WAS TUN, WENN DAS UNTERNEHMEN GEHACKT WIRD?
MASSNAHMEN AUS RECHTLICHER SICHT

Bei einem Hackerangriff versuchen Personen unberechtigt auf fremde PCs, Notebooks, Smartphones, Tablets oder auch ganze Unternehmensnetzwerke zuzugreifen.

Ein solcher Hackerangriff erfolgt meist mittels Schadsoftware. Das sind idR kleine, unscheinbare Programme, die auch als Trojaner, Viren oder Würmer breiter bekannt sind. Die Angreifer können dadurch auf das fremde IT-System zugreifen und es so entweder beschädigen, ausspähen oder durch Löschung oder Verschlüsselung überhaupt komplett den Eigentümern entziehen.

Die Angreifer agieren meist weltweit und sind daher sowohl im In- als auch im Ausland aktiv. Die Motive der Hacker sind unterschiedlich und reichen von bloßem Spaß am Können über Protestaktionen (meist ehemaliger Mitarbeiter) bis hin zu Spionage und Erpressung. Meist zielt ein Angriff aber auf finanziellen Gewinn ab. Dieser soll dabei vom angegriffenen Unternehmen bezahlt werden.

GEGENMASSNAHMEN

Da die Häufigkeit solcher Angriffe im vergangenen Jahr in Europa massiv zugenommen hat, betrachten wir im Folgenden den erfolgreichen Hackerangriff von Aussen, der die betroffenen Systeme so verschlüsselt, dass das Unternehmen überhaupt nicht mehr auf sein System zugreifen kann. In unserer anwaltlichen Praxis sehen wir mehrere Herausforderungen, die auf ein betroffenes Unternehmen zukommen, bevor wieder Normalbetrieb einkehrt:

1) **Identifikation des Hackerangriffs**
   Ein erfolgreicher Hackangriff zeigt sich in der Regel zuerst in der IT-Abteilung des Unternehmens, die ungewöhnlich gehäufte Ausfälle wichtiger IT-Systeme gemeldet bekommt. Die Analyse zeigt oft, dass auf die betroffenen Bereiche gar nicht weiter zugegriffen werden kann. Dies eben, weil die Unternehmensdaten von den Angreifern gelöscht oder so verschlüsselt wurden, dass das betroffene Unternehmen keinen Zugriff mehr auf seine eigenen Daten hat.

2) **Einrichtung eines Krisenstabs**
   Nach Feststellung des erfolgreichen Hackerangriffs ist ein Gremium zur Bewältigung des Hackerangriffs und seiner Folgen einzurichten. Dieser Krisenstab besteht aus Spezialisten aller benötigen Fachgebiete. Im Bedarfsfall können externe Berater / Spezialisten zur Bewältigung hinzugezogen werden, va. Computer Emergency Response Teams (CERT), IT-Forensiker, Rechtsanwälte und Kommunikations-Verantwortliche (intern va. zu Mitarbeitern und extern va. zu Kunden und ggf. Medienanfragen). Der Krisenstab tritt regelmäßig zu Meetings zusammen und berät die Geschäftsführung bei der Abwehr der Krise.

Nach Rückführung in die Normallage löst sich der Krisenstab wieder auf und der Normalbetrieb tritt wieder in Kraft.

3) Datenschutzrechtliche Meldepflichten

Die DSGVO versteht unter Verletzung des Schutzes personenbezogener Daten „*eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.*“

Dies sind insbesondere betriebliches Know-how, Geschäftsgeheimnisse, Kundendaten oder Mitarbeiterdaten sowie alle weiteren personenbezogenen Daten, aber auch alle sonstigen als vertraulich klassifizierten Informationen.

Ist eine Folge des Hackerangriffs eine solche Verletzung des Schutzes personenbezogener Daten, sind folgende Melde- und Benachrichtigungspflichten zu beachten:

- **Meldung an die zuständige Aufsichtsbehörde binnen 72 Stunden ab Bekanntwerden der Verletzung**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, und
- **Benachrichtigung der betroffenen Person**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Diese Benachrichtigungen haben klar definierte Informationen als **Mindestinhalte** zu enthalten. Die Informationen sind mit der zuständigen Datenschutzbehörde und ggf. auch mit der Datenschutzbehörde zu erörtern.

