SCWP SCHINDHELM

WHAT TO DO IF THE COMPANY IS HACKED?
ACTIONS FROM A LEGAL PERSPECTIVE

In case of a hacking attack, unauthorised attackers attempt to access external PCs, notebooks, smartphones, tablets or even entire corporate networks.

A hacking attack is usually done using malicious software. These are usually small, inconspicuous programs, which are also known as trojans, viruses or worms. This allows attackers to access the external IT system, either damaging it, spying on it, or completely depriving its owners of it by deleting it or encrypting it.

The attackers usually operate worldwide and are therefore active both domestically and abroad. The motives of the hackers vary and range from the mere fun of being able to do it, to protest campaigns (usually former employees), or even to espionage and extortion.

COUNTERMEASURES

Most often, however, an attack is aimed at achieving financial gain which must be paid by the attacked company. As the frequency of such attacks has grown massively in Europe over the past year, let's consider the successful external hacker attack that encrypts the affected systems in a way that the company cannot access its system at all.

In our legal practice, we see several challenges facing an affected company before normal operations return:

1) **Identification of the hacker attack**
   A successful hacking attack usually first appears in the company's IT department, which experiences unusually frequent outages of important IT systems. The analysis often shows that the affected areas cannot be accessed at all. This is because the company data was deleted by the attackers or encrypted in such a way that the affected company no longer has access to its own data.

2) **Setting up a crisis team**
   Once the successful hack has been determined, a committee must be established to manage the hack and its consequences. This crisis team consists of specialists from all areas of expertise. If necessary, external consultants/specialists can be consulted to manage this, Computer Emergency Response Teams (CERT), IT forensics, lawyers and communications leaders (internal to employees and external to customers and media inquiries, if applicable). The crisis staff meets regularly for meetings and advises management in the defence of the crisis. After returning to the normal situation, the crisis staff dissolves again and normal operation returns to force.

3) Data protection reporting obligations

The General Data Protection Regulation defines a personal data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data that was transmitted, stored or otherwise processed.*"

This includes, in particular, operational know-how, trade secrets, customer data or employee data, as well as all other personal data, but also all other information classified as confidential.

If a consequence of the hacker attack is a personal data breach of this kind, the following reporting and notification obligations must be observed:

- **report to the competent supervisory authority within 72 hours of becoming aware of the breach, whereby** the personal data breach is likely to result in a risk to the rights and freedoms of natural persons; and
- **notify the data subject if** the personal data breach is likely to result in a high risk to the personal rights and freedoms of individuals.

These notifications must contain clearly defined information as part of their **minimum content**. The information must be discussed with the competent data protection authority and, if applicable, also with the data protection authority.

Violations of these reporting and notification obligations could result in **fines of up to 2% of the total worldwide annual turnover** of the last financial year completed.

4) Restoration of all IT systems

CERT should have a containment effect in the short term to prevent attackers from further access to the compromised system, avoid further damage, and limit the resulting damage. Furthermore, vulnerabilities must be cleaned up to prevent similar incidents in the future.

However, before system operation begins, recovery of the system and company data must be completed. The complexity depends significantly on whether and in what form intact backups of company data are available or not. When the system resumes operation, the crisis team is tasked with defining the requirements for the restart plans.

5) Forensics

The IT forensics secure the electronic tracks that are intended to enable the investigation and processing of the hacking attack. Special technical procedures are required to prevent the loss of mostly volatile electronic data tracks and to document their evidentiary value in a court-proof manner. However, according to our practical experience, the attackers usually cannot be determined or traced to a national jurisdiction.

In any case, the data security measures of the company IT must be subsequently revised and adapted.

6) Communication

Of course, the general regulations for crisis communication must also be taken into account in case of hacking attacks. However, different types of crises impose different requirements for crisis communication. Therefore, it makes sense to consider different types of crises in advance. In particular, data subjects can be informed with press statements, which should also be reviewed in advance from a legal perspective in order to minimise liability risks.

IMMEDIATE HELP AND PREVENTION

Schindhelm Allianz has been advising its clients on acute hacking attacks for several years. Through our experience and expertise, as well as our options for cross-border legal representation and advice, we support our clients optimally in the event of such crises and to avoid legal consequences for our clients in the best possible way.

In addition, we are also happy to provide preventive advice and support for the creation of emergency plans and the delivery of training for your employees.

If you have any further questions, the experts of the Schindhelm Allianz are available at any time.

CONTACT

Austria:
Philipp Reinisch
P.Reinisch@scwp.com

Bulgaria:
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

China:
Marcel Brinkmann
Marcel.Brinkmann@schindhelm.com

Czech Republic/Slovakia:
Monika Wetzlerova
Wetzlerova@scwp.cz

France:
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Germany:
Rüdiger Erfurt
Ruediger.Erfurt@schindhelm.com

Hungary:
Beatrix Fakó
B.Fako@scwp.hu

Italy:
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Poland:
Konrad Schampera
Konrad.Schampera@sdzlegal.pl

Romania:
Helge Schirkonyer
Helge.Schirkonyer@schindhelm.com

Spain:
David Ramírez
D.Ramirez@schindhelm.com

Turkey:
Müge Sengönül
Muge.Sengonul@schindhelm.com

Publisher, media owner, editorial office: Saxinger, Chalupsky & Partner v.o.s., advokátní kancelá | 301 00 Plze , B. Smetany 2, Tel.: +420 377 330 163, plzen@scwp.com | 110 00 Praha 1 Tel.: +420 221 803 350, praha@scwp.com | Saxinger, Chalupsky & Partner v.o.s., advokátní kancelá is a member of SCWP Schindhelm Services SE, Alliance of European Commercial Law Firms | All information is subject to correction in spite of careful processing and cannot replace individual advice in individual cases. The liability of the authors or the publisher is excluded.