SMART BUILDING® Roadshow

PRINCIPI PER LA PROGETTAZIONE REALIZZAZIONE E GESTIONE DI EDIFICI INTELLIGENTI

Una iniziativa

SMART BUILDING ITALIA
Powered by Pentastudio

Con il Patrocinio di

ANCE ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

ANIE FEDERAZIONE

CONFINDUSTRIA

CSI ASSOCIAZIONE COMPONENTI E SISTEMI PER IMPIANTI

Contenuti

- Concetti di sicurezza tradizionale e sicurezza informatica
- Sicurezza degli IoT
- Quali sono i punti di attacco
- Cybersecurity nello Smart Building
- Impostazione e contromisure, come prevenire

Che cos’è la sicurezza informatica

La **sicurezza** tradizionale combatte...

La **sicurezza** informatica combatte...

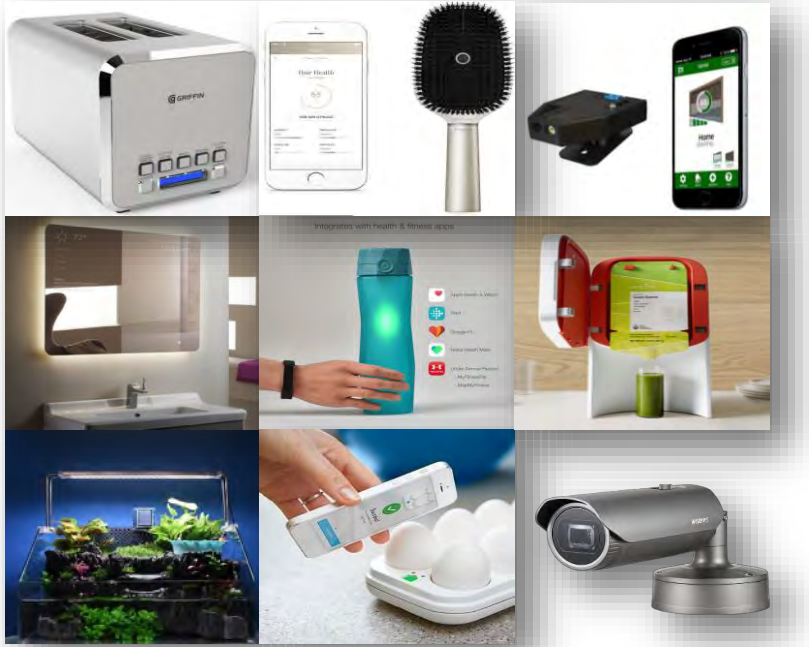
Il percepito…

Sicurezza

Costi

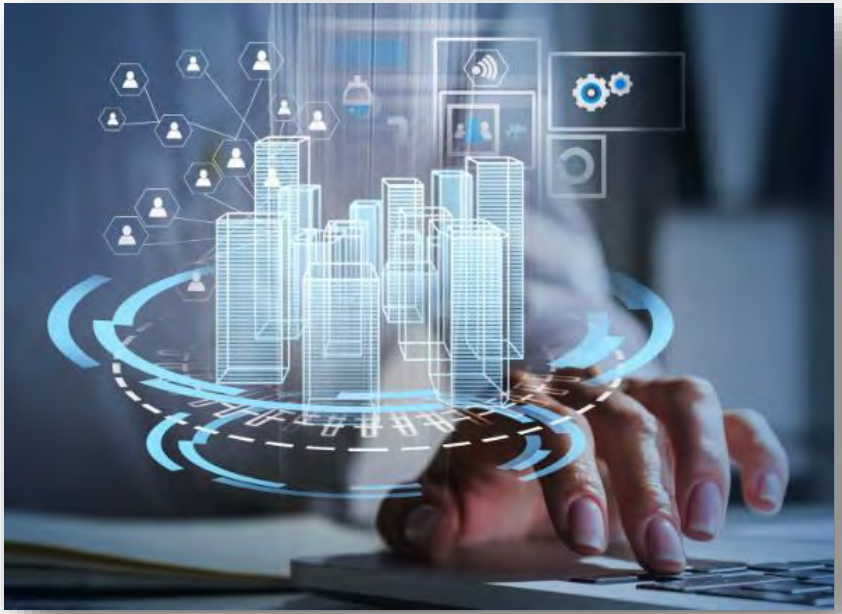
Prodotti IoT intelligenti

- Tostapane e specchio
- Acquario
- Bottiglia d'acqua
- Bollitore uova
- Apriporta da garage
- Spremiagrumi
- Telecamere
- ...e tanto altro



