Einmal Hack, bitte

Warum sich Unternehmen regelmäßig hacken lassen

Von Eva Roßner

Manche Unternehmen lassen Hard- und Softwareprodukte regelmäßig von Hackern zerlegen. Was auf den ersten Blick widersprüchlich scheint, ist alles andere als das. Wer die IT-Landschaft der Firmen angreifen darf und was sich hinter dem Geschäftsmodell der „Zerstörung" verbirgt: aus dem Alltag von Gehackten – und von Hackern.

© maxuser/iStock/Thinkstock

Mit einem Schlag hätte alles aus sein können. Kein Licht, Stillstand an den Supermarktkassen, keine Ampel hätte funktioniert, Menschen gefangen in Fahrstühlen, geschlossene Banken, alle Computersysteme auf null. Die Auswirkungen eines solchen Szenarios wurden Eberhard Oehler bewusst, als ein Hacker drauf und dran war, der Stadt Ettlingen den Strom abzudrehen. Der Geschäftsführer der Stadtwerke Ettlingen erinnert sich noch genau: „Ich war schockiert, wie schnell und leicht der Angriff möglich war", sagt er. 40.000 Bewohner ohne Wasser- und Gasversorgung – doch so weit kam es zum Glück oder besser gesagt dank Felix Lindner nicht. Er hatte die Energieversorgung zwar für kurze Zeit in der Hand, war von Oehler jedoch dafür engagiert worden.

Cyberangriff vor der Kamera

Der Einsatz fand im Rahmen von Dreharbeiten statt. Ein Sicherheitstest unter Livebedingungen, der für eine Dokumentation zum Thema „Cyberangriffe" gedacht war. Neben Tel Aviv und Las Vegas wurde auch in Ettlingen gedreht, eben genau dort, wo es kritische Infrastrukturen gibt. Eigentlich sollte Lindner gar nicht so weit in Oehlers System vorstoßen. „Wir dachten an einen Einbruch in unsere technische Software. Aber er kam überall rein. Der hat mir Mails vorgelesen, als stünden wir splitternackt vor ihm", erzählt der Geschäftsführer.

Unternehmen machen es Angreifern manchmal sogar recht einfach, in die Firmennetzwerke vorzudringen. „Einiges davon kann man sogar bei Amazon bestellen", erklärt Christian Schülke, als er seinen Koffer öffnet. Er zieht einen USB-Stick hervor. Mit dem modifizierten Speichergerät startet er Rechner neu, um dann ohne Passwort auf die Daten zuzugreifen. Alles, was über die Tastatur geschrieben wird, könnte er so mitlesen, sagt er. Einige seiner Kunden sind Privatleute, die meisten jedoch kleinere Unternehmen. „Viele Mittelständler wissen meist nicht einmal, dass sie angegriffen wurden", erklärt er. Deshalb überprüft er ihre Bedrohungslage, definiert Tätergruppen und erklärt, wie ein sinnvoller Sicherheitsplan aussehen kann. Der IT-Experte greift allerdings nicht „einfach so" an, sondern nur, wenn er darum gebeten wird. Laut Strafgesetzbuch § 202c steht der unbefugte Zugang zu Daten Dritter nämlich unter Strafe.

„Ich gehöre nicht zu den Bösen", erklärt er. Schülke ist Geschäftsführer eines IT-Beratungsunternehmens und unterstützt seine Kunden dabei, ihre digitale Infrastruktur abzusichern. Sich selbst bezeichnet er als Bastler, der seine Passion zum Beruf gemacht habe. Er legt viel Wert auf Präzision, wenn es um seine Tätigkeit geht. „Schnell werden Cyberkriminelle und Hacker sprachlich in einen Topf geworden", sagt er. Doch die Absicht eines Hackers sei eine andere. Der gute, also der White Hat, zerlege etwas, um die Schwachstellen ausfindig zu machen. „Um es dann zu verbessern!" Dieses Vorgehen habe nichts mit den kriminellen Varianten zu tun, die derzeit durch die Presse geisterten.

