WOMEN
for Security

Cybersecurity e IoT: come affrontare le sfide di un mondo connesso

Parola di Cyber Ladies

Sommario

Women for Security

La community Women for Security (WFS) nasce nel 2020 grazie a un gruppo di specialiste della Cyber Security; si pone l'obiettivo di mettere a fattor comune le competenze delle donne in ambito information security e di contribuire a stimolare l'interesse delle donne, soprattutto delle ragazze, verso questa disciplina.

Come si evince da molte statistiche, infatti, il numero delle donne che operano in ambito ICT (Information and Communication Technology) è decisamente inferiore a quello degli uomini: il rapporto DESI[1] indica quasi il 19% di donne impiegate nel settore ICT in Europa; per l'Italia la percentuale scende al 16%[2]; nel caso della Cyber Security, secondo il rapporto di ICS2[3] oggi, in tutto il mondo, le donne nel settore della sicurezza informatica sono solo il 24% della forza lavoro.

È importante, quindi, per le WFS contribuire a diffondere la cultura della Cyber Security anche verso le fasce più giovani della popolazione, con iniziative di formazione e orientamento verso le nuove professionalità che evolvono con il progresso tecnologico e digitale. In particolare, nel settore della Cyber Security la domanda di esperti è di gran lunga maggiore dell'offerta, indipendentemente dal fattore sesso: è un aspetto che la community cerca di sottolineare molto per invogliare le ragazze (ma in generale tutti i giovani) a formarsi in questo settore.

Coerentemente con la volontà di contribuire a diffondere la cultura del digitale e della Cyber Security, le WFS si sono impegnate nella stesura di questo libro che tratta il tema dell'Internet delle cose (IoT), uno dei più attuali e cruciali per lo sviluppo tecnologico, nella convinzione che possa essere utile a molte persone che già utilizzano l'IoT senza la necessaria consapevolezza.

---

1 Rapporto Desi 2021 Europa https://digital-strategy.ec.europa.eu/en/policies/desi

2 Rapporto Desi 2021 Italia, https://digital-strategy.ec.europa.eu/en/policies/desi-italy

3 Women in Cyber Security https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx

Introduzione

Le prime volte che si è cominciato a sentir parlare di "*Internet delle cose*" (Internet of Things - IoT) in modo più ricorrente, negli ambienti tecnici e di ricerca, è stato verso la metà degli anni 2000.
Era difficile ipotizzare cosa volesse dire e quali scenari figurarsi: oggetti connessi a Internet, ma quali? Come? Per fare cosa?
Avevamo da poco assimilato l'idea del Web 2.0 (quello per cui gli utenti possono immettere contenuti) ed ecco un'altra novità, complessa da delineare. Per molti anni questi temi sono rimasti confinati tra gli addetti ai lavori, ma oggi di IoT si parla anche sui media generalisti; questo però non vuol dire che tutti sappiano esattamente cosa sia, come funzioni, quali opportunità offra e quali rischi paventi.
Lo scopo di questa pubblicazione è proprio quello di esplorare il mondo dell'IoT con un approccio per "non addetti ai lavori", per tutti quelli che usano Internet tutti i giorni ma non sono dei tecnici.

Ma perché dovrebbero interessarsi all'IoT? Non basta "usarlo" con l'approccio "plug and play"?
Secondo noi no: per usare bene la tecnologia, sfruttarne le opportunità ed essere consapevoli dei rischi occorre conoscerla, sapere come funziona ed essere in grado di controllarla.
Questa pubblicazione non vuole essere un manuale, ma una raccolta di articoli di approfondimento sui vari aspetti dell'IoT, scritti in un linguaggio comprensibile, non tecnico.

Si parla anche di Cyber Security, perché è intrinseca nell'IoT come in ogni strumento o servizio o dispositivo che sia connesso alla rete (si veda a questo proposito l'apposita premessa di seguito).
Gli oggetti connessi attivi in Italia sono 110 milioni, poco più di 1,8 per abitante. A fine 2021 si contavano 37 milioni di connessioni IoT cellulari (+9% rispetto al 2020) e 74 milioni di connessioni abilitate da altre tecnologie di comunicazione (+25%). Nel 2021 in Italia è cresciuto anche il mercato dell'IoT che vale circa 7,5 miliardi di euro, di cui circa 3 miliardi di euro (pari al 40% del totale) relativi ai soli servizi, con un +25% rispetto al 2020[4].