Prodotti Smart Building

- Videosorveglianza
- Controllo accessi
- Video citofoni
- Rete dati
- Ascensori
- Servizi idrici
- Servizi riscaldamento
- Domotica e molto altro



Incidenti in Cybersecurity

- Furto d’identità (65-70%)
- Accesso ad account di utenti (15%)
- Accesso ad account finanziari (10%)
- Azioni di disturbo (5%)
- Altre tipologie (1%)

1 attacco ogni 11 secondi
Fonte: Cybercrime Magazine

Data Breach

Distribuzione geografica degli incidenti

- 60% → Nord America
- 30-35% → Asia/Pacifico
- 5% → Europa
- 1% → Medio Oriente
- < 1% → Africa

Principali scenari di attacco

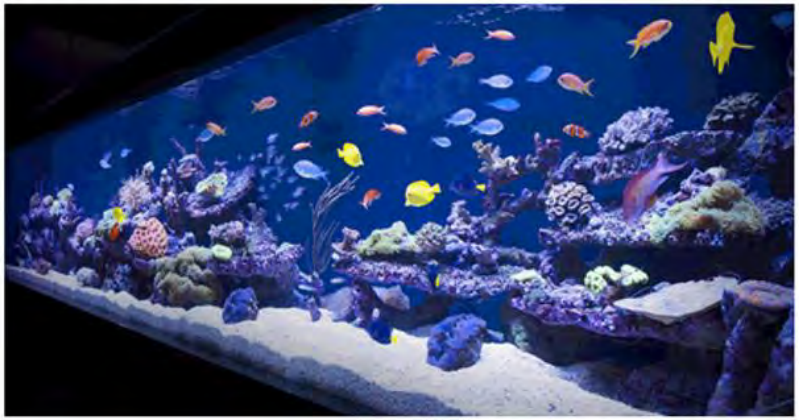
Obiettivi

- Propagare ransomware (67% degli attacchi)
- Installare trojan/backdoor
- Propagare malware per furti di identità e/o credenziali di accesso per furti finanziari (banker malware)
- Installare ed infettare con altre tipologie di malware (worm, adware, cryptominers, etc.)
- DDOS volti a causare disservizi

Articolo

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

April 16, 2018 Wang Wei



Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.

But of much greater concern, enterprises are unable to secure each and every device on their network, giving cybercriminals hold on their network hostage with just one insecure device.

Since IoT is a double-edged sword, it not only poses huge risks to enterprises worldwide but also has the potential to severely disrupt other organisations, or the Internet itself.

There's no better example than Mirai, the botnet malware that knocked the world's biggest and most popular websites offline for few hours over a year ago.

We have another great example that showcases how one innocent looking insecure IoT device connected to your network can cause security nightmares.

Nicole Eagan, the CEO of cybersecurity company Darktrace, told attendees at an event in London on Thursday how cybercriminals hacked an unnamed casino through its Internet-connected thermometer in an aquarium in the lobby of the casino.

According to what Eagan claimed, the hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud."

Although Eagan did not disclose the identity of the casino, the incident she was sharing could be of last year, when Darktrace published a report [PDF], referencing to a thermometer hack of this sort on an unnamed casino based in North America.

IoT & Security

Qual è la *minaccia* informatica tipica di cui sentiamo spesso parlare?