> „Ich war schockiert, wie schnell und leicht der Angriff möglich war."
>
> Eberhard Oehler, Stadtwerke Ettlingen

Einladung zum Angriff

Den Eingang zur IT-Landschaft eines Unternehmens findet Schülke sogar via Google-Suche im Internet. Alle Geräte, die online sind, kommunizieren dort über eine Infrastruktur aus Kabeln, Routern und Protokollen. Wenn Schülke nun einen Rechner über eines der Protokolle anspricht, kann dieser ihm mitteilen, mit welcher Software er betrieben wird. Sofern die veraltet ist, kommt das einer Einladung für Hacker gleich. „Manchmal finde ich den Zugang auch über die Firmenwebsite selbst", berichtet er. Dann tippt er in eine Anmeldemaske des Unternehmens einen Datenbankbefehl ein, mit dem die Seite nicht gerechnet hat. Sofern die dahinterliegende Datenbank antwortet, hat Schülke eine Sicherheitslücke definiert und könnte sich so die Kontrolle über das System verschaffen.

Enorme Verluste drohen

Nun zählt Schülke zu den guten, kein Black Hat also, der sich unerlaubt Zutritt zu Systemen verschafft und von krimineller Energie angetrieben wird. Doch die prominenten Fälle von Sony Pictures, Ashley Madison und nicht zuletzt der erste Hackangriff auf den Technologiegiganten Apple zeigen: Mit digitalen Geschäftsmodellen nehmen Sicherheitsverletzungen unvermeidlich zu. Das Ausmaß und die Frequenz der Attacken werden sich weiter erhöhen, davon ist auch Boris Piwinger überzeugt, Senior Manager des Digital Center of Excellence der Beratungsfirma A.T. Kearney. Doch viele Unternehmen sind zu langsam, um mit der rasanten Entwicklung der Angriffe Schritt zu halten. „Wenn Kriminelle erst einmal die Systeme eines Unternehmens infiziert haben, kann es Monate dauern, die Kontrolle zurückzugewinnen." Im Durchschnitt dauere es 243 Tage, bis ein Angriff überhaupt entdeckt werde, wie der Berater sagt.

Der Schaden ist schwer zu beziffern. Piwinger nennt eine Zahl des Innenministeriums: 50 Milliarden Euro jährlich in Deutschland. Doch diese Angaben seien nicht verifizierbar. Mit einem Blick auf die internationalen Berichte fasst er zusammen: Der Schaden läge durchschnittlich zwischen 0,5 Prozent und 3 Prozent des jeweiligen BIP. In Deutschland wären das bei einem BIP von 2,9 Billionen Euro im Jahr 2014 zwischen 15 und knapp 90 Milliarden Euro gewesen. Das ist viel Geld, doch das Ausmaß ist damit noch lange nicht abgesteckt. Der Berater beschreibt ein Beispiel, aus der Luft gegriffen, wie er sagt, denn über Kunden spricht er nicht gern. Realistisch sei es dennoch: ein internationales Vergabeverfahren. „Der Zweitbieter gewinnt im Bieterverfahren – doch die Differenz macht nur einige Tausend US-Dollar aus – bei einem Auftragswert in dreistelliger Millionenhöhe. Es ist unwahrscheinlich, dass es hier mit rechten Dingen zuging." Was Piwinger damit meint: Das konkurrierende Unternehmen wurde gehackt, nur um den möglichen Höchstpreis zu erfahren und ihn dann um wenige Cents zu unterbieten.

Martin Stemplinger, Mathematiker und IT-Sicherheitsspezialist bei British Telecommunications, arbeitet daran, Sicherheitslücken dieser Größenordnung zu schließen. „Als Einstieg bieten wir ein Vulnerability-Assessment für Applikationen und Netzwerk an. Nach Bedarf untersuchen wir die Schwachstellen dann genauer." Stemplinger führt also Schwachstellenanalysen ▸

Unternehmen unterschätzen die Gefahren eines kriminellen Cyberangriffs.

© Matej Moderc/iStock

durch, die nähere Untersuchung ist dann der Penetrationstest. Ein einigermaßen anspruchsvoller Pen-Test kann bei Stemplingers Arbeitgeber leicht einige Zehntausend Euro kosten.

