Medienmitteilung

Hacker-Angriff auf Schweizer Banken – Was tun?

Laut der Schweizer Internetregistrierungsstelle Switch ist derzeit eine grossangelegte Attacke gegen E-Banking-Konten von 12 Schweizer Banken im Gange. Zum Einsatz kommt dabei ein neuartiger Trojaner namens «Retefe».

Luzern, 23.07.2014 – Der Angriff läuft wie folgt ab: Der Kunde öffnet eine Spam-Mail, der darin enthaltene Trojaner «Retefe» manipuliert den Rechner. Er ändert den Eintrag auf einen gefälschten Namens-Server, so dass der Rechner selbst bei richtig eingegebener Adresse eine gefälschte Seite zurück erhält. Ebenso installiert er ein gefälschtes sogenanntes Root-Zertifikat, so dass der infizierte Rechner die gefälschte Seite sogar als angeblich «echt» bescheinigt. Anschliessend löscht sich der Trojaner selbst und wird somit nicht mehr als Schadsoftware erkannt – all dies ist äusserst hinterhältig!

Sobald der Kunde dann die E-Banking-Seite seiner Bank aufruft, wird er auf einen falschen Server umgeleitet. Dort sieht er eine gefälschte Seite seiner Bank, die wegen des gefälschten Root-Zertifikats als «echt» eingestuft wird. Damit ist es passiert. Der Kunde gibt seine Sicherheitsinformationen ein, diese gelangen an die Hacker. Danach wird der Kunde angehalten, auf seinem Smartphone eine manipulierte App zu installieren. Diese schickt dann die Sicherheits-SMS (mTAN) der Bank an die Hacker weiter. Die Angreifer haben damit volle Kontrolle!

Was tun? – Empfehlungen des Kompetenzzentrums Informationssicherheit der Hochschule Luzern:

- Im ersten Schritt des Angriffs handelt es sich um Phishing. Solche E-Mails werden von Finanzinstituten nicht versendet und sollten ungelesen / ungeöffnet gelöscht werden. Auf keinen Fall irgendwelche Links klicken oder Anhänge öffnen. Weitere Informationen: https://www.ebas.ch/phishing
- Des Weiteren ist von höchster Wichtigkeit, dass auf jedem Rechner ein aktuelles Antivirenprogramm installiert ist. Dieses erkennt allfällige Trojaner und warnt Kunden vor dessen Installation.
- Wenn Kunden beim E-Banking dazu aufgefordert werden, eine App auf dem Smartphone zu installieren, handelt es sich um einen Angriff. Jetzt oder bei anderen ungewöhnlichen Verhalten beim Einloggen sollte das Finanzinstitut schnellstmöglich kontaktiert werden. So können betrügerische Zahlungen gestoppt werden.

Weitere Informationen unter: https://www.ebas.ch

Dienstleitung «eBanking – aber sicher!»

Die Webseite www.ebankingabersicher.ch ist einer von vier Dienstleistungspfeilern, die die Hochschule Luzern den mittlerweile 38 Partner-Finanzinstituten anbietet. In einem ganzheitlichen Ansatz bietet «eBanking – aber sicher!» öffentliche Endkunden-Kurse an. Zusätzlich werden die Helpdesk-Mitarbeitenden und Kundenberatenden der Partner-Finanzinstitute zu aktuellen und sicherheitsrelevanten Themen geschult sowie die Schweizer Medienlandschaft bezüglich E-Banking-Sicherheit beobachtet.

Weitere Informationen: https://www.ebankingabersicher.ch/mediasection

---

Hochschule Luzern – Wirtschaft

Am Institut für Wirtschaftsinformatik der Hochschule Luzern – Wirtschaft wird das Competence Center Information Security betrieben. Ein Team von Dozenten und wissenschaftlichen Mitarbeitenden ist spezialisiert in der Informationssicherheit. Schwergewichte sind die Ausbildung (Bachelor und Master in Wirtschaftsinformatik), die Weiterbildung (z. B. Master of Advanced Studies in Information Security) sowie die Forschung und Dienstleistung für Dritte (EBAS, IT-Audits etc.).

Weitere Informationen: www.hslu.ch/iwi

Medienkontakt

Hochschule Luzern – Wirtschaft
Oliver Hirschi
Institut für Wirtschaftsinformatik
CH-6002 Luzern

https://www.ebas.ch/de/kontakt