
Business Punk
WORK HARD. PLAY HARD.
AUSGABE 01_2014 6€ Euro WWW.BUSINESS-PUNK.COM
INSIDE „STROMBERG“
CAST UND CREW VERRATEN: ALLES
NETFLIX
Die „House of Cards“-Erfinder wollen das deutsche Fernsehen plattmachen
SNAPCHAT
Selbstzerstörung als Prinzip: Darum pfeifen die Typen mit der Fotoapp auf die Facebook-Kohle
HASS IM BÜRO
Das Arschloch muss weg. So wird man es los
FUCK OFF, NSA!
Mit PIRATE BAY kämpfte er gegen die Webzensur, jetzt zieht Peter Sunde in den Krieg gegen den Abhörterror
PLUS DOSSIER IT-SICHERHEIT
NO-SPY-STARTUPS /// JAGD AUF SCHNÜFFLER /// CROWD GEGEN HACKER

HALT

Ausgabe
01
2014

↗ briefing

↗ play

↗ work

↗ quick'n'dirty

FOTOLIA, GARY S. AND VIVIAN CHAPMAN/GETTY IMAGES, WILLI WEBER/BRAINPOOL, JONAS LINDSTRÖM/REINVOLLENGA.BLOGSPOT.COM, SONY PICTURES TELEVISION, INC. AND SHOWTIME NETWORKS INC. ILLUSTRATION: RAMONA RING

DER SPION, DER MICH LEAKTE

Liest Barack Obama wirklich alle Mails von BMW? Ist in der **Wirtschaftsspionage** nach Prism die gute, alte Sexfalle noch zeitgemäß? Ein Security-Profi plaudert für uns aus dem Nähkästchen – und gibt Tipps fürs sichere Startup-Leben

Interview: **Joachim Hentschel**

Er sei „langjähriger Mitarbeiter einer deutschen Sicherheitsbehörde" gewesen, formuliert Frank Schurgers diplomatisch, wenn man ihn nach dem Lebenslauf fragt. Genauer wird die Auskunft nicht – sollte man auch nicht erwarten von einem Mann, der in der Branche dafür berühmt ist, Geheimnisse besser verteidigen zu können als alle anderen. Nach der ominösen Behördentätigkeit war Schurgers unter anderem Leiter der Konzernsicherheit bei Reemtsma, gründete 2004 seine eigene Security-Firma: Integris, ansässig in New York und Berlin, gehört zu den weltweit führenden Beratungsunternehmen für Opfer von Wirtschafts- und Betriebsspionage, für Vorbeugung, Nachermittlung. Keine der lustigen Detekteien, die von abenteuerlustigen Ex-Polizisten und Wachmännern eröffnet werden, sondern eine Agentur, die auch dahin geht, wo's richtig, richtig wehtut. Und dass Wirtschaftsspionage seit dem NSA-Skandal plötzlich auch bei Günther Jauch debattiert wird, kann dem Integris-Chef nur recht sein. Oder auch nicht.

Frank Schurgers, als die Snowden-Enthüllungen kamen und da plötzlich auch von Wirtschaftsspionage die Rede war, die die USA in Deutschland betrieben haben sollen – da stand das Telefon sicher nicht mehr still bei Ihnen, oder?

Nicht ganz, aber eine deutliche Zunahme der Anfragen gab es definitiv. Viele Firmen wurden durch die Nachrichten sehr verunsichert.

Ihr Kundenstamm hat sich vergrößert?

Ja, das hat er. Genaue Zahlen kann ich nicht nennen, weil man ja auch nicht voraussagen kann, ob das dauerhaft so bleibt oder eine Eintagsfliege war. Ganz grob: In den letzten sechs Monaten war es ein Zuwachs um rund 20 Prozent. Das Thema Wirtschaftsspionage ist ziemlich nach oben gekocht. Viele denken erst jetzt richtig darüber nach.

Das gehört auch zu Ihrem Job: die Wirtschaft für die ständige Gefahr zu sensibilisieren. Sind Sie Edward Snowden dankbar?

