SparkassenZeitung

29. November 2016 - 12:00 | Großbritannien

Sorge um IT-Sicherheit bei Banken wächst

Frances Palgrave

Nach der Cyber-Attacke auf die britische Tesco Bank drängen Regierung und Aufsicht die Institute der Insel, ihre IT-Systeme wirksamer gegen Hackerangriffe zu schützen. Die Lage sei besorgniserregend, heißt es.

"Systematische und ausgeklügelte Attacke": Online-Kriminelle erbeuteten rund 2,5 Millionen Pfund von Kunden der Tesco Bank. *(dpa)*

Bei einem großangelegten Cyber-Angriff auf die britische Tesco Bank Anfang November entwendeten Online-Kriminelle innerhalb von zwei Tagen 2,5 Millionen Pfund von 9000 Girokonten. Das Institut mit seinen 7,8 Millionen Kunden, das zu dem führenden britischen Einzelhändler Tesco zählt, sperrte sicherheitshalber seine insgesamt 136.000 Girokonten für Online-Transaktionen. CEO Benny Higgins sprach von einer „systematischen und ausgeklügelten Attacke“ und entschuldigte sich bei den Kunden. Die Betroffenen wurden entschädigt. Higgins versicherte, Kundendaten seien bei dem Übergriff nicht abhandengekommen.

Die National Crime Agency und die Finanzaufsicht FCA untersuchen den Vorfall, der in den Medien auch als bislang „größter Online-Bankraub in Großbritannien“ tituliert wird. Begleitet werden die Ermittlungen vom neuen National Cyber Security Centre (NCSC), das im Oktober als Behörde des britischen Geheimdienstes GCHQ aus der Taufe gehoben wurde und alle nationalen Maßnahmen gegen Cyber-Kriminalität bündeln soll. Bislang gebe es keine Hinweise darauf, dass sich aus dem Vorfall bei der Tesco Bank weiterreichende Implikationen für den britischen Bankensektor ergeben hätten, so das NCSC.

Dennoch hat sich die Bedrohung aus dem Cyberraum für die britische Finanzbranche in den vergangenen Monaten weiter verschärft. Für 2016 wurden der FCA bereits 75 Hackerangriffe auf Banken gemeldet, nach 27 Fällen im Vorjahr

und fünf Übergriffen in 2014. FCA-Chef Andrew Bailey bezeichnete den Diebstahl bei der Tesco Bank als „bislang beispiellos und gravierend“. Der Zustand der IT-Systeme der britischen Banken sei „besorgniserregend“. Mit Blick auf die fortschreitende Digitalisierung der Branche betonte er, je komplexer die IT-Systeme, desto mehr Angriffspunkte böten sich für Cyber-Kriminelle.

Veraltete Systeme

Aufsicht und Regierung fordern nun mit Nachdruck, die Banken sollten ihren IT-Sicherheitsschutz verstärken und dieses Thema auch strategisch umfassender angehen. Der FCA zufolge lassen sich die meisten Cyber-Attacken auf unzureichende Präventivmaßnahmen, veraltete IT-Systeme oder ein Mangel an Sicherheitsbewusstsein innerhalb der Häuser zurückführen. Ransomware-Attacken legten 2015 um 35 Prozent zu und dürften weiter steigen. Risiken seien auch die verstärkte Datenspeicherung in der Cloud und der Mangel an IT-Fachkräften in der Branche. Banken bräuchten „eine ganzheitliche Sicherheitskultur“, die nicht nur technologische Aspekte, sondern auch alle Mitarbeiter und Prozesse miteinbeziehe.

Der Notenbankausschuss für Finanzstabilität regte bereits regelmäßige regulatorische IT-Sicherheitstests an. Bislang können Banken ihre individuellen Schutzmaßnahmen freiwillig durch die Notenbank prüfen lassen. Die Bank of England will nun zusammen mit dem NCSC zusätzliche Maßnahmen zum Cyberschutz des Finanzsektors entwickeln.

Der Vorsitzende des Finanzausschusses im britischen Unterhaus, Andrew Tyrie, betonte, der Fall der Tesco Bank sei nur der jüngste in einer langen Serie von IT-Systemstörungen, welcher Millionen von Verbrauchern ausgesetzt seien. So könne es nicht weiter gehen. Die Banken benötigten mehr IT-Expertise in den Vorständen. Zudem müsse die Zusammenarbeit zwischen Aufsicht, Regierung und Sicherheitsbehörden gegen Cyber-Kriminelle besser koordiniert werden.

Der Bankenverband BBA verweist unterdessen darauf, dass die Banken bereits 700 Millionen Pfund jährlich in Schutzmaßnahmen gegen Cyber-Kriminalität investierten. Während die Institute ihre Systeme absichern, richten Cyber-Kriminelle vermehrt ihr Augenmerk auf die Bankkunden. Einer Umfrage zufolge beachten nur wenige Briten die Grundregeln zur Sicherheit im Netz. Knapp die Hälfte der Befragten nutzen die gleichen Passwörter für ihre Online-Konten, während gut 20 Prozent ihre Sicherheitssoftware nicht regelmäßig aktualisieren.

Auch in Deutschland wachsen die Herausforderungen an die Banken, sich besser vor Cyber-Angriffen zu wappnen. Die Finanz Informatik (FI) schützt ihre Systeme und die ihrer Kunden gegen aktuelle Bedrohungslagen, etwa DDoS-Angriffe oder Advanced Persistent Threats. Insbesondere beim Online- und Mobile-Banking setzt die FI moderne Sicherungs- und Authentifizierungsverfahren ein und unterstützt mit S-Cert die Sparkassen bei der Aufklärung ihrer Kunden über Sicherheitsrisiken.

Scannen Sie diesen Code mit Ihrem Smartphone und lesen Sie diesen und weitere Beiträge online