THINKING AHEAD PAYS OFF

Crime Scene Cyberattack: How Companies Can Protect Themselves From Lost Revenue and Losses

valantic

Dear reader,

As an experienced breach coach and cybersecurity consultant, I'm often asked for advice by organizations when things are already on fire. This is when the worst-case scenario has occurred, and the usual scenario my team and I are faced with is as follows: A cyber attack has been successful and has very far-reaching consequences for the company. Revenue-relevant IT systems and business processes fail - usually completely. Nothing works anymore.

The top priority for attacked companies is, of course, to get the affected systems up and running again as quickly as possible. In our experience, however, the obvious approach of rebuilding the entire compromised IT system as if it were a greenfield site is very time-consuming and cost-intensive. And every lost day costs a lot of money.

In this white paper, we would therefore like to introduce you to a smarter, faster and yet secure alternative to minimize the monetary consequences of a cyberattack and resume normal business operations as quickly as possible. Speaking from experience, we have implemented this method with great success at many companies that have been attacked in recent years.

Thinking of tomorrow today

Above all, preventive measures can effectively prevent loss of sales and losses. The best response to a cyber attack is undoubtedly to prevent it from happening in the first place. Darknet monitoring has proven to be an effective protective measure that can be used to detect cybercriminal attacks in advance. Further important details can be found in this white paper.

If you have any further questions, please feel free to contact me. My team and I will be happy to provide you with advice and assistance for an initial consultation and threat analysis.

Until then, I wish all readers an exciting, useful and inspiring read.

Yours sincerely, Thomas Lang

Thomas Lang
Partner & Managing Director

+49 6103 5086-0
thomas.lang@mc.valantic.com
www.valantic.com

Contents

The current situation

Cybersecurity is concerned with protecting computer systems, networks and data from digital threats. It is not just about protecting against unauthorised access, but also about ensuring the integrity, availability and confidentiality of data. The dangers that companies face range from malware, attempts at deception and extortionate ransomware attacks to sophisticated 'man-in-the-middle' attacks in which internal company communication channels are eavesdropped on. Each of these attacks can cause significant financial losses, damage a company's reputation and have legal consequences. Establishing sufficient resilience is therefore important for every company.

With its annual report on the state of cybersecurity in Germany, the Federal Office for Information Security (BSI) provides a comprehensive overview of the threats in cyberspace. In the report for 2023, the federal cyber security authority concludes that the threat in cyberspace is higher than ever before.

Increasingly, not only large, financially strong companies, but also small and medium-sized enterprises are in the attackers' crosshairs. The BSI has recorded a sharp increase in activity compared to the previous year, particularly in ransomware attacks, which use encryption to render the data and IT systems of attacked companies unusable.

In order to decrypt systems and data after a ransomware attack, cyber criminals usually demand a high ransom based on the value of the victim's company. To further increase the pressure, a second attack vector is becoming increasingly popular. The criminals have taken possession of sensitive company data and threaten to publish the stolen material.

The BSI offers three pieces of advice to prevent losses and damage:

- Companies should increase their cybersecurity and business continuity resilience as quickly as possible to prevent and be prepared for attacks.
- Cybersecurity must be actively organised in order to get ‘ahead of the wave’.
- In general, it is important to push ahead with digitalization. This is the only way for German companies to remain secure and competitive in the technologies of the future. This includes technologies such as artificial intelligence (AI), the cloud, eID (electronic online ID) and smart metering.

The ‘greenfield’ approach – sounds good, but is time-consuming and cost-intensive

Let‘s assume that cyber criminals have been successful with their attack, have penetrated a company‘s IT networks and have paralysed a large part or, in the worst case, all systems from enterprise resource planning (ERP) to warehouse management and point-of-sale systems. Normal business operations come to a standstill and the priority of the management and executive board is to at least get all time-critical business processes up and running again as quickly as possible.

The approach of reorganising the entire IT system, including all networks and desktop computers, laptops, switches and routers, seems obvious at first glance. At first glance, this method of reorganising the entire IT as if on a greenfield site is obvious. However, it is also very time-consuming and extremely cost-intensive. We know from our experience as breach coaches and security consultants that the effort and, above all, the complexity involved is usually significantly underestimated by the companies affected.

A practical example illustrates this: At one company that was successfully attacked, a total of 700 servers and around 7,000 desktop PCs and laptops were affected. Based on the very optimistic assumption that the complete reinstallation per computer and server takes around one hour, the time required for the ‘greenfield’ approach would be 7,700 hours, i.e. around 3 ½ to four man-years. One thing is certain: in this way, revenue-relevant business processes cannot be put back into productive use quickly enough.