Dazu muss man sagen, dass die Enthüllungen ja vor allem die technische Überwachung betreffen, Telefon, Internet, E-Mails. Aber das ist nur eine Facette des Problems. Menschliche Informationsbeschaffung ist mindestens genauso wichtig. Für die Geheimdienste bleiben die menschlichen Quellen ein Schwerpunkt. Die Aufklärung mit technischen Mitteln kommt dann hinzu.

Was dann ja heißen würde: So hilfreich die Leaks sind, sie lenken die Aufmerksamkeit zu stark auf die technisch basierte Spionage. Was eine falsche Sicherheit wäre.

Definitiv. Im Moment herrscht der Eindruck: Wir leben unter Totalüberwachung. Natürlich sind heute die technischen Möglichkeiten unglaublich weitreichend, und vor allem in der deutschen Wirtschaft gab es immer schon einen großen Mangel an Sensibilität, was Wirtschaftsspionage angeht, vor allem bei Mittelständlern und Startups, die sich keine eigene Security leisten. Wenn überhaupt etwas gemacht wird, dann eher technische Absicherung, aber das ist zu wenig. Informanten, eingeschleuste Agenten, menschliche Quellen, das sind die entscheidenden Punkte.

Wussten Sie als Insider denn schon vorher von Prism? Jetzt können Sie es ja zugeben …

Sagen wir es so: Dass Geheimdienste mit solchen Methoden arbeiten, dass da unter Umständen auch das Handy der Bundeskanzlerin abgehört wurde – natürlich passiert das, jeder weiß das! Wir haben seit Jahren mit unseren Kunden besprochen, dass man mit einem solchen Szenario rechnen muss. Wenn eine Firma im internationalen Wettbewerb steht, und in dem steht ja jedes größere deutsche Unternehmen, sollte man dieses Risiko ansprechen.

Gab es wenigstens noch etwas an den Enthüllungen, das Sie überrascht hat?

Ja, einen Punkt hatte ich so nicht erwartet: dass auch der postalische Briefverkehr in den USA kontrolliert und erfasst wurde. Das erinnert mich eher an die Stasi. Ich frage mich ernsthaft, ob hier die Ergebnisse den Aufwand rechtfertigen. Stellen Sie sich vor, Sie bieten über Ebay einen Artikel an, und eine Frau aus New York ersteigert ihn. Sie schicken ihr das Paket, schon stehen Sie im Computer mit ihr in Verbindung. Dummerweise wohnt vielleicht im Apartment neben ihr ein Mann, den aus irgendwelchen Gründen das FBI im Visier hat. Und es ist bekannt, dass sie ab und zu seine Post in Empfang nimmt. Plötzlich stehen Sie auf einer nicht öffentlichen Überwachungsliste! Tja, auch ein Geheimdienst verrennt

sich manchmal in Richtungen, die ihn am Ende ineffizient machen.

Es gibt seit Kurzem schwerfällige Versuche, die Auswüchse durch ein No-Spy-Abkommen zu unterbinden. Was halten Sie davon?

Wirtschaftsspionage unter Freunden unterbinden? Völlig naiv! Schauen Sie mal ins Lexikon: Die originäre Aufgabe eines Geheimdiensts ist der Schutz der Nation mithilfe nachrichtendienstlicher Erkenntnisgewinne. Welches effektive Vertragswerk soll hier Grenzen ziehen? Und dass die amerikanischen Dienste ihre Informationen auch an die Wirtschaft weitergeben, das ist eben so. Weil es in den USA eine viel stärkere Kooperation zwischen Staat und Wirtschaft gibt, viel stärker als in Deutschland.

Hatten Sie bei Integris Fälle, die am Ende auf US-Spionage hinausliefen?

