LA NAZIONE

03-AGO-2017
pagina 23
foglio 1

A voi la parola

Gli interventi vanno indirizzati a La Nazione,
viale Giovine Italia 17, 50122 Firenze - fax 055 2343646
o all'indirizzo mail: segreteria.redazione.firenze@monrif.net

di MASSIMO ARTINI*

L'HACKER NON VA IN VACANZA

NEL PERIODO *delle vacanze si tende a rilassarsi e spesso si abbassa la guardia. In ambito informatico si tratta di un errore che rischiamo di pagare molto caro. Spesso gli hacker approfittano delle opportunità offerte dai mesi estivi per incrementare certe tipologie di attacchi. Del resto in molti casi al cybercriminale di turno può bastare lanciare il proprio virus o malware impiegando appositi web robot (meglio noti come "bot) e lasciare che lavorino per lui mentre si gode la vacanza.*

QUESTI *software, infatti, sono in grado di operare in automatico colpendo le reti con diverse tipologie di attacco e se d'estate i CERT (Computer Emergency Response Team) e i SOC (Security Operation Center) delle aziende operano a ranghi ridotti per via delle ferie… beh, la cosa risulta ancora più facile! Anche il comune cittadino non è meno esposto ai rischi di tipo cibernetico. La ricerca online di hotel, traghetti, noleggi auto, viaggi organizzati e servizi di vario genere per le vacanze ci espone ancora di più al rischio di incappare in software maligni e attività di phishing. Non è un caso se generalmente è proprio nei periodi estivi che si registra un picco nelle clonazioni di carte di credito. Per di più, una volta in vacanza, la necessità di restare sempre connessi spinge molti a sfruttare le reti Wi-Fi libere messe a disposizione da locali, hotel, resort, ecc. che, purtroppo, nella maggior parte dei casi non sono criptate o, comunque, non offrono sufficienti livelli di sicurezza. Ovviamente esistono modi per ridurre al minimo rischi e pericoli.*

PER PRIMA *cosa è fondamentale effettuare tutti gli aggiornamenti di sicurezza dei propri software, via via che vengono rilasciate le varie patch o le nuove versioni. Basti pensare che il famigerato ransomware (virus che cripta i dati del computer e chiede un riscatto per "liberarli") Wannacry ha potuto colpire solo i computer che non erano stati aggiornati con la patch rilasciata da Microsoft poche settimane prima. Ovviamente bisogna sempre valutare attentamente l'attendibilità di un'email prima di aprirne il contenuto (soprattutto gli allegati in formato .pdf o di tipo eseguibile) perché potrebbe contenere virus di ogni tipo. Ancora maggiore attenzione bisogna fare nel rispondere alle email con le quali viene richiesto di fornire propri dati (soprattutto quelli bancari), l'accesso alle proprie reti di social network (Facebook, Linked-in, ecc.) o di comunicazione (WhatsApp, Telegram, ecc.). Attenzione anche alle app che si intende scaricare sul proprio smartphone. E va posta molta attenzione su quali dati si pubblicano nelle cloud e nei social network: dovrebbero essere lasciati accessibili solo a una cerchia di persone affidabili.*

*** Deputato Alternativa Libera**