Wer in anderer Leute Netzwerke eindringt und auf deren Festplatten spazierengeht, hat nicht immer Böses im Sinn. So genannte „weiße Hacker" testen im Auftrag von Unternehmen mögliche Schwachstellen. Foto: Thinkstock

Die Bösen schlafen nicht

Weder Schreckensmeldungen über Datenkriminalität noch der NSA-Skandal konnten die Mehrzahl der kleinen und mittleren Unternehmen ernsthaft beunruhigen. Doch sie wiegen sich in falscher Sicherheit, wenn man Experten glauben darf. Umfrageergebnisse, nach denen ein großer Teil der Mittelständler bereits Opfer von Hackern geworden ist, stützen diese Behauptung.

„Lücke im Google-Browser erlaubt heimliches Lauschen" – „Datendieb stiehlt und verkauft 2,5 Millionen Datensätze der Süddeutschen Klassenlotterie" – „17 Millionen Datensätze von Mobilfunkkunden der Telekom entwendet" – „Bankdaten von rund 21 Millionen Menschen zum Verkauf angeboten" – „Das Bundesamt für Sicherheit in der Informationstechnik warnt: 16 Millionen Online-Konten geknackt."

Wer morgens die Zeitung aufschlägt oder im Internet surft, muss nicht lange suchen: In den vergangenen zwei Jahren haben die Meldungen über Internetkriminalität und Datenklau rasant zugenommen. Allein die NSA-Affäre rund um das Spionageprogramm Prism dominierte die Medien monatelang. Dennoch zeigt sich der Mittelstand weiterhin wenig beeindruckt von den Vorfällen. Zumindest im eigenen Haus sei man sicher, scheint die weit verbreitete Meinung – und außerdem hat das Thema einen entscheidenden Nachteil, denn wenn man es angehen möchte, kostet es Geld. Auf die Frage, ob nach dem NSA-Skandal besondere Maßnahmen im Bereich Datensicherheit geplant seien, antworteten in einer Studie der Wirtschaftsprüfer von Price, Waterhouse, Coopers (PWC) satte 59 Prozent der Unternehmen mit „Nein".

Auch im Mittelstand der Region Stuttgart möchte sich beim Thema Datensicherheit kaum jemand zu Wort melden. Entsprechende Anfragen der Redaktion des IHK-Magazins Wirtschaft anlässlich des aktuellen Titelthemas „Datensicherheit" blieben weitgehend erfolglos. „Leider kann man bei uns noch nicht viel dazu sagen. Das soll und wird sich aber in Zukunft ändern", lautet beispielsweise die Antwort eines der befragten Unternehmen. Viele weitere Firmen, die sonst gerne und bereitwillig Auskunft geben, melden sich gar nicht erst zurück.

Mit einer Ausnahme: Herma in Filderstadt, ein führender Spezialist für Selbstklebetechnik mit 840 Mitarbeitern und einem Jahresumsatz von zuletzt 245,6 Millionen Euro, ist durchaus bereit, Auskunft zu geben – aber er hat auch etwas vorzuweisen. „Wir kümmern uns von jeher um die Datensicherheit und haben dafür auch die volle Unterstützung der Unternehmensführung", sagt Josef Marchner, der bei Herma für die IT zuständig ist. Nachvollziehen kann er dennoch, dass viele andere Unternehmen sich nicht äußern möchten. „Datensicherheit ist ein frustrierendes Thema – ganz einfach deshalb, weil es Geld und Manpower kostet und man es dennoch nie erschöpfend lösen kann." Auch bei Herma schwankt die Intensität der Vorbeugemaßnahmen, gesteht der IT-Manager. „Natürlich treten wir verstärkt in Aktion, wenn in den Medien wieder neue Themen hochkochen – oder wenn der Gesetzgeber mal wieder neue Vorgaben macht."