Ich kenne zumindest einen Fall, in dem ein deutsches Unternehmen feststellte, dass auf seine IT-Systeme zugegriffen wurde. Die Sicherheitsbehörden konnten den Datenklau eindeutig einem Amerikaner zuordnen, der sich in Deutschland aufhielt. Und es stellte sich dann heraus, dass er Mitarbeiter eines amerikanischen Geheimdiensts war. Er wurde dann ausgewiesen, das gab Ärger. Allerdings: Er hatte einen Fehler gemacht, sonst wäre er nicht erwischt worden. Die Dunkelziffer müsste in dem Bereich relativ hoch sein.

Die Amerikaner sind ja bei Weitem nicht die Einzigen, oder?

Ich habe vor zwei Jahren einen Fall bearbeitet, für ein relativ kleines deutsches Unternehmen, absolute Hochtechnologie im Bereich Automobilantrieb. Die Firma hatte nur ein einziges Produkt, damit stand man im vorderen Bereich der weltweiten Forschung, vielleicht ein, zwei Jahre vor der Markteinführung. Weil die Firma ständig auf der Suche nach Investoren war, wurden auch chinesische Stellen aufmerksam. Es gab Gespräche mit Delegationen, das zog sich hin. Etwa zur gleichen Zeit bewarben sich mehrere chinesischstämmige Personen bei der Firma als Mitarbeiter. Einer wurde eingestellt, ein hochqualifizierter Mann, der in dem relativ kleinen Unternehmen dann auch Zugriff auf alle Daten hatte. Was wir hinterher rekonstruieren konnten: Der Mitarbeiter hat in über einem Jahr systematisch alle Forschungsergebnisse und sonstigen Daten heruntergeladen und eins zu eins nach China weitergegeben. Dass da etwas faul war, merkten die erst, als die Delegationen ganz abrupt die Gespräche abbrachen. Da war es zu spät.

Und dann?

Für das Unternehmen war es das Ende. Ob das Produkt, um das es ging, mittlerweile von einer chinesischen Firma auf den Markt gebracht wurde, weiß ich nicht. Würde mich aber nicht wundern. Ein anderer Fall: ein deutsches Maschinenbauunternehmen mit Tochtergesellschaft in China. Eigentlich recherchierten wir einen Betrugsfall, aber dabei stießen wir auf Sachen, die uns komisch vorkamen. Unter anderem fanden wir heraus, dass in dem Unternehmen zwei Mitarbeiter des chinesischen Geheimdiensts saßen. Klar: In China ist es völlig normal, dass ein paar Leute aus der Firma an die Behörde berichten. Das Besondere hier war, dass der Dienst zwei seiner eigenen Leute implantiert hatte. Das gibt es eher selten. Die Firma gehört zwar zu den Weltmarktführern, ist aber schon seit 50 Jahren in China aktiv, hat fünf Fabriken dort, nichts Militärisches. Es passiert trotzdem.

Kann man sich dagegen überhaupt schützen?

In manchen Fällen schon, wenn man nicht zu naiv ist. Wir haben erlebt, dass ein Unternehmen neue Büros in Peking bezog. Die Etage darüber war komplett leer, was niemandem verdächtig vorkam. Später bemerkten wir, dass alle diese Büros komplett überwacht wurden, mit Videokameras und Mikrofonen, die in der Zwischendecke steckten. Das hätte das Unternehmen natürlich selbst herausfinden können, aber man hat bestimmte Fragen nicht gestellt: Wem gehört das Gebäude? Wer sind meine Nachbarn? Wieso ist die Etage über mir nicht vermietet? Der Metalldetektor aus dem Baumarkt hilft da natürlich nicht.

Der Beratungskonzern Ernst & Young hat im Sommer 2013 eine Umfrage veröffentlicht, für die deutsche Wirtschaftsvertreter das Gefährdungspotenzial bestimmter Länder einschätzen sollten. Die USA, die davor als eher harmlos galten, standen dieses Mal im Ranking schon knapp hinter China.

