

Raffica di Zero-Day mette a rischio gli edifici “smart”

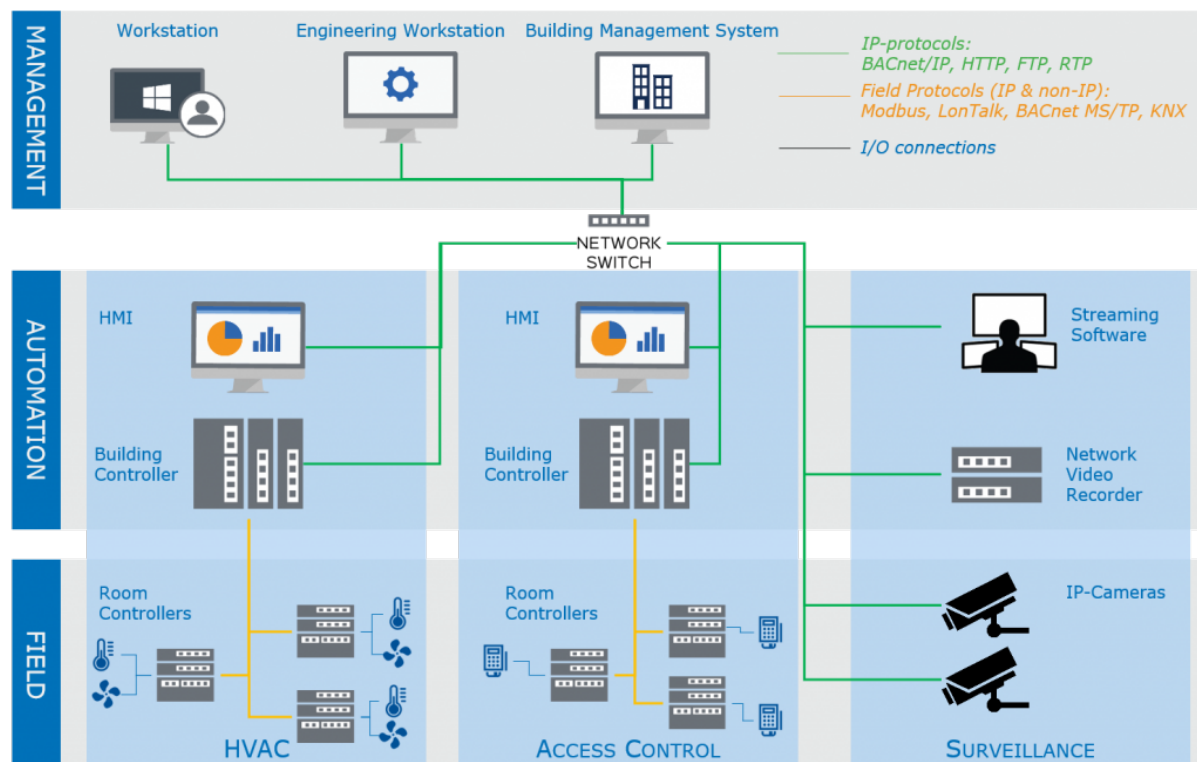
Gen 16, 2019 Marco Schiaffino In evidenza, News, Scenario, Tecnologia, Vulnerabilità 0

Sei vulnerabilità nei dispositivi e protocolli usati per gestirli permettono di violare i sistemi “intelligenti”. Un attacco potrebbe provocare il caos.

La spinta verso l'automazione attraverso la cosiddetta “Internet of Things” non interessa solo gli appartamenti privati, ma anche (e soprattutto) gli edifici nel loro complesso e in particolare edifici pubblici come aeroporti, ospedali, scuole e simili.

Nelle costruzioni moderne la digitalizzazione ha trovato posto ovunque. Dai sistemi di accesso a quelli di sorveglianza, passando per gli impianti antincendio e quelli di climatizzazione, tutto è controllato da dispositivi connessi tra loro in rete. **Inutile dire che tutto questo apre al rischio di attacchi informatici.**

