Eine sichere Bank...

...sind Geldinstitute und deren Kunden vor allem für Cyberkriminelle. Sophos-Sicherheitsexperte John Shier erklärt im Kurzinterview warum das so ist. Und bleibt.

Wiesbaden, 19. Dezember 2016 – Banken und ihre Kunden sind ein unverändert beliebtes Ziel für Online- und Offline-Kriminelle. John Shier, Sicherheitsexperte bei Sophos, gibt in einem Kurzinterview eine Übersicht über die zu erwartenden Angriffe sowie über mögliche Schutzmaßnahmen sowohl durch die Banken selbst wie auch durch Verbraucher.

Wie ist die aktuelle Bedrohungssituation für Banken und ihre Kunden?
Ein nach wie vor wichtiges Bedrohungsszenario sind Phishing-Attacken – sie haben bei Cyberkriminellen nichts an Beliebtheit eingebüßt. Banken und Bank-Kunden werden daher auch künftig Ziel von ausgeklügelten Phishing-Attacken sein. Inhalt dieser Attacken ist der Versuch durch die Kriminellen, die Marke, das Aussehen und den Auftritt eines Bankunternehmens so täuschend echt zu kopieren, dass Nutzer glauben, es bei gefälschten E-Mails mit dem echten Unternehmen zu tun zu haben. Phishing ist in Cyberkriminellen-Kreisen nach wie vor eine beliebte Methode, um an persönliche Anmeldeinformationen von Bankkunden zu kommen. Als Medium dienen dabei E-Mails und auch SMS. Klicken die User auf die bereitgestellten Links in der Phishing-Nachricht, so werden sie auf gefährliche Webseiten weitergeleitet, die gefälschte Versionen der Bankenwebseiten sind. Dort werden nicht nur Benutzername und Passwort abgefragt, sondern auch Information zur Benutzerüberprüfung wie Adresse, Kreditkarte und Bankverbindung. Diese Informationen können dann von den Kriminellen für ihre betrügerischen Aktivitäten verwendet werden. Oft werden diese Informationen zudem für die gleichen Zwecke an Dritte weiter verkauft.

Mit welchen Cyber-Gefahren müssen Banken außerdem rechnen?
Weitere Gefahren drohen Banken durch SWIFT-Angriffe. SWIFT ist der weltweite Standard-Dienstleister für Bank-Transaktionen. Angriffe auf das SWIFT-System ermöglichen es den Kriminellen eigene, illegale Transaktionen durchzuführen. Bislang bekannte Angriffe offenbarten dabei, dass die Gangster sich dabei gezielt die schwächsten Akteure aussuchen. Diese Art der Bedrohung ist wesentlich schwerer zu quantifizieren und es scheint, als ob die Angreifer über sehr gute Kenntnisse der in Banken eingesetzten IT inklusive des SWIFT-Systems verfügen. Dadurch sind diese Angriffe viel schwerer zu erkennen. Ein motivierter und fähiger Insider genießt womöglich das Vertrauen des Bankinstituts und hat bereits das nötige Wissen, um solche Angriffe durchzuführen. Es sei aber darauf hingewiesen, dass das Sicherheitsniveau von Bank zu Bank unterschiedlich ist und so einige Banken einem höheren Risiko ausgesetzt sind als andere.

Welche Angriffe sind am gefährlichsten?
Die Gefährlichkeit eines Angriffs hängt von der Perspektive ab. Aus Sicht der Banken kann der Verlust von Millionen an Euros durch betrügerische SWIFT-Transaktionen verheerend sein. Aber auch der Schaden durch den Vertrauensverlust bei womöglich hunderten und mehr Kunden, die einen Phishing-Angriff nun vielleicht für immer mit der Marke des Geldinstituts assoziieren kann enorme Ausmaße annehmen. Aber auch Verbraucher, die Opfer eines Phishing-Angriffs werden, können unter katastrophalen Folgen zu leiden haben. Nicht nur, dass ihnen durch die Cybergangster möglicherweise direkt eine Menge Geld

gestohlen wird; die Täter könnten obendrein zusätzliche Konten im Namen ihrer Opfer eröffnen und weiteren Schaden mit nachhaltigen Auswirkungen anrichten.

Wie sollten sich Banken auf diese potenziellen Bedrohungen vorbereiten?
Selbstverständlich haben die meisten Banken tatsächlich bereits die notwendige Technologie, um Cyber-Bedrohungen zu entdecken oder abzuwehren. Was aber oft noch fehlt ist eine effiziente Koordination von Personen, Prozessen und Werkzeugen. Die technischen Werkzeuge sind vorhanden, um Ereignisse zu entdecken, auf sie zu regieren und entsprechende Berichte zu erstellen. Ergänzend dazu sind aber auch Fachleute nötig, die jene Anomalien erkennen, die von den Maschinen nicht registriert werden können. Und schließlich sollten Prozesse eingeführt werden, die es ermöglichen, die durch die technischen Instrumente gesammelten und von den Menschen analysierten Informationen möglichst schnell an die relevanten Stakeholder des Unternehmens zu kommunizieren. Zu diesen gehören beispielsweise die Sicherheits- und Risikoteams, die betroffenen Geschäftsbereichsleiter und alle technischen Mitarbeiter, die zur Behebung des Problems erforderlich sind.

Wie können Verbraucher zur eigenen Sicherheit beitragen?
Verbraucher können sich schützen, indem sie wachsam sind und dem Drang widerstehen, auf Phishing-E-Mails oder SMS-Nachrichten zu reagieren. Dies passiert leider immer noch viel zu häufig. Deshalb: Wenn eine E-Mail eintrifft, die dazu auffordert einem Link zu folgen und dort dann persönliche Nutzerdaten zu aktualisieren, so wird sie nicht von der Bank kommen, sondern es wird sich um Phishing handeln. Banken geben diese Art von Kommunikation nicht an ihre Kunden weiter. Es gibt also keinen guten Grund, einer solchen Aufforderung in einer E-Mail oder SMS Folge zu leisten. Wer als Kunde unsicher ist, ob die E-Mail nicht vielleicht doch von der eigenen Bank stammt, der sollte lieber das Telefon zur Hand nehmen und für die endgültige Sicherheit bei der zuständigen Bankfiliale nachfragen.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de