to the installation of new, clean copies of all the systems in conjunction with modern defense and containment systems.

The "Pay" scenario – Advantages and disadvantages

The Pay scenario involves paying the extortionists, taking critical systems back into operation in an entirely isolated new environment, and "hand-picking" the data to be imported into that new environment. Because here, too, it's clear: **You'll never again fully trust a system that was once accessed illicitly using administrative rights.**

You might be wondering at this point why anyone would even consider paying an extortionist? In one of the cases, the situation was as follows:

- Daily backups were made to disk – but all the disks were also encrypted
- Weekly backups were made to tape
- Each month, tapes were removed from the tape library for remote storage

No-pay and pay scenarios present both risks and challenges in terms of future security and trust.

After detailed analysis, it was concluded that a three-week data gap could not be bridged. The attackers had been rummaging their way through the network for several weeks, spending a great deal of time mounting and erasing every single available tape in the tape library. In precisely those past few weeks, the company had been involved heavily in product development and pre-planning activities. Even a specialist data recovery firm was unable to restore the erased tapes, ultimately leaving the board members with no other alternative than to pay.

Also important to contemplate is that the capitulation path is not without complications: The time between the first contact with the extortionists and provision of the key to decrypt your data can be anywhere from 48 to 72 hours.

There are two other things to consider at this point:

1. Decrypting the data can take up to several days, depending on data volume.

2. How long would it take you to obtain a six- to seven-digit Bitcoin amount? True, there are exchanges where you can buy crypto-currencies. But the basic laws of supply and demand apply there as well, ultimately determining the price. It's therefore advisable to buy in many smaller margin tranches to avoid driving up your own costs. This too takes time.

Regular backups to protect against data loss

Regular backups can protect against data loss and unusable data. As a rule, a time-consuming full backup is only necessary once, at the very beginning. After that, it suffices to back up the so-called delta, i. e. data that have changed or been newly added since the last backup. It is important to make regular backups and store them fully isolated, without any network connection to the productive IT systems; in this way, the backups cannot be infected by a cyber attack.

Disaster Contingencies

It's a nail-biting tale, isn't it? The questions remain, however: How can one prevent such a situation? And how can one prepare for the eventuality of a disaster that cannot be entirely ruled out?

This requires a number of precautions to be taken and some questions to be answered beforehand:

- Would you be willing to yield to an extortionist's payment demands: Yes or No?
- Business Continuity Management (BCM): Do you have a security concept and disaster recovery plans for maintaining production and handling customer requests?
- Are crisis management and communication, including the responsibilities during a crisis, structured?
- Is it ensured that the affected systems can be quickly isolated and reinstated when disaster strikes?
- Is your company well equipped to collect evidence and document the course of events?

Geo-redundant data: Security with hidden risks

Cloud providers and data center operators generally offer their customers tiered security concepts tailored to their individual requirements. The complete, geo-redundant mirroring of data to the storage media of a second data center is very secure, but also costintensive. However, even geo-redundant mirroring offers little protection against so-called sleepers, i. e. crypto Trojans that only become active from a certain date in the future. This is because the "sleeper" has already been mirrored to the second backup data center and renders the data there unusable as well. Incidentally, this can also happen with backup tapes. During the next "restore", the "sleeper" wakes up and infects the data on the backups.

Update on the above disaster:

Cybercriminals increasing the pressure on companies

Cybercriminals have significantly leveraged their extortion potential in recent months. Not only do they continue to encrypt the data of the target company, making it unusable for further processing, but they are now also stealing sensitive data – such as employee files, design plans and market strategies – that should not fall into the hands of the competition. This is placing affected companies under much greater pressure since the attackers hold several trump cards in their hands.

Potential harm is not, however, limited to the compromised companies alone: Where cybercriminals obtain copies of employees' ID cards on HR servers, for example, this sensitive information could be used by human traffickers to forge documents for refugees, giving them illegal entry to the country. Secret recipes for popular fitness drinks, blueprints for innovations or other highly market relevant data are other examples of intellectual property that should be better kept out of unauthorized hands.

Companies are not, however, entirely defenseless in face of these risks: the latest generation of artificial intelligence-based virus scanners, which monitor end devices and IT systems 24x7 and raise an alarm when an anomaly is detected, already offer a high level of protection. Heuristic probability calculations, typical workload scenarios and atypical usage patterns are among the arsenal of countermeasures available here. In most cases, the infiltrated malware or ransomware can be isolated, preventing it from spreading to other IT subsystems and minimizing the damage. Companies should therefore optimize their defense strategy as much as possible. valantic recommends combining technology-based attack prevention techniques with organizational measures in a targeted manner: If an AI scanner raises an alarm, for example, a human security expert should initiate further antiintrusion and countermeasures and inform management and employees as quickly as possible. With such an approach, serious damage can usually be effectively prevented.