Bei Verstößen gegen diese Melde- und Benachrichtigungspflichten drohen **Geldbußen von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes** des letzten abgeschlossenen Geschäftsjahres.

4) Wiederherstellung aller IT-Systeme

Das CERT soll kurzfristig eindämmend wirken: Unterbindung des weiteren Zugangs der Angreifer zum kompromittierten System, Vermeidung weiterer Schäden und Begrenzung des entstandenen Schadens. Weiters müssen Schwachstellen bereinigt werden, um gleichartige Vorfälle zukünftig zu verhindern.

Vor einer Aufnahme des Systembetriebs muss jedoch die Wiederherstellung des Systems und der Unternehmensdaten abgeschlossen sein. Die Komplexität hängt wesentlich davon ab, ob und in welcher Form unversehrte Backups der Unternehmensdaten vorhanden sind oder nicht. Bei der Wiederaufnahme des Systembetriebs kommt dem Krisenstab die Aufgabe zu, die Anforderungen für die Wiederanlaufpläne festzulegen.

5) Forensik

Die IT-Forensiker sichern die elektronischen Spuren, die die Aufklärung und Aufarbeitung des Hackerangriffs ermöglichen sollen. Dabei sind spezielle technische Vorgehensweisen erforderlich, um den Verlust meist flüchtiger elektronischer Datenspuren zu verhindern und deren Beweiswert gerichtsfest zu dokumentieren. Nach unserer praktischen Erfahrung können die Angreifer jedoch meist nicht ausgeforscht oder einer nationalen Gerichtsbarkeit zugeführt werden. Jedenfalls sind die Datensicherheitsmaßnahmen der Unternehmens-IT in weiterer Folge zu überarbeiten und anzupassen.

6) **Kommunikation**
Selbstverständlich sind auch bei Hackerangriffen die allgemeinen Regelungen zur Krisenkommunikation zu berücksichtigen. Allerdings stellen verschiedene Krisentypen unterschiedliche Anforderungen an die Krisenkommunikation. Daher ist es sinnvoll, im Vorfeld Überlegungen zu verschiedenen Krisentypen, anzustellen. Insbesondere können Betroffene mit Pressestatements informiert werden, die jedoch auch vorab aus rechtlicher Sicht geprüft werden sollten, um Haftungsrisiken zu minimieren.

SOFORTHILFE UND PRÄVENTION

Die Schindhelm Allianz berät ihre Mandanten bereits seit einigen Jahren bei akuten Hackerangriffen. Durch unsere Erfahrung und Expertise iZm der grenzüberschreitenden anwaltlichen Vertretung und Beratung haben wir die Möglichkeit, auch in solchen Krisen zu unterstützen und rechtliche Konsequenzen für unsere Mandanten bestmöglich zu vermeiden.

Darüber hinaus beraten wir auch gerne präventiv und unterstützen bei der Erstellung von Notfallplänen genauso wie bei der Abhaltung von Trainings für Ihre Mitarbeiter.

Wenn Sie weiterführende Fragen haben, stehen Ihnen die Experten der Schindhelm Allianz jederzeit gerne zur Verfügung.

KONTAKT

Bulgarien:
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

China:
Marcel Brinkmann
Marcel.Brinkmann@schindhelm.com

Deutschland:
Rüdiger Erfurt
Johannes.Thoma@schindhelm.com

Frankreich:
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Italien:
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Österreich:
Philipp Reinisch
P.Reinisch@scwp.com

Polen:
Konrad Schampera
Konrad.Schampera@sdzlegal.pl

Rumänien:
Helge Schirkonyer
Helge.Schirkonyer@schindhelm.com

Spanien:
David Ramírez
D.Ramirez@schindhelm.com

Tschechien/Slowakei:
Monika Wetzlerova
Wetzlerova@scwp.cz

Türkei:
Müge Sengönül
Muge.Sengonul@schindhelm.com

Ungarn:
Beatrix Fakó
B.Fako@scwp.hu

Herausgeber, Medieninhaber, Redaktion: Zimányi & Fakó Rechtsanwälte | Lövőház u. 30 | 1024 Budapest | Registernummer: 2019 | Register: Budapester Anwaltskammer (H-1055 Budapest, Szalay u. 7.) | Tel: +36 1 270-9242, Fax: +36 1 270-9241 | budapest@scwp.hu | Zimányi & Fakó Rechtsanwälte ist Mitglied der SCWP Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien |