Bedrohliche Wirtschaftsspionage

Firmen werden systematisch gehackt und ausgenommen. Nicht nur mit Cyberangriffen, auch alte Methoden funktionieren. Rund 30 Prozent der Betriebe sind betroffen

Andreas Schmid

Die Chefsekretärin erhält den Auftrag kurz vor Feierabend. Vor 17 Uhr solle sie 30 000 Franken auf ein italienisches Konto überweisen, so steht es in einer E-Mail ihres Vorgesetzten. Es bleibt nur noch eine Viertelstunde Zeit, in der Eile verzichtet die Angestellte auf Rückfragen und zahlt das Geld via E-Banking ein. Die Nachricht ist ja von ihrem Chef.

Doch sie irrt, wie sich später herausstellt. Nicht ihr Chef, sondern ein Internetbetrüger hat per E-Mail die Überweisung veranlasst. Der Schaden lässt sich nicht mehr beheben und die Spur zum italienischen Konto ebenso wenig nachverfolgen.

Auch nicht vom Unternehmensschutzexperten Chris Eckert, der mit dem Fall betraut wurde. Der einstige Fahndungschef der Kantonspolizei Zürich unterstützt Firmen, die betrogen oder ausspioniert wurden. Mit raffinierten Methoden erzeugten Kriminelle Hektik, die Firmen und ihre Angestellten zu Fehlern verleite, sagt er.

Was kaum bekannt ist: Solche Nachlässigkeiten werden längst nicht nur zur schnellen Bereicherung genutzt, sondern vor allem für Industrie- und Wirtschaftsspionage. Diese funktioniert nämlich häufig nicht wie in Hollywood-Filmen, sondern ist so simpel, dass sie kaum auffällt. Eckert nennt Beispiele aus seinem Alltag: So würden Mitarbeiter von privaten Sicherheitsdiensten oder Reinigungsfirmen darauf angesetzt, während ihrer Einsätze Passwörter von Post-it-Zetteln abzuschreiben oder herumliegende Computer-Sticks einzupacken. Weil dies ausserhalb der Betriebszeiten geschehe, blieben solche Aktionen oft unbemerkt, sagt Eckert. «Wenn doch, stellt sich vielfach heraus, dass niemand die richtigen Personalien der getarnten Spione kennt, die Zutritt zur Firma hatten.»

Spionierende Handwerker

Chris Eckert weiss auch von Vorfällen mit Handwerkern, die in fremdem Auftrag in Sitzungszimmern Abhörgeräte installierten oder Präsentationen fotografierten. Wenn er dann eingeschaltet werde, fänden er und sein Team nur noch Netzgeräte oder abgerissene Kabel, sagt er.

Unternehmen sähen sich heute zudem permanent Cyberangriffen ausgesetzt und seien gezwungen, ihre IT-Infrastruktur unentwegt anzupassen, erklärt Eckert. Auf die Komplexität der Bedrohungen seien viele Betriebe nicht vorbereitet. Der Spezialist berät solche Unternehmen mit seiner Firma Swiss Business Protection, und ab Frühling wird er an der Hochschule für Wirtschaft Zürich einen neuen Lehrgang leiten, in dem er Firmenverantwortliche in Unternehmensschutz schult.

Um sich zu wappnen, müssten Firmen spezifische Abwehrmassnahmen treffen, sagt Eckert. Dafür müsse die ganze Belegschaft für Gefahren sensibilisiert werden. «Die grösste Schwachstelle ist nach wie vor der Mensch.» Sei es aus Naivität, sei es bewusst: Mitarbeiter, die Geschäftsgeheimnisse ausplauderten, Unbekannten Einblick in neue Entwicklungen gewährten oder sogar aktiv Konkurrenten bedienten, schädigten Unternehmen am meisten. «Viele Betriebe sind wie ein Löchersieb.»

GETTY IMAGES

Abwehrexperte Chris Eckert.

Bei der Hälfte der Fälle seien einst oder derzeit Angestellte einer Firma involviert.

