

Achtung – Datenklau!

Einbruchdiebstahl mit Hintergedanken

Wie die Fallschilderungen in den ersten beiden Artikeln dieser Reihe gezeigt haben, wird Wirtschaftsspionage durch fremde Nachrichtendienste in verschiedenen Formen und unterschiedlichen Gewändern betrieben. Durch bestimmte Personen- und Fallkonstellationen wird der Erfolg begünstigt, ebenso wie die Sicherheitsverantwortlichen in Unternehmen Personen und Situationen so beeinflussen können, dass sich die Erfolgchancen für „Wissensdiebe“ erheblich minimieren.



Bild: stockxpert.com

Eine besonders tückische Variante der Wirtschaftsspionage ist die, die im Gewand des (Einbruch)-Diebstahls daher kommt. Im Unterschied zu anderen Methoden, bei denen es darauf ankommt, dass die gesamte Aktion unbemerkt bleibt, genießt der Täter hier mehr Spielraum. Er muss einerseits nicht die Sorgfalt aufwenden, um zu vertuschen, dass etwas geschehen ist, und kann allein deswegen schon wesentlich schneller zuschlagen. Zum anderen kann er durch eine geschickte Spurenlegung am Tatort verschleiern, was das wirkliche Ziel der Aktion gewesen ist.

Der (Einbruch)-Diebstahl ist immer dann attraktiv, wenn es darum geht, fertiges Know-how in einem Schwung abzuziehen - im Unterschied zu Aktionen, die darauf zielen, ein Know-how, was sich in der Entwicklung befindet, in einem längeren Prozess kontinuierlich abzuschöpfen.

Hardware-Diebstahl

Nach den Erfahrungen der Spionageabwehr Nordrhein-Westfalen beschränken sich die Reaktionen der Geschädigten bei einem (Einbruch)-Diebstahl meistens darauf, Strafanzeige wegen des Verlusts der Hardware oder anderer Sachschäden zu erstatten. Leider fällt das Augenmerk bei viel zu wenigen Unternehmen und Forschungseinrichtungen auf die Daten, die auf

diesen Geräten gespeichert waren und die zugleich verloren gegangen sind. Daher ist vielen überhaupt nicht bewusst, dass sie Opfer einer Spionageattacke geworden sind, die viel weiter reichende Konsequenzen haben kann. Wie eine Studie des CSI/FBI aus 2005 zeigt, zählt der Diebstahl von Laptops und mobilen Endgeräten zu den wichtigsten Angriffen auf Computer und verursacht höhere Schäden als Systempenetrationen, Sabotage oder Betrug.

Fallkonstellationen

Obwohl die überwiegende Mehrheit der (Einbruch)-Diebstähle wirklich „nur“ das sind, was sie scheinen, stellen bestimmte Tatumstände starke Indizien dafür dar, dass die Täter eben doch ein anderes Ziel im Visier hatten.

→ In einem mehrstöckigen Firmengebäude drangen die Täter gezielt in die achte Etage ein und entwendeten dort ausgewählte Datenträger. Hierbei ließen sie andere lohnende Beutestücke wie Flachbildschirme, Notebooks oder Bargeld außer Acht.

→ Die Täter brachen in ein Firmengebäude ein und begaben sich – wie an den Spuren erkennbar war – auf direktem Wege in den IT-Bereich, wo versucht wurde, die Firmendaten vom Server herunterzuladen.

→ Eine Delegation ließ sich in einem Unternehmen eine neue Anlage durchführen. Die Steuerung des Verfahrens

erfolgte über ein älteres Notebook. Dies bewahrte der zuständige Ingenieur in seinem Büro im Schreibtisch auf. Die Täter drangen wenige Tage nach der Präsentation in das Gebäude ein und entwendeten das ältere Notebook aus dem Schreibtisch. Hierbei ließen sie ein neues Notebook samt Netzgerät außer Acht, das auf dem Schreibtisch stand.

Sorgfältig vorbereitet

Besonders erfolgreich sind Spione dann, wenn sie vor dem Spionageangriff Gelegenheit hatten, die örtlichen Gegebenheiten aufzuklären, in Erfahrung zu bringen, ob überhaupt interessantes Know-how vorhanden ist und genau zu lokalisieren, wo dies zu finden ist.

In einem Fall, den die Spionageabwehr Nordrhein-Westfalen bearbeitete, hatte der Auftraggeber zunächst einen „Kundschafter“ entsandt, der sich mit einem für das betreffende Unternehmen hochinteressanten Lebenslauf

→ AUTOR

Heike Vehling ist Referentin für Spionageabwehr im Innenministerium NRW, Düsseldorf.

Tel.: 0211 / 871 2821

E-Mail:

abteilung-vi@im.nrw.de

www.im.nrw.de





Integrationsfähigkeit mit Combi-Schlüssel

initiativ bewarb. Die Person wurde nicht nur hochrangig eingestellt, sondern erhielt sofort unbeschränkten Zugriff auf alle Daten im Firmennetz.