Conclusion

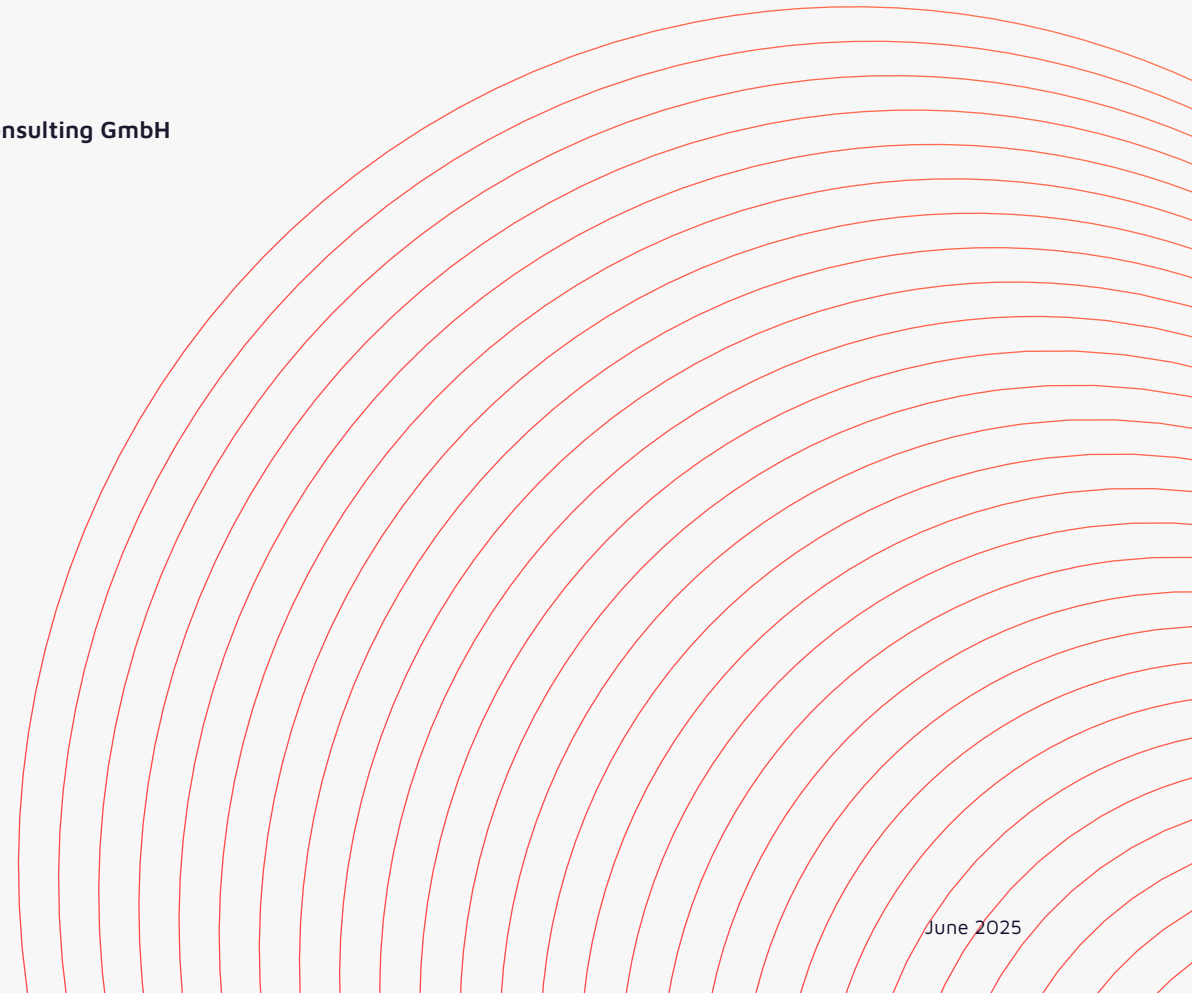
At the moment, the topic of cybercrime is more acute than ever, with case numbers rising steadily and ransom amounts, such as those demanded in ransomware attacks, becoming larger and larger. It is therefore advisable – well before an attack occurs – to implement a comprehensive security and disaster recovery management system and a business continuity concept, and decide on how best to respond, should disaster strike. If you'd like to learn more about how to effectively protect your own company, we'd be delighted to talk to you without any obligation on your part.

valantic

valantic Management Consulting GmbH
Dreieich Plaza 2A
63303 Dreieich
Germany

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

www.valantic.com



June 2025