

Datensicherheit

Hackerangriff auf JP Morgan wäre mit uns gescheitert

November 2014

Cyberattacken nehmen zu. Kaum ein Tag vergeht ohne einen neuen spektakulären Fall. Mit eperi zeigt ein deutsches Unternehmen jetzt erstmals eine Business-Lösung, die Netze und IT-Strukturen, insbesondere Datenbanken (95 Prozent aller Hackerangriffe haben Datenbanken als Ziel), vor Angriffen aus dem Cyberspace schützt.

Nach eigenen Angaben ist die US-amerikanische Großbank JP Morgan Opfer eines massiven Hackerangriffs geworden. Das meldet die überregionale Tageszeitung „Die Welt“ in Übereinstimmung mit internationalen Medien am 3. Oktober 2014. Vergleichbare Berichte sind beileibe kein Einzelfall. Sie sind nur die Spitze eines Eisbergs. So informierten US-Bundesbeamte die Öffentlichkeit am 20. Oktober 2014 darüber, dass in den zurückliegenden zwölf Monaten mehr als 500 Millionen Finanzunterlagen von Hackern entwendet wurden. Robert Anderson, Assistent der Geschäftsleitung des FBI Criminal Cyber Response and Services Branch, fasst die Situation nach Informationen von US Today wie folgt zusammen: „Die Situation ist so, dass eine einzelne Person aus ihrem Keller heraus 15.000 Banküberfälle an einem Tag begehen kann.“

Tagesaktuelle Medien veröffentlichen derartige Daten-Desaster beinahe täglich. Im aktuellen Fall lässt sich der Schaden noch nicht exakt beziffern. Fest steht aber soviel: Das Datenleck betrifft rund 76 Millionen Haushalte und sieben Millionen kleinere Betriebe. Durch den Angriff gelangten Kundendaten wie Namen, Adressen, Telefonnummern und E-Mail-Adressen in die Hände unbekannter Hacker.

„Vor Cyberattacken wie diesen ist kein Unternehmen gefeit“, weiß Elmar Eperiesi-Beck, Geschäftsführer der eperi GmbH mit Sitz im hessischen Darmstadt. Eperiesi-Beck verweist auf den Sicherheitstacho der Deutschen Telekom AG. „Unter sicherheitstacho.eu lässt sich die Gefahrenlage trefflich einschätzen.“ Die Telekom registriert täglich bis zu 800.000 Hackerangriffe auf Locksysteme, die sie weltweit installiert hat, um Cyberattacken anzuziehen. In nur drei Jahren hat der Konzern so rund neun Millionen Viren, Würmer und Trojaner gezählt. Tendenz: weiter steigend. Einer Studie des Software-Anbieters Symantec zufolge stieg die Zahl gezielter Spionageangriffe allein im Jahr 2012 um 42 Prozent. Bestätigt wird die steigende Gefahr auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Im BSI-Lagebericht 2013 heißt es,

dass Wirtschaftsspionage und Erpressung zugenommen haben. Außerdem hätten Sabotage und der Versuch politischer Einflussnahme durch Hackerattacken an Gewicht gewonnen.

Bis zur Europäischen Union ist die Sensibilität des Themas in der Zwischenzeit vorgedrungen. Die Politiker wollen Betreiber kritischer Infrastrukturen künftig dazu verpflichten, Hackerangriffe in einem zentralen Melderegister zu publizieren. Den Plänen zufolge wären von der Meldepflicht Bahn- und Fluggesellschaften, Banken, Telekommunikationsbetreiber sowie Strom- und Gas-Anbieter betroffen. Für den Sicherheits-Experten Eperiesi-Beck kann das allenfalls ein Anfang sein, denn: Für den gesamten Mittelstand bringen die europäischen Pläne erst einmal keine Verbesserung des Ist-Zustands. „Die weltweite digitale Vernetzung ist heute zur unabdingbaren Infrastruktur des Mittelstands geworden, bei dem das Cloud-Computing zu einem entscheidenden Wirtschaftsfaktor wird“, so Eperiesi-Beck. „Die deutschen Unternehmen müssen diesen Schritt mitmachen, um wettbewerbsfähig zu bleiben.“

Dass dieser Weg jetzt auch mit der erforderlichen Sicherheitsstruktur möglich ist, dafür haben Eperiesi-Becks Software-Entwickler bei eperi mit einer Aufsehen erregenden Software gesorgt. Weil rund 95 Prozent aller Hackerangriffe auf Datenbanken abzielen, schützt eperi alle sensitiven Daten durch eine effektive Open-Source-Verschlüsselung. „Im Unterschied zu allen anderen Lösungen des Marktes verschlüsseln wir die Daten, die in den Datenbanken gespeichert werden – und nicht nur die Datenbank-Dateien.“ Die Schwachstelle „Admin“ wird so wirkungsvoll ausgeschaltet. „Hätten die geschädigten Firmen unsere Software seinerzeit eingesetzt, dann hätten sich Hacker beim Versuch sensible Daten zu stehlen, die Zähne ausgebissen“, verdeutlicht Eperiesi-Beck das Sicherheitspotenzial seiner Software-Lösung. Der Ansatz des IT-Security-Spezialisten aus Hessen kommt an. Kürzlich hat eperi als erstes europäisches Unternehmen die Freigabe für den IBM Marketplace erhalten. Eperiesi-Beck führt diesen Erfolg nicht zuletzt auf die Open-Source-Basis zurück, die in Kooperation mit dem BSI entwickelt wurde.

4.565 Zeichen

Bildlegende



Elmar Eperiesi-Beck,
Geschäftsführer eperi GmbH

Unternehmensporträt

Das Darmstädter IT-Security-Unternehmen eperi bietet 100-prozentigen Hackerschutz für Datenbanken. Als Gemeinschaftsentwicklung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eperi u.a. bei deutschen Behörden, Medizinfirmen und Großkonzernen wie Evonik im Einsatz. Der USP der Lösung ist, dass selbst Administratoren (und somit eventuell erfolgreiche Hacker) nur verschlüsselte Daten sehen. Bei der Implementierung sind keine Anpassungen von Systemen notwendig.

Bei Veröffentlichung bitten wir um die Zusendung eines Belegexemplars.

Pressekontakt

Wolfgang Hennes
Uhlandstraße 9
64297 Darmstadt
presse@eperi.de