EVENTI

LA SICUREZZA SIAMO NOI

I criminali digitali sono sempre più aggressivi e sfruttano le debolezze delle aziende e delle persone. Per far capire meglio come i nuovi malviventi siano in grado di violare le aziende (e per quale motivo lo facciano) Redco Telematica e RSA, hanno organizzato insieme un evento unico. Una vera e propria sfida tra la tecnologia RSA e un Ethical Hacker. È stato un confronto avvincente che ha mostrato la tematica della sicurezza sotto una nuova luce. L'informazione su questi temi è fondamentale: Redco Telematica e RSA sono impegnate dal 2000 in una partnership profonda che non riguarda solo la commercializzazione di soluzioni, ma anche la diffusione della cultura «Esistono siti, facilmente raggiungibili, che offrono interi set di software per portare a compimento ogni tipo di attacco: dal furto delle e-mail ai DDos – ha spiegato Massimo Cotta, responsabile marketing di Redco Telematica –. Chiunque ormai può scaricarli e utilizzarli. Nessuno è davvero al sicuro. In pochi minuti si può entrare in una rete e scoprire le password di una Webmail. Per questo occorre ripensare l'atteggiamento nei confronti della security». Alessio L.R. Pennasilico è il security evangelist di Alba S.T. e hacker, nella vera eccezione del termine che si è confrontato con Redco e RSA. «Molte aziende – ha spiegato Pennasilico – vengono violate e non se ne accorgono nemmeno, perché l'obiettivo dei criminali digitali è cambiato: oggi puntano a entrare nelle reti aziendali, rubarne i segreti e uscirne senza che nessuno si accorga di nulla. Questi attacchi si chiamano Apt (Advanced persistent threat) e nessuno è al sicuro. Non si sfruttano solo le debolezze dei software ma soprattutto quelle umane attraverso il social engineering, ovvero il recupero di informazioni essenziali per mezzo dei social network, che permettono di conoscere i dipendenti e le aziende per avere i dati necessari a violare le reti. A volte le cose sono anche più semplici: se si vuole colpire un'azienda basta disseminare "in zona" delle chiavette Usb, magari da 32 Gb, con un malware al suo interno. L'esperimento è stato fatto e delle 100 memorie sparse ben 99 nel giro di 24 ore hanno cominciato a inviare dati all'esterno dell'azienda». Ma come proteggersi, allora, con la tecnologia? La maggior parte degli attacchi di successo (il 99,9%) sfruttano debolezze conosciute e basterebbe quindi aggiornare i sistemi per non essere colpiti. Ma soprattutto occorre inserire la sicurezza nella cultura aziendale. Anche RSA – produttore di tecnologia di sicurezza ad altissimo livello – è stata vittima di una attacco Apt; tuttavia il comportamento tenuto è stato esemplare. «Non solo RSA si è accorta dell'attacco e lo ha scoperto mentre era in corso – ha spiegato Gianni Napoli, presales manager Sud Emea di RSA –, ma lo ha comunicato subito ai clienti chiarendo che cosa stava succedendo. Questo ha permesso da subito di prendere le contromisure adeguate e di mettere tutto al sicuro». La cifratura a due fattori rimane una delle armi migliori contro le intrusioni, ma nulla è superiore al "firewall umano" rappresentato dalle nostre abitudini e dalla nostra prudenza. Tutti sanno che inserire una memoria Usb proveniente da fonte sconosciuta è rischioso, tuttavia basta poco per superare queste remore. Bisogna essere accorti anche quando si affida la gestione della sicurezza a un partner esterno: la sua preparazione è l'unica garanzia che la rete aziendale sia sicura. «La selezione è fondamentale – ha concluso Elisa Mancassola, direttore generale di Redco Telematica –. Non si può pensare di dotarsi dei migliori sistemi di protezione se poi si affida il proprio network a operatori poco qualificati. Redco Telematica ha un'esperienza trentennale e una lunga serie di casi successo».

Contatti
REDCO TELEMATICA SPA
Via Alba, 18/A
21052 Busto Arsizio (VA)
Tel. +39.0331.397600
Fax +39.0331.329901
redco@redco.it