Der Spion, der aus dem PC kommt

Hackerangriffe: Je forschungsintensiver und innovativer ein Unternehmen ist, desto eher gerät es in den Fokus der Industriespionage. Wie Lecks im Datenverkehr aufgespürt werden können, erläutert Sicherheitsexperte Markus Geier.

Foto: Fotolia

Mit moderner Analysetechnik kann die **Kommunikation im Netz** präventiv überwacht werden.

WirtschaftsKurier: Herr Geier, 2013 war das Jahr des Bewusstwerdens, dass es IT-Spionage in großem Stil gibt. Und dass nicht nur Große ausspioniert werden, sondern auch der Mittelstand.
Markus Geier: Ja. Wirtschaftsspionage ist so alt wie die Wirtschaft. Ein bekanntes historisches Beispiel ist die Seide. Im alten China war es bei Todesstrafe verboten, Seidenspinner, deren Raupen oder die Eier außer Landes zu bringen. Etwa im Jahr 550 herum soll es jedoch zwei Mönchen gelungen sein, einige Eier in den Westen zu schmuggeln. So verlor China sein Seidenmonopol. Ironie der Geschichte. Damals war China der Leidtragende, heute zählt es zu den besonders spionageaktiven Ländern. Und was die Größe der ausspionierten Unternehmen betrifft, da besteht nach unten kaum eine Grenze. Nach der Statistik des Bayerischen Innenministeriums betrafen 31 % der im Jahr 2012 registrierten Hackerangriffe Unternehmen mit höchstens 250 Mitarbeitern.

Nicht alle Daten und Fakten sind besonders schützenswert.
Nein, aber alle, die für den Erfolg des Unternehmens von zentraler Bedeutung sind, so rund 5 % bis 10 % der Daten. Dazu gehören alle Unterlagen zu strategischen Vorhaben, Einkaufsdaten, Kalkulationen, Bank- und Kundendaten. Und natürlich die Daten der Forschungs- und Entwicklungsabteilung. Solche „Juwelen" müssen in einen sicheren Safe und nicht ins Bahnhofsschließfach.

In einem Whitepaper warnen Sie vor einer Schatten-IT in den Unternehmen. Was verstehen Sie darunter?
So bezeichnet man IT-Anwendungen und Datenverbindungen, die an der IT-Abteilung vorbei von Fachabteilungen betrieben werden. Häufig ist damit die unautorisierte Nutzung von Cloud-Diensten wie Dropbox oder Google Drive verbunden. Diese werden zur Synchronisation von Dateien zwischen Computern und Personen verwendet, manchmal auch völlig unkontrolliert von Unternehmensfremden.

Die Technik muss stimmen, aber auch der Mensch ist gefordert. So belegen Studien, dass Spionage oft erst durch menschliche Sorglosigkeit möglich wird.
Ja. Es reicht manchmal schon, einen fremden Stick, den man irgendwo erhalten hat, auf einem Firmencomputer zu öffnen. Oder der Sohn des Inhabers schaut im Unternehmen vorbei, klickt dort mal schnell auf seinen Facebook-Account, um zu sehen, wer von seinen 450 weltweiten Freunden etwas Neues gepostet hat. Und schon kann Spy-Software auf dem Computer sein. Viele Unternehmer sind sich dieser Gefahren gar nicht bewusst. Und es gibt natürlich auch den Fall, dass ein Mitarbeiter mutwillig Daten weitergibt. Auf jeden Fall muss jede private Nutzung strikt getrennt werden von der Unternehmens-IT. Das gilt insbesondere auch für Smartphones.

ComCode bietet mit „CyberSpy" einen Service an, um Lecks im Datenverkehr aufzuspüren. Wie funktioniert das?
Mit unserem Service können wir den Datenfluss des Unternehmens transparent machen, ohne dass dieser in irgendeiner Weise gestört wird. Mit modernster und einfach zu installierender Analysetechnik überprüfen wir die gesamte Kommunikation des Netzwerks. Nach dieser Analyse können wir Unregelmäßigkeiten erkennen und so Empfehlungen zur Prävention oder Risikovermeidung geben. Selbstverständlich arbeiten wir dabei ausschließlich im Unternehmen, und die Daten verbleiben im Haus. Personenbezogene Daten werden nicht erhoben.

Wenn es um IT-Sicherheit geht, dann stehen E-Mails oft im Fokus. Sie gelten als besonders leicht abfang- und veränderbar. Raten Sie generell zur Verschlüsselung von E-Mails?
Cyber-Sicherheit ist ein Gesamtkonzept, das die Technik, Prozesse und den Menschen integrieren muss. Sicherlich ist die Verschlüsselung wichtiger Daten einer der Bausteine. Wichtig ist aber, den Schlüssel selbst in der Hand zu behalten oder einen zertifizierten Partner zu haben. Aber selbstverständlich gibt es weitere Bausteine. Bevor ein Unternehmen zum Beispiel eine neue Soft- und Hardware anschafft, muss ein geeignetes Konzept zum Schutz der sensiblen Daten maßgeschneidert werden. Dazu gehören Zugangs- und Zugriffskontrolle, Systemüberwachung, Notfallvorsorge, sichere Verträge mit Externen, ein ISO-27001-zertifiziertes Sicherheitssystem, um nur die wichtigsten Themen anzusprechen.

MIT MARKUS GEIER, GESCHÄFTSFÜHRER VON COMCODE, SPRACH JOSEF KRUMBACHNER