CYBER-SPIONAGE: DER KALTE KRIEG IM INTERNET

Veröffentlicht am 5. Februar 2014 von Rüdiger

Kürzlich ging eine beunruhigende Meldung durch die Presse. Hacker hatten 16 Millionen E-Mail-Adressen und Passwörter ermittelt. Mit diesen können die Kriminellen praktisch in Ihre Haut schlüpfen. Sie können in Ihrem Namen E-Mails versenden und durch Sie weitere Mail-Adressen und Passwörter in Erfahrung bringen. So kann es zu einem Flächenbrand kommen. Privat wie auch geschäftlich.

Der aktuelle Fall ist aber nur die Spitze des Eisbergs. In einem kürzlich gehaltenen Vortrag des Abteilungsleiters Spionageabwehr des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen wird die wahre Dimension der **Cyber-Spionage** deutlich: Die Datenfischer kommen aus aller Welt und Unternehmen stehen im Fokus ihrer Angriffe. Der Experte berichtete beispielsweise von folgenschweren Geschäftsreisen nach Russland und China. Bei einem Test in China ließ man einen passwortgeschützten Laptop kurzzeitig unbeaufsichtigt und fand auf ihm später **Späh-Software**. Das auf dem Computer gespeicherte Wissen war nun nicht länger geheim.

Doch auch Handys sind ein begehrtes Ziel, wenn es um trickreiche **Wirtschaftsspionage** geht. Die Freude über ein offenes WLAN-Netz oder eine öffentliche Handy-Ladestation kann verfrüht sein. Auf das verlockende Angebot folgt nicht selten ein böses Erwachen. Solche ungeschützten Kanäle können weit geöffnete Einfallstore für Spionage-Software sein.

Datendiebe müssen dabei nicht einmal mehr tief in die Tasche greifen und sitzen oft in der unmittelbaren Nachbarschaft. Spionage-Technik ist bezahlbar geworden und das auch für Ihre lokale Konkurrenz. Ab 100 Euro können Ihre Mitbewerber Spionage-Software kaufen und direkt einsetzen. **Kleine und mittelständische Unternehmen** sehen häufig nicht die Notwendigkeit Sicherheitsmaßnahmen zu ergreifen. Sie sind wie ein Ritter, der ohne Schild in die Schlacht zieht.

Sie fühlen sich an James Bond erinnert? Verständlich. Doch hier geht es nicht um einen spannenden

Agententhriller, sondern die Realität. Und es geht um die wirtschaftliche Zukunft kleiner und mittelständischer Unternehmen. Deren Know-how ist oft ihre Stärke. Doch wie lange noch? Gerade kleine Betriebe mit High-Tech-Produkten unterschätzen vielfach die Gefahren der Spionage über das Internet. Eine Naivität, die sie zu einem beliebten Ziel von Hackern macht.

Erst verliert man die Daten, dann die Firma

Es vergeht kaum ein Tag, an dem es keine Neuigkeiten zur **NSA** gibt. Weniger Beachtung finden der russische und der chinesischen Auslandsgeheimdienst. Zu Unrecht: Der russische SWR und das chinesische Ministerium für Staatssicherheit stehen der NSA um nichts nach. Beinahe alle Bürger, die im www unterwegs sind, werden von den Nachrichtendiensten überwacht.

Der Leichtsinn vieler Unternehmen führt zu Spionage-Schäden, die sich in Deutschland jedes Jahr auf einen zweistelligen Milliardenbetrag belaufen. Die Blauäugigkeit ist jedoch nur ein Grund für den Erfolg der Spione: Manche **Methoden** der Datenkraken sind sehr raffiniert. Zudem lassen sich viele internetfähige Geräte leicht für das Ausspähen von Daten präparieren.

Die Folgen für ein von **Cyber-Spionage** betroffenes Unternehmen können katastrophal sein. Wenn Ihr größter Konkurrent auf einmal exakt das gleiche Produkt wie Sie anbietet, ist ein **Kundenschwund** vorprogrammiert. Für manche Unternehmen sind Baupläne oder Kundendaten wie eine Lebensversicherung. Falls diese Informationen in falsche Hände geraten, können sie ihre Firma schließen.

Es lässt sich jedoch schlecht nachweisen, das eine **Firmeninsolvenz** einem Datenklau geschuldet ist. Die Aufklärungsquote bei solchen Spionagefällen ist laut Ministeriums-Angaben sehr gering. Das liegt nicht zuletzt an einer fatalen Unterbesetzung. In NRW mit seinen 18 Millionen Einwohnern befassen sich lediglich 100 Mitarbeiter mit der Spionageabwehr. Für die gleiche Einwohnerzahl sind in Russland 33.000 Mitarbeiter zuständig, von China ganz zu schweigen.