The better, faster and safer alternative: securing existing systems

Restarting after a cyberattack is faster, better and safer by securing existing systems and continuing to use them. As breach coaches and security consultants who are called in to help in crisis situations, we have already successfully implemented this method many times. Incident response service providers who are familiar with this solution have proven themselves even under the toughest conditions.

Such an incident response or advanced persistent thread service provider cleans the existing IT system, reacts immediately to malware or other attack vectors that may still be in the system and renders them harmless. This means that backups – which may also be infected – do not have to be restored and the entire IT architecture, including infrastructure and other components, does not have to be re-planned and deployed. Only the systems that were completely destroyed by the attacker are rebuilt or 'restored'. Clients in particular are often not or only partially affected by encryption. If you save yourself the reinstallation in our calculation example above, the time advantage is enormous.

One of our client companies was able to set a new production record just one month after the cyberattack. With the "greenfield" approach, such successes are beyond the realm of the achievable and possible due to the immensely increased time and costs involved.

Unfortunately, in practice we often see emotionally influenced decisions being made after a ransomware attack. The rebuild sounds as logical as it is imperative to ensure a safe restart. On a side note, the consultants who strongly recommend this are often the ones who benefit from this approach, as they can be sure of a large amount of work for weeks and months.

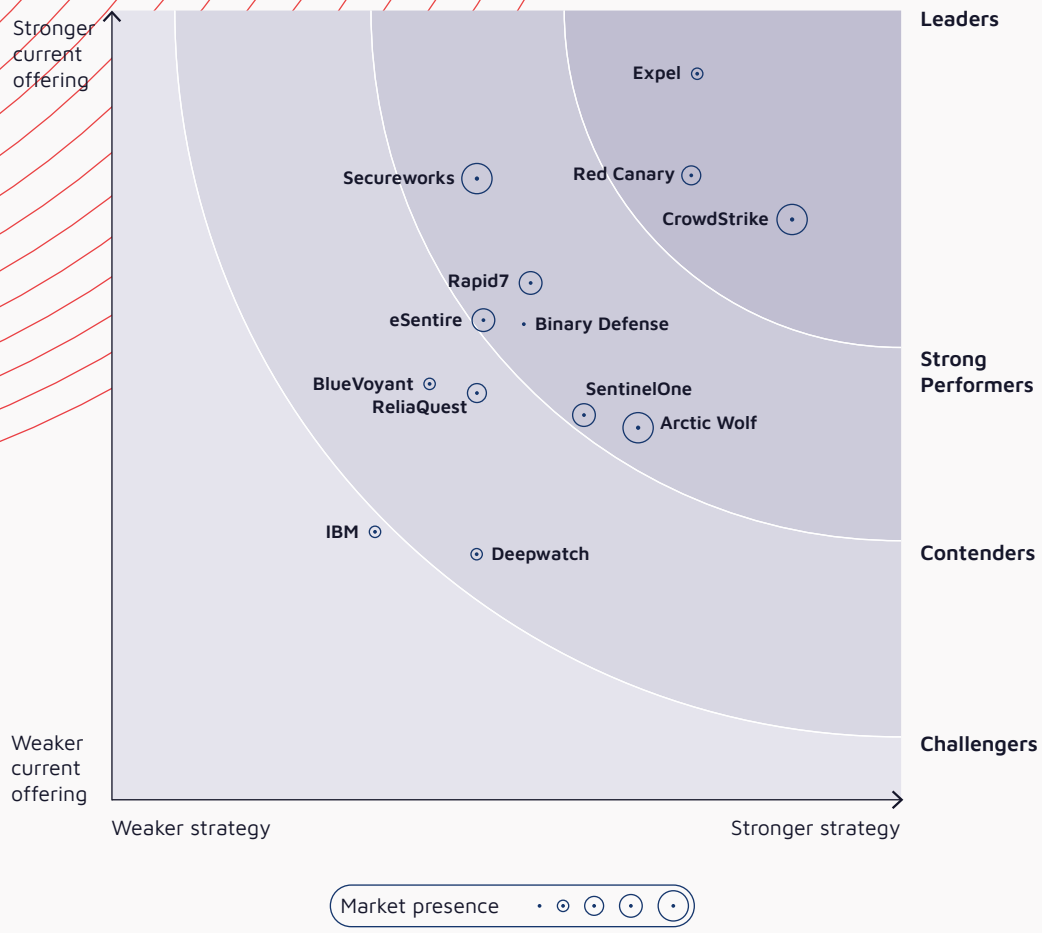
We therefore strongly recommend keeping abreast of developments. Successes, such as the case described above, are not achieved by chance. They become possible when companies are supported by experienced consultants in the event of a crisis who, in the best interests of the customer and using the latest technical possibilities, point out the options, make risks calculable and thus enable business operations to be restarted safely and quickly.

