[Ermanno Goletto](#)
Microsoft Most Valuable Professional
Microsoft Certified

IoT Security Analysis 2018

Introduzione

L'Internet of Things (IoT) o 'Internet delle cose è una evoluzione dell'uso di Internet in cui gli oggetti (le "cose") comunicano dati e accedono ad informazioni aggregate da parte di altri. Ovviamente man mano che gli oggetti di uso quotidiano vengono connessi a Internet diventa importante che siano rispettati requisiti di sicurezza stringenti sia per quanto riguarda i dati trasmessi che per quanto riguarda l'accesso e il controllo degli oggetti.

In questo articolo approfondiremo gli aspetti legati alla sicurezza dell'IoT e per avere una panoramica il possibile più completa sulla situazione degli eventi di Cybersecurity relativi all'IoT verranno analizzati i dati e le considerazioni contenuti in alcuni report annuali di sicurezza pubblicati da organizzazioni e produttori di soluzioni informatiche di sicurezza e servizi correlati all'IoT. Nella scelta dei report dei produttori di soluzioni informatiche di sicurezza e servizi è stato utilizzato il criterio di privilegiare i produttori che si sono posizionati nel 4 quadrante di Gartner, ovvero riconosciuti da Gartner come leader del settore, che hanno pubblicato Security Report di sicurezza contenenti dati e considerazioni circa la sicurezza dell'IoT.

Argomenti

CERT Nazionale - Annunci pubblicati nel 2017 e 2018

Negli ultimi tempi, come era logico aspettarsi, anche l'IoT è diventato un obbiettivo interessante dal punto di vista degli attacchi informatici come dimostrano i 14 annunci relativi a malware, vulnerabilità, minacce e compromissioni correlate all'IoT pubblicati dal CERT Nazionale. Di seguito un estratto delle news pubblicate dal CERT Nazionale negli ultimi due anni:

Data e descrizione minacce / incidenti	Tipo
12 ottobre 2018: ***3 vulnerabilità nell'infrastruttura Cloud di Xiongmai*** *possono consentire l'**accesso non autorizzato a circa 9 milioni di dispositivi** di videosorveglianza*	Vulnerabilità
28 settembre 2018: *Botnet per dispositivi IoT denominata **Torii** con un'architettura altamente modulare e ricca di funzionalità che consentono di catturare informazioni, eseguire un comandi sui dispositivi ed impiantare eseguibili malevoli*	Botnet
27 luglio 2018: ***20 vulnerabilità in SmartThings Hub**, una tecnologia di Samsung per connettere, automatizzare e gestire centralmente svariati dispositivi IoT compatibili installati in smart home (televisori, elettrodomestici, prese intelligenti, lampadine, termostati, rilevatori di fumo, sistemi di sorveglianza e altro ancora)*	Vulnerabilità
19 luglio 2018: ***Compromissione di circa 30.000 dispositivi IoT** di tipo DVR (videoregistratori digitali) prodotti dalla società Dahua Technology con firmware non aggiornato per risolvere la vulnerabilità CVE-2013-6117*	Breach Vulnerabilità
24 maggio 2018: *Malware **VPNFilter** modulare e avanzato che si stima abbia **infettato 500.000 dispositivi IoT** in 54 nazioni diverse prendendo di mira router in ambito SoHo (Small Office Home Office) e apparati NAS di diversi produttori tra cui router Linksys, MikroTik, Netgear e TP-Link e apparati NAS di QNAP*	Malware
15 gennaio 2018: *Nuova famiglia di malware per sistemi Linux, denominata **Mirai Okiru**, progettata per infettare dispositivi equipaggiati con CPU ARC allo scopo di creare una botnet da cui lanciare attacchi DDoS*	Botnet
23 ottobre 2017: Botnet formata da dispositivi IoT, denominata **IoTroop (o Reaper)**, basata su malware che sfrutta vulnerabilità note presenti nei diversi firmware di dispositivi, wireless router Wi-Fi, telecamere IP, telecamere di sorveglianza a circuito chiuso (CCTV), videoregistratori digitali (DVR) e videoregistratori di rete (NVR); al momento il malware sembrerebbe aver **colpito un milione di organizzazioni** in tutto il mondo, principalmente negli Stati Uniti ed in Australia	Botnet
14 settembre 2017: Serie di vulnerabilità denominate **BlueBorne** che affliggono diverse implementazioni del protocollo Bluetooth presenti nei più diffusi sistemi operativi mobili, desktop e per dispositivi IoT (inclusi Android, iOS, Linux e Windows)	Vulnerabilità
20 luglio 2017: Vulnerabilità denominata **Devil's Ivy** (CVE-2017-9765) che può essere utilizzata per causare condizioni di denial of service o eseguire codice arbitrario su dispositivi IoT equipaggiati con la libreria gSOAP di versione precedente alla 2.8.48 come le telecamere Axis Communications	Vulnerabilità
11 maggio 2017: Botnet, denominata **Persirai**, formata da dispositivi IoT in particolare telecamere IP wireless basata su malware che sfrutta una serie di vulnerabilità zero-day di pubblico dominio presenti nel firmware tipicamente di sistemi Linux embedded	Botnet
10 aprile 2017: Due diverse varianti del bot, denominato **BrickerBot**, in grado di danneggiare in maniera irreparabile i dispositivi IoT mediante attacchi di tipo Permanent Denial-of-Service (PDoS)	Bot
10 aprile 2017: Bot, denominato **Amnesia**, che attacca dispositivi IoT di tipo DVR (Digital Video Recorder) equipaggiati con sistemi operativi Linux embedded con lo scopo di prenderne il controllo e lo inserirlo in una botnet da cui lanciare attacchi DDoS di tipo HTTP flooding e UDP flooding	Bot Botnet
13 marzo 2017 Famiglia di malware per Linux, denominata **ELF_IMEIJ**, che prende di mira dispositivi IoT per la sorveglianza prodotti da Avtech	Malware
10 febbraio 2017: Nuovo trojan per i sistemi Windows, denominato **Trojan.Mirai.1**, progettato per infettare dispositivi IoT e realizzare una botnet dalla quale eseguire attacchi DDoS	Botnet