Die verbreitete Meinung, Wirtschaftsspionage komme nur gelegentlich vor, sei irrig, sagt Chris Eckert. In Konferenzräumen und in Hotels, in denen Geschäftsleitungen ihre Sitzungen abhielten, um nicht abgehört zu werden, habe er schon mehrfach Wanzen und andere Indizien für kriminelle Aktionen gefunden. Häufig seien es Mitbewerber, die ihre direkten Widersacher im Markt aushorchten. Manche praktizierten das auch, indem sie versuchten, Praktikanten in Konkurrenzfirmen einzuschleusen. Weil Spionageangriffe kaum zu entdecken und noch schwieriger nachzuweisen seien, blieben die Auftraggeber meist im Dunkeln. Eckert sagt aber, vieles deute darauf hin, dass diese nicht nur aus der Privatwirtschaft stammten. «Auch Staaten wie China, Nordkorea, Russland und andere osteuropäische Nationen scheinen im Hintergrund zu agieren.»

Der Nachrichtendienst des Bundes (NDB) erachtet Wirtschaftsspionage als ernst zu nehmende Gefahr für die Schweiz. Als Sitz internationaler Organisationen und multinationaler Konzerne sowie als Forschungsstandort und Schauplatz internationaler Anlässe sei unser Land «in vielerlei Hinsicht ein anziehendes Spionageziel», sagt NDB-Kommunikationschefin Isabelle Graber.

Hackerangriffe sind oft nicht nachzuverfolgen, die Urheber bleiben unerkannt und ihre Attacken unbemerkt.

«Internationale Spannungen widerspiegeln sich auch in Aktivitäten fremder Staaten, die ihre Gegner auf Schweizer Boden ausspionieren.» Graber räumt ein: Der NDB konzentriere sich auf die aktivsten und aggressivsten Geheimdienste, die gegen Schweizer Interessen handelten. Der Anstieg von staatlich initiierten Cyberattacken dürfte laut der Sprecherin anhalten.

Um wissenschaftliche Daten zu Wirtschaftsspionage in der Schweiz zu erhalten, liess der NDB am Institut für Strafrecht und Kriminologie der Universität Bern eine Studie erarbeiten. Darin stellen die Autoren fest, dass rund 30 Prozent der befragten Firmenvertreter Angriffe erlebt hatten. Entscheidend für die Gefährdung sei nicht die Grösse eines Unternehmens, sondern das Wissen, sagt Studienleiter Ueli Hostettler. Bei der Hälfte der entdeckten Fälle seien einst oder derzeit Angestellte einer Firma involviert. Als Lecks erwiesen sich etwa Betriebsführungen, Messen, Auslandsreisen von Personal sowie der Datenaustausch mit Kunden. Hostettler sagt, viele Firmen seien sich der Bedrohung durch Wirtschaftsspionage zwar bewusst, investierten aber trotzdem nur wenig in die Prävention.

Für Attacken besonders anfällig sind laut Fachmann Chris Eckert international tätige Konzerne, für die Forschung, Technologie und Infrastruktur massgebend sind. Als Beispiele nennt er Pharmaunternehmen, IT-Firmen oder Energiezulieferer. In diesen Branchen sei vor allem der Cyberschutz wichtig. Weil die Urheber von Attacken kaum auszumachen seien, zeitige ein strafrechtliches Vorgehen gewöhnlich keinen Erfolg.

Experten gehen davon aus, dass die meisten Cyberangriffe auf Firmen in der Schweiz nicht publik werden. Unternehmen befürchteten, Ziel weiterer Attacken zu werden und Schwächen im Abwehrsystem einzuräumen, wenn sie sich als Hacker-Opfer zu erkennen gäben, erklären Beobachter das Schweigen. Zudem bringe eine Meldung den Betroffenen keinen Nutzen, da keine staatliche Hilfe damit verbunden sei.