> **Eine E-Mail ist wie eine Postkarte – die kann jeder lesen, und ruckzuck ist ein internes Dokument weltweit für jeden einsehbar.**

Davon abgesehen aber gibt es im Unternehmen eine Sicherheitsphilosophie, die schon in den Anfängen des EDV-Zeitalters, bei Herma also vor rund 25 Jahren, etabliert und seither systematisch ausgebaut wurde. Aus dieser Zeit stammt beispielsweise eine Maßnahme, die man heute in kaum einer anderen Firma finden wird: Bis auf einige wenige Arbeitsplätze in der IT gibt es bei Herma nicht die Möglichkeit, CDs und DVDs zu brennen oder USB-Sticks zu benutzen. „Das kommt natürlich bei den Mitarbeitern nicht immer unbedingt gut an, ist aber einer von vielen Sicherheitsaspekten, die bis heute relevant sind

– eine Maßnahme, die uns mit Sicherheit schon viele Probleme vom Hals gehalten hat“, sagt Josef Marchner. Es soll damit dem Anwender auch kein grundsätzliches Misstrauen ausgesprochen werden; vielmehr ist Marchner zufolge eine gewisse Sorglosigkeit im Arbeitsalltag für viele Gefahren verantwortlich. „Da braucht nur mal jemand eine Preisliste per E-Mail um die Welt zu schicken. Eine Mail ist wie eine Postkarte – die kann jeder lesen, und ruckzuck ist so ein internes Dokument weltweit für jeden einsehbar.“

IT-Sicherheit ist ein Element der Existenzsicherung

Doch auch das ist nur eine kleine Facette all jener Sicherheitsthemen, mit denen sich die ITler von Herma befassen. „Datensicherheit bedeutet einen enormen administrativen Aufwand“, erläutert Josef Marchner, „weil man zunächst einmal etablieren muss, welche Daten man hat und welche davon wie und wovor geschützt werden sollen.“ So macht beispielsweise der Gesetzgeber Vorgaben zur Buchhaltung, zur Gehaltsabrechnung und zum Datenschutz der Mitarbeiter; gleichzeitig müssen das Produkt-Know-how, das Konstruktions- und Entwicklungswissen von Herma geschützt werden. Und dann sollte noch dafür gesorgt werden, dass den Mitarbeitern stets alle relevanten Daten zur Verfügung stehen, dass also die Unternehmens-IT nicht plötzlich durch einen Virus oder eine Botnetz-Attacke lahmgelegt wird.

Die IT-Sicherheit, so sieht es Josef Marchner, ist ein Element der Existenzsicherung des Unternehmens. „In regelmäßigen Abständen lassen wir deshalb unsere gesamte Sicherheitsinfrastruktur von externen Fachleuten auf den Prüfstand stellen. Und dann haben wir natürlich alles, was heute mindestens üblich ist: Firewall-Systeme, Virenschutz, Content-Filter.“ Und selbst da wird noch differenziert: Die Sicherheitsexperten kümmern sich sowohl um die Datenströme, die vom Unternehmen aus in die Welt geschickt oder von dort aus empfangen werden, als auch um die Datensicherheit am einzelnen Arbeitsplatz – damit beispielsweise keine rassistischen Daten, Pornographie oder Viren auf den Rechnern der 840 Mitarbeiter landen. Darüber hinaus werden verschiedene Netzwerkteile des Unternehmens voneinander abgetrennt. „Das funktioniert wie ein Empfangsbereich“, erklärt Josef Marchner, „die Daten, die ins Unternehmen gelangen, können beispielsweise nicht mit dem Server der Haupt-EDV-Anwendungen kommunizieren. Oder ein Produktionsrechner wird so eingerichtet, dass er nur mit jenen Netzwerken und Servern reden kann, mit denen er auch reden können muss.“


Foto: Jan Reich

Josef Marchner ist bei Herma in Filderstadt für die IT zuständig. Regelmäßig lässt er dort die gesamte Sicherheitsinfrastruktur von externen Fachleuten auf den Prüfstand stellen.

Denn dass es Attacken auf das Unternehmen gibt, davon ist Josef Marchner fest überzeugt. „Ich kenne die einschlägigen Studien, beispielsweise die von den Wirtschaftsprüfern der KPMG – ich würde sogar noch weitergehen und behaupten, dass nicht nur 95 Prozent, sondern 100 Prozent aller Unternehmen bereits entsprechende Angriffe gehabt haben.“ Zwar gebe es Firmen, die für die Hacker nicht so interessant seien, aber es müsse sich ja auch nicht um gezielte Angriffe handeln, sagt der Experte. „Pauschale Angriffe, bei denen eine entsprechend programmierte Software einfach mal prüft, ob sie überhaupt ins Unternehmen kommt, finden tagtäglich überall auf der Welt statt.“