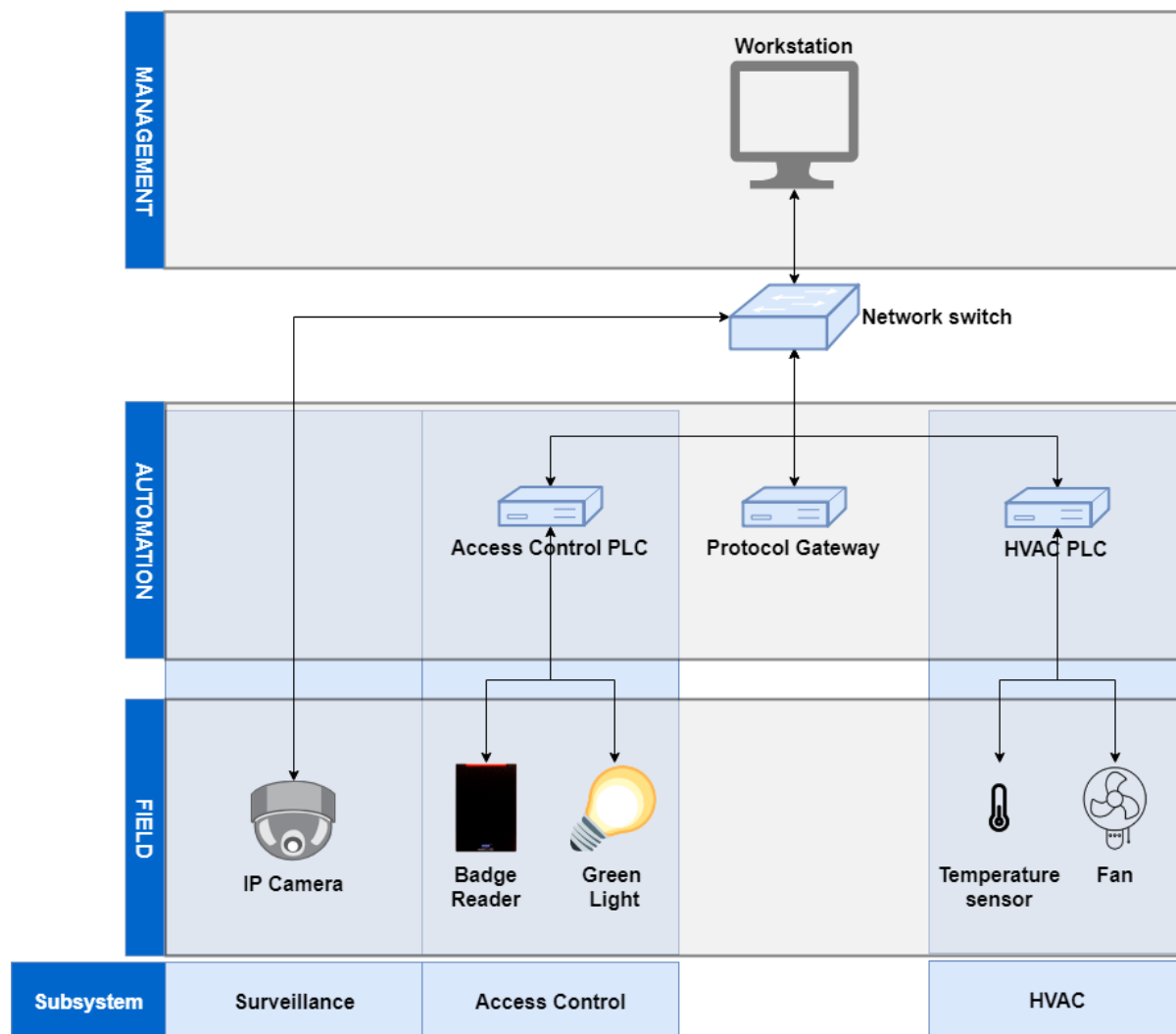
Il rischio, però, è decisamente più elevato di quanto si possa pensare e, soprattutto, **interessa migliaia di edifici in tutto il mondo.**



Secondo **Elisa Costante** di **Forescout**, che ha illustrato la questione nel corso di una sessione del convegno di sicurezza informatica S4X19 in corso in questi giorni a Miami, la situazione è decisamente allarmante.

La ricerca di Forescout è il frutto di un'intensa attività di penetration testing, nel corso della quale gli esperti di sicurezza dell'azienda hanno individuato **sei vulnerabilità zero-day** che interessano dispositivi e protocolli utilizzati in questo ambito e che consentirebbero a un pirata informatico di introdursi con facilità nei sistemi informatici dell'edificio.

La relatrice ha anche illustrato il funzionamento di un **Proof of Concept** realizzato dai ricercatori Forescout in grado di compromettere i sistemi di sorveglianza, accesso e climatizzazione.