Il PNRR (Piano Nazionale di Ripresa e Resilienza) prevede complessivamente 29,78 miliardi di euro dedicati direttamente o indirettamente al settore dell'Internet of Things: possiamo immaginare quindi un grande sviluppo nella diffusione di questa tecnologia, che sarà ancora più pervasiva.

[4] I dati sono dell'Osservatorio Internet of Things del Politecnico di Milano e risalgono ad Aprile 2022

Nei vari capitoli spiegheremo cos'è l'Internet delle Cose, fornendo i concetti principali per orientarsi in questo settore. Metteremo in evidenza i principali campi di applicazione, benché le potenzialità siano talmente tante che è difficile citarle tutte. Parlando di IoT non si può evitare di riferirsi anche a Big Data e Intelligenza Artificiale, perché ogni oggetto connesso in rete (in ottica IoT) porta a bordo uno o più sensori che raccolgono dati dall'ambiente circostante.

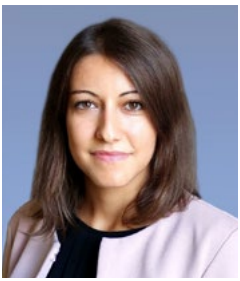
Questa grande mole di dati raccolti (detti Big Data) deve essere analizzata ed elaborata con tecniche di Intelligenza Artificiale, un'attività che comporta alcuni rischi soprattutto per la privacy degli utenti coinvolti (anche involontariamente) nella raccolta di dati.

Una volta analizzato lo scenario nel suo complesso, ci focalizzeremo sui rischi legati all'uso dell'IoT: vedremo come questi dispositivi vadano usati con attenzione e consapevolezza.
La diffusione dell'IoT a livello planetario ha fatto nascere la necessità di stabilire anche degli standard per la progettazione dei dispositivi connessi, realizzazione ed uso: approfondiremo la norma ISO/IEC 27400.

Affronteremo poi i "segreti" della Threat Intelligence, una nuova branca dell'Intelligenza Artificiale che si occupa di raccogliere e rielaborare i dati sugli attacchi per prevenirne di nuovi.

Infine, un "case study" che raccoglie molti dei concetti espressi contribuirà a esemplificarli e fissarli meglio. Nelle conclusioni ci avventureremo anche nella predizione/previsione di nuovi scenari.

Le autrici



Giorgia Dragoni

Si è laureata in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, con una Tesi sull'evoluzione di ruoli e competenze all'interno delle Direzioni ICT.
Dal 2014 è Ricercatrice presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi alla Cyber Security e Data Protection e ai Big data Analytics. Dal 2020 è Direttrice di un nuovo progetto di ricerca sui temi dell'Identità Digitale.
Nel 2022 ha conseguito l'Executive Master in Management presso il MIP Politecnico di Milano. Dal 2021 fa parte della community Women for Security.

Rosa Fiorenza

Italy Security Talent Community Lead in Avanade, dove guida un team di oltre 50 consulenti di sicurezza. Cyberlady di Women For Security dal 2022.
Laureata in Scienze dell'Informazione a La Sapienza di Roma nel 1997. Nel 2018 ha conseguito un MBA in Cyber Security all'Università di Coventry, Inghilterra.
Ha maturato 25 anni di esperienza nel mondo IT e da 23 anni si occupa di sicurezza.
Ha iniziato come SOC analyst, per poi spostarsi su temi di Governance, Risk and Management, dove come consulente ha supportato i clienti nello sviluppare le loro strategie di sicurezza.

Beatrice Ridolfi

Consulente in ambito sicurezza informatica, dopo una Laurea in Matematica ed esperienze di progetti di data analysis e system integration, si è dedicata maggiormente ai temi in ambito sicurezza delle informazioni, tra cui analisi del rischio, governance, conformità e Cyber Security awareness.
È lead auditor ISO/IEC 27001, di cui è anche lead implementer, PCI QSA e certificata CRISC.
Senior Information Security Consultant presso Bl4ckswan dal 2019, e cyberlady di Women For Security dal 2021.

Manuela Santini

Information & Cyber Security advisor e Associate Partner in P4I, si occupa di consulenza in ambito Cyber Security e Data Protection.
Ha maturato 15 anni di esperienza nell'IT e da oltre 10 anni si occupa di sicurezza.
È lead auditor ISO/IEC 27001 e ISO/IEC 22301.
Ha ricoperto ruoli di IT Security and Internal Audit Manager e Chief Information Security Officer.
È relatrice in webinar e convegni, nonché in corsi di formazione e autrice di articoli in materia di sicurezza delle informazioni.