Das Beispiel von Herma zeigt, dass es für den Mittelstand durchaus möglich und auch nötig ist, sich um die eigene digitale Sicherheit zu kümmern. Immerhin bieten mittlerweile zahlreiche Unternehmen den entsprechenden Service. Eines davon ist die GM Consult IT GmbH mit Sitz in Stuttgart. „Als Dienstleister im Bereich Dokumentenmanagement, der für den Umgang mit sensiblen Daten verantwortlich ist, stecken wir mittendrin in all den Fragen rund um die IT-Sicherheit“, erklärt Geschäftsführer Alexander Fuchs und erinnert sich: „Vor rund 15 Jahren kam das Thema richtig hoch. Damals ent-

Online-Special

Mehr Info über IT-Sicherheit finden Sie unter:
www.stuttgart.ihk.de, Dok.-Nr. 120957

schieden zahlreiche Banken und Versicherungen, dass nicht mehr jeder Finanzdienstleister ein eigenes Druckzentrum braucht, sondern man diesen Bereich genauso gut outsourcen könne.“ Diesen Part übernimmt die GM Consult IT – und tut alles dafür, technisch auf dem neusten Stand zu sein. „Ob Software oder Hardware, die ‚weißen Hacker’, die von uns engagiert werden, sind erstklassig. So bleiben wir mit den ‚schwarzen Hackern’ immer mindestens auf Augenhöhe.“

Das allerdings können Alexander Fuchs und sein Prokurist Karl Peter Jegglin längst nicht von allen Mittelständlern sagen, mit denen sie in der Region Stuttgart geschäftlich zu tun haben. „Ich weiß von mindestens zwei Global Playern, die mit sensiblen Daten schlampig umgehen – in diesem Fall nicht intern, da stimmt noch alles, sondern extern,

In den meisten Fällen fängt die Sorglosigkeit schon an der Unternehmensspitze an. Wir brauchen uns nur unsere Bundeskanzlerin anzuschauen.

wenn Partner involviert sind“, sagt Karl Peter Jegglin. Das Problem, erklärt der Fachmann, liegt darin, dass die betreffenden Unternehmen mit ihren Partnern möglichst nutzerfreundlich kommunizieren wollen – auf Kosten der Sicherheit. „In den meisten Fällen fängt diese Sorglosigkeit schon an der Unternehmensspitze an. Wir brauchen uns nur unsere Bundeskanzlerin anzuschauen: Sie möchte SMS versenden, will sich aber nicht jedes Mal authentifizieren und setzt auf diese Weise ihre Datensicherheit aufs Spiel.“ Bequemlichkeit, da sind sich die Experten einig, fungiert als Türöffner Nummer eins für Datendiebe.

Ein weiteres Hindernis ist der Gedanke: „Wir sind so klein, es interessiert doch niemanden, was wir kommunizieren, und das Geld für Datensicherheit möchten wir uns eigentlich auch lieber sparen.“ Hier können Alexander Fuchs und Karl Peter Jegglin nur kollektiv den Kopf schütteln. „Nehmen Sie ein Architekturbüro mit 40 Mitarbeitern, welches mit internationalen Kunden an einem Riesenprojekt arbeitet und Pläne hin- und herschickt. Wenn irgendjemand davon weiß und Hacker ansetzt, kann das ganze Know-how des kleinen Unternehmens plötzlich weg sein.“ Dabei könnte es so einfach sein, E-Mails zu verschlüsseln, erklären die Fachleute.

Interview „Wie Radioaktivität“

Experte: Datenklau macht wenig Angst, weil er so anonym ist

„Brauchen wir nicht, kostet nur Geld“ – gerade inhabergeführte Mittelständler zeigen sich erschreckend unbedarft, wenn es um Maßnahmen für mehr Datensicherheit geht, ist die Erfahrung von Sicherheitsfachmann Rainer Benne.

Herr Benne, wie kommt es, dass viele Unternehmen das Thema Datensicherheit noch nicht so richtig ernst nehmen?