Analizzando semplicemente le news pubblicate dal CERT Nazionale è possibile avere una panoramica sull'evoluzione degli eventi di Cybersecurity relativi all'IoT negli ultimi due anni che mostra **come i dispostivi IoT siano spesso bersagli di Botnet** che riescono a diffondersi tramite vulnerabilità che possono essere fruttate a cause della mancata installazione di aggiornamenti di sicurezza:

Anno	Eventi gravi	Botnet	Bot	Dispositivi compromessi
2018	6	2	-	9.530.000
2017	8	3	2	1.000.000

Per avere una panoramica più completa sulla situazione degli eventi di Cybersecurity relativi all'IoT di seguito vengono riportati dati e considerazioni contenuti in alcuni report annuali di sicurezza pubblicati da organizzazioni e produttori di soluzioni informatiche di sicurezza e servizi correlati all'IoT.

Clusit - Rapporto 2018 edizione Settembre

L'ultimo rapporto **Clusit (Associazione Italiana per la Sicurezza Informatica)** disponibile al momento è quello di **settembre 2018** che può essere richiesto al seguente link https://clusit.it/rapporto-clusit/ evidenza come **nel 2017 siano stati realizzati attacchi tramite centinaia di migliaia di device IoT compromessi** dal malware Satori (a riguardo si veda l'articolo Satori Botnet Malware Now Can Infect Even More IoT Devices).

Il rapporto del Clusit riporta come **nel 2017 il clima di allarme alimentato dai giornali** circa le nuove forme di spionaggio industriale e di criminalità elettronica, come **gli indirizzi di politica industriale su IoT/Industry 4.0** e le **nuove normative a tutela della privacy dei dati (GDPR)** hanno contribuito a formare una **consapevolezza sempre maggiore sul problema del rischio IT** evidenziando le **fondamentali fragilità che si nascondono dietro tecnologie che sono diventate in pochissimi anni le infrastrutture fondamentali sia per il modello di business di molte imprese che le stessi istituzioni che stanno alla base della società**.

