21/12/2020

internet4things.it

Argomento: Exprivia: si parla di noi

EAV: € 529
Utenti unici: 700

https://www.internet4things.it/sicurezza-iot/dispositivi-connessi-in-rete-e-cybersecurity-i-videogame-possono-essere-un-punto-debole/

Dispositivi connessi in rete e cybersecurity: i videogame possono essere un punto debole

Videogame e cybersecurity: se si sta utilizzando un computer o un dispositivo per entertainment, bisogna assicurarsi che lo stesso abbia tutti i controlli attivati, che il DNS sia opportunamente configurato, che la rete sia opportunamente protetta Uno degli effetti più evidenti della pandemia è che si passa più tempo a casa. A rendere più tollerabile il lockdown ci pensano, oltre che TV e Internet, anche tutte le soluzioni di intrattenimento, a partire dai videogame. Lavorare da remoto non ci rende tanto distanti dal mondo simulato e utilizzare in maniera intensiva il mondo simulato vivendo nel mondo reale aumenta sensibilmente la superficie di un possibile attacco che sfrutti le adiacenze tra i due mondi. Infatti, a meno che non si lavori con reti dedicate, si utilizzeranno gli stessi router per “giocare”, certo attraverso VPN, ma sempre con un dispositivo connesso in locale al router casalingo. D’altra parte, i sistemi e i protocolli utilizzati su entrambi i sistemi sono molto simili, da Unix-like ad Android-like, per finire a Windows. Emerge allora il problema della cybersecurity legata ai videogame, allo smart working e ai dispositivi connessi alla rete.Indice degli argomenti I numeri dei videogame in reteCybersecurity e videogamePirateriaPrivacyVulnerabilità dei sistemiConclusioniI numeri dei videogame in rete Il fenomeno dell’entertainment non è irrilevante dal punto di vista numerico. A novembre 2020 l’Osservatorio Exprivia sulla Cybersecurity ha rilevato un incremento del numero di dispositivi connessi- classificabili come entertainment – da 18.357 a 23.097. Cioè, man mano che le misure nei vari DPCM diventavano più restrittive, il numero di dispositivi dedicati all’entertainment collegati su internet aumentava. Sono numeri validi solo a comprendere il trend, non per fare delle valutazioni di carattere statistico; infatti, i dati sono stati calcolati osservando la porta 9295 spesso usata da applicazioni per

l’entertainment, fermo restando che questa porta potrebbe essere usata anche da altre applicazioni. Inoltre, le applicazioni per l’entertainment spesso usano Ip e porte classiche e solo un‘analisi del traffico tunnellizzato potrebbe identificare con esattezza il numero di dispositivi collegati e quelli reali. I numeri rilevati non sono però trascurabili se si pensa che una comune connessione a banda larga residenziale è capace di creare un traffico a 20 Mbps. In questo caso una botnet di appena 100 nodi sarebbe sufficiente per produrre un attacco DDoS di 2 GBpS.Cybersecurity e videogame Dividiamo in tre macro-aree le minacce da cui bisogna proteggersi: pirateria, privacy e vulnerabilità dei sistemi.Pirateria Oltre a frodare il fisco e il fornitore, chi usa materiale non originale usa versioni del prodotto che potrebbero essere volontariamente rese vulnerabili. Pertanto si può anche avere l’illusione di utilizzare il software legittimo, ma in realtà apriamo le porte al mondo del cybercrime scaricando malware, installando sessioni di command & control, botnet che possono essere utilizzate per movimenti laterali nella network casalinga o rendere l’abitazione inconsapevolmente partecipe a crimini perpetrati a danni di terzi.Privacy Il mondo dell’entertainment necessita la creazione di profili in cui inserire dati personali che vanno opportunamente protetti; profili che spesso consentono l’accesso alla piattaforma remotamente. Molti vendor, infatti, suggeriscono l’attivazione di meccanismi di strong authentication. WHITEPAPER Quali sono stati i casi di cybercrime più aggressivi degli ultimi anni? Scoprilo nel white paper Cybersecurity Scopri come Scarica il WhitepaperCosa fare: usare i meccanismi di strong authentication qualora fossero a disposizione, ma ricordarsi di applicare concetti di cybersecurity elementari quando si gioca con i videogame.Vulnerabilità dei sistemi I giochi sono applicazioni che necessitano di sistemi operativi, hanno meccanismi di autenticazione, si collegano alla rete e sono quindi sistemi complessi, con vulnerabilità che, se ben sfruttate, possono facilitare attacchi di vario tipo. Tra le debolezze più sfruttate dagli attaccanti, la ‘privilege escalation’: si fornisce all’utilizzatore la possibilità di usufruire dell’applicazione con autorizzazioni diverse da quelle legittimamente ottenute dal fornitore. Questa ‘scalata’, oltre a causare un danno economico a chi fornisce il servizio, potrebbe essere utilizzata anche per arrecare danni al profilo o all’applicazione favorendo movimenti laterali o diversi tipi di attacco (non solo permettere all’attaccante l’accesso a funzionalità avanzate dell’applicazione). Fino al ‘Kernel takeover’, che si manifesta quando l’attaccante integra nel sistema operativo una componente non necessaria al gioco, ma funzionale al tipo di attacco che si vuole perpetrare.Conclusioni In conclusione, quello che per molti è un gioco, per chi

attacca è un mestiere. Se si sta utilizzando un computer o un dispositivo per entertainment, bisogna assicurarsi che lo stesso abbia tutti i controlli attivati, che il DNS sia opportunamente configurato, che la rete sia opportunamente protetta. Insomma, anche se la natura ludica del gioco potrebbe indurre a non adottare tutte le necessarie precauzioni, non dobbiamo mai dimenticare che il gioco è un servizio erogato tramite sofisticatissime tecniche di comunicazione e programmazioni, e quindi sensibili a un potenziale attacco. I giochi pertanto appartengono alla categoria di dispositivi la cui sicurezza ha un valore intrinseco, un valore che va oltre quello del servizio erogato.