Politik schaltet sich ein

Der Bundesrat will nun allerdings erwirken, dass sicherheitsrelevante Cyberangriffe künftig gemeldet werden müssen. Im vergangenen Dezember beschloss er, dass Betreiber von kritischen Infrastrukturen wie Energieversorger, Telekommunikationsanbieter oder Banken verpflichtet werden sollen, Cyberattacken einer zentralen Stelle kundzutun. Bis Ende Jahr sollen die rechtlichen Grundlagen dafür geschaffen werden. Die Meldungen erlaubten dereinst das Absetzen von Frühwarnungen, begründet der Bundesrat. Heute können sich Betreiber kritischer Infrastrukturen freiwillig über Cyberangriffe austauschen; als Anlaufstelle dient das Nationale Zentrum für Cybersicherheit im Finanzdepartement.

Die Digitalisierung erhöhe die Risiken, dass die Kronjuwelen einer Firma – wichtige Daten, vertrauliche Entwicklungen und wertvolle Patente – entwendet würden, sagt Unternehmensschützer Chris Eckert. Cyberattacken richteten nicht nur materiellen Schaden an, sondern lädierten auch die Reputation. Deshalb seien vom Weltkonzern bis zum Familienbetrieb alle bedroht. Eckert zitiert einen deutschen Fachmann, der sagt: «50 Prozent der Unternehmen wurden schon gehackt, die anderen 50 Prozent haben es noch nicht gemerkt.»

In Kürze

Neuer Wahlmodus für Bundesanwalt?

Der Bundesanwalt soll künftig zwei Jahre nach den eidgenössischen Wahlen bestimmt werden. Die Rechtskommission des Nationalrats hat einer parlamentarischen Initiative zugestimmt, die diesen Modus vorschlägt. So könne eine Politisierung des juristischen Amts verhindert werden, lautet die Begründung für den Vorstoss. Die Nachfolge des zurückgetretenen Bundesanwalts Michael Lauber hätte im letzten Dezember geregelt werden sollen. Da keine geeignete Kandidatur vorlag, wurde die Stelle neu ausgeschrieben. *(zzs.)*

Raubüberfall im Kanton Aargau

Zwei unbekannte Personen haben am frühen Samstagmorgen in Staffelbach im Kanton Aargau ein Detailhandelsgeschäft überfallen. Die Täter erbeuteten mehrere tausend Franken. Sie bedrohten die Verkäuferin mit einer Pistole und verlangten Geld. Trotz sofort eingeleiteter Fahndung entkamen die zwei Männer, wie die Polizei mitteilte. Die Verkäuferin blieb unverletzt. *(zzs.)*

16 Bewohner nach Feuer evakuiert

In Bubikon im Kanton Zürich hat am Samstag ein Mehrfamilienhaus gebrannt. Die Feuerwehr musste 16 Bewohner der Liegenschaft evakuieren, wie die Polizei in einem Communiqué bekannt gab. Die Einsatzkräfte hätten das Feuer rasch unter Kontrolle gebracht. Verletzt wurde niemand. Der entstandene Schaden beträgt rund eine halbe Million Franken. Die Brandursache ist nicht bekannt. *(zzs.)*

Zwei tote Kinder in Gerlafingen

Im solothurnischen Dorf Gerlafingen hat die Kantonspolizei am Samstagmorgen zwei leblose Kinder in einer Wohnung aufgefunden. Aufgrund der Situation, die die Polizei vor Ort antraf, sowie nach ersten Ermittlungen sei von einem Gewaltverbrechen auszugehen. Die Mutter der Kinder wurde gemäss Polizeimitteilung als dringend tatverdächtige Person festgenommen. *(zzs.)*

Classe politique

Petra Gössi, Polit-Poliererin, veredelt ihr Tun. Unter dem Motto «Reden ist Silber, Handeln ist Gold» kündigte die Chefin der FDP zum Jahresbeginn an, man werde fortan alle vergangenen und künftigen Taten der Partei zugunsten des Umwelt- und Klimaschutzes auf der Website Blueprints.ch dokumentieren. Doch noch immer ist auf der entsprechenden Site nichts zu finden – ausser einer Rede von Gössi. Wir gratulieren ihr damit herzlich zur Silbermedaille.

