„Jedes Unternehmen wird angegriffen“

Bild: Anna Schwartz

Cyberattacken können Firmen um den Lohn ihrer Arbeit bringen – Ein Gespräch mit dem IT-Sicherheitsexperten Professor Dr. Hartmut Pohl

Spionage, Sabotage, Datenklau – das Know-how deutscher Unternehmen ist weltweit begehrt. Laut Digitalverband Bitkom ist jede zweite Firma in den vergangenen zwei Jahren Opfer von Cyberkriminalität geworden. Zwar haben die meisten bereits technische Sicherheitsmaßnahmen ergriffen. Doch die zunehmende Komplexität der Angriffe verlangt zusätzlichen Schutz. In „Circle Cologne“ spricht Professor Dr. Hartmut Pohl, geschäftsführender Gesellschafter der softScheck GmbH, über Fehleinschätzungen, Motive, Täter, Gefahrenquellen und sinnvolle Maßnahmen.

Herr Professor Pohl, laut einer Studie sehen neun von zehn Unternehmen ein hohes Risiko für deutsche Firmen, Opfer von Cyberattacken zu werden. Aber weniger als die Hälfte schätzt das eigene Risiko, betroffen zu sein, als hoch ein. Wie kommt es zu dieser Diskrepanz?

Das hat zum einen etwas damit zu tun, dass man sich das nicht vorstellen kann. Zum anderen weiß die Geschäftsleitung in vielen Fällen nichts davon – ob unbewusst oder absichtlich im Sinne von „Lassen Sie mich mit der Technik in Ruhe“. Generell fehlt es an Sensibilität für das Thema. Eigentlich müsste sie sich sogar fragen: Warum werde ich nicht angegriffen? Sie müsste wissen, dass heutzutage eigentlich jeder angegriffen wird. Damit will ich sagen, dass das Thema in Unternehmen ganz oben angesiedelt werden muss. Die Unternehmensleitung muss mit der Methodik, wie Angriffe erkannt werden können, zwar nicht vertraut sein. Aber ihre Mitarbeiter und die IT-Abteilung darauf hinweisen. Sonst gehen Angreifer in den Rechnern ein und aus.

Welche Branchen sind von Cyberverbrechen besonders betroffen?

Alle! Es sind alle im Blickpunkt. Selbst kleine und mittelständische Unternehmen. Es geht bei Angriffen immer um Geld und >>

Bild: Anna Schwartz

„Die meisten glauben, das Handy ist sicher. Aber das ist es nicht“, sagt Professor Dr. Hartmut Pohl.

>> Macht. Also um Wissen, Patentanmeldungen, Forschungsergebnisse, Planungen, Priorisierungen, Marketingstrategien und die Überlegung: Können wir das im eigenen Land machen? Das ist ein industrielles Vorgehen. Wenn ich ein börsennotiertes Unternehmen noch vor der Veröffentlichung von Umsatz und Gewinn ausspähe, kann ich früh Aktien kaufen. Im Wissenschaftsbereich wurden schon Promotionsarbeiten gestohlen und früher veröffentlicht. Selbst ein Hidden Champion kann betroffen sein – und plötzlich keiner mehr sein, weil sein Produkt nun woanders günstiger angeboten wird.

Wer steckt hinter solchen Angriffen?
In erster Linie sind das Nachrichtendienste. Sie haben den Auftrag, Industriespionage durchzuführen. Sofort danach kommt die organisierte Kriminalität, die gar nicht kontrolliert wird. Organisiert heißt: Das sind keine Einzeltäter. Es gibt Unternehmen, das sind nicht wenige, die Hacks durchführen als Auftragsarbeit. Diese Dienstleister verkaufen Sicherheitslücken mit der Auflage, sie nicht weiterzugeben. So wissen Käufer, wie diese ausgenutzt werden können – und dann greifen sie an.

Und wie gelangen diese in Firmennetze?
Gute Angriffe verlaufen so, dass ein Angreifer eine Sicherheitslücke ausnutzt, die noch nicht veröffentlicht, heißt unbekannt ist. **Der Betroffene merkt den Angriff gar nicht. Im Zweifel sind die Daten weg, bevor der Administrator der Unternehmensleitung eine Liste vorlegen kann. Wenn die Täter dann noch ihre Spuren verwischen, weiß niemand, was gestohlen wurde.** Und dann gibt es natürlich die Möglichkeit, einen Mitarbeiter anzurufen: „Ich bin der Administrator. Ich gebe Ihnen ein neues Passwort, das Sie erst mal testweise benutzen.“ Dann ist man drin und kommt an die Daten, die auf dem Rechner gespeichert sind, und kann im Netzwerk vordringen.