Ein Ergebnis der momentanen Stimmung, nicht viel mehr. Andere Nationen, die mindestens so aggressiv gegen deutsche Firmen arbeiten, werden in der Studie überhaupt nicht erwähnt. Südkorea, Japan, Frankreich. Jedes Land betreibt solche Maßnahmen im Rahmen seiner Möglichkeiten. Es gibt da keine Zurückhaltung. Warum auch? Das ist die originäre Aufgabe der Geheimdienste!

Aber ist es nicht gut, dass die Wirtschaft das Potenzial der USA ernst nimmt? Oder führt das wieder dazu, dass man andere Gefahren noch stärker ausblendet?

Es macht für mich ja keinen Unterschied, ob ich von einer amerikanischen, chinesischen oder russischen Stelle ausspioniert werde. Oder auch von einem Konkurrenzunternehmen. Alle Branchen sind betroffen, auch die, an die man nicht gleich denkt. Zum Beispiel: Agrartechnik. Die fällt den meisten nicht gleich ein, wenn man über Wirtschaftsspionage spricht. Aber für Länder wie China, Russland oder Indien ist die Versorgung der eigenen Bevölkerung ein Riesenthema.

Ist die Sicherheitsbranche im Aufschwung?

Man kann beobachten, dass sich in den letzten fünf Jahren die Investoren und Venture-Capitalists mehr und mehr für uns interessieren. Das sind Leute, die von dem Metier eigentlich keine Ahnung haben, aber da jetzt Potenzial sehen. Ich bin zuletzt oft angesprochen worden: „Wir würden eine Firma wie Ihre gern in unser Portfolio aufnehmen, hätten Sie nicht Lust, zu uns zu kommen?“ Es gibt weltweit eben viele kleine Einzelkämpfer, die entweder nicht lange überleben oder von Platzhirschen aufgekauft werden. In dem sehr speziellen Segment, in dem wir arbeiten, ist dagegen wenig Bewegung. Da gibt es Unternehmen, von denen hat die Öffentlichkeit noch nie gehört. Wenn Sie nicht genau wissen, wer das ist und wo die sitzen, finden Sie die gar nicht! Das sind die wirklich guten.

Für die es sicher nicht leicht ist, geeignete Mitarbeiter zu finden.

Gute Gegenspione.

Die Anzahl der Firmen, die das auf höherem Niveau machen, ist überschaubar. In Deutschland sind es maximal zwei oder drei, in den USA natürlich ein paar mehr. Meistens sind das Unternehmen, die von ehemaligen Geheimdienstmitarbeitern gegründet wurden, absolute Spitzenleute ihrer Dienste, die irgendwann in die Wirtschaft gegangen sind. Das sind Profis, die all ihre Erfahrungen und Kontakte aus jahrzehntelanger Agententätigkeit mitbringen. Davon gibt es nicht viele.

Business-Intelligence à la James Bond?

So stellen Sie sich das vor, ja? Ein Beispiel, um von der staatlichen Spionage wegzukommen: Ein französisches Unternehmen, Weltmarktführer in der Automobilbranche, beauftragt einen privaten Dienstleister mit Recherchen über einen unmittelbaren Wettbewerber in Osteuropa. Die wollen exakt wissen: Welche Marktstrategien hat die Konkurrenz, welche Preise, Lieferantenbeziehungen, Produktionskapazitäten? Alles Informationen, die Sie nicht über Google finden. Da geht es um Marktanteile, um Millionenumsätze. Dass ein Dienstleister hier alle Erfahrungen und nachrichtendienstlichen Fähigkeiten einsetzt – das heißt nicht, dass er illegale Methoden braucht. Sicher bewegt man sich ab und zu in einer Grauzone. Die Diskussion, ob Business-Intelligence legal ist oder nicht, die müssen wir jetzt nicht führen.

