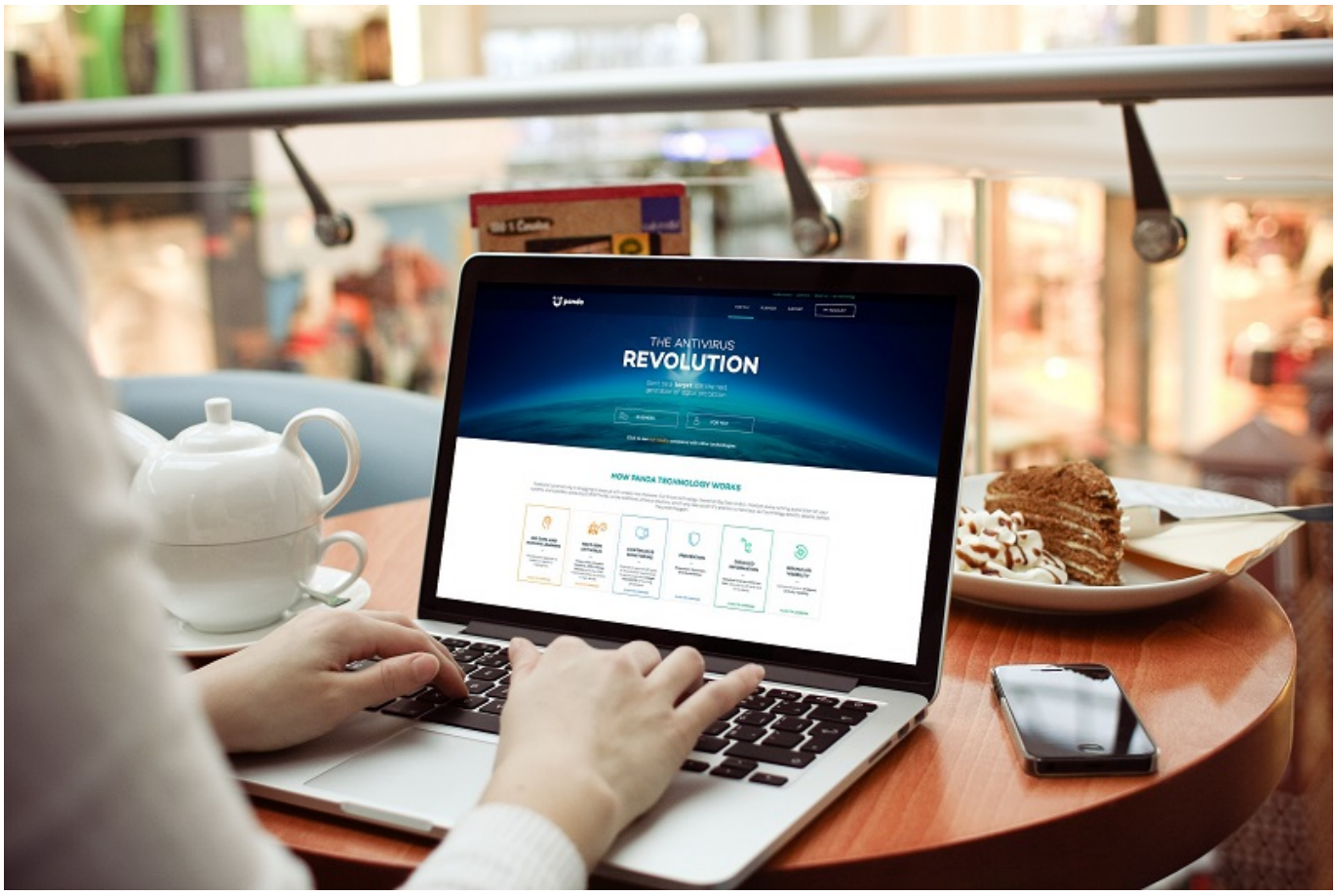
Cybersecurity: le previsioni per il 2021 di Panda Security e WatchGuard

- Ultima modifica: Sabato, 09 Gennaio 2021 18:47
Pubblicato: Domenica, 10 Gennaio 2021 07:21
Scritto da Palma Cristallo

Dopo un 2020 da dimenticare, anche sotto il profilo della sicurezza informatica, Panda Security e WatchGuard stimano che - nel 2021 - i rischi degli utenti online si moltiplicheranno per le vulnerabilità presenti nelle lacunose connessioni tra persone, dispositivi e reti aziendali.