Das heißt, die eigene Belegschaft kann eine Gefahrenquelle sein.
Natürlich. Das sind alles Menschen. Die meisten glauben zum Beispiel, das Handy ist sicher. Aber das ist es nicht. Im Gegenteil. Wer sich von draußen über das Internet einwählt, kann zum Beispiel das Mikrofon einschalten und Gespräche online mithören. Wenn das eine Vorstandssitzung ist, in der es um viel Geld geht, kann das für andere hochinteressant sein. In solchen Fällen sollten Handys vor der Tür abgegeben werden, und es wird kontrolliert, ob jemand zwei hat. SMS, WhatsApp, E-Mail – alles kann abgehört werden. Es sei denn, der Akku wurde vorher herausgenommen.

Ihr Unternehmen identifiziert Sicherheitslücken. Wie stellen Sie sicher, dass diese Daten nicht in die Hände von Dritten kommen?
Wir drucken unsere Prüfberichte auf Rechnern und Druckern, die nicht ans Internet angeschlossen sind. Damit stellen wir sicher, dass von uns nichts abfließen kann. Und am liebsten bringen wir unseren Bericht von Hand zu Hand zum Kunden. Das ist die sicherste Methode – auch für Firmen, die Angebote machen, bei denen es um hohe Summen geht.

Wie kann ich mein Unternehmen denn vor Cyberattacken schützen?
Am einfachsten, indem man Sicherheitslücken, die veröffentlicht sind, beheben lässt. Aber das muss sowieso gemacht werden. Das ist gesetzlich vorgeschrieben. Darüber hinaus müssen aber die unbekannten Sicherheitslücken identifiziert werden. Das kann für die wichtigste Software vollständig gemacht werden. Firewalls zum Beispiel schützen zwar. Aber sie enthalten auch Sicherheitslücken. Jeder, der diese kennt, kann die Firewall-Regeln ändern und kommt durch. Eine Software muss ich also prüfen und patchen lassen. Erst dann kann das Produkt eingesetzt werden.

„Große Firmen schützen sich in der Regel gut. Aber der Mittelstand tut zu wenig.“

Und dann sind da immer noch die Mitarbeiter?
Richtig. Aus meiner Sicht muss die Unternehmensleitung sensibilisieren und überzeugen. Ich muss als Mitarbeiter zum Beispiel wissen, wo Unsicherheiten lauern, damit ich handeln kann. Also zum Beispiel jede E-Mail angucken und entscheiden, ob ich diese öffnen muss oder sofort weglösche, ohne sie zu lesen. Dann ist die Frage, wie oft Passwörter geändert werden und wo sie dokumentiert sind. Sind sie vielleicht auf einem Zettel notiert, der am Bildschirm klebt? Um das Unternehmen haben Sie auch einen Zaun, Videokameras und Schlösser. Man muss aber zudem immer mal wieder gucken, ob der digitale Zaun dicht ist und die Kombination wechseln.

Ich muss mich als Unternehmen also nicht einfach daran gewöhnen, dass die Digitalisierung diese Form der Kriminalität mit sich bringt?
Nein. Es gibt eine ganze Reihe von Unternehmen, die sich nach unseren Erkenntnissen gut abgesichert haben. Wir sind davon überzeugt, dass diese angegriffen werden, aber erfolglos. Letztlich wird jeder angegriffen. Aber große Unternehmen haben wirksame Maßnahmen ergriffen. Das hängen sie jedoch nicht an die große Glocke.

Und wer tut zu wenig?
Das ist definitiv der Mittelstand. Ich vergleiche das gerne mit den Aufgaben eines Geschäftsführers: Der Kontostand wird jeden Tag angeguckt. **Ich würde mir immer überlegen: Welche Daten sind meine wertvollen und welche sind die wertvollsten für meine Mitbewerber?** Natürlich ist es in der Praxis nicht immer möglich, Daten nur auf Rechnern zu speichern, die nicht am Internet hängen. Aber dann muss ich mich zweimal im Jahr prüfen lassen. Und natürlich kann ich eine Versicherung abschließen, die den finanziellen Schaden ersetzt. Aber das ist nicht das Thema. Als Unternehmen will ich arbeiten, produzieren. Und das Wissen dafür muss ich schützen. Das geht nur vorbeugend.

Das Gespräch führte Björn Larsen

Auf den Punkt

Gesamtschaden

Laut aktueller Bitkom-Studie entstand in den vergangenen zwei Jahren durch Wirtschaftsspionage, Sabotage und Datendiebstahl deutschlandweit ein Gesamtschaden von 102 Milliarden Euro.

Faktor Mensch

Bei mehr als der Hälfte der Fälle war nach Angaben von Bitkom ein aktueller oder ehemaliger Mitarbeiter das Einfallstor ins betroffene Unternehmen. Dabei ist Social Engineering, also das Manipulieren von Mitarbeitern, mit 19 Prozent eines der häufigsten Delikte.