Cybersicurezza

Cresce il pizzo 4.0 Criminalità sempre più online

di **Alessia Cruciani**

Lo smart working si è rivelato una grande opportunità. E gli italiani hanno gestito il cambio culturale in tempi rapidi. Eppure, quanta più gente lavora da remoto, tanti più varchi si aprono per i cybercriminali, perché dati e connessioni sono trasferiti nell'ambiente domestico, non protetto come quello aziendale. Non a caso è già stato registrato un picco negli attacchi informatici e una crescita di quello che è definito il "pizzo 4.0": gruppi di hacker si infilano nei computer di un'azienda e, minacciando la diffusione di dati o di bloccare l'attività, chiedono un riscatto. Un pagamento in bitcoin, non tracciabile.

Facendo seguito a una tendenza in continua crescita fin da giugno del 36% in Italia, il numero degli attacchi si è impennato nelle ultime settimane (+60% le richieste di consulenza cybersecurity). A farne le spese in particolare le aziende quotate in Borsa, quelle con un know how coperto da brevetto o con informazioni confidenziali. Approfittando delle tante notizie sul Covid-19, si inviano mail di phishing sul tema (si usano anche sms e WhatsApp) che inducono l'utente a cliccarci sopra. «In tal modo si attaccano le back door all'interno dei computer aziendali — spiega Mirko Gatto, ceo di Yarix, divisione Digital Security di Var Group, specializzato in soluzioni ICT per imprese — .Tra gli attaccanti ci sono gruppi meno preparati ma nella maggior parte dei casi si tratta di organizzazioni criminali strutturate, con notevoli capacità tecniche, e il vantaggio del fattore tempo. Un attacco può durare mesi prima che arrivi a conclusione: gli hacker entrano nella rete, catturano le password dei device aziendali e, appena pronti, "sparano per uccidere", paralizzano l'azienda».

Attenti alle email

Di solito l'estorsione digitale è comunicata con una mail o un avviso sul desktop del cliente che trova le istruzioni per prendere contatto con l'attaccante e l'entità del riscatto. In Italia le richieste variano in base alle dimensioni dell'azienda: dagli 80 mila euro ai 5 milioni. «Nei mesi scorsi siamo intervenuti dopo che era stata paralizzata l'infrastruttura informatica di Firenze Fiera, permettendo di rientrare in possesso del patrimonio di dati e di sottrarsi a una richiesta di riscatto pari a 4 milioni di euro in bitcoin», aggiunge il ceo di Yarix. Che puntualizza: «È fondamentale che siano esperti a intervenire nella "scena del crimine". Alcuni clienti erano riusciti a salvaguardare il back up e hanno ripristinato tutto. Ma gli hacker hanno attaccato ancora facendo perdere tutto. Ci sono pratiche da seguire altrimenti si rischia di peggiorare l'entità del danno». In genere, dopo 2-3 giorni dall'intervento si riesce a far ripartire le aziende. Alcune sono invece state costrette a pagare perché, se si perde tutto, non c'è possibilità di recupero.

La notifica al garante è d'obbligo in caso di perdita o fuoriuscita di dati, secondo quanto stabilito dal regolamento europeo sulla privacy , la Gdpr. Se invece i dati sono stati criptati e si possono recuperare tramite backup non è necessario comunicare l'attacco. Ma i criminali ormai minacciano di pubblicare i dati sul darkweb, per provocare così un importante danno d'immagine, la cui gravità è proporzionale all'importanza del brand.

«Per questo noi suggeriamo sempre di non tenere nascosto l'incidente, si evitano brutte figure con gli stakeholder», conclude Gatto. Ricordando l'importanza della prevenzione.

Doppio danno Sotto attacco ci sono spesso anche i back up degli utenti

Mirko Gatto, 44 anni, ceo di Yarix (Var Group)