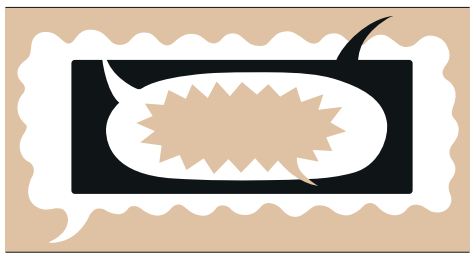
Walter Wobmann, Gesichtsleser, kriegt es mit unsichtbaren Mächten zu tun. Ein Baselbieter Informatiker hat ein Machine-Learning-Modell erfunden, das allein aufgrund der Texte im Abstimmungsbüchlein den jeweiligen Ausgang voraussagt. Und für den Präsidenten der Initiative für ein Burka-Verbot ist die Prognose keine gute: Die Chance, dass Wobmann damit am 7. März gewinnt, liegt demnach bei mickrigen 5,1 Prozent. Immerhin: Das ist immer noch weit höher als das Risiko, auf Schweizer Strassen einer Burka zu begegnen.

Petra Gössi

Walter Wobmann

FOTOS: KEYSTONE

Seid umschlungen, Despoten



Showdown
Daniel Friedli

Lieber Vorstand, liebe Eishockey-Familie. Ich bin zurück aus Minsk und kann euch Erfreuliches berichten. Das Treffen mit Staatschef Alexander Lukaschenko ist gut verlaufen. Wir bleiben im Dialog, um unsere Eishockey-WM im nächsten Mai wie geplant in Weissrussland durchzuführen.»

«Gratulation, Herr Präsident. Endlich wieder einmal gute News! Nur die Bilder, die natürlich sofort um die Welt gegangen sind, die waren schon etwas heikel.»

«Wieso denn?»

«Es geht um die Vorbildrolle, Präsident. Niemand versteht, wie man jetzt ein solches Treffen abhalten kann. Und dann noch die innige Umarmung von Lukaschenko.»

«Ich muss zugeben: Ich habe in Minsk etwas mit dem Feuer gespielt. Und wir haben uns etwas verbrannt. Aber ich bin überzeugt, dass ich nichts Falsches gemacht habe.»

«Natürlich nicht. Aber Sie wissen ja auch: Bilder sagen mehr als tausend Worte.»

«Aber das heisst doch nicht, dass man nicht miteinander reden soll. Ich kenne Lukaschenko seit 20 Jahren und habe früher mit ihm Eishockey gespielt. Ich wollte das nutzen, um etwas Gutes zu tun.»

«Völlig klar. Es geht uns nur um das Wie.»

«Genau. Und unser Wie ist der Sport. Wir wollen, dass diese WM zur Versöhnung von Regierung und Opposition führt. Ich bin ein Idealist des Sports. Sport hat die Macht, Menschen zu vereinen. Denkt daran, wie die Chinesen sagten, Olympia in Peking helfe ihnen, die Menschenrechte zu entwickeln. Oder wie Putin versprach, Sotschi werde Freundschaften vertiefen. Und mit der Fussball-WM in Katar und der Formel 1 in Bahrain bringen wir die Scheichs auf Schmusekurs.»

«Sicher. Aber auch der Sport muss sich an gewisse Regeln halten.»

«Ja, und die erste olympische Regel hiess bekanntlich: *All sports, all nations.* Und schon Kollege Gian Franco Kasper vom Welt-Skiverband hat ja richtig gesagt: In Diktaturen läuft eben alles etwas einfacher.»

«Logisch. Aber die Zeiten haben sich geändert, die Leute sind heute sensibler.»

«Ja Herrgott! Was wollt ihr denn hören?»

«Wir veröffentlichen eine Entschuldigung und räumen ein: Unser Präsident hätte bei dieser Umarmung selbstverständlich eine Corona-Schutzmaske tragen sollen.»