Non aprite quella mail

Sicurezza – Gli attacchi informatici che sfruttano la posta elettronica si sono moltiplicati. Intervista a Mario Gay, responsabile del servizio informatico dell'USI

/ 24.02.2020
di Guido Grilli

S.O.S. La nostra posta elettronica rappresenta sempre meno un «porto sicuro» per le nostre corrispondenze private, pubbliche o commerciali nel caso di istituzioni o aziende. Siamo sotto costante attacco da e-mail indesiderate. Virus. Tentativi di truffe informatiche. Una visione apocalittica o realistica?

Lo chiediamo a Mario Gay, tra il 1995 e il 2018 preposto alla gestione del servizio informatico Ti-Edu, una cooperazione fra USI, SUPSI e Canton Ticino per fornire servizi di tecnologie dell'informazione e della comunicazione al settore dell'insegnamento accademico e della ricerca nella Svizzera italiana e oggi responsabile del servizio informatico dell'Università della Svizzera italiana.

«È esattamente così: la posta elettronica è un vettore di attacchi importantissimo per i criminali informatici, anche perché inizialmente non è stata progettata per essere sicura. È nata agli albori di Internet mettendo l'enfasi sulla funzionalità piuttosto che sulla sicurezza. Ancora oggi falsificare e spedire posta elettronica in grande quantità è facile e costa pochissimo. Quindi i malintenzionati possono permettersi di spedire milioni di messaggi con la fondata speranza che qualcuno abbocchi. Alcuni messaggi sono scritti male, altri, ultimamente, sorprendentemente ben congegnati. Addirittura mirati. In questi casi i criminali si sono presi il tempo per attuare quella che si chiama "ingegneria sociale": studiare le persone e le loro abitudini, verificare se un dirigente di un'azienda è lontano dal posto di lavoro, spedendogli dapprima un messaggio e ricevendone conferma con una risposta di assenza automatica, per poi "impersonarlo", cercando di far effettuare versamenti dai suoi collaboratori simulando un'urgenza».

Come ci si può dunque difendere da queste insidie? «Sia come privati che come collaboratori di un'azienda o di un'istituzione, tra le misure più efficaci ci sono paradossalmente le più banali. Facciamo un parallelo con il Coronavirus oggi al centro delle cronache: mentre le università e le farmaceutiche cercano con ogni mezzo a disposizione un vaccino e una cura, cosa possono fare nel frattempo i singoli individui per almeno mitigare il rischio? Lavarsi le mani. Le misure d'igiene informatica a livello individuale sono, come per la salute pubblica, molto efficaci in rapporto al loro costo. Il sito della Confederazione dedicato alla sicurezza informatica, www.melani.admin.ch, alla voce "come mi proteggo", riporta alcune misure semplicissime: la prima, usare password forti, vale a dire complesse e diverse per ogni servizio online utilizzato; e la seconda, impiegare un po' di sana prudenza quando si aprono le e-mail. È sorprendente quanti utenti non applichino queste avvertenze».

Come valuta oggi la situazione? «Le minacce informatiche – non è un mistero per nessuno – da diversi anni crescono costantemente. La sfida organizzativa, sia nel settore privato che in quello

pubblico, è quella di disporre di risorse che stiano al passo con l'aumento di questi pericoli. È chiaro che in momenti di ristrettezza finanziaria non è facile ottenere queste risorse. Noi, a livello di università, abbiamo il vantaggio di poterci appoggiare a Switch, la fondazione che gestisce la rete di comunicazione accademica svizzera e che possiede un reparto sicurezza molto solido e professionale, che offre consulenza e servizi».

Dalle spam al furto di password: può illustrare le insidie informatiche più comuni? «Se parliamo di posta elettronica, semplificando molto, in una prima fase lo spam è consistito essenzialmente in pubblicità commerciale indesiderata. Quella era tutto sommato un'"epoca felice", perché questi messaggi si limitavano a provocare uno spreco di risorse e un fastidio agli utenti. In seguito, invece, sono arrivati gli allegati con i virus – file .zip, .exe e altri ancora – file che se aperti con un clic danno avvio a una serie di operazioni malevole: da trasmettere a terzi i nostri dati fino a, per esempio, mettere a disposizione i nostri Pc come base ai criminali per successivi attacchi ad altre persone. Relativamente nuovi sono poi i cosiddetti *ransomware* (letteralmente, *ransom* è il riscatto): si tratta di attacchi che cifrano i dati sul nostro Pc o, ancora peggio, sui server aziendali rendendo tutti i documenti illeggibili a meno di disporre di una password che ovviamente viene fornita dai criminali solo a seguito del pagamento di un riscatto, magari versato su un conto anonimo in bitcoin. Negli Stati Uniti si sono verificati casi di aziende e perfino di enti pubblici che hanno visto pagare riscatti rilevanti, a volte senza oltretutto ottenere nulla in cambio. Ulteriore attacco veicolato dalle e-mail è il cosiddetto *phishing*: si tratta di messaggi coi quali i truffatori chiedono di fornire le nostre credenziali informatiche facendoci credere che la casella di posta elettronica è piena o che un versamento in banca ha un problema. Purtroppo sulle migliaia di persone toccate, qualcuno che ci casca c'è sempre. Anche in questo caso l'obiettivo dei criminali è di impersonare la vittima, per esempio per cercare di farsi versare denaro dai suoi conoscenti, fingendo di essere all'estero in gravi difficoltà».

Quanto è importante investire nei servizi informatici aziendali? «La criminalità informatica è diventata una vera propria industria che può contare su informatici molto preparati e agguerriti e che è arrivata ad avere una divisione del lavoro, per cui ci sono organizzazioni specializzate che producono strumenti tecnologici per attaccare i nostri computer; altre che li acquistano per sfruttarli e altre che rivendono infine quanto è stato ottenuto truffando le vittime. È importante quindi che le aziende, per restare al passo con le minacce, investano in strumenti e specialisti in sicurezza, specialisti che non è facile trovare in questo momento di carenza di personale informatico. Non bisogna però assolutamente tralasciare di investire anche nella formazione sulla sicurezza del proprio personale».