Comunicato stampa

Attacco degli hacker a banche svizzere – che fare?

Secondo l'ufficio di registrazione svizzero Switch è in corso un massiccio attacco contro i conti e-banking di 12 istituti finanziari svizzeri. Viene utilizzato un nuovo cavallo di Troia, «Retefe».

Lucerna, 23.07.2014 – Un attacco si svolge così: il cliente apre un'e-mail di spam e il cavallo di Troia contenuto al suo interno, «Retefe», manipola il computer. Il software dannoso modifica la registrazione impostando un server dal nome contraffatto, affinché il PC apra una pagina contraffatta anche se l'indirizzo viene inserito correttamente. Allo stesso tempo installa un cosiddetto certificato root contraffatto, di modo che il computer infetto possa persino certificare come «autentico» il sito contraffatto. Alla fine il cavallo di Troia si cancella e quindi non viene più riconosciuto come malware – l'intera procedura è estremamente subdola!

Non appena il cliente apre la pagina del sistema e-banking della banca, viene indirizzato a un server errato, nel quale troverà un sito contraffatto che il certificato root falso farà classificare come «autentico». E il dado è tratto: il cliente inserisce le proprie informazioni di sicurezza e queste finiscono nelle mani degli hacker. Il cliente viene poi esortato a installare sullo smartphone un'app manipolata, che inoltra agli hacker l'SMS di sicurezza (mTAN) della banca. Ora i malintenzionati hanno pieno controllo sul sistema!

Che cosa si può fare? – Raccomandazioni del centro di competenza per la sicurezza dell'informazione della Scuola universitaria di Lucerna:

- La prima fase dell'attacco rientra nella categoria del phishing. Queste e-mail non vengono mai inviate dagli istituti finanziari e quindi andrebbero cancellate senza essere nemmeno lette o aperte. In nessun caso bisogna fare clic su eventuali link o aprire gli allegati. Ulteriori informazioni: https://www.ebas.ch/phishing
- Inoltre è della massima importanza che su ogni computer sia installato un programma antivirus aggiornato, capace di riconoscere eventuali cavalli di Troia e di avvisare il cliente prima che vengano installati.
- Se durante una sessione di e-banking i clienti vengono invitati a installare un'app sullo smartphone, si tratta di un attacco. In questo caso o in presenza di altri comportamenti insoliti in fase di login, è opportuno contattare il proprio istituto finanziario nel minor tempo possibile. Così facendo si potranno bloccare i pagamenti fraudolenti.

Per ulteriori informazioni: https://www.ebas.ch

Servizio «eBanking – ma sicuro!»

Il sito Internet www.ebankingmasicuro.ch è una delle quattro colonne portanti dei servizi offerti dalla Scuola universitaria di Lucerna ai 36 istituti finanziari partner: seguendo un'impostazione complessiva, infatti, il progetto offre anche corsi per i clienti finali aperti al pubblico. Il sistema comprende inoltre la formazione ai collaboratori dell'helpdesk e ai consulenti alla clientela degli istituti finanziari partner per quanto riguarda tematiche attuali e importanti dal punto di vista della sicurezza, come pure il monitoraggio dei media svizzeri sui temi attinenti alla sicurezza nell'e-banking.

Ulteriori informazioni: https://www.ebankingmasicuro.ch/mediasection

---

Scuola universitaria di economia di Lucerna

Presso l'Istituto di informatica di gestione della Scuola universitaria di economia di Lucerna è operativo il centro di competenza in Information Security. Un team di docenti e collaboratori scientifici è specializzato nella sicurezza dell'informazione. Punti cardine sono la formazione (Bachelor e Master in informatica economica), corsi di perfezionamento (come il Master of Advanced Studies in Information Security), attività di ricerca e offerta di servizi a terzi (EBAS, IT-Audit, ecc.).

Ulteriori informazioni: www.hslu.ch/iwi

Contatti per i media

Scuola universitaria di economia di Lucerna
Oliver Hirschi
Istituto di informatica di gestione
CH-6002 Lucerna

https://www.ebas.ch/it/contatti