Benne Das liegt an der Form der Kriminalität: Sie tut zunächst nicht weh, es liegt niemand zusammengeschlagen am Boden, es geht nicht einmal eine Fensterscheibe zu Bruch! Der Täter steigt nicht mehr über den Zaun. Datenkriminalität ist wie Radioaktivität. Man sieht sie nicht, man hört, schmeckt, riecht und fühlt sie nicht, aber trotzdem ist sie da und sie ist gefährlich, denn der Feind schläft nie. Nicht umsonst investieren Großkonzerne deshalb viele Millionen in ihre Datensicherheit.

Warum zeigt sich insbesondere der inhabergeführte Mittelstand beratungsresistent?

Benne Zunächst einmal kostet Datensicherheit Geld, und solange sie selbst noch nicht betroffen waren, meinen viele Unternehmer, sich dieses Geld sparen zu können. Darüber hinaus fehlt die Einsicht, denn gerade die Inhaber mittelständischer Unternehmen können gut schweigen. In der realen Geschäftswelt sind sie mit Informationen und Geld höchst vorsichtig – aber nicht in der virtuellen Welt!

Und so werden Sie meist erst im Schadensfall gerufen?

Benne Ganz genau. Da wird ein Unternehmen beispielsweise überraschend von außen mit strategischem Wissen konfrontiert, das eigentlich nur auf dem eigenen Server liegen dürfte. Oder höchstsensible Unterlagen sind plötzlich in Zeitungsberichten nachzulesen. Früher habe ich immer gedacht, als Kriminalbeamter sei mir nichts fremd. Heute weiß ich: Alles geht, der Fantasie sind keine Grenzen gesetzt.

Dennoch: Ist die Angst nicht übertrieben?

Benne Die Meinungsforscher aus Allensbach haben bei ihrem Cyber Security Report 2013 ermittelt, dass fast 90 Prozent aller deutschen Unternehmen schon Ziel von IT-Attacken gewesen sind. Ich denke, diese Zahl spricht für sich. Selbst wenn zunächst nichts passiert, weil es durchschnittlich drei Monate dauert, bis der Schaden nach einem Datendiebstahl eintritt. Datenkriminalität gleicht der herkömmlichen Kriminalität: Es wird der Schwache angegriffen, der nicht vorgesorgt hat. Aus der Praxis kenne ich ein Unternehmen, das bis 800 000 Angriffe pro Woche auf seine IT abwehrt.


Foto: Benne

Unser Interviewpartner

Rainer Benne

Der ehemalige Kriminalbeamte war bei der Fraport AG für den Flughafenschutzdienst und später bei Porsche für die Konzernsicherheit zuständig. Heute ist er Unternehmensberater in Sachen Sicherheit und Compliance.

In der Allensbachstudie bezeichnen die Führungskräfte auch die eigenen Mitarbeiter als erhebliches Sicherheitsrisiko.

Benne Das stimmt leider. Aktuelle Studien belegen, dass rund 50 Prozent der Täter aus dem eigenen Unternehmen kommen. Diese Täter sind die gefährlichsten, da ihr Vorgehen Bestandteil normaler Geschäftsprozesse ist und daher lange unentdeckt bleibt.

Wie gehen Sie vor, wenn Sie in ein Unternehmen gerufen werden?

Benne Wie beim Arzt erfolgt zuerst die Anamnese: Das IT-System des Unternehmens wird von einem Team professioneller ‚weißer‘ Hacker auf den Prüfstand gestellt. Anhand der Ergebnisse stelle ich ein Informations-Sicherheits-Management-System auf, kurz ISMS. Dabei handelt es sich um ein ISO-zertifiziertes Grundschutzprogramm, das man mindestens haben sollte und das jede Menge Themen umfasst: Passwortschutz, Vier-Augen-Prinzip, Virenschutz, Firewall, Datenbankverschlüsselung... Und schließlich geht es vor allem um die Aufklärung und Sensibilisierung der Führungsebene und der Mitarbeiter – praxisnah und für jedermann verständlich. Nur so lassen sich die Gefahren der virtuellen Welt verdeutlichen.

Viele Unternehmen wollen möglichst nutzerfreundlich kommunizieren, wissen Karl-Peter Jegglin (li.) und Alexander Fuchs von GM Consult IT in Stuttgart. Ein Verschlüsselung

Sie setzen auf regimail, die patentierte und datenschutzgeprüfte Lösung des technologisch führenden Unternehmens Regify, die weltweit einsetzbar und leicht anzuwenden ist. „Dort gibt es eine permanente Weiterentwicklung. Das ist wichtig, denn die Bösen schlafen nicht", fasst Alexander Fuchs das Problem zusammen.

