Banche, la sfida della sicurezza informatica

LUGANO / In una tavola rotonda promossa dall'ABT sottolineata l'importanza dei comportamenti personali nella gestione dei rischi collegati al flusso di dati sensibili – Spesso ai furti si unisce il ricatto e il blocco dell'attività

La difesa dalla criminalità informatica nelle banche, come altrove, non è solo una questione tecnologica ma di comportamenti personali. Il tema, quanto mai attuale e complesso, è stato al centro di una tavola rotonda organizzata dall'Associazione Bancaria Ticinese (ABT), moderata dal suo direttore Franco Citterio, con la partecipazione di Alessandro Trivilini, responsabile del Servizio informatica forense della SUPSI, di Luca Previtali, Head of Technology and Innovation di BancaStato ed Enea Bonaiti, Chief Information Security Officer & Data Protection di Cornèr Banca. Secondo gli specialisti in ogni organizzazione tutto il personale deve essere sensibilizzato e coinvolto, tanto più alla luce delle nuove regolamentazioni e delle responsabilità che comportano. La Finma emette normative continue e le leggi, sia svizzere che europee, impongono adempimenti stringenti.

L'ambito della cybercriminalità si è esteso molto anche a causa dell'home working

L'attività bancaria presenta aree di elevato rischio, dalle carte di credito ai trasferimenti di denaro, oggi spesso fatti via smartphone ed altri mezzi digitali. Una grande minaccia è rappresentata dal phishing via e-mail che riproducono il sito della banca od una pagina apparentemente nota, i cui mittenti andrebbero controllati telefonicamente nei casi dubbi.

Ma chi sono gli hacker? Governi e organizzazioni che agiscono a scopo geopolitico e ideologico, per spionaggio o estorsione; altri che operano per vendetta o malcontento, ma più spesso (nell'80% dei casi), semplici criminali alla ricerca di denaro, dilettanti ma anche ben organizzati e tecnologicamente avanzati. Ai furti si unisce spesso il ricatto e il blocco dell'attività. Un nuovo tipo di criminalità informatica è costituito da reti di robot che attaccano simultaneamente il sito di una istituzione.

Il «territorio» della cybercriminalità si è esteso, anche a causa dell'*home working*, dell'*outsourcing* di vari servizi e dell'avvento dei cosiddetti «cloud».

Quanto alle criptovalute, vanno distinte quelle principali e «gestite» dalle banche (oggi a livello ancora limitato) e da piattaforme regolamentate, tali da assicurare una certa tracciabilità, rispetto a quelle modificate, ad esempio Monero, usate dalla criminalità nelle operazioni illegali.

Gli specialisti hanno fornito alcuni consigli pratici, al di là della normale attenzione che ogni utilizzatore di tecnologia e di apparati digitali deve porre nelle proprie azioni: estrema cautela nell'uso dei social media e nelle informazioni che vi sono immesse, uso di password complesse, diversificate per i diversi accessi e detenute in modo confidenziale, impiego di antivirus efficaci e loro aggiornamento costante, back-up dei dati e attenzione nel navigare, controllando fra l'altro il fatidico «lucchetto» che compare nell'indirizzo del sito web. **Gian Luigi Trucco**