Malware

Abbreviazione di **mal**icious soft**ware**
(software dannoso o malevolo)
E’ un software creato per danneggiare dispositivi e sistemi informatici, agendo contro l'interesse degli utenti

La Cybersecurity nello Smart Building

Scenario estremamente complesso

- Ogni prodotto IoT può rappresentare il potenziale **punto di accesso** per un hacker
- Con il numero crescente di dispositivi IoT in ogni ambiente interconnesso, i punti di ingresso aumentano in modo esponenziale così come le superfici di attacco per le cyber minacce
- Con un singolo dispositivo IoT compromesso e violato, se le difese informatiche non sono adeguate, un utente malintenzionato può accedere a una rete molto più ampia o anche all'intera rete IoT

Cosa potrebbe succedere

- Gli hacker possono utilizzare, per le loro attività illecite, i punti deboli di uno smart building. Possono essere messe in atto **manomissioni e richieste di «riscatto»**
- Automazioni perimetrali come cancelli, porte, tapparelle, elettrodomestici connessi in rete sono strumenti usualmente utilizzati dagli **hacker per compiere sabotaggi**
- Molti hacker violano questi sistemi e riescono a utilizzare le videocamere di sorveglianza per «spiare» case e altri immobili sempre a scopo di riscatto

Criticità e necessità

- Fornitori diversi promuoveranno prodotti diversi
- Ogni settore verticale (con progetti attuali o futuri) avrà necessità differenti che richiederanno competenze differenti
- Il trasporto dei dati tra gli apparati potrebbe essere non sicuro (protocolli non criptati)
- La progettazione diventa parte integrante della sicurezza dell'impianto
- La manutenzione sarà programmata e continua anche come aggiornamento software
- E' necessario un continuo monitoraggio delle risorse per poter intervenire prontamente

- La Cybersecurity nello Smart Building deve essere a livello informatico
- Va pensata e prevista a livello progettuale e di design sia dei sigoli prodotti che dei sistemi in connessione tra loro
- L'intervento a livello progettuale è sicuramente più semplice e funzionale rispetto a cercare successivamente soluzioni alle falle informatiche delle singole apparecchiature
- Sia a livello di singolo prodotto (tecnologico o domotico) sia a livello di progetto specifico è possibile realizzare un'analisi ed una mappa delle potenziali minacce
- Serve realizzare un asset delle possibili vulnerabilità esterne per prendere delle misure adeguate a livello di sicurezza
- Ad integrazione, prevedere la realizzazione di appositi penetration test sulle strutture per validare quanto valutato negli asset

Scenario in sicurezza

Il futuro è l'AI Intelligenza Artificiale

- Una tecnologia che sta incontrando una cresente applicabilità è l'Intelligenza Artificiale
- Algoritmi alla base dei software AI possono essere opportunamente addestrati per elaborare constantemente i dati che provengono da sensori dislocati in varie parti dell'edificio
- Questi programmi sono in grado di analizzare gli input ricevuti, ricavandone correlazioni difficilmente rilevabili dall'uomo e suggerire o mettere in atto direttamente delle azioni per riportare gli apparati ad un funzionamento ottimale aumentando così l'efficienza operativa

→ *Esempio: controllo della temperatura e dell'umidità nelle stanze ed intervento correttivo in automatico*

- Sicuramente l'AI apre degli scenari interessanti come performance e come ottimizzazione delle risorse
- Il machine learning è fondamentale che sia progetto ed ottimizzato in maniera specifica su ogni singolo impianto perchè sia fonte di operatività e non punto debole del sistema di interconnessione
- Errori di programmazione o definizione durante la fase di machine learning hanno portato a risultati disastrosi

Il futuro è l'AI Intelligenza Artificiale

Cybersecurity | Contromisure

Utilizzare password complesse tramite un gestore password e non codividerle mai

Pianificare continui aggiornamenti di tutti i device IoT

Disconnessione automatica di tutti gli accessi manutenzione quando non utilizzati

Utilizzare prodotti consolidati che garantiscono programmi di protezione e aggiornamenti periodici

Proteggere la rete dati (firewall / VPN / SSL)

Test periodici (penetration test)

