CYBER SECURITY

Ogni 39 secondi avviene un attacco hacker: quanto è vulnerabile il tuo sistema IT?[1]

18 MARCH 2021

Una conseguenza dei progressi a livello di digitalizzazione e connettività è che offrono ai criminali informatici nuove strade e opportunità di attacco dei sistemi IT. E poiché, per via del Covid-19, sempre più persone lavorano da casa o da remoto, i criminali informatici hanno un campo d'azione più ampio. In effetti, le segnalazioni di crimini informatici ricevute dall'Internet Crime Complaint Center (IC3) dell'FBI sono aumentate di tre volte dall'inizio della pandemia.[2] Si stima che il costo della criminalità informatica globale per l'anno 2021 possa ammontare a 6 trilioni di dollari.

Allo stesso tempo, è stato registrato un aumento degli attacchi informatici contro le interfacce di programmazione delle applicazioni (API), con conseguente adozione di ulteriori misure di sicurezza.[3] Secondo quanto emerso da un recente sondaggio tra i principali esperti di sicurezza informatica, il 91% afferma che la sicurezza delle API diventerà la loro priorità nei prossimi due anni.[4] Tuttavia, trovare un approccio olistico alla sicurezza informatica continua a essere una missione complessa.

Quindi, come proteggersi al meglio? Ecco alcune misure che è possibile adottare come primo passo per assicurarsi che la propria organizzazione sia protetta.

Condurre un controllo della sicurezza IT

Un buon punto di partenza è intraprendere un controllo completo della sicurezza dell'organizzazione e dei sistemi IT. In questo modo sarà più facile identificare eventuali vulnerabilità e debolezze. Ricorda che tutte le interfacce digitali sono potenziali punti di ingresso per i criminali informatici: e-mail, siti Web, app, cloud storage, dispositivi connessi, e così via.

Non dare per scontato che qualcun altro si stia già occupando della sicurezza informatica

Un problema comune, soprattutto nelle organizzazioni più grandi, è che di solito si presume che la sicurezza informatica sia una responsabilità di altri. Si immagina che qualcuno abbia il controllo della situazione, quando in realtà l'incarico, nei vari dipartimenti, è stato trascurato. La sicurezza informatica deve essere considerata come una funzione separata e al contempo come una parte essenziale di tutti i processi aziendali.

Assicurarsi che tutte le applicazioni siano protette

Sapevi che il 76% delle applicazioni mobili archivia i dati in modo non sicuro e quindi è vulnerabile agli attacchi informatici?[5] Di conseguenza, le informazioni sensibili sono esposte ai rischi e l'89% di queste vulnerabilità può essere sfruttato senza che sia necessario un vero e proprio accesso fisico.

Non ritenersi mai soddisfatti

I criminali informatici esplorano e cercano continuamente eventuali vulnerabilità informatiche ed escogitano nuovi metodi per entrare illegalmente nei sistemi di aziende e organizzazioni. Non devi mai abbassare la guardia. Assicurati sempre che la protezione del software sia aggiornata, che tutte le nuove interfacce digitali siano sicure e di essere sempre al passo con tutte le tendenze e le minacce emergenti.

Nel complesso, occorrono più livelli di protezione per creare un sistema sicuro per tutti i computer, i dispositivi connessi, le reti e i programmi software. Ma l'efficienza di un sistema di sicurezza informatica non dipende esclusivamente dalla tecnologia e dai sistemi; occorre anche confidare nel fatto che il personale dell'organizzazione sia al corrente dei rischi e prenda decisioni intelligenti per quanto riguarda la difesa dagli attacchi informatici.[6]

La buona notizia?

Non è necessario essere un esperto di sicurezza informatica per comprendere e mettere in pratica delle valide tattiche di difesa dagli attacchi. Se hai bisogno di assistenza per aggiornare i tuoi sistemi IT, contatta gli esperti Modis.

Vuoi saperne di più? Vai su *modis.com*

1 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
2 https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
3 https://www.zdnet.com/article/api-security-becomes-a-top-priority-for-enterprise-players/?&web_view=true
4 https://www.imvision.ai/2021-api-security-survey/
5 https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/
6 https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html