Tecnologia - *Yarix: ecco i 5 dispositivi di uso quotidiano hackerabili*

Roma - 28 dic 2023 (Prima Notizia 24) **Dalle stazioni di ricarica pubbliche alle auto iperconnesse.**

La tecnologia sta semplificando la nostra quotidianità: serrature smart, menu consultabili direttamente dal cellulare, frigo e lavatrici intelligenti, ma quanto sono sicuri questi dispositivi per la nostra privacy? Nella corsa alla digitalizzazione della quotidianità, la parola d'ordine è semplificazione. Ma la digitalizzazione è un cambiamento che sappiamo governare? Quanto incide il livello di sicurezza? Quali sono i dispositivi hackerabili o le occasioni che ci mettono a rischio hackeraggio? Yarix - divisione Digital Security di Var Group che da oltre 20 anni fornisce servizi e soluzioni di cyber security a industrie, enti governativi e militari - ha stilato una short list di alcune tipologie di tecnologie e di situazioni con le quali ci confrontiamo quotidianamente, a cui è necessario prestare attenzione: Stazioni di ricarica pubbliche Sono sempre più presenti stazioni pubbliche di ricarica per i dispositivi mobili, tipicamente sotto forma di comode e gratuite prese USB, esempio lampante quelle disponibili negli aeroporti, che permettono di sfruttare l'attesa non consumando la batteria del proprio dispositivo. Le porte USB però, oltre alla possibilità di caricare i dispositivi, consentono anche di scambiare dati con i dispositivi collegati. Come fare allora per essere (relativamente) tranquilli che utilizzandole non stiamo anche consentendo a "qualcuno" di compromettere il nostro dispositivo? Il team di cyber esperti consiglia dunque di fare attenzione alle notifiche che il dispositivo presenti al collegamento alla presa USB, non accettando l'accesso ai propri dati, ma solo la carica dello stesso. Può essere utile in mobilità utilizzare un USB data blocker, dispositivo che si interpone e consente di ricaricare in sicurezza da qualsiasi porta di ricarica USB senza alcun rischio di trasferimento dei dati dallo smartphone. Basta semplicemente collegare la presa USB a un'estremità e l'altra al cavo di ricarica. Menù in QR Code Pratici, funzionali, ecologici e igienici, i menù visualizzabili attraverso QR Code fanno parte del percorso di digitalizzazione che ha investito la ristorazione dal periodo post pandemico in poi Nonostante gli innumerevoli benefici, è bene fare attenzione: attraverso QR Code lasciati ad esempio sui tavolini del bar all'aperto, i malintenzionati potrebbero diffondere malware o far collegare gli utenti a siti di phishing in grado di rubare le credenziali, semplicemente lasciando che l'utente li apra inconsapevolmente E allora come arginare il rischio? Basterà assicurarsi che quanto troviamo sul tavolo sia materiale ufficiale dell'esercizio commerciale! Gli altoparlanti smart Alexa, Google home e chi più ne ha più ne metta. Ormai sono gli assistenti domestici di cui non riusciamo a fare a meno. Previsioni meteo, timer per la pasta, musica, sveglia mattutina, supporto nell'accensione luci e così via, gli assistenti smart ci accompagnano nella nostra quotidianità. Ma quanto sono sicuri da un punto di vista informatico? Gli altoparlanti smart sono sicuramente un aggregatore di informazioni personali e un punto di accesso all'intimità della nostra casa. Sebbene in passato ci siano state delle segnalazioni riguardo a vulnerabilità, le imprese

produttrici sono particolarmente sensibili ai temi della privacy e della sicurezza informatica e costantemente impegnate nell'arginare i tentativi di hacking. Senza contare la stretta sulla privacy richieste dall'Europa e la valutazione d'impatto della protezione dei dati (DPIA) prescritta dal GDPR. Elettrodomestici smart Alcune tipologie di dispositivi smart, come lavatrici, tv, frigo e altri elettrodomestici smart nelle prime fasi di lancio presentavano delle vulnerabilità che furono di fatto sfruttate dai cybercriminali: non per accedere all'interno delle abitazioni ma per lanciare attacchi DDoS verso obiettivi esterni. I dispositivi elettronici intelligenti, se presentano vulnerabilità o configurazioni insicure, possono essere vittime di attacchi da parte di malintenzionati esterni, ad esempio botnet, reti che mirano a mettere fuori gioco temporaneamente servizi di imprese lanciando attacchi su larga scala e sovraccaricandone i siti target (attacchi DDoS). In questo caso viene sfruttata la potenza di una rete estesa di dispositivi IoT: un singolo frigorifero ha capacità limitate di attacco, ma una rete fatta da più "thingbot" può invece costituire una problematica reale. Auto iper-connesse L'arrivo dei computer di bordo e poi delle chiavi elettroniche, ha gettato qualche perplessità sulla sicurezza informatica dell'auto che guidiamo. Sebbene le case automobilistiche si siano ingegnate per tempo per evitare che i nostri mezzi di trasporto diventassero oggetto di attività di hacking, e dunque in qualche modo pericolose per la nostra sicurezza non solo fisica, ma anche tecnologica, i criminali informatici hanno a loro disposizione ulteriori punti di accesso. Il rischio riguarda soprattutto le app di terze parti, che offrono più funzionalità rispetto a quelle ufficiali, ma con procedure di gestione di sicurezza lungo il ciclo di vita che probabilmente non possono competere con quelle di una casa automobilistica. Per funzionare, alcune di queste richiedono l'accesso completo all'app del produttore: se sono presenti bug, possono fungere da vettori involontari di minacce e consentire a terzi l'accesso a sistemi di bordo. Collezionano dati di parcheggio, consumi, tragitti, "spiando" il guidatore. E, nelle situazioni più critiche, potrebbero sfruttare delle falle per dare vita ad azioni non autorizzate.

(Prima Notizia 24) Giovedì 28 Dicembre 2023