Die Hemmschwelle ist bei Internet-Tätern sehr niedrig

Die Bösen schlafen nicht – das unterschreibt auch Sicherheitsberater Rainer Benne. Der ehemalige Kriminalpolizist, der überdies jahrelang unter anderem für die Datensicherheit bei Porsche zuständig war und heute als selbstständiger Sicherheitsberater arbeitet, kann einiges zum modernen Täterprofil des Internet-Kriminellen sagen. „Die Täterhemmschwelle bei diesen Menschen ist sehr gering", erläutert er. „Das liegt daran, dass der Täter seinem Opfer nicht in der realen Welt gegenübersteht – er sieht dem Opfer nicht in die Augen, er weiß nichts von der alten Dame, der er online das Geld geklaut hat."

Rainer Benne meint, dass aus diesem kaum vorhandenen Unrechtsbewusstsein heraus auch durchaus die eigenen Angestellten zum Unsicherheitsfaktor werden – nach dem Motto, „wenn ich im Unternehmen einen Stapel Papier mitgehen lasse oder ein paar Informationen weiterleite, dann macht das doch gar nichts". Er hinterfragt deshalb das Einstellungsverhalten bei Unternehmen. „Die Personalpolitik hängt eng mit der Unternehmenskultur zusammen und hat enorme Auswirkungen auf die interne Sicherheit. Werte, Normen und Tugenden können nun mal nur Top-Down glaubwürdig kommuniziert werden. Wenn schon der Chef bestimmte Sicherheitsthemen nicht ernst nimmt, warum sollte es dann der Angestellte tun?" Rainer Benne ist vertraut mit den Beispielen der so genannten „Neutralisierungstechniken" des Täters: Von „das macht doch jeder" über „die kümmern sich nicht um mich, also bin ich auch nicht loyal" bis hin zu „das bisschen Schaden tut niemandem weh" reicht die Palette.

Selbst wer schon geschädigt worden ist unterschätzt das Risiko noch

Und neben der internen Gefahr des Leichtsinns droht höchst professionelle kriminelle Energie von außerhalb, warnen die Fachleute vom Bundeskriminalamt. „Wirtschaftsunternehmen sind heute in hohem Maß auf das Internet als Kommunikations-, Logistik-, Steuerungs- und Vertriebsplattform angewiesen. Deutlich wird dies am Beispiel systematischer, koordinierter Angriffe auf Unternehmensserver mittels so genannter Botnetze. Die ange-

ihrer E-Mails glauben sie, sich sparen zu können.

griffenen Server brechen unter der Last der großen Anzahl paralleler Anfragen zusammen, wodurch Dienstleistungen nicht mehr verfügbar sind. Die damit einhergehenden Schäden und Reputationsverluste sind beträchtlich“, fassen die Kriminaler zusammen.

Eindrücklich genug? Bei weitem nicht. Obwohl zwei Drittel der befragten Unternehmen in einer Studie der Wirtschaftsprüfungsgesellschaft KPMG angeben, dass sie innerhalb der nächsten Jahre eine signifikante Zunahme elektronischer Kriminalität erwarten, fühlt sich kaum einer direkt betroffen. „Paradox“ finden es denn auch die Verfasser der Studie, dass nur knapp ein Drittel der bereits von Datenkriminalität betroffenen Unternehmen und sogar nur ein Viertel der bisher nicht betroffenen Unternehmen das eigene Risiko hoch einschätzt, zum Opfer zu werden. Stattdessen scheinen sie zu glauben, dass eher „die anderen Unternehmen“ betroffen sein könnten.