Sofia Scozzari

Appassionata di tecnologia da sempre, ha maturato oltre 15 anni di esperienza nella Cyber Security e più di 30 nell'IT.
Da 5 anni risiede negli Emirati Arabi Uniti dove ha fondato e dirige Hackmanac, con cui elabora dati sulle minacce Cyber a supporto di attività di Risk Management.
Fa parte del Comitato Direttivo di Women For Security e del Comitato Scientifico Clusit.
È co-autrice del Rapporto Clusit fin dalla prima edizione oltre che di articoli e numerose pubblicazioni di Cyber Security.
La Cyber Security Awareness è il suo focus principale ed è trainer e relatrice in webinar, eventi e convegni in materia.

Anna Vaccarelli

È Dirigente Tecnologo del Consiglio Nazionale delle Ricerche; responsabile delle Relazioni esterne, media, comunicazione e marketing del Registro .it, gestito dall'Istituto di Informatica e Telematica del Cnr.
Dal 2010 coordina e promuove la diffusione della cultura di internet nelle scuole, con laboratori dalle primarie alle secondarie di secondo grado attraverso la Ludoteca del Registro .it.
È tra gli ideatori di Internet Festival e coordinatore del Comitato Esecutivo del Festival.
Fa parte del Comitato Direttivo di Women for Security dal 2020 ed è stata docente in corsi di Cybersecurity, responsabile scientifico di progetti nazionali e internazionali, oltre che coautore di oltre 100 pubblicazioni scientifiche e tecniche.

Premessa: la Cyber Security

In questa pubblicazione si fa riferimento continuamente alla Cyber Security.
Non è questo il luogo per parlare diffusamente di Cyber Security (occorrerebbe un'altra pubblicazione) ma riteniamo utile dare alcune nozioni di base.

La Cyber Security protegge i dati dall'accesso **digitale** illegale.
Per dati si intendono:
- dati fisici e locali, cioè quelli che risiedono su pc/tablet/smartphone
- dati remoti: per esempio le email sui server, cloud storage, instant messaging
- dati in transito, che vengono intercettati per esempio per fare l'analisi del traffico.

La Cyber Security interessa molti ambiti: quello domestico (per i dispositivi connessi che abbiamo in casa), quello industriale (per l'automazione legata all'industria 4.0), quello della pubblica amministrazione, quello delle infrastrutture critiche (rete di trasporti, rete di distribuzione dell'energia, del gas, dell'acqua ecc.).
Per il NIST[5] americano, la Cyber Security consiste nella "capacità di proteggere o difendere l'uso del cyberspazio dai cyber-attacchi", intesi come attacchi intenzionali, che avvengono nel dominio digitale.

Ma quali sono i rischi che corriamo? Solo a titolo di esempio:
- furto di informazioni e di dati
- furto di profili
- violazione della privacy
- indisponibilità delle risorse: per esempio siti web bloccati, servizi bancari non raggiungibili, il nostro computer inutilizzabile ecc.
- email o SMS ingannevoli (rispettivamente phishing e smishing).

Quello che la Cyber Security cerca di preservare nei dati, nei sistemi, nei dispositivi, ecc. sono tre caratteristiche principali:
- **Riservatezza:** solo le persone autorizzate possono accedere ai sistemi informativi, alle informazioni, ai dati. Riservatezza (o Privacy) è il diritto di un individuo di decidere quando, che cosa, perché e chi può gestire le sue informazioni personali.
- **Integrità:** i dati, i sistemi informativi e le informazioni non possono essere modificati in modo non autorizzato. È la certezza che le informazioni inserite, elaborate, trasmesse e custodite sono integre cioè esenti da manomissioni o alterazioni, volontarie o involontarie, e che su tale integrità possono fare affidamento tutti coloro (utenti o programmi) che le utilizzano per lo svolgimento dei compiti assegnati.

[5] National Institute of Standards and Technology, https://www.nist.gov/

- **Disponibilità**: i dati, i sistemi informativi e le informazioni sono accessibili agli utenti autorizzati nei tempi e nei modi previsti. È la capacità di fornire agli utenti in ogni momento utile le informazioni inserite in un sistema informatico o i servizi erogati. È anche la capacità di un sistema di continuare a funzionare soddisfacendo i requisiti di sicurezza nonostante il malfunzionamento di un componente o la violazione - accidentale e non - di uno dei requisiti (resilienza del sistema).

Queste caratteristiche possono essere violate se i sistemi presentano qualche vulnerabilità, qualche punto debole che può essere sfruttato da un attaccante.

