VareseNews

Consigli pratici per neutralizzare gli attacchi hacker: webinar gratuito di Reti

Pubblicato: Martedì 30 Novembre 2021

Reti, tra i principali player italiani nel settore dell'IT Consulting, specializzata nei servizi di System Integration, B Corp e società benefit quotata su Euronext Growth Milan, **organizza per il 1° dicembre, dalle ore 18:00, il webinar online gratuito "Security Awareness: consigli pratici per neutralizzare gli attacchi hacker"** in collaborazione con **ENAIP Lombardia,** l'ente regionale che dal 1951 si occupa di formazione.

Secondo il Rapporto Clusit 2021, nell'ultimo anno **l'incremento degli attacchi cyber a livello globale è stato pari al 12%** e la **cifra dei danni generati dal solo cybercrimine è stata calcolata in 945 miliardi di dollari.** Inoltre, nello stesso anno **la spesa globale in ICT security è stata di 145 miliardi di dollari** (di cui 1,5 miliardi in Italia).

Gli investimenti in tecnologie però non bastano, è fondamentale acquisire una buona conoscenza per tutelarsi e garantire la sicurezza dei dati. La maggior parte delle violazioni informatiche, infatti, sono causate dal comportamento umano inconsapevole ed è proprio per questo che la formazione e l'informazione su questi temi sono un elemento necessario e imprescindibile per affrontare la quotidianità, soprattutto nell'epoca dove lo smart working è predominante.

Bruno Paneghini, Presidente e Amministratore Delegato di Reti commenta: "Essere informati sul tema della cybersecurity è essenziale perché è un ambito che riguarda non soltanto la sfera professionale

e aziendale ma anche pubblica e sociale. Ogni giorno, infatti, assistiamo a innumerevoli casi di attacchi informatici che testimoniano come questo fenomeno stia raggiungendo dimensioni sempre più impattanti a livello economico. È, dunque, fondamentale investire sia in tecnologie e software avanzati ma anche in formazione, perché in questa battaglia le persone possono fare la differenza".

Durante il webinar, **Nicola Losco, esperto di Cybersecurity in Reti,** introdurrà i temi della sicurezza informatica, per capire in termini pratici come proteggersi dalle frodi informatiche ed evitare le relative conseguenze. Inoltre, saranno messe in evidenza le otto regole per farsi trovare pronti e difendersi dagli attacchi hacker.

La prima regola è tenere aggiornati i sistemi, in particolare tutte quelle categorie di software che a vario titolo sono connesse con l'apparato normativo (ad esempio, i sistemi di gestione paghe, i sistemi per la presentazione di documenti per le gare d'appalto, ecc.) o **i software di progettazione, ecc.**. In tutti questi casi un mancato o tardivo aggiornamento del software può generare anomalie molto al di là delle inefficienze.

La seconda è utilizzare un antivirus o un EDR (Endpoint Detection and Response) **e tenerlo aggiornato.** Nello specifico, l'Endpoint Detection and Response raggruppa gli strumenti avanzati che hanno il compito di rilevare minacce ed eseguire attività di indagine e risposta, inoltre ricoprono un ruolo fondamentale nella protezione dei dispositivi utilizzati dai dipendenti o dai collaboratori.

La terza regola è usare password diversificate e cambiarle spesso, oltre ad utilizzare sempre e se possibile, l'autenticazione a due fattori (username e password/PIN, oltre all'utilizzo di un token/chiavetta o lo smartphone). Inoltre, è indispensabile usare strumenti per riuscire a ricordare le tante e differenti password da gestire. Si stima, infatti, che oggi un utente medio abbia circa un centinaio di password. A tal proposito, sono di grande aiuto i password manager, applicazioni dedicate a conservare tutte le proprie password in modo sicuro e crittografato.

La quarta regola consiste nell'effettuare una valutazione delle vulnerabilità, un esame sistematico delle debolezze di sicurezza in un sistema informativo, per tenere sotto controllo la propria infrastruttura e poter sanare eventuali vulnerabilità.

La quinta è quella di esporre al pubblico solo i sistemi necessari e filtrare correttamente gli accessi a tutto il resto. Il nodo del collegamento ai server aziendali è essenziale per la sicurezza dei dati e bisogna prevedere un sistema semplice da usare, ma completamente sotto il controllo del reparto IT aziendale (o del partner che fornisce il servizio).

La sesta regola è fare particolare attenzione agli attacchi veicolati tramite mail (ad esempio il phishing), **oltre a fare attenzione a cliccare sui link sospetti** e all'inserimento dei propri dati personali su siti non sicuri. La corretta gestione delle identità e degli accessi è prioritaria. La grande maggioranza degli attacchi informatici, infatti, oggi avviene attraverso un presunto accesso autorizzato. La mancanza di opportuni strumenti di gestione e di policy che definiscano puntualmente cosa può fare e fin dove si può spingere un dipendente all'interno della rete aziendale sono il primo, grande, aiuto che si può dare a chi vuole rubare informazioni.

La settima è quella di effettuare sempre backup dei server, soprattutto quelli critici per il core business. La perdita dei dati locali è probabilmente il secondo problema più noto, dopo i guasti hardware. È quindi fortemente consigliabile ricorrere a un'ulteriore struttura di backup per quella parte di documenti la cui perdita avrebbe un impatto estremo sulla vita dell'azienda.

L'ottava ed ultima regola è quella di non connettersi a wi-fi pubbliche. È consigliabile predisporre, infatti, un punto d'accesso sicuro alla propria rete tramite una VPN o virtual private network. Una VPN permette di estendere la rete aziendale su Internet, consentendo l'accesso solo a dispositivi opportunamente verificati con un "tunnel" che attraversi tutti i nodi di Internet necessari alla

comunicazione. In questo modo il portatile di un dipendente può “entrare in rete” e collegarsi al dominio come se fosse in ufficio, fisicamente allacciato alla rete cablata dell’azienda o connesso tramite Wi-Fi.

Link per iscriversi all’evento gratuito:
https://www.eventbrite.it/e/biglietti-webinar-security-awareness-come-neutralizzare-gli-attacchi-hacker-199769525027

Redazione VareseNews
redazione@varesenews.it