Per quanto riguarda il 2018 il rapporto del Clusit cita le considerazioni di IDC emerse nel nel FutureScape 2018 secondo cui alcune tendenze tecnologiche proseguono nel loro processo di rinnovamento come l'**attestazione di piattaforme sempre più integrate per il consolidamento del parco applicativo**, la **diffusione di nuovi strumenti per la gestione degli attacchi automatici e persistenti** (*deception programs*), l'**affermazione dei programmi di tracciamento della filiera e di certificazione in termini di sicurezza delle componenti hardware che si stanno rivelando una *conditio sine qua non* per la realizzazione di paradigmi IoT e Industry 4.0**. Inoltre si prevede che **entro il 2020 un settimo dei dispositivi IoT saranno certificati per garantire che durante il processo di produzione e distribuzione non siano stati compromessi** dal punto di vista della Sicurezza IT, **certificando il livello di rischio sia a livello di firmware che di hardware**.

Check Point's 2018 Security Report

Anche nel rapporto del 2018 pubblicato da Check Point e disponibile al seguente 2018 Security Report viene riportato come il 2017 sia stato un anno particolarmente critico dal punto di vista della sicurezza in **cui hanno assunto particolare rilevanza le botnet IoT** insieme ai ransomware, i data breaches e i mobile malware.

Scendendo nel dettaglio, secondo il report di Check Point, **nel 2017 il 24% delle aziende ha avuto attacchi DDOS** (Distributed Denial of Service) e **negli ultimi anni tali attacchi sono spesso lanciati dispositivi IoT compromessi**. I dispotivi IoT sono spesso oggetto di attenzione da parte degli attaccanti perché sono sempre online e spesso presentano debolezze nell'autenticazione.

Anche il report di Check Point evidenza come ci siano state diverse botnet che hanno colpito dispositivi IoT come Hajime, BlueBorne e, IoTroop. Tendenza che viene anche confermata dal Check Point's Cyber Attack Trends: 2018 Mid-Year Report:

*"**IoT vulnerabilities (CVE-2018-10561, CVE-2018-10562)** – This year security flaws were found in over one million Dasan GPON home routers, exposing them to a wide range of attacks. These vulnerabilities allow any attacker to access the router's settings by appending a certain string to any URL and gain control over the device. The vulnerabilities were widely leveraged by botnet herders to recruit their armies, among them the Satori, Mirai and TheMoon botnets."*

Di seguito alcuni consigli e raccomandazioni contenuti nel report per la gestione della sicurezza dei device IoT che evidenziano come sia necessaria la segmentazione di tali device, il controllo del traffico e il monitoraggio:

"… to protect IoT devices, thorough discovery and awareness of what is connected within the healthcare environment needs to be known. Only then can proper segmentation of these devices, and proper access policies, be carried out. This will enable prevention of potential attacks by deep-packet inspection and URL filtering, for example, to maintain the integrity of the data that these devices hold and the operations that they perform."

Dal momento che l'IoT comprende anche i dispositivi utilizzati a livello domestico questo significa che sottovalutare gli aspetti di sicurezza può consentire ai criminali informatici l'accesso alla rete domestica:

"Beyond the large-scale DDoS attacks we saw in 2017, home IoT devices will be exploited by cyber criminals to gain access not only to a victim's home network but also directly to snoop around their physical home too. This was highlighted by our report into LG's Smart Home Devices last year. As home users are generally not aware of the security element of their home IoT devices, they tend to leave the default settings in their original state. This leaves the door open for attackers to constantly have access to a user's home network."

Inoltre dal momento che i dispositivi IoT saranno la base su cui costruire le soluzioni di Smart City sarà necessario prendere in seria considerazione la prevenzione di potenziali attacchi:

"Smart City IoT initiatives will continue their momentum, helping cities to provide better customer service while substantially reducing costs. At the same time fifth generation cyber security solutions will need to be seriously considered every step of the way in order to prevent potential attacks."

