Datenklau: Risikofaktor Mitarbeiter

Heute, 10:59 Uhr

Adriana Zilic

1 2

Kommentare

Wenn es um die Sicherheit ihrer Informationen geht, brauchen vor allem Klein- und Mittelunternehmen (KMU) Nachhilfe. Experten schätzen, dass jeder fünfte Betrieb Ziel von Wirtschaftsspionage wird. Ursache sind oft Angestellte.

Der Fall «EMS-Chemie» ist keine Seltenheit: 2006 schickte ein Mitarbeiter einem befreundeten Unternehmen E-Mails mit geheimen Informationen. Am Freitag wurde er dafür verurteilt.

Bei Schweizer KMU leckt häufig die Informationssicherheit. Der Nachrichtendienst des Bundes ist zum Schluss gekommen, dass «Verbesserungspotenzial» vorhanden sei.

Nun liefert eine deutsche Studie von 2012 Zahlen, welche die Problematik der Industriespionage fassbar machen. Auch für die einheimischen Firmen. Der selbstständige Sicherheitsberater und Experte Wolfgang Sidler ist überzeugt: «Die Ergebnisse sind aufgrund der gleichen Kultur vergleichbar mit unseren Werten».

Mehr zum Thema

Ehemaliger Ems-Mitarbeiter wird schuldig gesprochen

Gestohlene Kundendaten: IT-Mitarbeiter vor Gericht

Via Drucker zu heiklen Daten

Vor allem KMU betroffen

So sei jedes fünfte Unternehmen von Industriespionage betroffen. Ziel von Industriespionage, also Wirtschaftsspionage und Konkurrenzausspähung, sind grösstenteils mittlere Unternehmen, in 25 Prozent der Fälle. Es folgen Konzerne mit fast 20 Prozent und Kleinunternehmen mit 15 Prozent. Der Studie zufolge sind die Zahlen in den vergangenen vier Jahren gestiegen. Und sie geht davon aus, dass sich der Trend fortsetzen wird.

Fast immer spielt das Internet eine Rolle. Angriffe übers Netz haben gar einen Namen: Cyberwar. Also das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung oder Veränderung und Zerstörung des Inhalts einer Webseite. «Ich stelle immer wieder fest, dass ein Sicherheitsbewusstsein zwar vorhanden ist, die Verwaltungsräte und Präsidenten vieler KMU es jedoch nicht vorleben», kritisiert Sidler.

Ungeduldige Manager

Diese Denkweise kann auch Roland Rupp, Vizepräsident des Schweizer KMU-Verbandes, bestätigen: «Leider wird dieses Problem von den Verwaltungsräten und Präsidenten der KMU eher stiefmütterlich behandelt». Dies liege daran, dass der Grossteil nicht wisse, worum es eigentlich geht. «IT-Fachpersonen und Personen aus der Chefetage stammen aus zwei unterschiedlichen Welten.»

Als Beispiel führt Sicherheitsberater Sidler im Ausland angeschaffte Mobiltelefone oder Laptops an: «Statt sie zuerst einem Sicherheitstest zu unterziehen und auf allfällige Risiken und Schwachstellen zu prüfen sowie einen Zugangscode einzubauen, laden sie ihre geschäftlichen E-Mails ungeschützt und direkt darauf. Ein fataler Fehler». Funktionalität und Bedienbarkeit vor Sicherheit.

Das Problem vieler KMU, insbesondere der kleinen: Sie verfügen kaum über einen IT-Sicherheitsbeauftragten und sind schlecht organisiert. Ersteres soll gewährleisten, dass keine Externen in die Unternehmensdatenbank einbrechen oder keine Viren das System befallen. «In der zweiten Situation geht es darum,

Mehr zu Wirtschaft

Gesucht: Ein neuer Chef für Microsoft
23.8.2013

Spionage bei Ems-Chemie: 4000 Franken bedingt
23.8.2013

Goldman Sachs, Morgan Stanley und Co. droht Abstufung des Ratings
23.8.2013

Deutschland erarbeitet Milliarden-Überschuss
23.8.2013

Computerprobleme legen Nasdaq lahm
22.8.2013

Wirtschaft

dass keiner der Mitarbeitenden weiss, wer eigentlich welche Zugriffsberechtigungen zu Unternehmensdaten hat», erklärt Sidler.

Eine weitere Antwort auf leckende Standards in der Informationssicherheit sind unzufriedene Mitarbeiter. Konkret: IT-Spezialisten. Aus ihrer Unzufriedenheit verschaffen sie sich Zugang zu hochsensiblen Kundendaten oder internen Kennzahlen. «Eine hohe Gefahr», resümiert Sidler. Auf diese Weise lassen sich Reihen von Daten auf Excel-Liste problemlos per E-Mail versenden oder auf einen USB-Stick kopieren. «Bei der neuen Arbeitsstelle kommen diese dann zum Einsatz», sagt Sidler. Oder aber sie werden an die Konkurrenz verkauft.

Risiko Mitarbeiter

In der Studie wird dieses Risiko untermauert: «Die häufigsten Schäden entstehen durch eigene Mitarbeiter, externe Geschäftspartner und Hackerangriffe.» Mitarbeiter, die bewusst Informationen weitergeben oder Daten stehlen würden, seien in rund der Hälfte der Fälle Schuld am Informationsabfluss.

Die finanziellen Folgen sind schmerzhaft. Der deutschen Wirtschaft gingen durch Industriespionage jedes Jahr schätzungsweise 4,2 Milliarden Euro verloren, umgerechnet fast 5,2 Milliarden Franken. Zum Vergleich: Die UBS zahlte ihren Mitarbeitern diesen Winter Boni in der Höhe von 2,5 Milliarden Franken. Dabei sind die Fälle, die ans Licht kommen, nur die Spitze des Eisberges, ist Sidler sicher.

Vermeintliche IT-Serviceangestellte

Die dritte Antwort: Leichtsinnigkeit durch Mitarbeiter: Ein Externer betritt ein KMU und gibt sich als IT-Serviceangestellter aus. Er müsse ein Problem mit den Computern beheben. Unmittelbar erhält er Zugang zu sämtlichen elektronischen Daten der Firma. Nach einem Auftrag wird nicht gefragt.

Diese Szene ist nicht aus einem Hollywood-Krimi gegriffen. Sie entspricht der Realität. Siedler bestätigt: «Das kommt tatsächlich vor. Für solche Durchlässigkeit müssen sich die KMU aber selbst verantworten».

Als Faustregel gilt: 8 bis 10 Prozent des IT-Budgets sollten für die Sicherheit eingesetzt werden. Sicherheitsberater Sidler schätzt, dass die effektiven Beträge weitaus tiefer sind.

(Regionaljournal Graubünden, 24.8., 17:30 Uhr; fasc)