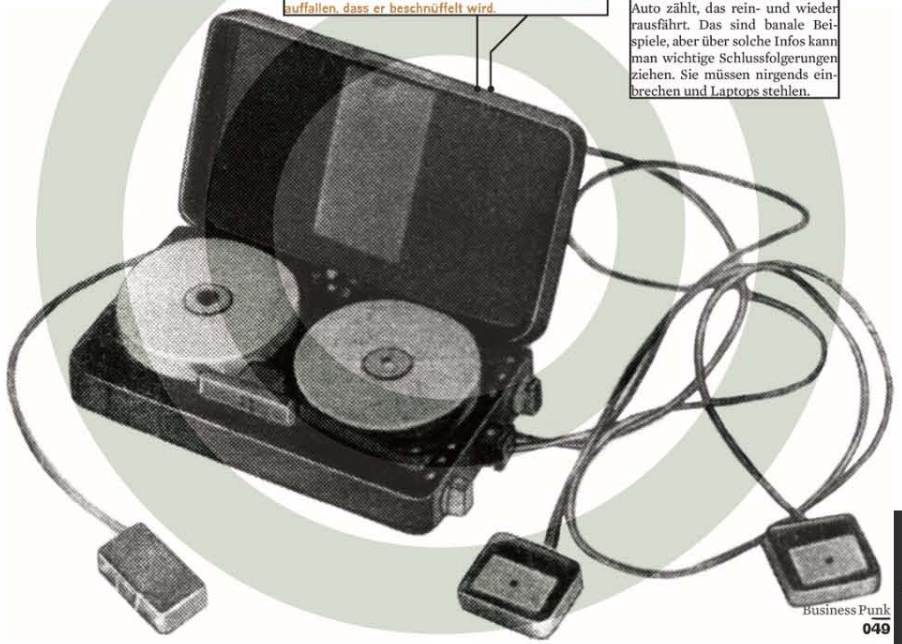
Trotzdem könnte es dem anderen Konzern natürlich auffallen, dass er beschnüffelt wird.

Ist ihm aber nicht aufgefallen. Obwohl es solche Fälle ja gibt, sehr prominent: Samsung gegen Apple, Procter & Gamble gegen Unilever, SAP gegen Oracle. Da haben Business-Intelligence-Recherchen vor Gericht geendet. SAP musste an Oracle vor ein paar Jahren 120 Mio. Dollar zahlen, für offenbar geklaute Software und Datenbanken. Da geht es schon ans Eingemachte.

Wo würden Sie die Linie ziehen?

Qua Definition ist Business-Intelligence legal. Es gibt so viele Möglichkeiten, Informationen völlig legal zu beschaffen und auszuwerten. Die meisten Unternehmen haben nur nicht die Expertise oder die nötigen Verbindungen. Zum Beispiel: Luftaufklärung. Ich kann mir ein Flugzeug mieten, über ein Firmengelände fliegen, Fotos machen, alle paar Monate. Und ich sehe, ob Produktionskapazitäten dazugekommen sind. Dazu stelle ich dann noch jemanden unten vor das Betriebsgelände, der jedes Auto zählt, das rein- und wieder rausfährt. Das sind banale Beispiele, aber über solche Infos kann man wichtige Schlussfolgerungen ziehen. Sie müssen nirgends einbrechen und Laptops stehlen.

»WEM GEHÖRT DAS GEBÄUDE? WER SIND MEINE NACHBARN? WIESO IST DIE ETAGE ÜBER MIR NICHT VERMIETET?«



Um mal an die Grenzen zu gehen: Was ist mit der berühmten Sexfalle? Eine Frau lauert dem CEO bei einer Konferenz auf, lässt sich mit aufs Zimmer nehmen, horcht ihn beim Techtelmechtel aus. Legal?

Ich bin kein Jurist, aber aus meiner persönlichen Sicht würde ich sagen, dass das noch keine Straftat ist. Wenn die Dame dem Chef nicht sagt, warum sie an ihm so interessiert ist, ist das natürlich ethisch verwerflich. Aber solange sie ihn nicht erpresst, mit Fotos oder Videos – wenn er so dumm ist, sich darauf einlässt und nach dem dritten Glas Champagner über Interna redet, dann hat er das Problem!

Warum reden Menschen in solchen Situationen?

