



— VARESE

Attacco hacker all'Ats

«Nessuno è al sicuro»

Il parere dell'esperto dopo che sono stati violati i circuiti informatici
Il rimedio è aggiornare i sistemi

Servizio a pagina 15

Ultimatum per il 2 giugno

dopo l'attacco hacker all'Ats

L'analisi dell'esperto: «Nessuno può essere al sicuro»

La digitalizzazione, un mercato dei dati in continua crescita e un momento storico in cui la guerra si combatte anche online.

Tre fattori che insieme stanno portando a quello che fino a ieri era un fenomeno noto solo agli esperti e che ora coinvolge tutti: la violazione dei sistemi di sicurezza per mandare in tilt siti pubblici e di aziende, ma anche per rubare i dati che custodiscono per chiedere un riscatto o rivenderli nel dark web. Quello che è accaduto ad Ats **Insubria**, con l'attacco hacker ai sistemi informatici e il furto di dati sensibili e identificabili, non è un episodio isolato. Sempre più spesso se ne sente parlare e nel mirino dei pirati della rete è finito anche il Ministero della Difesa. «Ogni giorno, in ogni momento ci sono tentativi di violazione dei sistemi e più i dati che proteggono sono appetibili, più frequenti e intensi saranno - spiega Sabrina Sicari, docente associata di Sistemi di elaborazione dell'informazione al corso di laurea in Informatica dell'Università dell'**Insubria** - allo stesso modo ci sono diversi livelli di sicurezza da adottare per proteggersi, ma deve essere chiara una cosa: non esiste un sistema di sicurezza che non possa essere violato».

Il rischio non è mai nullo, ma ci sono delle precauzioni che si possono e si devono prendere, soprattutto se si trattano dati sensibili e identificabili. «Per prima cosa è buona norma monitorare e aggiornare co-

stantemente i sistemi, perché più sono obsoleti più aumenta il loro livello di vulnerabilità. Dopodiché i dati sensibili e quelli identificabili andrebbero conservati in data base separati e criptati».

Nel caso di Ats, i pirati hanno invece avuto accesso ai dati completi. Lo si è constatato con la pubblicazione in rete dell'assaggio di quello che potrebbe accadere il 2 giugno, se non verrà corrisposto il riscatto richiesto. Sono nove le cartelle rese pubbli-

«Ogni giorno, in ogni momento, ci sono tentativi di violazione dei sistemi e più i dati che proteggono sono appetibili più frequenti e intensi saranno gli attacchi»

che, seppur nella parte sommersa della rete, con dati sensibili e identificabili di un migliaio di pazienti. Dati che possono avere un valore nel mercato nero del web e, come questi, praticamente tutti quelli che ogni giorno produciamo e mettiamo in rete, anche da soli.

«Noi oramai abbiamo una vita digitale e se non l'avessimo avuta, la pandemia ci avrebbe distrutto. Immettiamo una quantità di dati impressionanti anche attraverso l'utilizzo dei social, i dati umani, e poi c'è

Data: 27.05.2022 Pag.: 1,15
Size: 697 cm2 AVE: € 13243.00
Tiratura:
Diffusione: 28000
Lettori:



tutto il segmento dell'internet of thing e dei dispositivi interconnessi. Ci sono un sacco di dati ed il dato è valore, è business». Questo significa che dovremo pensare di installare un antivirus anche nei nostri telefonini cellulari. Se i dati valgono oro, ci saranno ladri che rapinano gioiellerie, ma anche quelli che si accontentano di una furto in appartamento. È questa la direzione in cui si sta andando? «La digitalizzazione avanza, ma si è creata anche una cultura e una preparazione. Una volta non ce lo si ponevamo nemmeno il problema della sicurezza. Oggi le misure sono diffuse e obbligatorie e si sviluppano già in

fase di progettazione dei sistemi. Ci sono anche sempre più persone che conoscono i sistemi digitali, ma quella contro gli hacker è una battaglia che si può fronteggiare».

Impossibile invece fermare i dati dopo la loro diffusione online. Se il 2 giugno, termine di scadenza del riscatto del gruppo BlackBite, i dati rubati ad Ats dovessero veramente essere pubblicati, sarebbe impossibile cancellarli. «Il diritto all'oblio deve essere garantito, ma se i dati sono rimasti in rete un tempo sufficiente per eseguire una copia è tutto più difficile».

Valentina Fumagalli

© RIPRODUZIONE RISERVATA

I PIRATI DELLA RETE



La violazione dei sistemi di sicurezza per mandare in tilt siti pubblici e di aziende si sta diffondendo a macchia d'olio creando danni incalcolabili ai singoli e alle imprese. Nel riquadro Sabrina Sicari