Scenari presenti e futuri

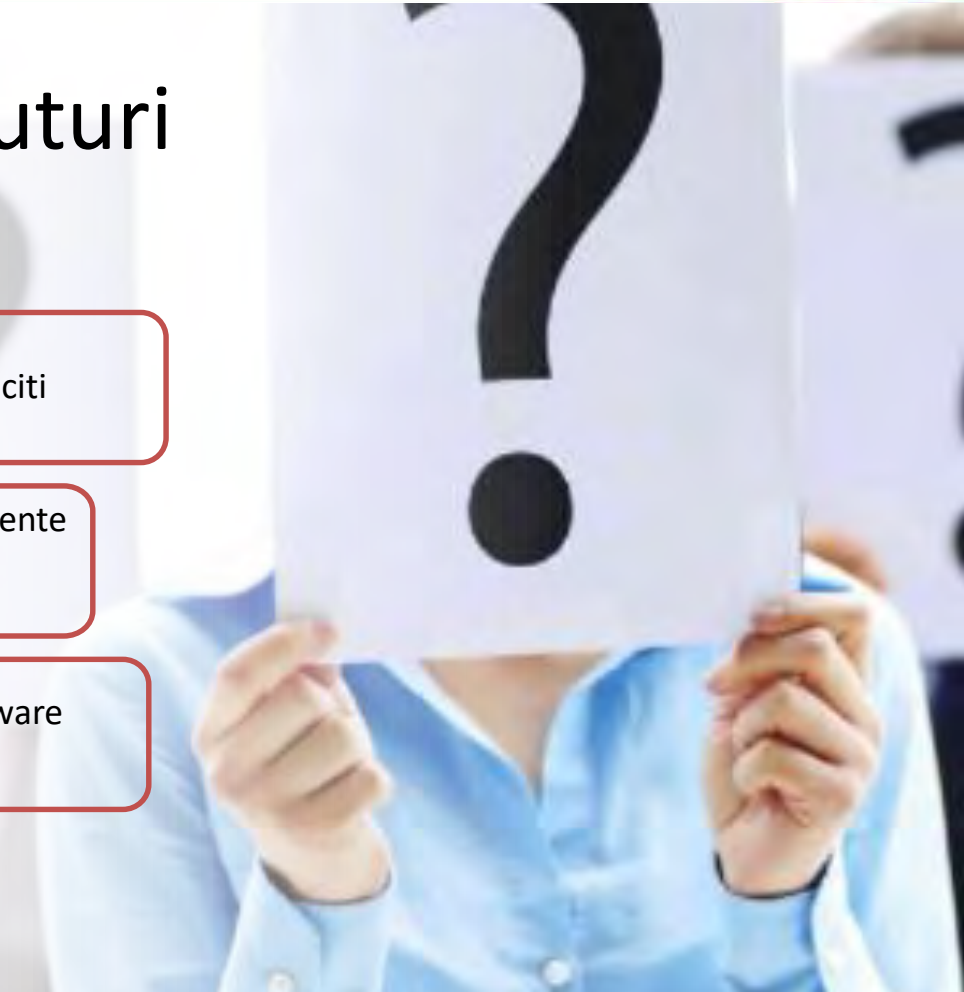
Punti da mitirgare

L'attacco tramite software e controlli leciti

Commettere errori di ingegnerizzazione dei chip è storicamente un punto di ingresso in qualsiasi Sistema che sfrutti un microprocessore (Spectre, Meltdown, Pacman)

Generazione di errori nelle risposte dei software integrano Intelligenza Artificiale

Gli errori di configurazione se non opportunamente rilevati sono il punto principale di attacco di qualsiasi struttura informatica



- Cofondatore, Socio e Responsabile tecnico Alfa Due Snc
- Cofondatore, Socio e Senior Business Developer in The Software Tailors Sagl
- Formatore Securindex Formazione
- Responsabile settori IoT, Reti e Cyber Security Securindex Formazione

Luca Girodo

luca.girodo@alfa-due.com

www.linkedin.com/in/luca-girodo