Weil sie sich positiv verkaufen wollen. Das ist eine menschliche Schwäche: Man will gut dastehen. Es geht um Egos, um die Verteidigung von Männerdomänen. Profis werden dafür gezielt trainiert: Wie muss ich mit jemandem reden, um solche Informationen aus ihm herauszuholen? Menschen sind eitel, die reden nachts an der Bar über Dinge, über die sie sonst nicht reden würden. Das ist ja wiederum auch unsere Aufgabe, also Manager zu sensibilisieren und zu schulen, dass sie das nicht tun.

Sie selbst dürfen Ihre Berufsgeheimnisse ja auch nicht ausplaudern.

Das ist eine Selbstverständlichkeit, ich arbeite ja seit 30 Jahren in dem Bereich.

Die Manager müssten es eigentlich auch wissen.

Erinnern Sie sich an den Vorfall mit Michael Hayden, vergangenen Herbst? Der ehemalige NSA-Chef, der im Zug saß und am Telefon so laut über Interna sprach, dass ein anderer Fahrgast mithörte und alles über Twitter verbreitete? Der Mann ist ein absoluter Profi, wie kann der so einen Fehler begehen? Die Antwort, ganz banal: menschliche Schwäche!

Also auch ohne Alkohol und hübsche Agentinnen?

Setzen Sie sich doch mal in die Bahn und fahren von Berlin nach Frankfurt oder Hamburg. Gehen Sie mal in die Business-Lounge der Lufthansa. Kaum sitzen Sie da drin, schon können Sie sich gar nicht mehr retten vor all den Interna und Details, die Ihnen um die Ohren fliegen. Rundherum unterhalten sich da die Manager über ihre Projekte und Strategien, führen Telefonate. Mir dreht sich da der Magen um! Es gibt Geheimdienste, kein Scherz, die setzen reisende Agenten ein, die den ganzen Tag nichts anderes tun, als im Flugzeug, in Zügen oder Business-Lounges zu sitzen und zuzuhören. Und das ist wahnsinnig effektiv! Menschen sind so schwach. Je höher sie in der Hierarchie kommen, desto eitler werden sie. Und desto einfacher ist es, sie auszuhorchen. Ein Topmanager, irgendwo allein im Ausland, einsam, keiner kümmert sich um ihn – wenn Sie den richtig anpacken, redet und redet und redet der. Und merkt es nicht.

Das klingt alles so einfach. Hatten Sie nicht auch knifflige Fälle?

Über die wirklich kniffligen kann und will ich nicht sprechen. Ich sage es mal so: Integris arbeitet auch in Ländern, in denen die Informationsbeschaffung äußerst schwierig ist. Asien und der Mittlere Osten sind unsere Schwerpunkte, auch diverse Projekte in Osteuropa. Vor allem im Mittleren Osten gibt es viele Länder, die für die meisten Geheimdienstler sehr schwierig sind. Die haben da kaum Möglichkeiten zu arbeiten. Und in einigen dieser Länder gehören wir zu den wenigen privaten Dienstleistern, die dort erfolgreich operieren.

Wird es für den Business-Intelligence-Agenten da auch richtig gefährlich?

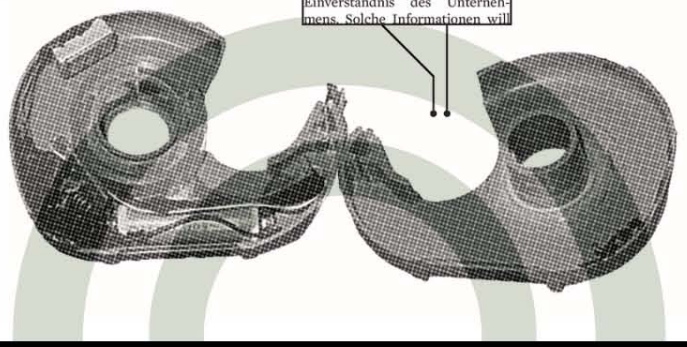
Wir haben es in der Regel ja auch mit mächtigen Gegnern zu tun. In China zum Beispiel hat sich im Februar 2013 die Gesetzeslage geändert. Bestimmte Informationen unterstehen mittlerweile einem verstärkten Datenschutz, das hat Konsequenzen. Informationen zu Unternehmen und Personen, zum Beispiel Gründungsdaten, all das war für Anwaltskanzleien früher frei zugänglich. Jetzt bekommt man sie nur noch mit Einverständnis des Unternehmens. Solche Informationen will man natürlich einsehen im Vorfeld einer neuen Geschäftsbeziehung, aber das geht nicht mehr so leicht. Mehrere Ermittler, Leute aus meiner Branche, sind da zuletzt bei Recherchen erwischt und festgenommen worden, manche wurden verurteilt, sitzen dort im Gefängnis. Die chinesischen Behörden gehen konsequent vor. Das macht unsere Arbeit deutlich schwerer.