Wie Sie sich schützen können

Schützt mich nicht der Staat? Eine berechtigte Frage, da jedes Bundesland eine eigene Spionageabwehr unterhält. Die ist der Aufgabe allerdings aufgrund ihrer Unterbesetzung nicht gewachsen.

Daher müssen Sie selbst aktiv werden. Ohne Wenn und Aber! Die folgenden **Maßnahmen** machen den Cyber-Spionen das Leben schwer:

- **Mitarbeiter-Schulung:** Auch wenn Sie Ihren Angestellten vertrauen, müssen Sie ein

wachsames Auge behalten. Firmengeheimnisse verlassen aber auch aufgrund von Unachtsamkeiten die Firma. Ein Mitarbeiter muss in der Regel nur **bestimmte Daten** auf eine Geschäftsreise mitnehmen. Und was er unbedingt braucht, muss er bestmöglich vor unbefugtem Zugriff schützen. Dieses Bewusstsein muss geschärft werden.

- **Personal-Rekrutierung:** Der Leiter des IT-Notfall-Teams der Deutschen Telekom begegnet perfekten Bewerbungen aus dem Ausland mit Skepsis. Wer geringe Gehälter akzeptiert, steht eventuell bereits woanders auf der Gehaltsliste. Seien Sie bei der Personal-Auswahl also vorsichtig.
- **Gedankenaustausch:** Die Cyber-Spionage betrifft nicht nur Sie. Was ihrem Partnerunternehmen schlimmes widerfahren ist, soll sich bei Ihnen nicht wiederholen. Am besten tauschen Sie sich mit befreundeten Berufsgenossen über das Thema aus. Wer die **Bedrohungen** kennt, kann besser auf sie reagieren.
- **Trau, schau, wem?:** Nach Feierabend sollten sich nur Personen in Ihrem Firmengebäude aufhalten, die Ihr uneingeschränktes Vertrauen genießen: Die undichte Stelle kann beispielsweise eine bestochene Reinigungskraft sein.
- **Feind hört mit:** Sogar unbewusst kann ein Mitarbeiter mit verwanztem **Handy** interne Informationen nach außen schleusen. In vielen Konzernen sind Mobiltelefone in Besprechungen bereits Tabu. Diese lassen sich fremdsteuern, sogar wenn sie ausgeschaltet sind. Wenn es bei einem Meeting in Ihrer Firma um sensible Themen geht, sollte ein Handyverbot gelten.
- **Datenmanagement:** Nicht alle Informationen müssen äußerster Geheimhaltung unterliegen. Unterteilen Sie Ihr **Firmenwissen** nach seiner Wichtigkeit. Was darf auf keinen Fall die Firma verlassen und was kann ruhig jeder wissen? Nicht alles muss auf allen PCs abgespeichert sein. Je nach Position und Tätigkeit können Sie in Ihrem Firmennetzwerk **unterschiedliche Zugriffsrechte** vergeben. Die größten Geheimnisse sollten Sie gesondert speichern.
- **Internetnutzung:** Wer nicht mit den sozialen Medien arbeitet, muss sich auch nicht dort aufhalten. Bei der Benutzung von **Facebook** können sich Nutzer einen Trojaner einfangen. Der ist dann Türöffner für Schadsoftware wie etwa **Späh-Programme**. Gleiches gilt für die private Nutzung von E-Mail-Konten. Sie stellt ein vermeidbares Risiko dar und sollte nicht erlaubt sein.
- **Testen Sie sich:** Das nordrhein-westfälische Innenministerium stellt Unternehmen einen Selbsttest zur Verfügung, mit dem Sie Ihren Gefährdungsgrad ermitteln können.

Fazit: Von **Cyber-Spionage** sind auch kleine Unternehmen bedroht. Wenn Sie im Wettbewerb der Zukunft bestehen wollen, müssen Sie Ihre Daten schützen. Sonst wird es keiner tun. Die Methoden der Kriminellen sind schwer zu durchschauen. Deshalb rät es sich auf der Hut zu sein. Sollten Sie etwas Verdächtiges (Mitarbeiter macht grundlos Fotos o. ä.) beobachten, können Sie sich an das jeweils zuständige Innenministerium (in NRW: www.mik.nrw.de) wenden. Nehmen Sie also die Bedrohung ernst und ergreifen Sie Maßnahmen zur Sicherung Ihrer Daten. Dann müssen Sie auch keine Angst vor der Zukunft haben.