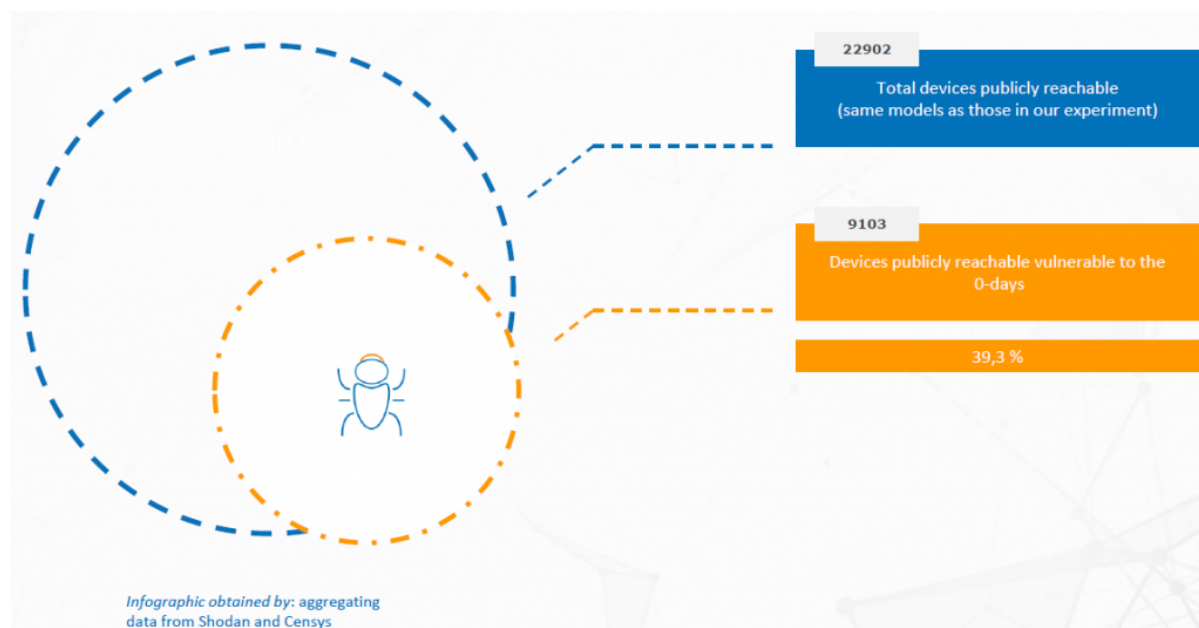


L'attacco sfrutta falle di sicurezza che riguardano principalmente il protocollo utilizzato dai PLC (Programmable Logic Controller) utilizzati per automatizzare i servizi e alcuni specifici prodotti, come il sistema di climatizzazione.

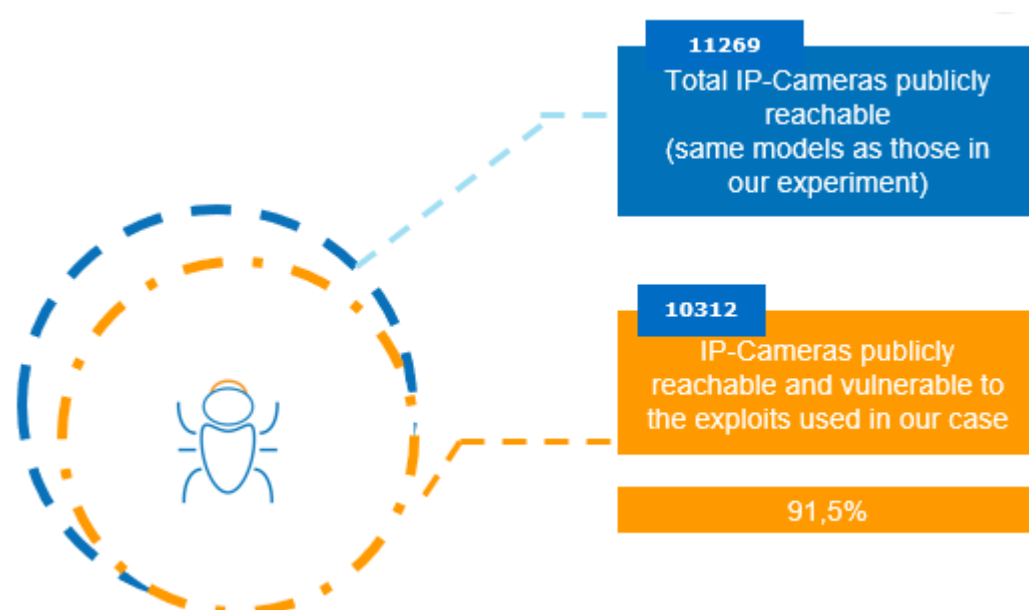
Le più gravi tra le falle individuate permettono attacchi **Cross Site Scripting (XSS)** che consentono di rubare i token di sessione e prendere di conseguenza il controllo dei dispositivi.

Altre, più specifiche, riguardano singoli componenti e rientrano nel novero delle "normali" vulnerabilità che siamo abituati ad aspettarci nei dispositivi IoT: password predefinite inserite nel codice del software, possibilità di aggirare il sistema di autenticazione o di cancellare in remoto dei file.

Secondo Costante, un'analisi incrociata attraverso strumenti di mappatura online (come **Shodan**) ha individuato migliaia di dispositivi esposti su Internet e vulnerabili agli attacchi.



La ricerca fornisce anche delle conferme sui dispositivi più esposti agli attacchi. Tanto per cambiare, la parte del leone la fanno le telecamere di sorveglianza. **Su 11.269 videocamere raggiungibili via Internet individuate dai ricercatori, 10.312 (il 91,5%) era vulnerabile alle loro tecniche di attacco.**



Forescout ha ovviamente comunicato i dettagli delle vulnerabilità ai produttori, che hanno reso disponibili le

patch che correggono le falle di sicurezza. **Il problema però è il solito: quanti amministratori IT implementeranno gli aggiornamenti con tempestività?**

Il problema però è più ampio e riguarda principalmente l'architettura delle reti utilizzate per l'automazione negli edifici. Accorgimenti come la **segmentazione delle reti** o l'attenzione per evitare che i dispositivi siano raggiungibili in remoto sembrano ancora lontani dall'essere patrimonio condiviso di chi si occupa di IoT.

Please follow and like us:



Falle di sicurezza in tutti i maggiori servizi di Web Hosting

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/01/16/raffica-di-zero-day-mette-a-rischio-gli-edifici-smart/>