Wie oft müssen Sie Ihre Kunden daran erinnern, in ungeschützten Mails nichts Entscheidendes über laufende Fälle zu schreiben?

Immer! Das ist ja die wichtigste erste Frage, die man einem Kunden stellt: Wie können wir eine sichere Kommunikation herstellen? So trivial ist das auch nicht – in China und Russland zum Beispiel sind verschlüsselte Mails gesetzlich verboten. Wenn das bemerkt wird, und das wird es, ziehen Sie sofort die Aufmerksamkeit auf sich. Ich habe das selbst erlebt, als ich in Russland war und mit Verschlüsselung gearbeitet habe. Nach 20 Minuten standen zwei Herren vor meiner Hotelzimmertür und haben gesagt, ich solle das besser lassen. „Gut!“, habe ich gesagt. Und weitergemacht. Bis die Leitung plötzlich tot war. Da muss man dann kreativ werden und Alternativen finden. Die gibt es.

Lehnen Sie auch Aufträge ab?

Sie glauben gar nicht, wie oft das passiert. Wir haben klare Grenzen. Immer wieder kommen Firmen und sagen: „Wir wüssten so gerne, was in diesem oder jenem Meeting gesprochen wird, können Sie den Raum nicht verwanzen?“ Ich sage dann: „Nein, das machen wir nicht.“ Und meistens endet das Gespräch an dieser Stelle. ■



DIE KLEINER! DE/PETER MALTZ, AKG-IMAGES/RIA NOWOSTI, BETTMANN/CORBIS, MILLENNIUM IMAGES/LOOK-FOTO

VERTEIDIGUNG? ANGRIFF!

Die kalifornische Firma Crowdstrike schützt Unternehmen vor Cyberattacken. Und wird dafür selbst zum Hacker

Text: **Thorsten Schröder**

„Wenn jemand auf Sie schießt, sollte es Ihnen relativ egal sein, wie groß das Kaliber ist“, schreibt George Kurtz in seinem Blog „Security Battlefield“. „Sie sollten sich fragen: Wer schießt auf mich und warum – und wie kann ich es stoppen?“ Es ist diese etwas archaische Analogie, der sich der Mitgründer von Crowdstrike bedient, um den Kern seiner Mission zusammenzufassen.

Und die die Firma zum Jungstar der amerikanischen IT-Sicherheitsbranche hat werden lassen.

Das Startup aus Kalifornien will Hacker mit ihren eigenen Waffen schlagen. Crowdstrike nutzt Algorithmen und lernfähige Programme, um Attacken bereits zu erkennen, während sie passieren. „Wir wissen, wie ein Angriff aussieht, wer dahintersteckt und was ihre Motive sind“, sagt Kurtz' Geschäftspartner und Chief Technology Officer (CTO) Dmitri Alperovitch. Dazu pflanzt Crowdstrike eine Art Flugschreiber in die Systeme seiner Kunden ein. Der Schreiber sammelt Informationen über Eindringlinge und gibt diese in Echtzeit an Crowdstrike weiter. Auf diese Weise soll aus rohen Daten eine riesige intelligente Onlinedatenbank entstehen, in der die Profile von Cyberkriminellen aus aller Welt enthalten sind und die so Verhaltensmuster erkennt. Ganz nach dem Motto: dem Feind immer einen Schritt voraus. „Irgendwann macht jeder einen Fehler“, sagt Alperovitch.

