UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 9 Giugno 2023

Attacchi informatici: le misure di difesa dell'Ateneo nell'ultimo mese

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo.

Ad oggi non ci sono state perdite di dati grazie alle misure di protezione adottate che hanno ben anticipato le intenzioni malevole e messo al sicuro il lavoro interno svolto.

La sicurezza collettiva dipende molto anche dalla responsabilità del singolo nell'utilizzare i propri dispositivi, tenerli aggiornati e relazionarsi con l'Area Sistemi Informativi qualora non si senta adeguatamente protetto.

I numeri sotto riportati evidenziano infatti ancora margini di miglioramento nel comportamento di ciascuno di noi oltre alla necessità di un costante lavoro interno ad ogni struttura al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 11 pc infetti che sono stati segnalati e bonificati e circa 151 comunicazioni C&C rilevate e bloccate oltre a 2 minacce Zero-Days bloccate.

Queste tipologie di attacchi rappresentano uno dei primi fenomeni da monitorare poiché potrebbero nascondere malware, cryptolocker o altri fenomeni malevoli che approfondiremo nei successivi numeri di questa newsletter.

In questo numero della newsletter relativa alla cybersecurity tratteremo della protezione degli impianti domotici in casa e in ufficio.

Malware and Attacks

11
Computers Infected with Bots

151
Communications with C&C* Sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

4 Known Malware Downloaded by

10 Users

2 Zero-Days Downloaded

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

123
Unique Software Vulnerabilities were Attempted to be Exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

6
High Risk Web Applications

19.4MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0
High Risk Web Sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

SaaS Applications

0
SAAS Applications Seen

1
Users Using SAAS Application

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines.

Data Loss

0
potential data loss incidents

0
sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

La cyber security e la domotica

Introduzione

Internet of things (IoT) & smart device sono sempre più numerosi nella nostra quotidianità. Le nostre abitazioni sono sempre più gestite da home assistant, elettrodomestici intelligenti, smart tv, smartphone e dispositivi vari, tutti collegati al wi-fi e strumentazioni di domotica che si basano sull'Intelligenza artificiale e machine learning. Vere e proprie strutture Smart che abbondano di dispositivi connessi che, se non adeguatamente protetti, possono essere oggetto di attacchi hacker e violazione della privacy.

Secondo quanto si evince della ricerca dell'Osservatorio Internet of Things della School of Management del Politecnico di Milano, presentata a febbraio scorso durante il convegno online "Stay at home, stay in a Smart Home: la casa intelligente alla prova del Covid" il mercato degli home smart device nel 2020 ammontava a euro 505 milioni. Un mercato – secondo i dati pubblicati da IDC (società mondiale di ricerche di mercato in ambito IT) – cresciuto del 10,3% nel 2021 e che continua a presentare problematiche in termini sia di sicurezza informatica dei dispositivi e dei sistemi smart home sia di privacy e integrità dei dati prodotti e consumati, la maggior parte dei quali, di natura personale e sensibile. La pandemia, provocando l'accelerazione del processo di digitalizzazione ed innovazione, ha aggravato enormemente il problema.

Luci ed ombre della smart home

Dobbiamo essere sempre più consapevoli che la smart home e i dispositivi IoT, se da un lato possono essere utili, dall'altro lato, possono presentare vulnerabilità critiche imprevedibili.

La vulnerabilità della cybersecurity delle smart home si evince anche uno studio di Euroconsumers – condotto in Spagna, Portogallo, Belgio ed in Italia tramite Altroconsumo – dal titolo emblematico "Hackable Home", che esamina quanto i dispositivi intelligenti a cui sono connesse siano tutt'altro che a prova di hacker.

Sono state testate la sicurezza e l'affidabilità di 16 dispositivi "intelligenti" ad uso domestico – tra cui sistemi di allarme, router WiFi, baby monitor, smart tv, etc. – delle principali marche presenti sul mercato dei quattro Paesi europei coinvolti. È risultato che ben 10 dei 16 dispositivi testati non hanno una comunicazione criptata adeguata atta a proteggere la privacy e la sicurezza dei dati degli utenti e tale vulnerabilità è stata classificata come "altamente grave" o "critica".