Il 2020 è stato certamente un anno molto particolare nell'ambito della **sicurezza informatica**, con la pandemia che anche in questo campo ha lasciato il segno, caratterizzando una grande mole di attacchi informatici. Il Clusit ha evidenziato recentemente come la tematica Covid-19 sia stata infatti utilizzata per perpetrare **durante il primo lockdown 119 attacchi gravi**, pari al 14% di quelli complessivamente noti.

In particolare, è stato sfruttato - nel 72% dei casi - il momento per pratiche di cybercrime finalizzate all'estorsione di denaro, mentre gli scopi di "Espionage" e di "Information Warfare" hanno riguardato il 28% degli eventi. Gli attacchi a tema Covid-19 sono stati condotti nel 61% dei casi con campagne di "Phishing" e "Social Engineering", anche in associazione a "Malware" (21%), colpendo tipicamente i cosiddetti "bersagli multipli" (64% dei casi). Il 12% degli attacchi a tema Covid-19 ha avuto come obiettivo il settore Governativo, Militare e l'Intelligence: sono stati in questo caso prevalentemente attacchi di natura "Espionage".



A livello complessivo, gli attacchi verso le Infrastrutture Critiche sono aumentati dell'85% rispetto allo stesso periodo del 2019. Quelli che hanno avuto come obiettivo il settore della Ricerca e delle Istituzioni scolastiche sono cresciuti del 63%. Inoltre, il rapporto Clusit cyber sottolinea come manchino nel settore della cybersicurezza **investimenti in ricerca ed innovazione**, essenziali per arginare il fenomeno del cybercrime, che è in continua evoluzione.

Infatti, nel 2021, **Panda Security e WatchGuard** prevedono che, con il proseguo della pandemia e dello smart working, **gli utenti correranno rischi maggiori**, date le vulnerabilità presenti nelle lacunose connessioni tra persone, dispositivi e reti aziendali. Al fine di prendere precauzioni per mettere in sicurezza la propria attività online, Panda e Watchguard hanno recentemente pubblicato una serie di previsioni che riguardano le principali vulnerabilità:

L'automazione porterà ad una crescita delle campagne di spear phishing
Nel 2021 i cybercriminali sfrutteranno i nuovi strumenti di automazione per semplificare gli aspetti manuali della creazione delle campagne di spear phishing (attacchi mirati a singole persone) ed estrarre dati precisi e specifici delle vittime dalle reti dei social media e dalle pagine web aziendali. Questo comporterà un aumento notevole del volume di e-mail di spear phishing dettagliate ed altamente credibili con contenuti personalizzati per ogni vittima. La speranza è che siano meno sofisticate e più facili da individuare rispetto a quelle tradizionali generate manualmente. È facile ipotizzare come molti di questi attacchi faranno leva sui timori relativi alla pandemia da Covid-19.

I provider dei cloud hosting contrasteranno gli abusi informatici tramite i loro servizi
Nel 2021, si prevede che i provider di Cloud-hosting inizieranno a combattere il phishing e altre truffe implementando strumenti automatizzati e di analisi dei file capaci di individuare siti di autenticazione fasulli. La maggior parte dei servizi di Cloud-hosting offre un'archiviazione dei dati che consentono agli utenti di caricare qualunque genere di file. Questi servizi sono esposti alla rete attraverso sottodomini o percorsi URL personalizzati. Gli hackers abusano comunemente di queste caratteristiche per ospitare file HTML di siti web progettati per imitare la forma di autenticazione di un sito legittimo come Microsoft365 o Google Drive e rubare le credenziali inviate da vittime ignare.

