FAST LTA

Factcheck

The importance of rapid recovery after cyberattacks

Since: March 2025

While the global damage from cyber attacks was $3 trillion in 2015, this figure is expected to more than triple by 2024[1]. In Germany alone, damages from data theft, industrial espionage and sabotage reached an alarming record of 266 billion euros[2].

Ransomware attacks in particular are increasingly filling cybercriminals‘ wallets: According to a survey by Bitkom (Germany’s digital economy trade association), six in 10 companies were targeted by such an attack between September 2023 and September 2024. Almost one in three companies in Germany (31%) suffered damage in the form of production downtime, costs for IT service providers or payments to the perpetrators.

Only 40% of affected companies were able to recover the data themselves. The recommendation of Felix Kuhlenkamp, head of security policy at Bitkom e.V., therefore comes as no surprise: „All companies should step up their technical IT security, train employees to **recognise attacks at an early stage and, above all, make regular backups.**“

But backups alone are not enough.

It is not only crucial that data is backed up, but also that recovery strategies work smoothly in case of emergency. The speed of the recovery process also plays an important role, as any delay multiplies the economic damage caused by downtime.

Fact

This is the duration it takes organisations to recover

The time to fully recover from a cyber attack takes an average of 7.3 months globally, with 5% of organisations taking more than 18 months and 1% assuming full recovery never happens[3].

If we isolate the data from the global survey for the DACH region alone, the picture is even gloomier: On average here, it takes 8.6 months to make a full recovery, with 7% taking more than 18 months and 2% assuming that a full recovery will never happen[4].

However, well-prepared organisations recover from security breaches 41% faster than less well-prepared organisations. The Cyber Recovery Readiness Report lists 5 criteria that significantly reduce not only the risks but also the impact of security breaches:

1. **Early warning systems**

   Use of security tools for early detection of cyber risks.

2. **Isolated location for emergencies**

   Provision of a separate, secure environment for rapid recovery of operations after cyber attacks.

3. **Immutable data backup**

   Maintaining isolated, tamper-proof data backup in a remote infrastructure.

4. **Structured response**

   Defined contingency plans, roles and processes for efficient response to cyber incidents.

5. **Measurable preparedness**

   Regular recovery exercises and risk assessments to test the effectiveness of plans and identify potential weaknesses.

Fact

Here is how much a security breach costs

The cost of production downtime depends largely on the duration and size of the company. A company with 100 employees, 70% production and an average hourly wage of 35 euros already faces downtime costs of 100 × 35 × 0.7 = 2,450 euros per hour.

For large companies, this can quickly result in damages running into millions. Even the sky is not the limit - as data from Delta Airlines proves. When the airline‘s data centre was down for 5 hours, the damage already amounted to $150 million dollar[5].

And it was just a power outage, without the added cost of a security breach:

- IT overtime for recovery
- External cyber experts for forensic investigations
- PR budget for crisis communication with employees, business partners and the public[7]

Lost customer trust

However, the financial impact of cybercrime goes far beyond the direct costs mentioned above. Companies that fall victim to security breaches often face long-term reputational damage, reduced customer trust and higher customer acquisition costs: 65% of consumers say they would lose trust in a company after a data breach, and 85% would no longer do business with a company if they were concerned about its security practices[6].

While the figures say nothing about the impact of recovery time on customer trust, one thing is clear: a quick recovery can help reassure customers and is already a first step in regaining lost trust.

Falling stock prices

With the loss of customer and investor confidence, the share price is also falling. According to an analysis by Morningstar, the share price drops 2-3% within the first 4 days of the announcement. Although a few companies recover after only 12 days, in most cases the share price continues to plummet, reaching its lowest point on average after 59 days, with a 5.3% loss in value relative to the sector index. While the sector indices of the analysed companies recorded an average gain of 10.15% after a year, the companies that fell victim to a cyber attack recorded a loss in value of 0.65%.

With the Data Privacy and Security (DP&S) Management Score, Morningstar has another risk assessment tool. While investment experts do not openly communicate exactly how this is calculated, it should not be too different from the MSCI calculation. It includes several factors that also have an indirect impact on recovery rates and are very reminiscent of the five criteria mentioned at the beginning. For example, employee training, responsibilities and the scope and nature of the emergency plan are assessed for this score.

The difference between companies with a high DP&S Management Score and those with a low score was significant: while companies with a score of 0 or no score at all were on average 12.42 percentage points behind their sector after one year, those with a score of 75 or higher were almost on par with their sector (-1,74[8]).

Organisational challenges

In the days following a cyber-attack, affected companies are in a state of emergency. They are under enormous pressure to get back online as soon as possible for the reasons mentioned above. Paradoxically, recovering too quickly can lead to already compromised systems being reactivated and compound the damage. Responding with the necessary expertise requires a cool head and under no circumstances hasty expertise, which is increasingly lacking in times of shortage of skilled personnel.

In late 2022, the BSI (German Federal Office for Cybersecurity) warned of a ‘fundamental shortage’ of incident response staff. Particularly serious: even external experts are „sometimes fully staffed and then unable to accept new incidents“.[9] The search for expertise alone threatens to bring the company to a standstill.

