Cyber Incident Response

Managing crises and cyber attacks securely

Cyber attacks are becoming not only more frequent, but also more complex and targeted. The attackers pursue different targets and often cause great economic damage.

The ability to manage cyber attacks and their possible consequences and crises in complex situations is a clear business advantage. In the event of operational disruptions, a fast and complete recovery of data, systems and processes has the highest priority, whereby digital traces and evidence must be protected. The temporary unavailability of IT systems, data loss or data theft has immediate and serious consequences for the profitability of businesses in all industries.

Why Grant Thornton?

Our experienced experts help you to react optimally to potential cyber incidents with Cyber Incident Response.

Cyber Incident Response means not only finding and closing security gaps, but also investigating the "break-in" and all damages as well as tracing the perpetrator. Therefore, the underlying causes in your IT environment are investigated and the extent of damage is determined. On request, we also cooperate closely with your lawyers, your cyber insurer or the authorities.

Our report includes recommendations on how to design your IT environment, optimize processes and perfect your organization to avoid disruptions of all kinds. We are familiar with current cybercrime attack patterns, such as malware that infects your data carriers, encrypts them, and then claims money to unlock them (known as "ransomware"), or fraudsters who pretend to be members of the executive team in order to force employees to make foreign bank transfers (known as "fake president fraud").

Together with you we assess:

- What does the disruption cost you per day/hour specifically?
- What are the operational and economic consequences of data theft for you?
- What time factors must be observed in order to minimize further economic damage?
- Which technical and organizational measures are necessary and sensible for your business purposes in the event of damage?
- Which technical and organizational measures are necessary to avoid similar incidents in the future?

Your added value

Should an incident occur, our Digital Forensic experts will support you in all IT Security incidents such as hacker attacks, data loss, etc. The immediate closure of security gaps, damage assessment and the tracing of the attacks are in the forefront, along with data and system recovery, in order to minimize financial and operational damage and avert further negative effects and losses.

The German Federal Office for Security in Information Technology (BSI) has audited us and recommends us as a "qualified service provider for APT-Response".

We have performed numerous Cybercrime Investigations and can assist you in the area of Cyber Incident Response with our extensive experience.

„Fake President Fraud“: Cybercrime in the financial sector

A company in the insurance industry asked us to investigate a cybercrime incident: The Chief Financial Officer had received a deceptively genuine e-mail, supposedly from the group's Management Board, with clear instructions to immediately (and strictly confidentially) carry out banking transactions amounting to 3.2 million euros abroad – and acted accordingly. We were able to fully clarify the matter with the client and helped with the return transfer of 2.1 million euros. Since 2015, the number of customized attacks of this kind “Fake President Fraud“ has increased significantly. The best preventive countermeasure is a customized ”Cybercrime Awareness Training“ for selected employee groups.

Cyber Incident in the extractive industry – internal sabotage with millions in damage

Our client approached us after some inexplicable disruptions had occurred in the internal company network. During the creation of the overall situation picture, we were able to clearly identify seven events as internal sabotage amongst a large number of incidents. The internal perpetrator could be convicted with the help of forensically collected evidence and unambiguous digital traces. A comprehensive catalogue of recommendations for the improvement of the entire IT environment as well as IT Security in particular was created which the client implemented immediately afterwards. The optimization of IT Security helped the client to return to normal business operations after six months of “emergency state”.

Current malware threats

We were commissioned by several medium-sized companies after their networks had been infected by the malware “Emotet“. For one of the clients, the infection led to a production stop lasting several days and causing millions worth of damage. Current malware like Emotet is modularly constructed, extremely persistent and extremely difficult to detect at the same time. It can also reload malware specifically tailored to the infected target in order to cause maximum damage. We were able to help contain the infection, identify the infection pathways and close the security gaps that made an extensive infection possible in the first place.

Botnet Attacks

In 2017, the number of IoT devices overtook the world's population. With more than 40% a good part of these systems serves as a so-called bot according to recent studies. Mergers of a large number of such bots, so-called botnets, are responsible for a large proportion of current DDoS attacks and spam waves. In recent years, there has also been an increase in data collections such as Collection #1, which collect and publish several hundreds of millions of e-mail addresses. The combination of these data volumes together with a botnet enables cyber criminals to carry out targeted brute force attacks against individual companies. We were commissioned to investigate such an attack on the office cloud solution of an insurance company. The investigation enabled us to verify that the company's security measures were sufficient and that there was no unauthorized access to the internal system.

International Competence

You can rely on our high-quality standards also if you have questions with an international dimension. For cross-border assignments, we combine global scale with local insight in our powerful Grant Thornton International network. Over 62,000 people in more than 140 countries with their commitment to excellence that delivers a quality service on a global scale leverage local expertise with the advisory services you need to meet your challenges.

Your Contacts

Dr. Frank Hülsberg
Partner
T +49 211 9524 8527
M +49 172 1598840
E frank.huelsberg@de.gt.com

Dr. Florian Scheriau
Senior Manager
T +49 211 9524 8625
M +49 172 8245859
E florian.scheriau@de.gt.com

Grant Thornton

grantthornton.de