Le principali categorie di attacco sono:
- social engineering: per attuare questo tipo di attacco, bisogna convincere qualcuno a fornire informazioni riservate sul sistema che si vuole attaccare, per esempio credenziali di accesso, password, configurazione dei sistemi, ecc. Si gioca sulla buona fede di chi è depositario delle informazioni.
- impersonazione di un altro soggetto (macchina o persona). Questo attacco consiste nel fingersi un'altra persona/soggetto: per esempio sostituire una pagina web che richiede identificatore e password verso un utente ignaro e leggere la password e l'identificatore che questi immette, inviare una email al cliente di una banca fingendosi la banca, ecc.
- sfruttamento di vulnerabilità. Possono esserci errori di progettazione o di programmazione in un determinato sistema: alcuni programmi mirano a sfruttare le vulnerabilità esistenti per entrare in un sistema e danneggiarlo.

O, più probabilmente, una combinazione di questi.

Alcuni attacchi possono essere realizzati con l'aiuto di *software malevolo* (il "malware") che si annida o si propaga attraverso i nostri dispositivi.
Deriva dalla contrazione di "malicious" e "software", significa "programma malvagio". Indica un qualsiasi programma informatico in grado di danneggiare il funzionamento e la sicurezza del sistema operativo.
Si trasmette attraverso Internet, spesso tramite la posta elettronica o la semplice navigazione.
Ci sono molti tipi di malware, di cui si sente spesso parlare anche nei media: trojan, ransomware, worms, spyware, adware, bot… Ciascuno di essi ha un diverso meccanismo di funzionamento ma l'obiettivo è sempre lo stesso: danneggiare il sistema destinatario. Nel caso del ransomware, in particolare, oltre a rendere inutilizzabile un sistema, gli attaccanti chiedono anche un riscatto per "liberarlo".

Anche i tipi di attacco possono essere diversi e sono in continua evoluzione: i principali, più ricorrenti, sono:

- **Denial-of-service** (in italiano "negazione del servizio", abbreviato in DoS): è un attacco per far esaurire le risorse di un sistema informatico che fornisce un servizio ai clienti, fino a renderlo non più in grado di funzionare. L'aggressore, in pratica, provoca una "negazione del servizio", sovraccaricando, con una miriade di richieste, le connessioni di rete di un sistema responsabile dello scambio di dati esterni: se la quantità di richieste supera il limite di capacità, il sistema rallenta o collassa
- **Sniffing (intercettazione)**: viene intercettato il traffico di rete. L'hacker può quindi ottenere password, numero di carte di credito e altri contenuti sensibili che l'utente invia sulla rete interessata. Spesso si verifica su reti WiFi libere (aeroporti, aree pubbliche, ecc.)
- **Man in the middle:** consiste nell'interporsi nello scambio tra due persone o due computer per intercettare i contenuti e modificarli. L'hacker deve ricevere i messaggi da ciascuna delle due parti e rispondere a ciascuna di esse facendosi passare per l'altra.

Per cercare di evitare e di prevenire i rischi bisogna farne una valutazione a priori (valutazione del rischio), che comprenda anche eventuali danni economici e di immagine, soprattutto se si tratta di un'azienda o di una organizzazione.
Sulla base della valutazione si stabiliscono delle contromisure atte a prevenire i danni e commisurate ad essi, che possono essere basate su comportamenti corretti e/o sui meccanismi di sicurezza.

Della prima categoria fanno parte:

- protezione del proprio pc, dei dispositivi mobili e in generale dei sistemi;
- robustezza, protezione e custodia delle credenziali;
- riconoscimento dei tentativi di truffa e intrusione;
- politiche e controlli di sicurezza;
- buone pratiche di prevenzione e di risposta in caso di attacco.

Possiamo invece schematizzare i meccanismi di sicurezza in tre categorie principali:

- Identificazione/autenticazione: è basata su quello che conosci (ad esempio la password o il pin) o quello che hai (una carta di credito, cellulare, un token) o quello che sei (impronta digitale, l'iride, la retina).
- Crittografia: è la tecnica per nascondere il contenuto di un messaggio e, in alcuni casi, anche per individuare con certezza il mittente di un messaggio. La usiamo continuamente, per esempio, nelle chat di Whatsapp.
- Sistemi di identificazione e prevenzione delle intrusioni: possiamo proteggere i nostri sistemi con metodi anche forti di identificazione per consentire l'accesso,

come pure attraverso firewall per bloccare attacchi dall'esterno. Attenzione però: le statistiche dimostrano che la maggior parte degli attacchi proviene dall'interno (quindi il firewall non può proteggere) e l'attaccante è probabilmente in possesso di credenziali di accesso di qualche soggetto interno complice o anche lui ignara vittima di un furto di credenziali.

