«Eine Firma, die sich schützt, ist ein Mehrwert!»

Chris Eckert ist Founding Partner und Geschäftsführer der Swiss Business Protection AG sowie Inhaber der econplus GmbH. Er verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben als Ermittler und Fahndungschef bei der Kantonspolizei Zürich sowie als Kommissariatsleiter der Bundeskriminalpolizei. Hier spricht er über Cyberkriminalität sowie Wirtschaftsschutz.

Bild: zVg

Chris Eckert: «Wenn Firmen Opfer eines Angriffs werden, geht der ganze Betrieb unter.»

Chris Eckert, Ihre Firma, die Swiss Business Protection AG sagt von sich, ein Partner für Wirtschaftsschutz zu sein. Was ist Wirtschaftsschutz?
Chris Eckert: Es geht darum, die Firma gegen Angriffe etwelcher Art von aussen und innen zu schützen. Das gilt für Firmen aller Grössen, also von gross bis klein.

Was heisst «Angriffe von aussen und innen» konkret? Gibt es Beispiele?
Klar: Studien belegen, knapp 50% der Angriffe auf Firmen – sei es konventioneller Art oder digital – haben ihren Ursprung intern, das heisst bei aktuellen und ehemaligen Angestellten. Oft wissen die Mitarbeiter gar nicht, dass sie missbraucht wurden, um einen Angriff durchzuführen oder vorzubereiten. Diese Instrumentalisierung ist aber unter den Hackern sehr beliebt und zielführend.
Ich mache das Beispiel eines Cyberangriffs. Man stellt sich oft vor, dieser geschehe rein elektronisch durch einen Hacker, der weit weg an einer Konsole sitzt. Das ist so falsch. Denn in der Regel geschieht vor einem solchen Angriff human hacking, das so genannte Social Engineering. Darunter versteht man Informationsbeschaffung durch oder mit manipulierten Menschen. Das macht den Angriff dann einfacher, günstiger und schneller.
Im Durchschnitt werden Firmen vier Monate vor dem Angriff «ausspioniert». Das merkt man als geschädigtes Unternehmen noch nicht. Das kann, wie gesagt, geschehen, indem man einen Mitarbeiter aushorcht oder von ihm anderweitig Informationen bekommt. Diese werden dann ausgewertet und aufgrund der so gemachten Erkenntnisse wird der gezielte Angriff umgesetzt.

Und externe Angriffe?
Das sind dann die anderen Themen, die wir kennen: konventionelle Delikte, Diebstahl, Betrug, Drohung, Erpressung und die Cyberangriffe aus der Ferne, also ohne human hacking.

Wirtschaftsschutz ist also ein ganz weiter Begriff?
Natürlich. Oft wird nur über Cyberangriffe gesprochen. Aber es gibt auch und immer noch Betriebsspionage, Betrug, und so weiter. Firmen können auf unterschiedlicher Weise Ziel krimineller Aktivitäten werden und müssen sich dagegen wappnen.
Ich sage es auch anders: Kriminelle oder Menschen und Organisationen mit kriminellen Absichten haben einen Werkzeugkasten. In diesem Kasten sind verschiedene Tools und Anwendungen, die sie gegen ihre Ziele einsetzen können: von Diebstahl bis zu Wirtschaftsspionage.

In der Regel werden die Werkzeuge aus dem Kasten miteinander kombiniert. Deshalb braucht es integralen Wirtschaftsschutz, also einer, die die Kombination der eingesetzten Werkzeuge und ihre möglichen Modus Operandi versteht, die offenen Lücken im Unternehmensschutz kennt und gezielt rechtzeitig die erforderlichen Abwehrmassnahmen organisiert und umsetzt.

Der kriminellen Kreativität sind also keine Grenzen gesetzt.
Nein, Grenzen gibt es keine. Die Akteure suchen die grössten offenen Lücken. Die Schwachstelle bei den Geschädigten, egal ob Unternehmen, Institutionen oder Private, ist seit Jahrzehnten dieselbe: Angriffe sind nur erfolgreich aus Unterlassung. Das Management bis hin zum Verwaltungsrat oder die Eigentümer z.B. in einer Firma schenken dem Thema Integrale Unternehmenssicherheit oder Wirtschaftsschutz keine Beachtung. Sie betreiben keine Früherkennung und beziehen die Mitarbeiter auch nicht ein. Das macht sie zu beliebten und einfachen Zielen.

