Hacker auf Bestellung

HEILBRONN *IT-Sicherheitsfirma Cirosec hilft ihren Kunden, ihre Systeme vor Angreifern zu schützen*

Foto: gangdshan/stock.adobe.com

Von unserem Redakteur Manfred Stockburger

Die Hälfte seiner 40 Mitarbeiter sind Hacker: IT-Spezialisten, die in fremde Systeme eindringen. Stefan Strobel ist aber kein Mafia-Boss und arbeitet auch nicht für irgendeinen ausländischen Geheimdienst: Seine Firma Cirosec hackt im Auftrag ihrer Kunden, die das Ziel haben, ihre IT-Systeme so sicher wie möglich zu machen – damit keine bösartigen Hacker den Weg durch die virtuellen Bollwerke finden. Im Zeitalter von Industrie 4.0 ist das ein florierendes Geschäft.

Stefan Strobel
Foto: Cirosec

„Große Autohersteller, Großbanken, Pharmakonzerne – 90 Prozent der Dax-Konzerne sind Kunde bei uns", sagt der Geschäftsführer, der im Heilbronner Gewerbegebiet Schwabenhof gerade sein neues Büro bezogen hat. Ist auch die Bundesregierung Kunde? Bei dieser Frage schweigt Strobel eisern. Behörden und Ministerien hätten allerdings ebenfalls kaum eine Chance, professionelle Hacker-Angriffe von fremden Nachrichtendiensten oder Staaten zu erkennen oder zu verhindern, ist er überzeugt: „Für einen Profi mit genügend Zeit und Ressourcen findet sich eigentlich immer ein Weg in fremde Netze."

Häufig werde in solchen Fällen spezielle Schadsoftware für einen bestimmten Angriff programmiert. „Dann kann sie ein herkömmliches Schutzprogramm gar nicht erkennen. Das sucht ja nur nach bekannten Malware-Typen", erklärt er die Problematik.

Verbesserung Den Kopf in den Sand stecken sollten Firmen und Privatleute dennoch nicht: Es gibt Vieles, was unternommen werden kann, um Produkte und Dienstleistungen sicherer zu machen. Bei Banken etwa habe sich in den vergangenen Jahren viel getan. „Wenn meine Leute da etwas finden, dann sind das meistens Kleinigkeiten und keine dramatischen Schwachstellen." Und doch bleibt Cirosec mit den sogenannten Penetrationstests gut im Geschäft, weil auch die Beseitigung solcher Kleinigkeiten Eindringlingen die Arbeit erschwere.

Was den Pionier unter den IT-Sicherheitsspezialisten – Strobel beschäftigt sich seit 1995 mit dem Thema – zurzeit besonders umtreibt, ist das Thema Industrie 4.0. „Früher waren Maschinen sicher, weil sie nicht vernetzt waren", sagt er. Das hat sich geändert – mit einer speziellen Suchmaschine lassen sie sich ganz einfach finden. Fehlen Sicherheitsvorkehrungen, dann können solche Anlagen leicht von externen Eindringlingen übernommen werden. In der Regel sind die Geräte schlecht gesichert – weil das ja auch gar nicht notwendig war, solange sie nicht mit dem Internet verbunden waren. Handelt es sich um einen Saugroboter im Wohnzimmer, mag das nicht so schlimm sein. Bei einem Hochregallager kann das ganz anders aussehen. „Da passiert viel Schlimmes."

Privatleuten empfiehlt er deswegen, darauf zu achten, dass Computer mit aktuellen Betriebssystemen laufen. „Bei Windows 10 gab es letztes Jahr zwei große Updates mit neuen Sicherheitsfunktionen", sagt Strobel. „Die sollte man machen, auch wenn es eine Weile dauert."

Smart-TV Obwohl er die Sicherheitssysteme der großen IT-Konzerne wie Google, Amazon oder Apple für ziemlich sicher hält – eine sprachgesteuerte Alexa kommt ihm nicht ins Wohnzimmer. Und auch nicht ins Büro. Kritischer sieht er aber Geräte wie Smart-Fernseher oder Spielkonsolen, die mit dem Internet verbunden sind. Dass die sprechende Puppe Hello Barbie anfällig für Hackerangriffe ist, hatte schon vor einigen Jahren für Schlagzeilen gesorgt, wie Strobel in Erinnerung ruft: Unbefugte konnten die Gespräche nachhören, die Kinder mit ihrer Puppe geführt hatten. Auch per Funk ins Hausnetz eingebundene Türklingeln könnten ungebetene Eindringlinge jedenfalls virtuell ins Haus lassen.

Cirosec gehen die Themen also nicht aus – und auch nicht die Kunden. Wer sich von den Heilbronnern nicht hacken lässt, dem bietet das Unternehmen Trainings an, bei denen der richtige Umgang mit neuen Technologien und ihren Sicherheitsrisiken vermittelt wird.

Unsichere Kindersicherungen

Bei einer Untersuchung verschiedener Parental-Control-Apps, mit denen Eltern den Internetzugang ihrer Kinder regulieren können, hat Cirosec-Berater Kai Kunschke eine Reihe von Schwachstellen festgestellt – obwohl sie vom Institut AV-Test zertifiziert waren.

Die Applikationen ESET Parental Control, Kaspersky Safe Kids, Symantec Norton Family sowie die App Sophos Mobile Security bieten unter anderem Funktionen zur **Filterung von Webseiten**. Dazu werden die Seiten an den Hersteller geschickt – wodurch das Surfverhalten des Anwenders preisgegeben wird. Teilweise würden die Daten sogar unverschlüsselt übers Internet geschickt, wie das Unternehmen mitteilt. Zudem würden die Kontrollmechanismen der Apps durch Abstürze außer Kraft gesetzt. Ebenso könnten der Safe Mode von Android, die Mehrbenutzerfunktionen oder die Debug-Schnittstelle ADB verwendet werden, um die Apps zu umgehen. Bei Kaspersky habe dafür ausgereicht, sich ein anderes Benutzerprofil auszuwählen. Lediglich Symantec Norton Family weise Eltern darauf hin, wie das Gerät eingerichtet werden muss, um Angriffe zu verhindern. *red*