Sebbene la maggior parte degli attacchi parte da un comportamento poco accorto o imprudente, è bene sottolineare che i risultati migliori si ottengono applicando una combinazione di soluzioni appartenenti ad entrambe le categorie.

Cos'è l'IoT

Anna Vaccarelli

Primi anni '80, all'Università Carnegie Mellon, lo studente David Nichols – laureando del dipartimento di Computer Science – ha sete, però il distributore automatico di bevande è molto distante dal suo ufficio e il rischio di trovarlo vuoto o che le bottigliette al suo interno non siano belle ghiacciate è elevato.
Come risolvere il problema? David coinvolge due studenti e un ricercatore di ingegneria in quella che sarà una piccola rivoluzione: controllare a distanza la presenza delle bevande nel distributore e la loro temperatura.
Il gruppo decide di monitorare la macchina tramite un computer, sfruttando i sensori del distributore che comunicano se una colonna è vuota o quando una bottiglietta viene acquistata.
Collegando il distributore alla rete ARPANET[6], allora ancora piuttosto giovane, il team riesce a sapere con estrema precisione lo stato del distributore, evitando di fare un viaggio a vuoto quando gli viene sete.
Nel 1990 per la prima volta John Romkey connette a Internet un tostapane e l'anno successivo un gruppo di studenti dell'università di Cambridge usa il primo prototipo di webcam per controllare la quantità di caffè disponibile nella macchinetta del laboratorio informatico (i distributori automatici sembrano essere uno stimolo costante per l'Internet of Things!).
Lo fanno programmando la webcam affinché scatti tre foto della caffettiera al minuto. La webcam invia le immagini ai computer locali così gli utenti possono verificare se il caffè è disponibile.
Ma è nel 2000 che LG Electronics introduce il primo frigorifero al mondo con connessione Internet. Questo permette ai clienti di acquistare cibo on-line. Nel 2008 all'Internet of Things viene dedicata la prima conferenza scientifica internazionale in Svizzera.
Nel 2010 il governo cinese annuncia che l'Internet of Things sarebbe stata una priorità strategica nel proprio piano quinquennale. Forbes e Wired dal 2012 iniziano a utilizzare sempre più spesso nei loro articoli la parola IoT.
Al di là della storia e delle definizioni, certamente l'Internet of Things sta cambiando rapidamente gli scenari delle nostre vite quotidiane.
Ormai quando parliamo di Internet non intendiamo solo siti web o piattaforme di streaming, ci riferiamo a una complessa rete di dispositivi che dialogano costantemente tra loro. Ciascuno di essi, per farlo deve essere dotato di sensori che raccolgono specifici dati e di un "computer" in grado di collegarsi alla rete, trasmettere dati e ricevere "comandi".

---

[6] ARPANET, https://it.wikipedia.org/wiki/ARPANET

Le tecnologie utilizzate dagli oggetti per collegarsi alla rete sono diverse.

I primi a essere utilizzati per la comunicazione e la trasmissione di dati tra oggetti sono stati i tag RFID (acronimo di *Radio-Frequency IDentification*)[7], ma in tempi più recenti sono emerse nuove tecnologie come il protocollo IEEE 802.15.4[8].
Alcuni dispositivi vengono dotati di schede SIM in grado di collegarsi autonomamente a Internet tramite un servizio di traffico dati mobile, mentre molti elettrodomestici si collegano via WiFi alla rete domestica, per accedere a Internet.
Alcuni dispositivi, come i grandi elettrodomestici e quelli da incasso, potrebbero anche utilizzare connessione via Ethernet, visto che si tratta di oggetti fissi e già cablati dalla rete elettrica.

Figura 1: *Internet delle cose*

Per poter dialogare con altri dispositivi, tutti gli oggetti connessi in rete devono avere un indirizzo IP[9]; quindi, anche tutti i sensori dell'IoT devono averlo.