Gli hacker infesteranno le reti domestiche con i Worms
Il lavoro da remoto, che proseguirà in maniera massiccia nei prossimi mesi, ha spinto i cybercriminali a cambiare il loro approccio e a creare attacchi specifici verso il lavoratore a domicilio. I cybercriminali spesso includono moduli di funzionalità worm nei malware, progettati per spostarsi verso altri dispositivi connessi alla rete. Rappresentando delle vie di accesso privilegiate a preziosi dispositivi aziendali, è facile prevedere come nel 2021 le reti domestiche subiranno un incremento degli attacchi malware.

I caricabatterie smart potranno portare i cybercriminali ad hackerare le auto intelligenti

Nel 2021 anche le smart car, finora poco attaccate, possano diventare preda dei cybercriminali grazie ai caricabatterie intelligenti. I cavi di ricarica delle smart car trasportano più di semplice energia, infatti hanno una componente dati che li aiuta a gestire la sicurezza della ricarica. Panda e WatchGuard prevedono che potrebbero essere trovate vulnerabilità nei componenti di ricarica delle smart car, sfruttabili per impedire l'accensione o l'uso dell'auto o la sua ricarica, magari finché non è stato pagato il "riscatto" chiesto dall'hacker.

Rischio di attacchi a sciame su VPN e RDP con lo smart working
Il lavoro da casa è diventato una norma per molte aziende ed ha cambiato il profilo dei software e dei servizi su cui si basa un'azienda media. Mentre in precedenza molte aziende utilizzavano meno sia le soluzioni Remote Desktop Protocol (RDP) che Virtual Private Networking (VPN), questi servizi sono diventati fondamentali per consentire ai dipendenti di accedere ai dati e ai servizi aziendali al di fuori del tradizionale perimetro di rete. Nel 2021, è possibile prevedere che gli aggressori aumentino significativamente gli assalti a RDP, VPN ed altri servizi di accesso remoto.

Lacune di sicurezza negli endpoint
Gli endpoint costituiscono un obiettivo altamente prioritario dato il maggior numero di dipendenti che lavorano da casa, senza alcune delle protezioni basate sulla rete lavorativa: gli aggressori si concentreranno sulle vulnerabilità dei pc, del software e dei sistemi operativi obsoleti. Windows 7 (e per relazione, Server 2008) era una delle versioni più popolari di Windows prima del 10. Dato che la versione 8 era ritenuta non efficiente, molte aziende hanno scelto di rimanere con Windows 7, non aggiornandosi così ad una versione più recente. Nel 2021, i cyber criminali potrebbero sfruttare falle nella sicurezza di Windows 7 per attaccare gli endpoint.

Ogni servizio senza MFA subirà una violazione
I cybercriminali hanno un notevole successo tramite gli attacchi volti a rubare i dati di autenticazione, sia perché spesso non si dispone delle protezioni adeguate, sia perché gli utenti utilizzano le stesse credenziali per più servizi. Basta guardare quanti database di password ci sono nel darkweb per capire la facile reperibilità dei dati di accesso.

Queste banche dati, abbinate alla facilità di automatizzare attacchi di autenticazione, rappresentano la vulnerabilità principale di qualunque servizio esposto a Internet, tranne i servizi che utilizzano l'autenticazione multifattoriale (MFA). È prevedibile che nel 2021 ogni servizio che non ha abilitato l'MFA subirà una violazione o una compromissione dell'account.

Le previsioni sulle vulnerabilità appena descritte possono **mettere in guardia privati ed aziende** sulle proprie difese così da limitare l'efficacia di eventuali attacchi subiti. Purtroppo, con il prorogarsi della pandemia, **le possibilità di attacco dei cybercriminali si sono moltiplicate**, basti pensare che questi nuove minacce potrebbero prendere di mira anche i membri della famiglia del dipendente stesso, infiltrandosi nella rete domestica. Per questo

anche i dispositivi solitamente collegati alla rete domestica debbono essere protetti, così da evitare attacchi di questo genere. Il resoconto completo è disponibile qui.