Hack ist nicht gleich Hack

Der Mathematiker reagiert ebenfalls empfindlich, wenn bei der Tätigkeitsbeschreibung nicht die entsprechende Trennschärfe gewahrt wird. Was nachvollziehbar ist, immerhin bieten die Experten mit Sitz in Eschborn „Ethical Hacking" an. Dabei unterscheiden sich die Testverfahren: Beim Whitebox-Test werden die Tests mit Kenntnissen über die innere Funktionsweise des zu testenden Systems entwickelt. Der ethische Hacker arbeitet also in Kenntnis der Software und wirft beispielsweise einen Blick in den Quellcode. Beim Blackbox-Test wird eine Software ohne Kenntnisse über die innere Funktionsweise untersucht. Der Pen-Tester verhält sich hier also wie ein Hacker von außen. „Da die Unternehmen aber in der Regel nicht unbegrenzt Zeit und Geld haben, entscheiden sie sich meist für einen Whitebox- oder einen Greybox-Test", erklärt Stemplinger. Am aufwendigsten sei jedoch ein Blackbox-Test.

Mit den verschiedenen Testverfahren kennt sich auch Gerold Hübner aus. Er ist Chief Product Security Officer bei SAP und leitet dort das Team für Produktsicherheit. Hübner und sein Team kümmern sich darum, dass die Softwareprodukte von SAP sicher sind – auch während der Programmierung. Das nennt sich „Security by Design", eine SAP-Software durchläuft dadurch einen sehr aufwändigen Sicherheitsprozess. Und hacken zählt dazu. Doch Hübner gefällt dieser Begriff überhaupt nicht. „Der Bezeichung Hacker heftet ein negatives Image an", sagt er. Er stelle nur die Besten ein – nicht unbedingt diejenigen, die den größten Coup gelandet hätten. Hübner hält mit seinem Team die Augen in der ganzen Welt offen für neue Talente. Dazu besuchen sie sogar Konferenzen wie die US-amerikanische Black Hat. Dort referieren Sicherheitsexperten über ihre aktuellen Erkenntnisse zum Thema Sicherheit und gefundene Schwachstellen.

Erst kürzlich traf Hübner wieder jemanden auf einer der Konferenzen, den er für richtig gut hält. „Bevor wir ihn beauftragen, setzen wir einen Vertrag auf", erklärt er. Dort sei festgeschrieben, dass die entdeckten Sicherheitslücken exklusiv an SAP berichtet werden. Und wenn doch etwas durchsickert? Davon hat Hübner noch nichts gehört. Ohnehin sei die Branche sehr überschaubar. Man kenne sich, und jeder müsse sich an seinen Referenzen messen lassen. Es lohnt also nicht, hier unsauber zu arbeiten.

Vertrauen schaffen

„Rechte und Pflichten können in Verträgen definiert werden. Das Vertrauen jedoch nicht", erklärt ATK-Berater Piwinger. Er rät zur klassischen Referenzprüfung, also dazu, dem Leumund des Hackers auf den Zahn zu fühlen und mit anderen Unternehmen darüber zu sprechen. Sogenannte CERT-Verbände, also Computer-Emergency-Response-Teams, seien eine gute Adresse. Diese Plattformen eigneten sich gut zum Austausch. „Sie sind erreichbar, aber rein kommt nur, wer nachweislich in Unternehmen an der Sicherheitsfront arbeitet", so Piwinger. Was er darüber hinaus noch rät: „Die Übersetzung von Technik auf die Geschäftswirkung, das muss ein Pen-Tester leisten. Sonst bringt er dem Unternehmen nur die Hälfte."

In Ettlingen arbeitete Geschäftsführer Oehler gemeinsam mit dem Sicherheitsexperten Lindner an der Optimierung der Sicherheitsstrategie. Lindner übersetzte ziemlich genau. „Am Ende überreichte er uns eine 50-seitige Ausarbeitung; dort stand, was wir tun können", sagt Oehler. Bei den Stadtwerken hat seither nicht mehr jeder Rechner einen Zugang zum Internet. Die USB-Zugänge sind ebenfalls stark limitiert. Oehler spricht dabei von „back to the roots". Er möchte sich in seinem Netzwerk auf das Notwendigste konzentrieren, um leistungsfähig zu sein – und so Gefahrenquellen reduzieren. Mit Lindner steht er bis heute in Kontakt. Sicher fühlt er sich aber nicht. Im Gegenteil, er hat den Eindruck, als unterschätzten viele die Bedrohungen von außen. Oehler rät: „Lasst euch hacken. Wir werden das in gewissen Abständen wiederholen, das ist eine Daueraufgabe, da wir mit jedem Softwareupdate selbst neue Lücken schaffen." ■

eva.rossner@frankfurt-bm.com