Cisco - Report annuale sulla cybersecurity 2018

Anche nel rapporto Report annuale sulla cybersecurity 2018 pubblicato da Cisco viene data un'ulteriore conferma che l'IoT è entrato a far parte della lista degli obbiettivi sensibili dal punto di vista della sicurezza.

Gli aspetti principali correlati all'IoT evidenziati nel report di Cisco sono i seguenti:

Punto 1: Spesso i dispositivi IoT sono privi di patch e di controllo

Le aziende con dispositivi IoT passibili di attacchi non sembrano neanche motivate ad accelerare la risoluzione del problema e probabilmente tali aziende hanno molti più dispositivi IoT vulnerabili nei loro ambienti IT di quanto credono.

Stando all'analisi di Qualys su dispositivi campione di 7328 dispositivi che includevano serrature, pannelli di allarme antincendio, lettori di schede e sistemi HVAC basati su IP l'83% dei dispositivi IoT del campione presentava vulnerabilità critiche dovute alla mancata installazione di aggiornamenti. Secondo Qualys, sono diversi i motivi che soggiacciono all'inerzia nell'applicazione delle patch:

- Dispositivi non aggiornabili.
- Necessità di richiedere il supporto diretto da parte del fornitore.
- Mancanza di chiarezza in merito chi all'interno dell'azienda sia tenuto a occuparsi della manutenzione dei dispositivi IoT.

Punto 2: Le botnet IoT si stanno espandendo e stanno diventando più mature e automatizzate:

Le botnet IoT prosperano perché **aziende e utenti implementano rapidamente dispositivi IoT a basso costo senza curarsi quasi per nulla della sicurezza**. Ciò consente alle botnet IoT di crescere in termini di dimensioni e potenza e diventando sempre più efficaci nello scatenare potenti attacchi che potrebbero compromettere gravemente Internet **La compromissione grave dei servizi Internet pare sia lo scopo principale di tali attacchi dal momento che gli attaccanti sfruttano sempre più il livello applicativo**. Infatti le botnet IoT sono utilizzate per lanciare attacchi DDoS (Distributed Denial-of-Service) avanzati.

Punto 3: Per i team di sicurezza è difficile difendere gli ambienti sia cloud che IoT

Spesso **ciò è dovuto alla mancanza di chiarezza riguardo a chi precisamente sia responsabile della protezione di tali ambienti**, ma occorre tenere presente che **gli attaccanti consci di questa situazione sfruttano le lacune nella sicurezza derivate dall'espansione dell'IoT e dall'uso di servizi cloud**. **I dispositivi IoT sono sistemi basati su Linux e Unix**, quindi sono s**pesso obiettivi di file binari in formato eseguibile e collegabile** (ELF, Executable and Linkable Format), inoltre **è meno impegnativo prenderne il controllo rispetto a un PC**. Un'altra caratteristica che semplifica l'attività di compromissione e contemporaneamente rende interessante i dispositivi IoT una volta compromessi è che **sono attivi 24 ore su 24**.

Punto 4: Le vulnerabilità legate all'IoT e alle librerie di terze parti si sono fatte minacciose nel 2017

Tra il 1° ottobre 2016 e il 30 settembre 2017, i ricercatori delle minacce di Cisco hanno scoperto 224 nuove vulnerabilità in prodotti non-Cisco, di cui 40 sono state collegate con le librerie software di terze parti incluse in questi prodotti e 74 con dispositivi IoT. Ciò evidenzia **la necessità di esaminare in modo più approfondito le soluzioni di terze parti che forniscono il framework per molte reti aziendali**. Non è sufficiente assicurarsi di utilizzare l'ultima versione del software o che non siano state segnalate CVE (vulnerabilità comuni) aperte, ma, ad esempio, è necessario assicurarsi che le funzioni di aggiornamento automatico o di controllo degli aggiornamenti siano eseguite in modo sicuro utilizzando una comunicazione su un canale sicuro (ad esempio SSL) e che il software sia provvisto di firma digitale.