Goldene Zeiten für Hacker also, möchte man meinen. Das stimmt – es trifft allerdings nicht nur auf die Bösewichte, sondern vor allem auch auf die so genannten ‚weißen’ oder ‚ethischen’ Hacker zu. Sie bieten ihr Können als Dienstleistung an und erleben einen wahren Boom. So zum Beispiel Diplominformatiker Sebastian Schreiber, der als kleiner Junge Commodore-Spiele knackte und heute sagt: „Hacken ist eine Leidenschaft, hacken ist mein Leben.“ Hacken ist für ihn überdies sein Unternehmen, die SySS GmbH mit Sitz in Tübingen, die mittlerweile 49 Mitarbeiter zählt. Der Gründer, Alleingesellschafter und Geschäftsführer kann sich noch gut an die Anfänge erinnern: „Als ich 1998 die SySS GmbH gegründet habe, gab es noch gar keine Nachfrage nach Penetrationstests“, sagt er. Heute kann sich der Unternehmer vor Aufträgen kaum retten. Sein Team ist nicht nur darauf spezialisiert, sich in Unternehmen „reinzuhacken“, sondern auch auf die Forensik von digitaler Kriminalität, sprich darauf, die Spuren von elektronischer Kriminalität gerichtsverwertbar zu sichern und aufzubereiten.

Wichtig ist dabei, dass die SySS GmbH keine Security-Services anbietet. „Wir machen das System unserer Kunden nicht sicher!“, warnt Sebastian Schreiber. „Wir haben vielmehr einen Ethik-Katalog, der es uns sogar verbietet, Schwachstellen zu beheben.“ Der Informatiker erklärt, warum das so sein muss: „Es käme zu einer Konfliktsituation, denn wer eigentlich Firewalls verkaufen möchte, wird den Prüfbericht entsprechend abfassen.“ Das aber geht nicht – die professionellen sauberen Hacker legen großen Wert darauf, dass sie keine Umsätze mit Sicherheitsmaßnahmen machen. Einmal beauftragt, greifen sie von Tübingen aus an, und zwar zunächst mit einem Perimeter-Test von außen, um zu prüfen, ob sie auf dem virtuellen Weg ins Unternehmen gelangen. Als nächstes wird die Sicherheit von B2B-Plattformen getestet. Und schließlich erfolgt der Angriff von innen: Könnte es beispielsweise dem Fremdmitarbeiter einer Zeitarbeitsfirma im Unternehmen gelingen, sensible Daten einzusehen?

„Wir finden die Schwachstellen des Systems und der Kunde kann die Löcher daraufhin stopfen. Minimale Tests zeigen bereits eine Menge spannender Ergebnisse “, sagt Sebastian Schreiber. Und sei es auch nur die kleine Agentur eines Versicherungsmaklers: „Stellen Sie sich vor, da wird die Website geknackt und jeder kann die Daten der Versicherten einsehen – das an sich wäre für den Versicherungsmakler schon der Super-GAU.“ Aber auch größere Kunden, die bereits Maßnahmen vornehmen, sind längst nicht vor digitalen Attacken geschützt, ist Sebastian Schreibers Erfahrung. „Da will dann ein Geschäftsführer zeigen, wie top in Schuss seine IT ist, und wir schaffen es dennoch, seine E-Mails zu lesen. Entsprechend groß ist anschließend der Überraschungseffekt und die Einsicht, dass etwas getan werden muss.“

Entsprechend groß ist auch die Freude bei den SySS-Mitarbeitern, denn für sie gibt es nichts Schöneres, als ihr Können unter Beweis zu stellen. „Wir haben kein Problem, Nachwuchs zu finden. Was kann sich auch ein junger Informatiker Besseres vorstellen, als sich legal in Unternehmen zu hacken und dafür gutes Geld zu bekommen, anstatt ins Gefängnis zu wandern?“, fragt Sebastian Schreiber. Auch die gehackten Kunden sind dankbar. „Wir haben sehr treue, zufriedene Kunden, die solche Tests bis zu einmal im Monat durchführen lassen.“ Allerdings kommen Neukunden oft erst auf die SySS GmbH zu, wenn etwas passiert ist. „Am Anfang steht häufig der Notfall, etwa, wenn das Unternehmen gehackt und anschließend erpresst wird. Das sind große, hässliche Projekte“, sagt Schreiber. Ihm und den anderen Sicherheitsfachleuten wäre lieber, gerade der Mittelstand würde sich rechtzeitig kümmern. Denn eins ist tatsächlich sicher, sagt der Fachmann: „Mag sein, dass ein Unternehmen noch kein Opfer war, aber über kurz oder lang wird ein Angriff kommen.“ ❮