Presseinformation

Wirtschaftsspionage wächst: Was sind gestohlene Firmendaten wert?

München, 18. August 2014. Schneller als die meisten deutschen Wirtschaftszweige wächst die Wirtschaftsspionage gegen deutsche Unternehmen. Jedes zweite deutsche Unternehmen hatte in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu verkraften. (1) 26,9 Prozent konnten einen Angriff feststellen, bei weiteren 27,4 Prozent gab es einen Verdachtsfall. Das entspricht einem Wachstum allein der gezählten Fälle von 5,5 Prozent gegenüber dem Jahr 2012. All das stellte Corporate Trust, eine Unternehmensberatung für Risiko- und Krisenmanagement (2) fest. Die Ergebnisse finden sich in ihrer „Studie: Industriespionage 2014“ (1), die im Internet heruntergeladen werden kann. Sie trägt zwar den aktuell klingenden Untertitel: „Cybergeddon der deutschen Wirtschaft durch NSA & Co.?“, macht aber andererseits im Inhalt deutlich, dass die gefährlichsten und erfolgreichsten Angriffe von Hackern und Abhörern aus Asien, den russisch dominierten GUS-Staaten und Osteuropa drohen, und erst in zweiter Linie von westlichen Bündnispartnern wie den USA. Ein weiteres interessantes Ergebnis ist, dass offenbar der Mittelstand prozentual noch stärker betroffen ist als die Großen unter den deutschen Konzernen. Wenig überraschend sind mehr als die Hälfte der deutschen Schäden durch Wirtschaftsspionage in den Branchen Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbau zu verzeichnen.

Schäden durch Wirtschaftsspionage

40,8 Prozent aller Unternehmen hatten einen materiellen Schaden durch Wirtschaftsspionage zu verzeichnen. Bei 53 Prozent von diesen bestand er im Ausfall, im Diebstahl oder der Beschädigung von IT- und Telekommunikationsgeräten. Doch welche immateriellen Werte sind deutschen Unternehmen dadurch verloren gegangen beziehungsweise welcher zusätzliche Schaden ist entstanden? Eine allgemeingültige Antwort darauf ist schwer zu formulieren. Denn anders als bei einem gestohlenen Notebook sind die Daten nicht verschwunden, sondern noch an mehreren Stellen im Unternehmen vorhanden. Sie werden im Normalfall vom Hacker oder

Spion kopiert und existieren nun zweimal: beim Unternehmen als rechtmäßigem Eigentümer, der sie unter Umständen mühsam erarbeitet hat, und beim unrechtmäßigen Besitzer, der eine Kopie durch eine kriminelle Tat erworben hat. In Deutschland existiert nicht einmal eine rechtlich verbindliche Vorgehensweise für eine Unternehmensbewertung.(3) Noch schwerer ist es, den Wert von Firmendaten zu taxieren. Ansätze zur Bewertung ergeben sich aus der Arbeit, die das Unternehmen zur Herstellung dieser Daten geleistet hat und aus dem, was das Unternehmen mit den Daten in Zukunft erwirtschaften kann.

Was sind Firmendaten wert?

Anhand dieser Überlegung haben Corporate Trust und die betroffenen Unternehmen den jährlichen finanziellen Gesamtschaden durch Industriespionage zu beziffern versucht. Für die Berechnung des Schadens wurden 300.000 Unternehmen in Deutschland und 42.000 Unternehmen in Österreich befragt. Bei der Studie wurden nur Unternehmen mit mehr als 10 Mitarbeitern sowie einem Umsatz bzw. einer Bilanzsumme von mehr als 1 Million Euro berücksichtigt. Der Schaden beläuft sich hier demnach auf 11,8 Milliarden Euro (zum Vergleich: in Österreich auf insgesamt 1,6 Milliarden Euro). 77,5 Prozent der betroffenen Unternehmen in Deutschland hatten durch die Wirtschaftsspionage einen finanziellen Schaden zu verzeichnen. Bei den meisten Firmen lag der Schaden zwischen 10.000 und 100.000 Euro. 4,5 Prozent hatten jedoch einen Schaden von über 1 Million Euro zu beklagen.

26,8 Prozent der betroffenen Firmen erlitten Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. 37,1 Prozent der Unternehmen hatten weitere immaterielle Schäden durch Industriespionage zu verzeichnen. Am häufigsten waren Patentrechtsverletzungen bei 54,3 Prozent sowie Imageschäden gegenüber Kunden oder Lieferanten bei 26,8 Prozent der Firmen.

Schutz gegen Wirtschaftsspionage verbessern

Deshalb ist es für deutsche Firmen dringend geboten, ihre wertvollen Daten professionell zu schützen. Eine Lösung, die die gestiegene Bedrohung deutscher Firmen durch Wirtschaftsspionage berücksichtigt, gibt es jetzt mit der IDGARD-App. Mit IDGARD tauschen Arbeitnehmer versiegelt Dokumente und Nachrichten im Internet aus, ob vom PC oder vom Smartphone oder vom Tablet-PC aus.