[7] Identificazione a radiofrequenza, https://it.wikipedia.org/wiki/Identificazione_a_radiofrequenza

[8] Standard IEE 802.15.4, https://it.wikipedia.org/wiki/IEEE_802.15.4

[9] Internet Protocol: la parte del protocollo di comunicazione della rete (il TCP/IP) che consente di individuare ogni risorsa di rete (sia essa un dispositivo o una pagina web) attraverso un indirizzo numerico univoco, formato da 4 gruppi tre cifre comprese tra 0 e 255 e separate da un punto. Per maggiori informazioni si veda https://it.wikipedia.org/wiki/Indirizzo_IP

Si stima che durante il 2021 ci siano stati oltre 46 miliardi di dispositivi connessi all'Internet of Things e gli esperti prevedono che si arriverà a superare i 100 miliardi di dispositivi nel 2030[10].
Per far fronte a questa richiesta molto aumentata e in continua crescita, negli ultimi anni si è passati dal protocollo IPv4 (versione 4)[11] che consentiva di indirizzare al massimo 2^{32} (circa $4{,}3 \times 109$ cioè 10 miliardi) oggetti, allo standard IPv6[12] che consente di associare alle rete 2^{128} (circa $3{,}4 \times 1038$) oggetti.
Quante volte abbiamo immaginato come fantascientifico il fatto che il frigo ci dicesse se il latte era scaduto o di arrivare a casa e trovare la lavatrice pronta da scaricare?
Adesso è possibile: non è più fantascienza, basta avere per esempio la lavatrice predisposta ad una connessione Internet, uno smartphone con un'app in grado di dialogare con la lavatrice e siamo in grado di decidere a che ora deve mettersi in funzione, con quale programma, ecc… purché sia carica!
Certamente impressionante!

Ambiti principali

IoT non è solo domotica, al contrario ci sono moltissimi ambiti di applicazione, tra cui:

Wereable

Forse tra i primi dispositivi connessi in rete di cui si è parlato sui media generalisti: le scarpe sportive che trasmettono dati sulle prestazioni dell'atleta che le indossa o le t-shirt che hanno la stessa funzione, per non parlare degli "smart-watch", gli orologi intelligenti che ci monitorano durante l'attività fisica.

Smart agricolture

In questo caso i sensori raccolgono i parametri micro-climatici a supporto dell'agricoltura per migliorare la qualità dei prodotti, ridurre le risorse utilizzate e l'impatto ambientale.

Smart car

Le auto sono sempre più connesse sia per comunicare informazioni in tempo reale al consumatore, sia per scambiarle tra veicoli o con l'infrastruttura circostante per la prevenzione e la rilevazione degli incidenti.

Smart city

Si parla molto di città intelligenti in cui il monitoraggio e la gestione, per esempio, dei mezzi per il trasporto pubblico, dell'illuminazione pubblica, dei parcheggi, dei parametri di inquinamento, ecc. ne migliorino vivibilità, sostenibilità e competitività.

Smart mobility

Prevede la raccolta di informazioni da treni o veicoli sulle autostrade per il control-

[10] https://www.kaspersky.it/resource-center/definitions/what-is-iot

[11] IP versione 4, https://it.wikipedia.org/wiki/IPv4

[12] IP versione 6, https://it.wikipedia.org/wiki/IPv6

lo del traffico, la gestione di incidenti, l'ottimizzazione dei percorsi.

Smart home

Le ormai note case "domotiche" in cui vengono realizzate soluzioni per la gestione in automatico e/o da remoto degli impianti e degli oggetti dell'abitazione connessi in rete, sia per ridurre i consumi energetici che per migliorare il comfort, la sicurezza dell'abitazione e delle persone al loro interno.

Smart building

Gli impianti degli edifici (ad esempio, quelli per l'illuminazione e la climatizzazione) possono essere gestiti automaticamente per migliorare il risparmio energetico, il comfort, la sicurezza dello stabile e delle persone al suo interno.

Smart metering

Si tratta di contatori (misuratori) connessi in rete (Smart Meter) per la misurazione dei consumi (elettricità, gas, acqua, calore), la loro corretta fatturazione e la telegestione.

Industria 4.0

Prevede la connessione dei macchinari, degli operatori e dei prodotti a specifici sistemi di controllo digitale e robotico per promuovere e realizzare nuove logiche di gestione della produzione.

Smart health

Sono ormai sempre più numerosi i dispositivi medici collegati in rete capaci di trasmettere e ricevere i dati e i parametri dei pazienti.

Questi sono solo alcuni degli esempi principali, che già oggi sono una realtà.
L'espansione dell'IoT è continuamente in crescita ed è legata allo sviluppo di (nuovi) sensori e alla capacità di collegarne alla rete un numero sempre maggiore.
L'avvento del 5G, per esempio, da questo punto di vista, costituisce un facilitatore perché, per unità di superficie, consente la connessione a un numero di oggetti molto maggiore dell'attuale.