Leider stellte es sich aber heraus, dass die Person überraschenderweise weniger kompetent war, als es ihre persönlichen Daten erwarten ließen. Dennoch war sie sehr „fleißig“, was ihre Recherchen im Firmenrechner und das Herunterladen von Daten betraf. Sie fiel insgesamt eher dadurch auf, dass sie sehr viele Fragen stellte, die häufig auf Bereiche zielten, mit denen sie unmittelbar nichts zu tun hatte. Bevor die Firma dann Schritte unternehmen konnte, kündigte sie aus eigenem Antrieb. Wenige Monate nach diesem Vorfall, wurde in die Geschäftsräume des Unternehmens eingebrochen, und es wurden genau die Rechner entwendet, auf denen die wichtigsten Daten zu einer Produktneuentwicklung gespeichert waren. Ein Zufall?

In einem weiteren Fall gingen die Täter noch raffinierter vor. Bei einer mittelständischen Firma entdeckte der Wachdienst am Wochenende bei seinem Rundgang um das Firmengebäude eine Verwerfung im Erdreich. Als er dies genauer untersuchte, entdeckte er eine Plastikkdose mit augenscheinlich elektronischem Gerät, von der aus Kabelverbindungen durch die Außenmauer in das Gebäudeinnere führten.

Der Wachdienst war zwar so geistesgegenwärtig, dass er die Kabel sofort durchtrennte, die Firmenleitung wurde aber leider erst am darauffolgenden Montag informiert. Da war die Plastikkdose samt Inhalt bereits entfernt worden. Durch genaue Beschreibungen des Wachdienstes und aufgrund der Umstände vor Ort, konnte das Geschehen aber rekonstruiert werden. Offenbar hatten die Spione einen W-LAN Router in der Dose platziert und diesen mittels Kabelverbindungen durch die Gebäu-
deaußenmauer zu einem innerhalb des Gebäudes liegenden Switch geleitet.

Dieser war – trotzdem er unmittelbaren Zugriff auf die zentralen Firmenrechner ermöglichte – von innen frei zugänglich. Der Täter konnte also, indem er von außen – vielleicht aus einem geparkten Wagen – mit seinem Rechner Verbindung zu dem W-LAN Router aufnahm, unbemerkt Informationen aus dem Unternehmensrechner

abziehen. Wie er Zutritt zum Gebäudeinneren erlangte, darüber ließ sich nur spekulieren. Auffällig war aber, dass kurz vor diesem Vorfall von einem Mitarbeiter der Verlust einer Zutrittsberechtigungskarte gemeldet worden war. Die Funktion dieser Karte war aber nicht gesperrt worden, so dass sie unbemerkt hätte weiter verwendet werden können.

Verhaltenstipps

Die wichtigste Regel für die Prävention eines Know-how-Abflusses als Folge eines (Einbruch-)Diebstahls ist auch hier wieder die Datensicherung. Sind die Daten – wie es sein muss – professionell mit Passwort und/oder Kryptierung gesichert, können sie nur erschwert abgezogen werden, selbst wenn man den Datenträger in der Hand hält. Datenträger müssen darüber hinaus ständig lokalisierbar sein, damit ein Abhandkommen sofort bemerkt wird.

Wenn es zum Diebstahl kommt, muss sofort überprüft werden, welche Daten auf dem Rechner vorhanden und wie sie gesichert waren. Hat ein Einbruch stattgefunden, ohne dass ein Diebstahl festgestellt werden kann, oder wurden nur geringwertige Gegenstände entwendet, muss immer auch geprüft werden, ob vielleicht etwas hinzugekommen ist, das heißt, ob an den Datenträgern manipuliert wurde.

In diesem Zusammenhang ist unabhängig von den drahtlosen Verbindungen, die W-LAN ermöglicht, auch darauf zu achten, dass keine „Keyghosts“ an die Rechner angebracht wurden. Diese Geräte sind klein, ungefähr in Feuerzeuggröße, unauffällig, und werden einfach zwischen Tastatur und Rechner eingestöpselt, von wo sie unmittelbar Daten abziehen können.

Ist ein Unternehmen Opfer eines Diebstahls und/oder Einbruchs geworden, auf den eine der oben geschilderten Fallkonstellationen zutrifft, sollte neben der Polizei auch immer die Spionageabwehr benachrichtigt werden. Die Spionageabwehr verfügt nicht nur über spezielle Erfahrungen aus anderen Spionageattacken, sie arbeitet auch – anders als die Polizei – nach dem Opportunitätsgrundsatz. Dadurch kann den anzeigenden Unternehmen ein Höchstmaß an Vertraulichkeit zugesichert werden. □



Der neue
Combi-Schlüssel
Vom Schlüssel zum
Identifikationsmedium

KOMFORT | ORGANISATION | SICHERHEIT

