ALLARME HACKER
PIÙ CYBERATTACCHI ALLE SCUOLE COME DIFENDERSI IN TRE MOSSE

Salgono del 40% a quasi 5 mila ogni settimana le intrusioni nel sistema d'istruzione italiano, più della media mondiale «Fenomeno senza precedenti», dicono gli esperti. Si cercano i dati negli archivi delle segreterie. Le regole per evitare danni

di **UMBERTO TORELLI**

L'anno scolastico è iniziato con una novità: il divieto di usare il telefonino per gli alunni delle elementari e delle medie, voluto dal ministro dell'istruzione Giuseppe Valditara. Ma rimangono da risolvere i problemi della sicurezza informatica legati al mondo Internet, sia per le scuole e le università, sia per i professori, gli studenti e il personale di segreteria. A sorpresa, infatti, l'Italia figura tra i Paesi più colpiti dai cyberattacchi nel settore dell'istruzione. Lo indicano i dati di Check Point Research rilevati tra gennaio e luglio scorso.

Le nostre strutture scolastiche, dalle primarie all'università, sono posizionate al terzo posto nel mondo con una media di 4 mila 730 attacchi settimanali, in aumento del 53,2% rispetto alla media mondiale e del 40% dall'anno precedente.

I rischi

Il mondo dell'istruzione resta dunque nel mirino degli hacker che hanno individuato nuove vulnerabilità per sferrare gli attacchi. Si tratta di intrusioni di varia entità, anche gravi. Come il blitz avvenuto il 9 settembre all'Università di Genova, dove i cybercriminali hanno sottratto 18 gigabyte di informazioni. Trattandosi di un virus ransomware è stato chiesto un riscatto economico, di cui non è nota l'entità. Ma nel caso in cui non venga pagato, si fa concreto il rischio che i dati trafugati dai criminali del gruppo RansomHub siano resi pubblici e venduti sul dark web.

Il 9 settembre all'Università di Genova sono stati sottratti 18 gigabyte d'informazioni: è stato chiesto un riscatto economico

Secondo la ricerca è proprio il settore education a essere preso di mira dai pirati informatici, un comparto che registra nel mondo la media di 3 mila 86 attacchi settimanali: ben superiore ai 2 mila 54 dei comparti governativi e ai 1.936 del settore salute (vedi grafico). L'India si trova al primo posto in fatto di vulnerabilità via Internet del sistema scolastico, con 6 mila 874 attacchi settimanali (+97% in un anno). Il primo Paese per popolazione (1,4 miliardi di persone), che ha superato la Cina, conta in totale oltre 800 mila scuole. La maggior parte segue una didattica online, dunque un pubblico altamente vulnerabile.

Il caso tricolore

Per quanto riguarda l'Italia: «Il settore istruzione ha registrato un volume di attacchi senza precedenti quest'anno — spiega Cristiano Voschion, della sede milanese di Check Point —. Scuole e università sono in prima linea nell'agenda dei pirati informatici». Parte dell'interesse da parte degli hacker deriva dall'enorme quantità di dati, anche sensibili, conservati negli archivi digitali delle segreterie scolastiche.

Oltre a professori e personale amministrativo, sono gli studenti ad avere accesso alle reti senza i vincoli dei rigidi processi di autenticazione. A scuola i dispositivi digitali, operando in spazi condivisi tramite wifi pubblici e hotspot, hanno scarse protezioni di sicurezza.

«Ebbene — continua Voschion — questa combinazione di eventi genera la tempesta perfetta sfruttata dai cybercriminali per sferrare attacchi online». Allora che cosa fare per difendersi e almeno limitare i danni? Tre le regole di base.

I comportamenti

Per quanto riguarda le strutture, la prima regola riguarda l'aggiornamento di sistemi operativi, dei software e antivirus installati. Ogni scuola ha un responsabile delle strutture informatiche: a lui spetta il compito di adeguare le applicazioni, i programmi e i dispositivi obsoleti.

Spiegano gli esperti di Check Point: «È importante che vengano separate le zone di memoria riservate alle operazioni degli uffici, da quelle usate da professori e studenti per le attività didattiche». Dunque, hard disk interni e aree di memoria sul cloud devono prevedere differenti password di accesso.

Bisogna poi informare gli utenti sulle azioni da compiere e quelle da evitare, per minimizzare i rischi. Attenzione agli attacchi phishing, dove con la pubblicità ingannevole e le false identità vengono catturati i dati personali. A risultare pericolosi sono i link, collegati spesso a fake news. Resta valida la regola di non aprirli, così come non vanno scaricati programmi e dati da siti sconosciuti.

Con il phishing gli studenti e gli insegnanti, anche in modo involontario, diventano veicoli di propagazione dei virus sulle reti interne.

Il terzo e ultimo consiglio degli esperti riguarda la ricerca di informazioni online. Per quanto possibile, è bene evitare i siti web non criptati, assicurandosi che quelli a cui si accede siano provvisti dei cosiddetti certificati Ssl (Secure sockets layer).

Consentono la connessione criptata e sicura tra server e browser, garantendo la sicurezza dei dati trasmessi verso gli utenti. Ad esempio informazioni sensibili come password e carte di credito.

Per capire quando un sito risulta criptato, basta osservare l'inizio dell'indirizzo. Deve comparire una «s» dopo le lettere http. Quindi se leggete https:// renderete più difficile la vita ai pirati informatici.

4.730
Violazioni
I cyberattacchi ogni settimana nel sistema d'istruzione italiano (primi sette mesi 2024)

@utorelli