Aber Hand aufs Herz: Warum sollte eine kleine Schreinerei oder ein Blumenladen integralen Wirtschaftsschutz benötigen? Sie können unmöglich interessante Ziele sein.
Das ist die weit verbreitete Meinung seit Jahren. Sie ist komplett falsch. Nach 14 Jahren Selbständigkeit bin ich fest der Überzeugung, dass selbst die kleine Dorfmetzgerei mit einem seit Generationen überlieferten und geheim gehaltenen Rezept für eine einmalige Wurst kann Opfer werden. Die Realität gibt mir auch Recht, denn selbst Kleinst- und Kleinunternehmen werden angegriffen.
Man muss sich in die Lage der Täter versetzen: Sie haben zwei Ziele, Geld und Macht oder beides. Kleine Täter wollen vielleicht ein bisschen Geld und grosse wollen Geld und Macht ausüben. Und sie wollen erfolgreich sein. Je weniger eine Firma sich schützt, desto erfolgreicher ist der Täter. Fakt ist, viel Kleinst-, Klein- und mittelgrosse Firmen schützen sich nicht oder nicht ausreichend und machen sich so zu Zielen.
Es gibt noch etwas anderes: Jedes Unternehmen hat Kronjuwelen. Diese Kronjuwelen – auch Unternehmenswerte genannt – ist das, was der Betrieb erfolgreich macht. Kronjuwelen können Rezepturen sein – auch für Brot oder Wurst –, sie können Datensätze über Kunden sein, sie können die eigenen Lieferanten sein. Kronjuwelen können alles sein: Prozesse, Lieferantenlisten, Patente, Projekte. Sie sind immer betriebsspezifisch. Aber wenn sie Opfer eines Angriffs werden, geht der ganze Betrieb unter. Das habe ich schon bei vielen Firmen gesehen.
Sie wollen erfolgreich sein. Um hier erfolgreich zu sein, wenden sie alle Mittel ein. Kleinkriminelle wollen Geld, grosse Angreifer wollen auch Macht. Das sieht man heute auf der Ebene der Geopolitik.

Was muss man als KMU tun, um die Kronjuwelen zu schützen?
Zunächst muss man sie kennen oder identifizieren. Dann muss man sie firmenintern kommunizieren. Dann muss man einen Früherkennungsmechanismus aufbauen und durchziehen. Ich mache ein Beispiel aus meiner Praxis.
Eine Firma im Lebensmittelbereich hat die eigene Rezeptur als Kronjuwelen identifiziert. Sie hat die Mitarbeiter angewiesen, niemandem die Rezeptur, Teile davon oder auch die Lieferanten zu nennen. Sie hat die Mitarbeiter auch gebeten, wenn Kundenfragen zur Rezeptur kommen, sich den Kunden und die Frage diskret zu merken und zu melden.
Natürlich kann es reines Interesse der Kunden sein. Umso besser. Aber es kann auch ein Fall von Wirtschaftsspionage sein. Zweiteres würde man nie merken, wenn man nicht frühzeitig die Mitarbeiter einbezogen hätte und nicht relativ systematisch die Informationen gesammelt hätte.

Das hört sich aber für die Firma mühsam an.
Niemand arbeitet gerne im Schutzmodus. Das ist auch gut. Umso wichtiger, wenn die Früherkennung möglichst niederschwellig und sozusagen automatisch erfolgt. Im Übrigen gibt es hier auch einen unternehmerischen Quick Win, also ein direkter Vorteil: Die Auseinandersetzung mit den Kronjuwelen führen dazu, den eigenen Betrieb und die eigene Wertschöpfungskette besser zu verstehen.

Gibt es Ratschläge für einfache Massnahmen, die jeder Betrieb umsetzen kann?
Man sollte mit folgender Geisteshaltung anfangen: Die meisten Mitarbeiter haben ein Interesse an der Firma. Sie wollen den Job weiter ausführen und die wollen, dass es allen gut geht. Das heisst, je mehr sie über den echten Wert des Unternehmens kennen, desto mehr Interesse haben sie am eigenen Job. Diese positive Motivation spielt eine grosse Rolle – auch im Sinne der Produktivität.