Nella nostra vita quotidiana usiamo l'IoT quando sblocchiamo con un'app una bici in bike sharing, quando interpelliamo Alexa[13] (o assistenti vocali simili), quando programmiamo il riscaldamento di casa da remoto, quando l'app dell'autobus pubblico ci avvisa dell'arrivo o del ritardo del mezzo che stiamo aspettando…
Una delle ricadute più importanti della diffusione dell'IoT è la raccolta dei dati dai vari sensori collegati in rete. È una enorme mole di dati (si chiamano infatti *Big data*) che, opportunamente elaborati, possono fornire molte informazioni sui sistemi controllati dai sensori e sui loro utilizzatori.
Oggi i dati vengono spesso definiti il "nuovo petrolio", perché la loro raccolta ha potenzialmente un enorme valore economico.

[13] Amazon Alexa, https://it.wikipedia.org/wiki/Amazon_Alexa

Ad esempio, nel caso dell'applicazione dell'IoT all'industria, grazie ai dati sul funzionamento di un impianto, è possibile applicare la manutenzione predittiva e limitare l'interruzione della produzione, mentre nell'applicazione di *smart metering* è ragionevole ricavare indicazioni per ridurre i consumi.
I dati sul traffico collezionati dalle auto possono essere utilizzati in tempo reale dai navigatori per una migliore programmazione del viaggio e per la pianificazione di percorsi alternativi o, più banalmente, possono essere venduti a terzi interessati a quelle informazioni (teoricamente con tutti i consensi previsti dalla normativa sulla privacy!).

Il risvolto della medaglia

Qual è il risvolto della medaglia? La sicurezza.
Tutti i sensori e i dispositivi connessi in rete dovrebbero implementare "*by design*" strumenti e misure di sicurezza, che li proteggano da attacchi e violazioni.
Basti pensare a cosa accadrebbe se qualcuno prendesse il controllo dei sensori a bordo della nostra auto, attaccando il sistema in qualche suo punto vulnerabile: potremmo perdere completamente il controllo dell'auto.
Oppure potrebbe essere alterata la misura dei consumi dei contatori di casa o, ancora peggio, ad essere alterati potrebbero essere i parametri rilevati sui pazienti da dispositivi biomedicali, come ad esempio un pacemaker!
Purtroppo, questo non è uno scenario improbabile perché manca ancora l'abitudine a progettare la sicurezza "nativamente" per tutti questi sensori e il loro collegamento in rete.

Un altro elemento messo a rischio dall'IoT o, meglio, che è collegato all'uso dell'IoT, è la privacy: i dispositivi "connessi" generano dati che potrebbero essere stati raccolti o condivisi senza il nostro consenso.
Qui la porzione del sistema a dover essere protetta (soprattutto per evitare la condivisione non voluta) è quella relativa ai Big data e alla conservazione ed elaborazione di dati.

Campi di applicazione

Beatrice Ridolfi

Esistono differenti ambiti di applicazione dell'IoT e sono rappresentati dai vari contesti nei quali ci sono "oggetti" che possono "comunicare", sfruttando le connessioni di rete.
Con IoT si indica, quindi, qualunque dispositivo che scambia dati attraverso Internet, in modo mirato, in funzione dello specifico ambito di applicazione, e ha lo scopo di monitorare, controllare e trasferire informazioni per poi svolgere azioni.
Dove possiamo trovare dispositivi IoT?
Un classico esempio è nell'ambiente domestico, ovvero nelle smart home, per poi passare a smart building, e anche a smart city.
Un ulteriore ambito di applicazione molto interessante, su cui si sta investendo molto, è sicuramente quello medicale.

Smart home, smart building e smart city

All'interno dell'ambiente domestico possono essere vari i campi di applicazione dell'IoT, da non confondere con la domotica. Spesso, infatti, questi due termini vengono utilizzati come sinonimi, ma in realtà rappresentano due tecnologie diverse, che però hanno in comune l'obiettivo di facilitare la vita dell'utente, automatizzando alcuni specifici processi, consentendo un controllo da remoto, ed ottimizzando la gestione di un ambiente.

La *domotica* è un sistema "chiuso", costituito da dispositivi interconnessi tra loro, che permette di centralizzare la gestione di un ambiente domestico e coordinare diverse funzionalità, ma che non necessita delle comunicazioni con l'esterno.
Attraverso un'unica centralina, è quindi possibile gestire, ad esempio, l'impianto di riscaldamento, di climatizzazione, di illuminazione e gli elettrodomestici, permettendo di gestire anche dispositivi non smart (come lampadine ed elettrodomestici).
D'altra parte, con il termine *IoT* si raggruppano tutti i dispositivi che sono in grado di raccogliere informazioni da Internet o dall'ambiente circostante, elaborarle per poi svolgere azioni e semplificare la vita dell'utente. I dispositivi IoT sono quindi "aperti", e non interagiscono obbligatoriamente fra loro.
Con **smart home** s'intende quindi un ambiente domestico che utilizza dispositivi IoT.

