«SWIFT rüstet auf im Kampf gegen Cyber-Attacken»

Die TEMET AG ist SWIFT-Partner und registrierter Cyber Security Provider mit Spezialisierung auf IT-Sicherheit. Dr. Alexander Rhomberg erläutert, wie sich die Bankenwelt vor Angreifern schützen kann.

IM INTERVIEW

Dr. Alexander Rhomberg
Partner und Mitbegründer
TEMET AG

Herr Dr. Rhomberg, es war ein Hackerangriff, wie ihn die Bankenwelt bis dahin noch nicht kannte: Im Februar 2016 schafften es Hacker, gefälschte Überweisungen über mehr als 950 Millionen US Dollar bei der Bank Bangladesh ins SWIFT Netzwerk einzuspeisen. Wie konnte es dazu kommen?

Es zeigte sich, dass zum einen die betroffene Bank erhebliche Mängel in der Sicherheit ihrer IT aufwies. Zum anderen waren die Angreifer nicht nur über die eingesetzte Software und IT-Infrastruktur genauestens informiert, auch wussten sie, wo exakt die Schwachstellen lagen und zu welchem Zeitpunkt ihr Angriff erfolgen musste. Neben der Erwirtschaftung des grösstmöglichen Profits verfolgten die Hacker das Ziel, die Überweisungen lange geheim zu halten, um das Geld von den Zielbanken weiter transferieren oder in bar abholen zu können.

Hätte das auch jede andere beliebige Bank treffen können?

Die Angreifer sind hochprofessionelle Organisationen. Sie versuchen es überall und machen dort weiter, wo sie den schlechtesten Schutz vorfinden und sehen, dass etwas zu holen ist.

Welche Konsequenzen zog die SWIFT, die dafür verantwortlich ist, den Nachrichten- und Transaktionsverkehr von rund 10'000 Banken zu standardisieren?

Fakt ist: Damit die Angreifer an die Software herankommen können, müssen sie sich bereits sehr tief ins System der Bank hacken. Die SWIFT wies darauf hin, keine Schwachstellen im System zu haben. Dennoch trat sie in Aktion und erarbeitete ein Sicherheitsprogramm, das Customer Security Controls Framework, das umfassende Sicherheitsempfehlungen beinhaltet.

Wie wurden die neuen Vorschriften von den Banken aufgenommen?

Der erste Entwurf enthielt viele Massnahmen für kleinere SWIFT Teilnehmer mit wenig ausgebauter IT Sicherheit, die aber für alle gegolten hätten. Diese stiessen bei grösseren Schweizer Banken auf starken Widerstand. Nach intensiven Besprechungen wurde eine Stellungnahme der Schweizer SWIFT-Teilnehmer erarbeitet. Das Framework wurde schliesslich überarbeitet. Es setzt in der publizierten Version Kontrollziele, die mit verschiedenen Umsetzungen erreicht werden können.

Diese Sicherheitsempfehlungen finden in der Finanzbranche starke Unterstützung. Was beinhalten sie im Einzelnen?

Das Programm umfasst eine Reihe von Vorschriften zum Schutz der SWIFT-Systeme und eine Plattform, über die SWIFT ihre Kunden schnell über Gefahren informieren kann. Bei den Vorschriften geht es beispielsweise darum, die Systeme, mit dem das SWIFT-Netzwerk verbunden ist, von anderen Systemen abzutrennen. Zudem soll eine sichere Identifikation der User, nicht nur per Passwort, sondern ebenso über ein zusätzliches Identifikationsmittel wie eine Smartcard erfolgen.

Bis Ende 2017 soll von allen SWIFT-Kunden eine Selbst-Deklaration durchgeführt werden. Wie sieht diese aus?

SWIFT hat in ihrem Framework in 16 obligatorischen und elf empfohlenen Kapiteln Schutzziele definiert. Die Banken müssen bis Ende 2017 auf der SWIFT-Plattform eintragen, ob sie diese Ziele erreichen. Diese Informationen werden anschliessend den Finanzmarktaufsichtsbehörden kommuniziert.

Inwiefern kann die TEMET AG ihren Kunden bei der Selbst-Deklaration zur Seite stehen?

Wir unterstützen die Banken darin, diese Vorgaben bezüglich der vorhandenen Infrastruktur und Sicherheitslösungen zu analysieren. Zudem beurteilen wir, ob ein Kontrollziel erreicht wird und an welcher Stelle wir Verbesserungen des Sicherheitsumfelds empfehlen. Da wir den Entstehungsprozess und jede Version des Frameworks im Detail kennen, sind wir in der Lage, Banken den optimalen Weg zur Erreichung der Kontrollziele aufzuzeigen.

Wie wahrscheinlich ist es, dass trotz diverser Sicherheitsvorkehrungen Hacker in naher Zukunft sich erneut in diesem Masse die Finanzabläufe einschalten?

Mit den neuen Sicherheitsvorkehrungen wird es den Hackern deutlich erschwert, in die SWIFT Infrastruktur der Banken einzugreifen. Nun liegt es jedoch an den Finanzinstituten selbst, sich genau zu überlegen, wie solche Zahlungen generell zu verhindern sind. Denn klar ist auch: Hacker sind Organisationen mit detailliertem Wissen über die eingesetzten Computersysteme, die jederzeit auf der Suche nach dem schwächsten Glied in der Kette sind.

Der Schutz vor Diebstahl via Überweisungen muss heutzutage gewährleistet sein.