Dann ist es auch einfach, mit externen Moderatoren ein Bewusstsein zu schaffen für solche Sachen wie: Will ich Firmeninternas herausposaunen, zum Beispiel über social media? Habe ich gute Passwörter? Sind meine privaten und geschäftlichen Passwörter unterschiedlich? Kann ich Privates von geschäftlichem Trennen, zum Beispiel auf dem Computer oder das Telefon?
Es ist mir schon klar, dass das alles im kleinen Bereich ist. Aber man kann sich gar nicht vorstellen, wie viel das ausmacht. Wenn man diese Aspekte adressiert hat, hat man schon ein ganz anderes Schutzniveau erreicht.

Ist Wirtschaftsschutz nur ein Kostenfaktor? Kann es auch zur Wertschöpfung beitragen?
Eine Firma, die wirklich integrale Sicherheit betreibt, ist auch für Kunden, Mitarbeiter und Lieferanten ein Mehrwert. Dieser Mehrwert bringt auch ökonomische Vorteile, zum Beispiel höhere Produktivität bessere Konditionen und später auch tiefere Versicherungsprämien. Integrale Sicherheit schafft Vertrauen und Vertrauen ist ein wichtiger Hebel des Geschäftserfolgs.

Kann man das in Franken und Rappen beziffern?
Jede Firma misst ihre Produktivität oder die Konditionen individuell. Also könnte man den Vorteil in Geld auch nur individuell beziffern. Am verlässlichsten kann gemessen werden, wenn schon ein Schaden stattgefunden hat und er dank den Schutzmassnahmen viel kleiner ausfällt als er ohne Schutzmassnahmen ausgefallen wäre.

Wie bin ich als Privatperson auch vulnerabel?
Wenn man nirgendswo arbeitet und das Internet nicht nutzt, ist man wenig vulnerabel. Doch solche Leute sind nicht in der Mehrheit heute. Also: Wenn man irgendwo arbeitet, kann man schnell zum Ziel werden. Selbst wenn man meint, nur ein «kleiner Fisch» zu sein, kann man für Kriminelle interessant werden.

Wenn man Opfer eines Angriffs wird, was soll man tun?
Dann ist das leider zu spät. Erste Priorität sollte sein, dass man technisch nicht weiter angreifbar ist. Also sollte man alle Prozesse unterbrechen und angegriffene Systeme isolieren.
Die Kommunikation gehört auch zu den wichtigsten Sofortmassnahmen. Es ist ganz schlecht, nichts zu sagen. Man sollte spezifische Botschaften für Mitarbeiter, Kunden und Lieferanten vorbereitet haben. Dann braucht man auch einen Notfallplan: Wer macht was und was wird wem delegiert.
Es ist darauf zu achten, dass das Krisenmanagement nicht von der gesamten Geschäftsleitung gemacht wird. Das Notfall- und Krisenmanagement bewältigt die Krise. Die Geschäftsleitung ist für die Weiterführung der Firma zuständig. Beides parallel zu erledigen ist gerade bei den heutigen Angriffsformen mit mehreren Tagen Krisenmodus zum Scheitern verurteilt. Herkules und James Bond in einer Person gab es noch nie im richtigen Leben.
Man muss sich auch von Anfang überlegen, ob und mit welchen forensischen Mitteln und Ermittlungshandlungen ich herausfinden kann, wer mich wie angegriffen hat und ob ich mit der Täterschaft allenfalls verhandeln kann, z.B. bei Ransomware Angriffen. Schliesslich spielt der Gedanke über das Erstatten einer Strafanzeige ebenfalls eine Rolle.

Interview: Henrique Schneider

Zur Person:

Chris Eckert ist seit 2009 selbständig tätig und Geschäftsführer sowie Gründungspartner der Swiss Business Protection AG swissbp.ch. Als Senior Consultant, Kriminalist und CSO befasst er sich mit den Bereichen Informationssicherheit, Forensik und Kriminalprävention. Er unterrichtet zu diesen Themen wie auch zu Social Engineering / Human Hacking an anerkannten Ausbildungsinstituten. Er ist zudem Studiengangsleiter CAS Business Protection an der HWZ. Ch. Eckert verfügt über mehr als 30 Jahre kriminalistische Erfahrung, zuerst als Ermittler und Fahndungschef bei der Kantonspolizei Zürich, anschliessend als Kommissariatsleiter der Bundeskriminalpolizei im Bereich der Organisierten Kriminalität. Sein praktisches Wissen und die Erfahrungen in Wirtschaftskriminalität, Cyberattacken sowie Industrie- und Wirtschaftsspionage gibt er gerne weiter.

https://fh-hwz.ch/produkt/cas-business-protection/