WOLF THEISS

PRESSEMITTEILUNG

CYBER ATTACKS: DIE ERSTEN 72 STUNDEN ZÄHLEN

DIE JÜNGSTEN CYBERATTACKEN - NATIONAL UND INTERNATIONAL

Wien, 30.06.2016 – Laut aktuellen Schätzungen des FBI liegt der durch Cyber-Delikte verursachte Schaden jenseits der 3 Milliarden US-Dollar-Grenze. Zu den klassischen Hacker-Angriffen gesellen sich in der jüngeren Vergangenheit auch Social Engineering-Attacken. Die ersten 72 Stunden nach einem Cyber-Angriff können für die Rechtsverfolgung entscheidend sein, erklärten Wolf Theiss–Rechtsexperten im Rahmen eines Pressegesprächs.

WOLF THEISS Rechtsanwälte
Schubertring 6
1010 Wien
Österreich

T +43 1 515 10
F +43 1 515 10 25
wien@wolftheiss.com
www.wolftheiss.com

"Zeit ist das bedeutendste Element", erklärt Angelika Hellweger, Counsel Wolf Theiss, Praxisgruppe Dispute Resolution: "Lässt man sich zu lange Zeit, würde man bald nicht mehr Herr der Lage sein. Auch die Rückholung überwiesener Gelder könne eher erfolgen, wenn zeitgerecht reagiert würde", warnt die Expertin. Schritt Nummer eins sei jedenfalls die Kontaktaufnahme mit einem Anwalt und die Aufstellung eines Notfall-Teams.

Die ersten 72 Stunden: Rechtliche und technische Sofortmaßnahmen

Mit der neuen Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 in Kraft treten wird, wird auch eine Verpflichtung von Meldungen an die Datenschutzbehörde eingeführt und dafür eine Frist von besagten 72 Stunden eingeräumt ("unverzüglich und möglichst binnen 72 Stunden"). Die Strafen für Verstöße gegen die Verständigungspflicht werden aber von nunmehr EUR 10,000 auf dann bis zu EUR 10 Mio oder 2% des weltweiten Konzernumsatzes drastisch erhöht. Roland Marko, Partner Wolf Theiss, Praxisgruppe IP/IT: "Die 72 Stunden sind dann eine 'harte' Deadline, wenn von der Cyberattacke auch personenbezogene Daten betroffen sind." Schon nach dem heute anwendbaren Datenschutzgesetz 2000 hätten Unternehmen, wenn ihnen bekannt wird, dass Daten aus einer ihrer Datenanwendungen (i) "systematisch und schwerwiegend unrechtmäßig verwendet wurden" und (ii) den Betroffenen Schaden droht, darüber unverzüglich die Betroffenen in geeigneter Form zu informieren, so der Datenschutz-Experte von Wolf Theiss. Durch den neuen Strafrahmen nach der DSGVO erhält die Frist von 72 Stunden aber völlig neue Dimension.

Wenn entdeckt wird, dass durch eine Cyber-Attacke Gelder transferiert wurden, sind folgende Schritte zu setzen:

1) Schadensermittlung und Beurteilung der Lage: Es ist zu klären, welche Systeme betroffen waren, ob Gelder entwendet und/oder Daten ausgelesen wurden und worin das Risiko besteht. Diese Beurteilung ist für das weitere Vorgehen essentiell und muss daher mit großer Sorgfalt durchgeführt werden.
2) Wenn Gelder entwendet wurden: Sofortige Rückholmaßnahmen bei den Banken starten. Wenn möglich, Überweisungen stoppen lassen

bzw. Bemühungen setzen, dass Gelder rücküberwiesen werden. Dies sollte aber aus Sicherheitsgründen nicht durch Personen erfolgen, die selbst vom Angriff betroffen waren, da zu diesem Zeitpunkt auch eine mögliche Mittäterschaft noch nicht wird ausgeschlossen werden können.

3) Sobald klar ist, wohin Gelder überwiesen wurden (meistens außerhalb des Landes): geeignete "Asset Tracer" vorab informieren, das sind Dienstleister, die beim Nachverfolgen und Auffinden der Gelder behilflich sind.
4) Sofortige Einbindung der Behörden und Anzeige, insbesondere wenn das Geld ins Ausland überwiesen wurde, auch ein Ersuchen, dass Interpol eingeschaltet wird. Ebenso etwaige ausländische Botschaften.
5) Technische Sofort-Sicherungsmaßnahmen setzen und neben der Wiederherstellung der IT-Sicherheit auch darauf achten, dass "elektronische Spuren" nicht verwischt, sondern für eine spätere Beweisführung konserviert werden.
6) Betroffene Personen sofort befragen
7) Arbeitsrechtliche Sofortmaßnahmen setzen: Betroffene Mitarbeiter sollten sofort dienstfrei gestellt und vom Arbeitsplatz abgezogen werden. Diese sollten auch nicht eher wieder ihre Arbeit aufnehmen, solange nicht geklärt ist, was passiert ist und ob der Mitarbeiter möglicherweise selbst involviert ist.
8) Wenn personenbezogene Daten vom Angriff kompromittiert wurden und den betroffenen Kunden, Lieferanten etc. daraus Schaden droht, sind betroffene Nutzer zu informieren.
9) Gibt es eine Cyber-Versicherung, die das Risiko eventuell abdeckt?
10) Regulatorische Maßnahmen setzen.
11) Geeignete Rechtshilfe im Ausland suchen

Laut aktueller Cyber-Crime-Studie von KPMG ist fast jedes zweite (!) österreichische Unternehmen bereits Ziel von Cyber-Crime Angriffen gewesen. Angreifer sind Konkurrenten, ehemalige Mitarbeiter oder Berufsverbrecher.