Fortinet - Threat Landscape Report Q3 2018

Nel Threat Landscape Report Q3 2018 pubblicato da Fortinet conferma che c'è un'evoluzione degli attacchi rivolti a infrastrutture critiche e dispositivi IoT oggetto di malware finalizzati a costruire botnet.

Il report pubblicato da Fortinet inoltre mostra che **nel Q3 del 2018 sono cresciuti gli exploits in generale e in particolare sono cresciti maggiormente sono quelli legati all'IoT**, di seguito l'analisi suddivisa per categorie che mostra come router e telecamere siano al momento i dispositivi maggiormente colpiti secondo l'analisi di Fortinet:

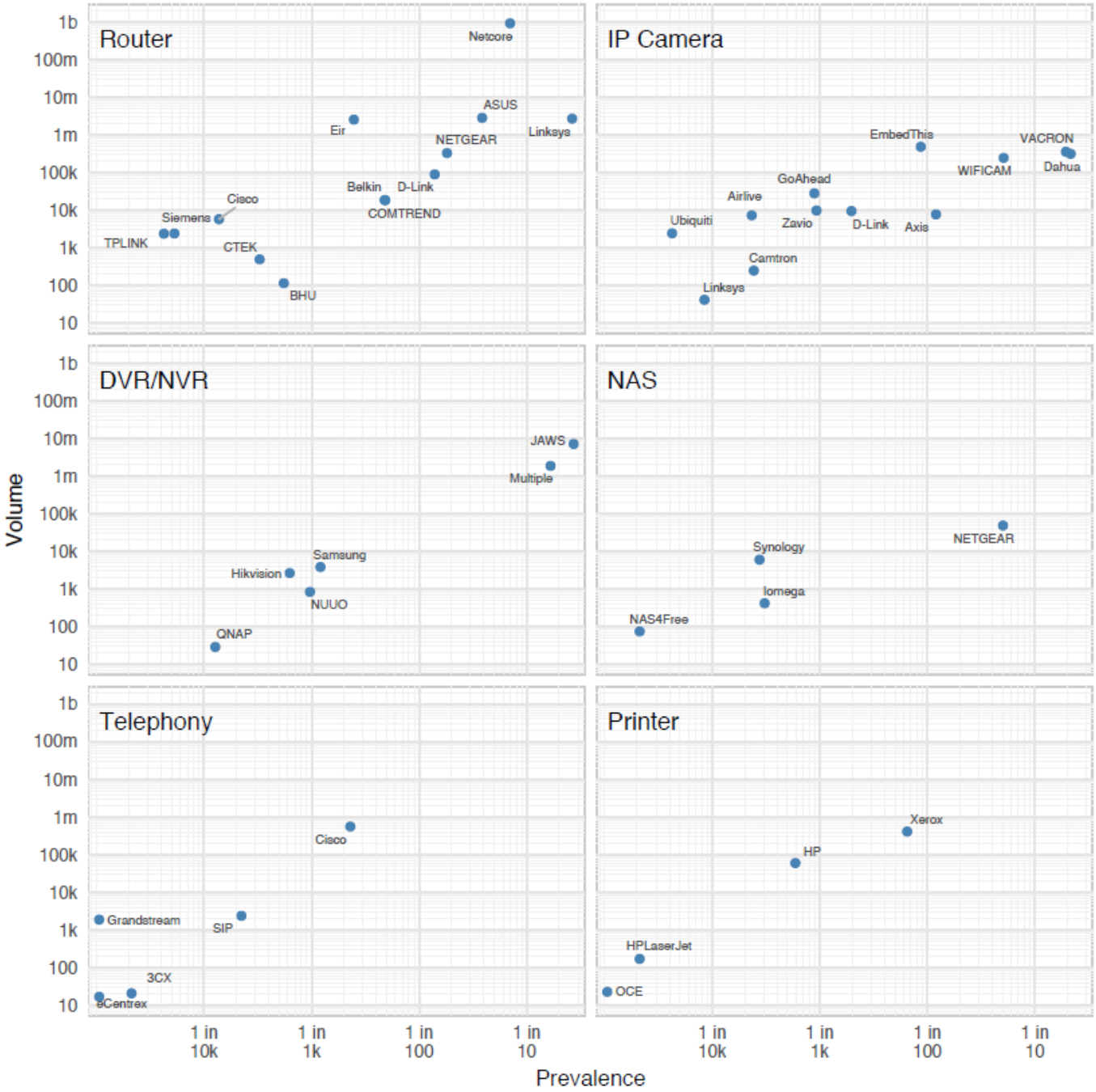

FIGURE 6: PREVALENCE AND VOLUME OF IOT EXPLOITS BY DEVICE CATEGORY.

Di seguito le indicazioni di Fortinet per contrastare gli attacchi legati all'IoT:

"Several exploits targeting IoT devices topped our charts this quarter. We recommend our Learn, Segment, and Protect approach to quell the storm that seems to be brewing. This starts with learning more about devices connected to networks, how they're configured, and how they authenticate. Once complete visibility is achieved, organizations can dynamically segment IoT devices into secured network zones with customized policies. Segments can then be linked together by an integrated, intelligent, and protective fabric across the network—especially at access points, cross-segment network traffic locations, and even into multi-cloud environments."

Sophos - Security Threat Report 2019

Il Security Threat Report del 2019 pubblicato da Sophos evidenzia che nel 2018 si è assistito ad una maggiore diffusione di malware trasmesso a smartphone, tablet e altri dispositivi IoT. In particolare per quanto riguarda l'IoT i maggiori eventi di cybersecurity sono legati al malware VPNFilter e alle botnet Mirai Aidra, Wifatch e Gafgyt da cui sono stati lanciati attacchi automatizzati utilizzando dispositivi di rete per effettuare attacchi DDOS, minare cryptomonete e infiltrarsi nella rete.

Anche il rapporto di Sophos punta il dito sul fatto che spesso gli attacchi sono avvenuti perché la sicurezza è stata trascurata:

"In 2018, SophosLabs saw significant growth in the volume of attacks targeting IoT devices. While in many cases simply changing the default passwords used by a class or brand of device was sufficient to prevent reinfection, there were some standout cases that deserve special mention."

Conclusioni

Sebbene al momento quando si parla di IoT nei report e negli avvisi di sicurezza non viene fatta una distinzione tra IoT domestico e IoT in scenari di Smart City o industriale appare comunque evidente che **la principale minaccia è rappresentata dalle botnet** spesso utilizzate per attacchi DDOS. Le botnet IoT a loro volta riescono a diffondersi grazie all'**incremento delle vulnerabilità e degli exploit**.

Occorre quindi non sottovalutare gli aspetti legati alla sicurezza quando si decide di implementare soluzioni IoT perché **i device IoT possono diventare facile preda degli attaccanti in quanto sono sempre attivi**. Ciò implica che **per gli attaccanti è più semplice sfruttare rapidamente errori di configurazione o vulnerabilità non corrette** con l'installazione degli opportuni aggiornamenti. Esistono infatti portal come Shodan in grado di indicizzare i device connessi ad Internet indicizzando le informazioni che questi espongono consentendo talvolta di ottenere l'elenco di quelli in cui sono presenti specifiche vulnerabilità.

Dai report emerge anche che **occorre gestire centramente le soluzioni IoT** in modo da **avere sempre sottocontrollo l'elenco di tutti i device IoT** di cui è composta la propria rete e **monitorare lo stato di aggiornamento di software e firmware**. Inoltre occorre **gestire la segmentazione di rete dei dispositivi IoT** in modo da non consentire agli attaccanti di poter compromettere la rete aziendale nel caso riescano a compromettere i dispositivi IoT.

Riferimenti

- CERT Nazionale - annunci relativi a malware, vulnerabilità, minacce e compromissioni correlate all'IoT
- Rapporto Clusit
- Check Point Research - Attack Reports
- https://www.cisco.com/c/it_it/products/security/security-reports.html
- Cisco Annual Reports
- Fortinet Threat Intelligence
- Sophos Industry Analysis and Reports