Inoltre, lo studio ha evidenziato le seguenti problematiche più diffuse e anche più rischiose:

- Autenticazione Wi-fi che può essere manipolata da hacker esperti disconnettendo il dispositivo e disattivando, quindi, la rete internet.
- Possibili violazioni di dati sensibili degli utenti, a causa di problemi strutturali dell'hardware.
- Impostazioni di fabbrica non sicure principalmente a causa della violabilità delle password preimpostate.

Gli attacchi che rendono vulnerabili i dispositivi IoT che utilizziamo quotidianamente delle nostre case o uffici si presentano su una vasta gamma. Basti pensare ai dispositivi intelligenti esterni (i.e. apriporta, i campanelli wireless, irrigatori intelligenti, telecamere, ecc.) che possono essere facilmente violati da qualche hacker che si trova in prossimità con un computer o un altro trasmettitore Wi-fi. Di fatto, i dispositivi intelligenti all'aperto possono essere utilizzati come punti di ingresso, consentendo agli hacker di accedere all'intera rete domestica intelligente.

Per evitare che uno sconosciuto spii la rete, è importante controllare come questi prodotti memorizzano i nostri dati: se il sistema del dispositivo memorizza le nostre informazioni personali ed è connesso alla rete domestica principale, esiste la possibilità che una violazione di un dispositivo sulla rete possa rivelare i nostri dati ad un hacker. Anche le Smart TV possono essere un facile bersaglio di cyber attack: gli hacker potrebbero potenzialmente accedere a un televisore non sicuro e prendere il controllo cambiando canale, regolando i livelli di volume e persino mostrare contenuti inappropriati ai bambini. Inoltre, gli elettrodomestici intelligenti sempre più diffusi nelle nostre cucine e facilmente comandabili dal cellulare o utilizzando l'attivazione vocale, possono anch'essi essere compromessi da abili hacker.

Cybersecurity domotica

È evidente che più dispositivi connessi abbiamo in casa o in ufficio, maggiori sono le opportunità che i criminali hanno di infiltrarsi nella nostra rete, raggiungere altri dispositivi ricchi di dati, con il rischio di veder compromesse le informazioni private e sensibili ivi contenute. Pertanto dobbiamo adottare un approccio cyber resilience-oriented anche per i dispositivi domotici, mettendo in pratica una serie di azioni necessarie per tutelare la nostra sicurezza e privacy. In particolare:

- **Protezione della rete Wi-fi** - solitamente la maggior parte dei router Wi-fi non sono protetti o utilizzano una password predefinita come "admin", rendendo più facile per gli hacker accedere ai dispositivi collegati al router: Pertanto, si consiglia di proteggere la rete Wi-fi con una password complessa e di evitare di collegarsi ad essa da reti Wi-fi pubbliche. Inoltre è necessario ricordarsi di rinominare

e riavviare il router regolarmente.