Mitarbeiter können damit sogar unterwegs sicher auf geschäftliche Unterlagen zugreifen, ohne ihre Firma in Gefahr zu bringen. Bearbeiten können sie die Dokumente in beliebigen Apps auf ihren verschiedenen Geräten. Jeder nutzt also seine gewohnte Umgebung zum Arbeiten und kann ohne Angst vor Spionage weiterhin Reise- oder Wartezeiten effizient und produktiv nutzen. Der Versand von Dokumenten erfolgt nämlich sicher über IDGARD. Zusätzlich gibt es in der App ein schnelles und unkompliziertes Messaging, das Tools mit Sicherheitslücken wie Viber oder Whatsapp überflüssig macht. Zum Beispiel lassen sich Push-Benachrichtigungen empfangen und versenden. Jeder Kollege ist also potenziell in Echtzeit mit dem Büro verbunden und profitiert von kurzen Reaktionszeiten. Die Daten stehen offline zur Verfügung, also auch bei schlechtem Empfang.

Daten gehören in verschlüsseltes Rechenzentrum

Im Hintergrund von IDGARD arbeitet die Sealed Cloud. (4) Sie gewährleistet mithilfe von IDGARD auf dem Endgerät, dass alle Daten des Nutzers in der Sealed Cloud bleiben. Das gilt besonders für vertrauliche Dokumente, die beim Betrachten auf Smartphones und Tablets oft automatisch auf ausländische Server geladen werden, zum Beispiel in die iCloud. Dank der Sealed Cloud wird verhindert, dass iCloud und ähnliche Dienste mit Daten beliefert werden. Das Unternehmen stellt mit dem Einsatz der IDGARD-App also sicher, dass Daten vom Smartphone nicht versehentlich mit anderen Diensten synchronisiert werden, etwa von Google und Apple, die ebenfalls leicht zum Ziel von Spionage und Datenklau werden können. Das Konto des Mitarbeiters kann auch remote geschlossen und zurückgesetzt werden, zum Beispiel, wenn Handy oder Tablet PC gestohlen wurden. Dann erhält der Dieb zwar das Gerät, aber keine Firmendaten.

Alle in IDGARD genutzten Daten werden in einem besonders gesicherten deutschen Rechenzentrum gelagert. Denn auf den Servern der meisten Rechenzentren sind Daten zum Beispiel während der unverschlüsselten Verarbeitung dem Personal prinzipiell zugänglich. Daraus resultieren wesentliche Risiken, weil zum einen die Betreiberfirma des Datenzentrums selbst, zum anderen ein externer Angriff auf das Rechenzentrums die Daten in Gefahr bringen können. Die Sealed Cloud Technologie des Münchner Sicherheits-Unternehmens Uniscon (5) verschließt daher diese Sicherheitslücke auf technische Weise. Bei der Sealed Cloud hat nicht einmal der Hersteller Unsicon selbst den Schlüssel zum Dechiffrieren der Informationen in der Cloud. Nur der Cloud-Nutzer selbst hat den Schlüssel zu diesen Daten und somit vollständige Kontrolle.

Ein Schutz der Verbindungsdaten ist ebenfalls sichergestellt. Verbindungsdaten können zum Beispiel verraten, wer mit wem, wann, wie oft und wie lange über das Internet verbunden war. Sie verraten also potenziell die Strategie eines Unternehmens, Firmen-Informationen und Beziehungen. Bei der Sealed Cloud kann der Betreiber der Cloud die Verbindungsdaten nicht einsehen.

Bei Technologiewettbewerb des BMWi prämiert

Im Technologiewettbewerb „Trusted Cloud“ des Bundeswirtschaftsministeriums (BMWi) war die Sealed Cloud erfolgreich im Wettbewerb mit 115 anderen Lösungen. Seither fördert das BMWi die Weiterentwicklung dieser Technologie für die deutsche Industrie.

Dank dieser Sicherheitsfunktionen kann man bei IDGARD von einem abhörsicheren Kommunikationsdienst für Unternehmen sprechen, der mittels moderner Technologien hohen Nutzerkomfort erreicht und die Produktivität steigern kann. Mitarbeiter können mit IDGARD sicher und ohne weitere Software Dokumente mit den gerade genutzten PCs, Notebooks, Smartphones und Tablet PCs austauschen, Nachrichten schreiben und abhörsicher chatten. Sie können also jederzeit mit Kunden, Partnern und Lieferanten sicher kommunizieren und in Teams arbeiten, ohne Sicherheitsprobleme zu verursachen. Betriebswirtschaftliche Analysen zeigen außerdem, dass sich die Investition in den Dienst durch die Zeitersparnis bereits im ersten Nutzungsmonat amortisiert. Das Risiko finanzieller Verluste, welches durch eine weniger hohe Sicherheit besteht, ist dabei noch gar nicht einbezogen.

(1) http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf
(2) http://www.corporate-trust.de
(3) http://www.ihk-schleswig-holstein.de/starthilfe/unternehmensnachfolge/739856/berechnung_untwert.html
(4) http://www.uniscon.de/sealedcloud
(5) http://www.uniscon.de/firmenprofil

Über Uniscon GmbH –

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service ID|GARD für

Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt
Uniscon GmbH/Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
presse@uniscon.de
www.uniscon.de

PR-Agentur Xpand21 GmbH
Doris Loster
Romanstr. 10
80639 München
0170 / 21 53 172
uniscon@xpand21.com
www.pr-agentur-xpand21.de