Stellt das System einen Angriff fest, kann Crowdstrike eingreifen, indem bestimmte Verbindungen gekappt werden oder ein beschädigtes System heruntergefahren wird. „Stop the bleeding“ nennen sie das intern. Dann folgt der Gegenschlag: Der Eindringling wird in eine Falle gelockt, wird mit falschen Informationen gefüttert oder bekommt seinerseits eine Dokumente Trojaner eingepflanzt, die dann Informationen über den Angreifer sammeln. „Im Kern geht es darum, die Kosten für Angreifer zu erhöhen“, sagt Alperovitch.

3,2 Mrd. Dollar haben Firmen 2013 laut Schätzungen der Beratungsfirma Gartner für Antivirenprogramme und Firewalls ausgegeben. Doch Systeme, die vor allem darauf setzen, „alle Fenster und Türen zu schließen“, seien gegen moderne Cyberattacken unwirksam, meint Alperovitch. „Die bösen Jungs sind in den letzten Jahren immer besser geworden.“ Je nach Schätzung kosten Hackerangriffe Unternehmen und Regierungen zwischen 300 und 1000 Mrd. Dollar jährlich. „Zieht man die Wände höher“, so Alperovitch, „bringen die Eindringlinge eben eine höhere Leiter mit.“

Weil Crowdstrike so unkonventionell vorgeht, ist der Buzz entsprechend groß. Kein anderes Jungunternehmen der Branche bekommt derzeit mehr Aufmerksamkeit. Crowdstrike, schrieb Kolumnist Fritz Nelson auf der Tech-Seite „Pando Daily“, sei „die Kim Kardashian der Informationssicherheit“. Der Business-Insider setzte das Unternehmen auf die Liste der wichtigsten Sicherheits-Startups. Erst vor wenigen Wochen erhielt die Firma in einer zweiten Finanzierungsrunde 30 Mio. Dollar; die Kriegskasse ist mit 56 Mio. Dollar gut gefüllt. „Unser Unternehmen schnappt sich reihenweise Kunden“, posaunte Kurtz vollmundig durch die US-Medien. Dabei tauchte Crowdstrike erstmalig Anfang 2012 auf der Branchenkonferenz der RSA für Kryptografie und Informationssicherheit in San Francisco auf. Erst seit Juli 2013 ist das Startup offiziell am Start.

Die Köpfe hinter Crowdstrike sind Veteranen im Sicherheitsgeschäft. Kurtz gründete 1999 die Sicherheitsfirma Foundstone. Als der Antivirenspezialist McAfee die Firma 2004 übernahm, wechselte Kurtz gleich mit. Alperovitch war bei McAfee verantwortlich für die Aufklärung der Attacken asiatischer Hacker auf Google im Jahr 2009. Und Shawn Henry, der Sicherheitschef, war 24 Jahre beim FBI, zuletzt als Leiter der Abteilung Cyberverbrechen. Seit Ende Oktober letzten Jahres gehört auch ein Oberst der Air Force zum Team.

Bei aller Begeisterung: Die Firma ist nicht unumstritten. Fraglich ist, ob Crowdstrike mit der offensiven Strategie nicht an rechtliche Grenzen stößt. Kritiker meinen, die Firma ermutige ihre Kunden, selbst zu Hackern zu werden: So soll Crowdstrike etwa falsche Informationen in Firmenbilanzen einschleusen, und das könne zu Kurseinbrüchen an der Börse führen. Alperovitch dementiert allerdings solche Praktiken: „Diese Leute haben ganz offensichtlich falsche Informationen über das, was wir machen“, sagt er. Crowdstrike schalte lediglich den Schützen aus, bevor das digitale Projektil sein Ziel trifft. Bäm! Und tot. ■