The recommendations of the BSI and leading analyst firms

Incident response service providers – also known as APT response providers – provide a high level of security more quickly, thereby minimizing revenue losses and protecting companies from cyber threats in the future. In order to increase transparency on the market and make it easier for companies to select providers, the German Federal Office for Information Security (BSI) has put APT providers through their paces.

The thorough evaluation process was divided into two phases:

1. **Review of the documentation provided by the service provider**
   The service provider first had to provide complete documentation. This included descriptions of the products and services as well as explanations regarding compliance with the criteria set by the BSI. It was also possible to provide existing certifications from data centers or the company itself.



Quelle: The Forrester Wave: Managed Detection and Response 2023

2. Conducting a technical interview
In a meeting lasting several hours at the BSI, the service provider had to demonstrate its ability to handle the situations in a professional and targeted manner using fictitious scenarios. Attention was paid to the service provider's general approach as well as the questions asked and the processing of the information received.

A complete list of all APT response service providers evaluated by the BSI and recognized as particularly reliable can be found on the BSI website. CrowdStrike (Nasdaq: CRWD), with whom valantic works closely, is one of these BSI-qualified APT response service providers.

CrowdStrike has been recognized as a Leader in Managed Detection and Response Services by leading analyst firms such as Gartner and Forrester. Forrester writes about CrowdStrike in its "Managed Detection and Response (MDR)" report 2023:

"CrowdStrike seamlessly connects products, platforms and services for its customers. Few companies can boast such a successful track record as CrowdStrike. The service provider has become an outstanding incident response company and a dominant player in the endpoint security space. CrowdStrike provides an exceptional MDR service and has shown cybersecurity firms how Software-as-a-Service (SaaS) companies work. CrowdStrike's comprehensive view of the threat landscape and incident response services give the organization an edge when it comes to threat intelligence and managed detection."

Darknet Monitoring – staying one step ahead of cyber criminals

As already mentioned, the best response to cyberattacks is to prevent a successful attack from occurring in the first place. Darknet monitoring offers the opportunity to detect attacks in the preparatory phase before major damage can occur and thus stay one step ahead of the cyber criminals.

A brief background to cybercrime: stolen and often confidential data, logins, PINs, passwords, identities or e-mail access are traded on the darknet, the invisible, not easily accessible part of the World Wide Web. Today, cybercrime is highly professionally organized, which is why "professional groups" based on a division of labour have emerged among hackers. Particularly exciting are the initial access brokers, the real estate agents of the darknet, so to speak. They offer the fraudulent accesses for sale in darknet forums, similar to an eBay marketplace. The buyer, i.e. the actual cyber attacker, uses the purchased accesses for the actual attack, for example to encrypt IT systems and demand a ransom.

Insurance case study: Cyber attack foiled

In the course of their research on the darknet, our security experts came across the access data of a large German insurance company that was being offered for sale on one of the marketplaces. Naturally, the security specialists immediately reported the "find" to the insurance company. There is usually some time between the sale of the data and the attack. The company was therefore able to initiate protective measures in good time and thwart the attack.

Such information, researched through darknet monitoring using the latest technology, is worth its weight in gold. It helps to prevent damage running into millions.

Conclusion & advice

As experienced cybersecurity consultants, we enable the executive board, management and IT management to make well-founded, independent decisions. As experienced cybersecurity consultants, we enable the executive board, management and IT management to make well-founded, independent decisions. Thinking ahead pays off: Companies should decide in advance what is best to do in an emergency. Both a business impact analysis to evaluate business processes and a risk profile tailored to your company that identifies and secures weak points can help. We are happy to support you with our many years of expertise and experience from dozens of successfully implemented cybersecurity projects.

Thomas Lang is Partner and Managing Director of valantic Management Consulting GmbH. Prior to valantic, he founded several companies in the service industry and gained more than 20 years of IT experience, including 15 years in consulting.

Thomas Lang
Partner & Managing Director
+49 6103 5086-0
thomas.lang@mc.valantic.com
www.valantic.com

valantic

valantic Management Consulting GmbH
Dreieich Plaza 2A
63303 Dreieich
Deutschland

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

www.valantic.com

April 2025