Cyber-Crime ist zum "Business" geworden und erfordert von potentiell betroffenen Unternehmen daher auch business-getriebene Antworten. Cybersicherheit muss daher als wesentlicher Bestandteil des Risikomanagements begriffen werden, und zwar auch in Branchen, die für sich genommen kein "E-Business" im eigentlichen Sinne betreiben, das zeigen insbesondere auch die nachstehenden Beispiele:

"**Fake President" Fraud cases / CEO/CFO email scam und andere Social Engineering Angriffe**

Im Zusammenhang mit Business Email Compromise Scams hat das FBI erst jüngst neueste Zahlen veröffentlicht. Diese Betrugsart kam in 79 Ländern vor, es gibt derzeit über 22,000 Opfer und der geschätzte Verlust beträgt $3.1 Milliarden

(Status Mai 2016; Zeitraum Oktober 2013 bis Mai 2016).
http://www.securityweek.com/losses-business-email-compromise-scams-top-31-billion-fbi

Die weitaus überwiegende Anzahl der Gelder wird auf Bankkonten asiatischer Banken in China und Hongkong transferiert. Derzeit ist nicht klar, nach welchen Kriterien die "Opfer" ausgewählt werden, es ist aber davon auszugehen, dass diese in den meisten Fällen ausspioniert werden.

SWIFT Attacken
Angriffe über das SWIFT System (internationales Zahlungsverkehrssystem). Hacker haben die Datenbank modifiziert, die die Aktivität der Bank über das SWIFT-Netzwerk protokolliert. In weiterer Folge war es möglich, Transaktionen zu überwachen und auch abzufangen. So konnten Überweisungen, die die Hacker angefordert hatten, direkt freigegeben werden.

Es gab seit Anfang 2015 mehre Angriffe auf Banken: u.a. in Vietnam, Ecuador und Bangladesch.

Angriff im Jänner 2015 - Ecuadors Banco del Austro (BDA) - in 12 Transaktionen wurden insgesamt $12 Mio an Konten in Hongkong, Dubai in die USA überwiesen. http://www.securityweek.com/third-swift-attack-transfers-12-million-hong-kong-dubai-and-us

Angriff im Februar 2016 - Ziel Zentralbank von Bangladesch - Verlust: $81 Mio. Insgesamt $951 Mio angewiesen. Es wurde sich Zugang zum SWIFT-Kommunikationsnetz verschafft und betrügerische Geldüberweisungen wurden in Auftrag gegeben. Ein großer Teil der Überweisungen wurde allerdings blockiert. $81 Mio wurden auf Konten auf den Philippinen gelenkt und dort an Kasinos weitergeleitet.

Malware, Betriebsspionage, Wirtschaftsspionage

Aus unserer Praxis stehen momentan vor allem Attacken "von innen" (Mitarbeiter und ehemalige Mitarbeiter) und Attacken durch Wettbewerber auf der Agenda ganz oben:

- Mitarbeiter bemächtigten sich vor Austritt Geschäfts- und Betriebsgeheimnisse und nehmen diese zur Konkurrenz mit
- Konkurrenzunternehmen nutzen gezielt Lücken in der IT-Sicherheit von Unternehmen aus, um an Geschäfts- und Betriebsgeheimnisse heranzukommen.

Ferner ist die Zahl an Erpressungsversuchen gestiegen:

- IT-Systeme werden gekapert und lahmgelegt oder Daten verschlüsselt und nur gegen Zahlung eines Lösegeldes wieder freigegeben.

- Privatpersonen werden zu verfänglichen Handlungen aufgefordert, gefilmt und erpresst. Das kann auch unternehmensbezogen werden, wenn es Teil einer "Social Engineering" Strategie gegen ein letztlich unternehmerisches Opfer wird

ÜBER WOLF THEISS

Die 1957 gegründete Rechtsanwaltssozietät Wolf Theiss gehört zu den führenden zentral-, ost- und südosteuropäischen Anwaltssozietäten mit Schwerpunkt im internationalen Wirtschaftsrecht. An den dreizehn Standorten in Albanien, Bosnien & Herzegowina, Bulgarien, Kroatien, Österreich, Polen, Rumänien, Serbien, Slowakei, Slowenien, Tschechien, Ungarn und der Ukraine sind 340 Juristen für lokale und internationale Industrie-, Handels- und Dienstleistungsunternehmen sowie Banken und Versicherungen im Einsatz. In der Verbindung von Recht und Wirtschaft entwickelt Wolf Theiss umfassende und konstruktive Lösungen auf der Basis von rechtlichem, steuerlichem und unternehmerischem Know-how.

Rückfragehinweis:

Mag. Barbara Fürchtegott
PR & Communications Manager

Wolf Theiss Rechtsanwälte / Attorneys-at-Law
Schubertring 6, A-1010 Wien

Tel.: +43 1 51510 / 3808
E-Mail: barbara.fuerchtegott@wolftheiss.com

www.wolftheiss.com