Cyber recovery is a labour-intensive process that requires not only the expertise of IT specialists. Managers, the legal department, communications teams and sometimes even law enforcement agencies also need to be involved. A clear division of roles and responsibilities is essential for a successful recovery. An effective recovery plan should clearly define which people are responsible for which functions.

Success factors for rapid recovery

„Our research shows that the companies with the best cyber resilience are those that continuously test and optimise their recovery strategies. They learn from every security incident and strengthen their defences," said Commvault CTO Brian Brockway, referring to the Cyber Recovery Readiness Report[10]. However, lessons can also be learned from incidents at other companies.

Case study Maersk

4 million containers, 1,000 warehouses, 900 ships, 1 malware. The NotPetya attack, originally targeting Ukraine, exploited a compromised update of Ukrainian operating software M.E.Doc in 2017 and also infected global companies - including Maersk. After the malware managed to access domain administrators' credentials, it quickly spread throughout the network.

At 10am, Maersk's network monitoring team noticed the first irregularities, before the connection to the global network monitoring centre in the UK went down completely shortly afterwards. The entire network was immediately shut down, but by then 49,000 laptops and computers had been infected and 1,200 business-critical applications had become inaccessible. The entire Active Directory appeared to be lost, phone directories had been synchronised and therefore also disappeared. Maersk had lost its global communication capacity and initially had no clarity on the nature and extent of the attack.

The next morning, Microsoft had managed to decrypt one computer, but this took 22,000 hours of computation and the code only helped this one device. Decryption on a large scale was therefore impossible. Trying to recover lost data was also too risky, as this could also reactivate the malware. The only option was to start all over again.

A lucky coincidence came to Maersk's rescue in the form of a power failure in Lagos, Nigeria. The office there was offline at the time of the attack and had a complete, unencrypted copy of the Active Directory, which formed the basis for rebuilding the entire network.

After 14 days, Maersk had restored basic business technology and was operational again, albeit with reduced volume. It took another four weeks to reach full capacity, mainly due to the purchase of 17,000 new end devices. In total, the incident caused $350 million worth of damage.

Lessons learnt

Partnerships, transparency and resilience

Maersk has learned crucial lessons from the incident, which have been integrated into the company culture and security strategy. The key “lessons learnt,” which are also essential for other companies, can be summarized as follows:

Partnerships are crucial

From the outset, Maersk relied on external expertise. Deloitte was chosen as the forensic partner, not because of an extensive evaluation process, but due to geographic proximity and the rapid availability of resources. Support from technology partners such as IBM and Microsoft in the global distribution of data was essential for the swift reconstruction.

Transparency builds trust and support

Maersk opted for open communication, both internally and externally. Regular video updates kept employees and customers informed. External transparency played a significant role in gaining goodwill and even concrete support from other companies, for example in the form of borrowed Azure cloud experts.

Focus on recovery capabilities

The ability to quickly restore critical infrastructure such as Active Directory, DHCP, and DNS is vital for survival. Maersk needed 14 days to restore basic business technology. Now, everything is focused on being able to operate again within just 24 hours.

Resilience through redundancy and backup

The accidental Lagos backup highlights the importance of redundant systems and up-to-date, offline backups of critical infrastructure components such as Active Directory.[11]

Conclusion

The available data shows a significant increase in economic losses due to cybercrime, both globally and in Europe. The amount of damage has more than tripled in just a few years, with ransomware attacks in particular posing a growing threat to businesses.

A major area of concern is the time companies need to fully recover from cyberattacks. The global average is more than seven months, and even longer in the German speaking (DACH) region. This prolonged downtime results in substantial costs due to production loss, IT recovery measures, and reputational damage.

References

1 https://cybersecurityventures.com/cybersecurity-almanac-2024/

2 https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/

3 https://learn.fastly.com/rs/025-XKO-469/images/Global%20Report%202024%20-%20Global%20Deck.pdf?version=0

4 https://learn.fastly.com/rs/025-XKO-469/images/DACH%20%20Deck%20-%20Global%20Report%202024%20.pdf?version=0

5 https://www.five9sdigital.com/knowledge/delta-airlines-our-5-hour-data-center-outage-cost-us-usd150m/

6 https://www.kiteworks.com/de/cybersecurity-risikomanagement/anstieg-von-cyberangriffen-um-92-in-zwei-jahren-der-risiko-score-index-2024-enthuellt-alarmierende-trends/

7 https://www.techbold.at/blog/die-ransomware-rechnung-was-ein-hackerangriff-in-summe-kostet

8 https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/analysis-strong-data-privacy-and-security-management-pays-off

9 https://www.handelsblatt.com/technik/it-internet/it-sicherheit-an-der-belastungsgrenze-experten-fuer-die-cyberabwehr-werden-knapp/28881154.html

10 https://ap-verlag.de/cyberresilienz-und-cyber-recovery-vorbereitung-zahlt-sich-aus/90581/

11 https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html

FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**