- **Mappatura di tutti i dispositivi domestici smart** - Tutti i dispositivi connessi alla rete, dovrebbero essere ben "contabilizzati" in termini di impostazioni, credenziali, versioni del firmware e patch recenti in modo tale da essere in grado di valutare quali misure di sicurezza adottare e individuare quali dispositivi sostituire o aggiornare.
- **Impostare password complesse ed univoche sugli account di ogni dispositivo** - Creare una password lunga almeno 12 caratteri, contenente una combinazione di lettere maiuscole, lettere minuscole, simboli e numeri e che sia univoca per ogni account, in modo che quando un account viene compromesso, gli altri siano al sicuro, e ricordarsi di cambiarla periodicamente. Si consiglia di optare per gestori di password difficili da attaccare e che tracciano la frequenza con cui si modifica la password.
- **Scouting & intelligence preventiva prima di acquistare un dispositivo intelligente** - Verificare sempre l'affidabilità e la reputazione del produttore del dispositivo, oltre a prendere nota delle informazioni/dati raccolti dal dispositivo IoT e come essi sono gestiti/utilizzati dal fornitore, verificando altresì che tipo di controllo si ha in termini di privacy e sull'utilizzo delle informazioni (i.e. funzione di rinuncia alla raccolta delle nostre informazioni/dati o di accesso ed eliminazione delle informazioni/dati raccolti).
- **Effettuare (ove possibile) l'abilitazione dell'autenticazione a più fattori** - Contemplare l'autenticazione a due fattori che implica l'inserimento di un codice univoco del sistema a due fattori per verificare la propria identità, in modo tale da impedire agli hacker di utilizzare tattiche di riempimento delle credenziali (in combinazioni di e-mail e password per compromettere i profili online) per accedere alla rete o all'account.
- **Effettuare periodicamente l'aggiornamento software dei propri dispositivi** - Si consiglia altresì di aggiornare le app per dispositivi mobili che si accoppiano con il dispositivo IoT oltre ad abilitare le impostazioni per attivare gli aggiornamenti software automatici, in modo da avere sempre le patch di sicurezza più recenti.
- **Monitorare e proteggere la propria rete** - Dato che il router è il sistema centrale che collega tutti i dispositivi domotici, è necessario verificarne il livello di sicurezza. Dopo averne modificato la password e il nome predefinito, è necessario assicurarsi che il nome della rete non fornisca il proprio indirizzo, in modo che gli hacker non possano individuarlo. Successivamente, controllare che il router impieghi un metodo di crittografia che garantisca comunicazioni sicure, oltre a considerare di installare un firewall o un software di protezione.

Inoltre, anche se non molto diffusa come precauzione, sarebbe consigliabile configurare una "rete dedicata" per i propri dispositivi IoT. Ovvero, una rete che consente di mantenere i computer e gli smartphone separati dai dispositivi IoT. In questo modo, se un dispositivo viene compromesso, un hacker non può accedere a tutte le preziose

informazioni salvate sui computer.

Riflessioni

Indubbiamente le smart home sono una grande opportunità e comodità, ma devono garantire agli utenti la tutela della propria sicurezza e privacy, soprattutto considerando che la casa o l'ufficio sono il luogo che, per definizione, deve garantire intimità e protezione. Ne consegue che dobbiamo incorporare anche nella nostra vita quotidiana la cultura della cyber resilience. Solo così potranno venire minimizzati i rischi e colti i benefici prospettati da questa evoluzione tecnologica.

Una maggiore sicurezza informatica per Smart building e domotica va innanzitutto pensata e prevista a livello progettuale e di design, dei singoli prodotti e sistemi in connessione tra loro. Intervenire a livello di progetto è molto più semplice ed efficace rispetto a cercare di mettere poi delle 'patch' alle falle informatiche di ogni apparecchiatura.

Poi, sia a livello di singolo prodotto tecnologico e domotico, sia a livello di progetto specifico, che può riguardare un edificio o un quartiere, è possibile realizzare un'analisi e una 'mappa' delle potenziali minacce e intrusioni esterne, per poi prendere delle misure adeguate in base al livello di sicurezza necessario: inutile allestire super-protezioni se non servono, come allo stesso modo non bisogna invece creare barriere troppo deboli quando invece ci sono in gioco funzioni e servizi importanti, e le conseguenze di un cyber-attacco potrebbero essere molto gravi.

Per ogni progetto in edifici e Smart building è poi possibile e auspicabile realizzare dei 'penetration test', delle simulazioni di attacchi informatici, per mettere alla prova le protezioni esistenti, e dopo questi test è necessario applicare un sistema di monitoraggio e verifica costante, nel corso del tempo, per tenere aggiornato e allineato tutto il sistema domotico e i suoi meccanismi di funzionamento.

Per saperne di più...

- per informazioni: **https://trasformazionedigitale.unipv.it**
- per contattare l'Area Sistemi Informativi: **https://sos.unipv.it**
- se sei uno studente scrivi a questo indirizzo: **smart@ unipv.it** oppure contatta un tecnico del tuo dipartimento per ottenere informazioni
- informazioni in tempo reale su attacchi informatici: **https://www.csirt.gov.it**

Fonti

- Wikipedia portale sicurezza informatica - "*Domotica"*
- inDomus.it - "*Sicurezza e domotica*"