Finlex

Claims examples
Cyber

Economic life is becoming increasingly digital due to rising data volumes and increasing connectivity in the value chain. For companies, this brings both opportunities and risks. IT, cyber and information security has become one of the top issues for business managers. Even with a defined IT, cyber and information security policy, and proper delegation of implementation to employees or external service providers, the responsibility and liability remains with the management.

Cyber incidents are no longer a rarity and affect every company – regardless of size and sector. The causes of damage range from the negligent use of mobile devices by employees, such as smartphones or laptops, to targeted professional and criminally motivated attacks on the IT infrastructure of a company, sometimes prepared over a long period of time.

There are countless possible claim scenarios of cyber incidents. We have compiled below a selection of typical loss events in which the cyber insurer has provided cover.

→ Malware:

By clicking on an infected email attachment, the system (including production IT) of an automotive supplier was infected with malware. As a result, the machines stood still for days. The costs for the clean-up and recovery of the system as well as the business interruption damage amounted to several hundred thousand euros.

→ Microsoft-Security Breach:

Due to a Microsoft security breach, a damaging malware got into the system of a housing association (Hafnium Hack). However, the malware had not yet been activated and could be removed from the system by IT forensic experts. The costs for the removal were in the five-digit range.

→ Spam:

Through a targeted attack on the online presence of a small business, the server was manipulated and used for sending spam mails. Various customers complained about the dubious mails and threatened to sue. The IT forensic expert recommended by the insurer was able to quickly find the cause, clean up the system and stop the distribution. A PR agency managed the apology or justification to the customers.

→ Ransomware I – Encryption:

Due to a security breach, a hacker group was able to gain access to the IT system of a medium-sized mechanical engineering company and install encryption software. The company stood still for several days. After paying a ransom, the hackers decrypted the systems. The costs for the ransom and the business interruption amounted to several million euros.

→ Ransomware II – Publication of Data

A group of hackers deliberately gained access to sensitive customer data belonging to a medium-sized industrial company. The hackers threatened to release the data, which would have caused significant reputational damage and the loss of major contracts. A ransom of millions of dollars was paid to prevent the publication of the data.

→ Suspected Case:

A law firm was concerned that it had been the victim of a cyberattack. After a call to the insurer‘s cyber incident hotline and subsequent investigation by the insurer‘s recommended IT service provider, the all-clear was given. It was just a software error.

→ Investigation by Data Protection Authority:

A financial services company was target of a cyberattack that compromised personal data. The breach was closed by the insurer‘s IT service provider and the incident was duly reported to the data protection authorities. The authorities initiated data protection proceedings against the financial services provider. The insurer paid for the services of a law firm specialising in data protection law. The imposition of a fine was avoided.

→ Immaterial Damages:

A telecommunication company unlawfully disclosed customer data to unauthorised third parties. An affected customer claimed immaterial damages, and the data protection authority imposed a fine. The insurer covered both the legal fees for the unsuccessful defence against the fine and the fine itself.

→ Money Transfer to Wrong Account:

A retailer‘s employee‘s email account was hacked. The attacker sent a fake invoice from the hacked employee‘s email account to a colleague in the retailer‘s finance department. The colleague then transferred tens of thousands of euros to the attacker‘s account, believing it to be a genuine invoice from the colleague. Thanks to an optional coverage extension, the incident was insured.

→ Mishandling:

An employee of a toy retailer accidentally changed various settings in the configuration of the online shop, making it inaccessible for several days. The cost of recovery and business interruption amounted to several thousand euros.

→ DDOS attack:

An online shop was victim of a denial-of-service attack. The online shop was unavailable to customers for more than two days, despite the best efforts of the internal IT team and the insurer‘s IT specialist to defend against the attack. The costs, including loss of business, amounted to hundreds of thousands of euros.

→ Cloud Service Outage:

The platform of a supplier service is operated via the cloud services of a major provider. The cloud service was partially unavailable for almost a day, resulting in many orders not reaching the delivery service. The insurer paid part of the lost profit.

→ Tampered Card Reader:

In a department store, the credit card reader was tampered by unknown persons in order to obtain customers‘ credit card details. The affected customers sued the owner for damages. In addition, it was necessary to monitor the customers‘ credit cards to prevent further misuse. The costs of compensation, lawyers and monitoring amounted to several hundred thousand euros.