Esempi di dispositivi IoT presenti in una smart home sono:

- sistemi di videosorveglianza e/o rilevamento, che permettono di controllare l'abitazione dallo smartphone quando si è fuori casa;
- frigoriferi, che monitorano i cibi contenuti e procedono con l'ordine nel caso qualche cibo sia terminato;

- dash button (come gli Amazon Dash Button), delle "chiavette", simili ai token che le banche utilizzano per la generano delle OTP (One Time Password)[14], che permettono di ordinare direttamente il prodotto che è stato associato al dispositivo, solamente premendo il tasto presente su di essi;
- robot per pulire la casa, in grado di mappare le stanze della casa per pulirle in modo efficace, e di ricevere comandi anche quando si è fuori casa, tramite smartphone;
- termostati intelligenti, in grado di imparare le abitudini degli abitanti della casa, prevedere le condizioni meteo e di conseguenza regolare o meno l'accensione dell'impianto di riscaldamento.

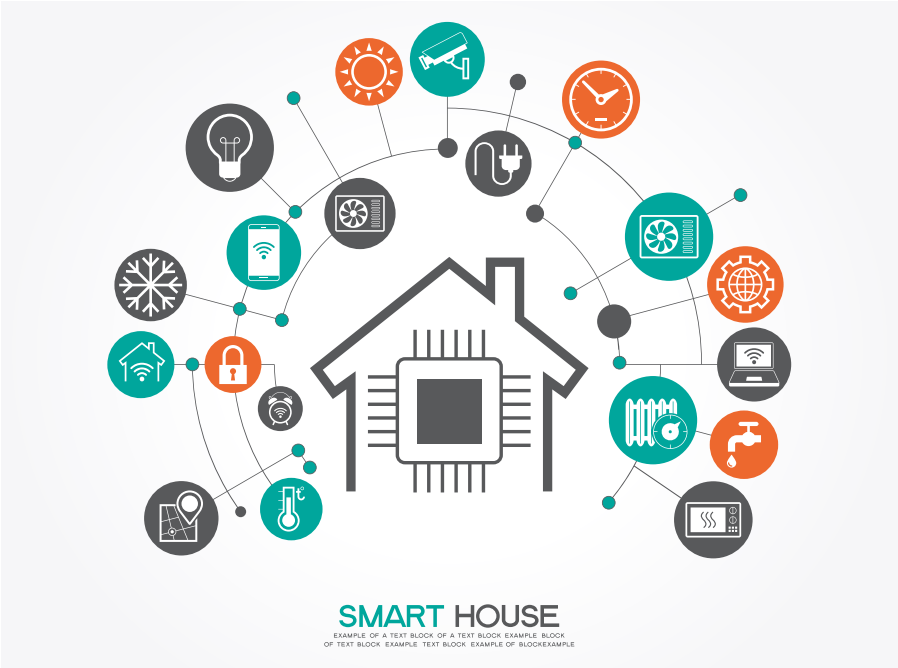


Figura 2: *La casa "smart"*

Esistono poi edifici intelligenti, o **smart building**, dotati di dispositivi IoT che interagiscono con l'ambiente esterno e che permettono di monitorare l'edificio, coniugando efficientamento energetico, bassi impatti ambientali e controllo automatizzato di strutture ed impianti, andando quindi a migliorare anche le attività di manutenzione e a ridurne i costi.

[14] One-Time Password, https://it.wikipedia.org/wiki/One-time_password

Al mondo attualmente esistono alcuni smart building già attivi, come ad esempio l'edificio *The Edge*, ad Amsterdam (Olanda), che al suo interno ha tantissimi sensori che permettono di monitorare e misurare in modo continuativo l'occupazione delle sale, il movimento delle persone, i livelli di illuminazione, l'umidità e la temperatura.
Inoltre, ogni persona che lavora nell'edificio ha a disposizione un'applicazione sullo smartphone, che permette di suggerire agli utenti dove trovare parcheggio, dove si possono trovare scrivanie libere o gli altri colleghi, e permette di segnalare problemi al team che gestisce le strutture.

Infine, esistono città intelligenti, o **smart city**, che consistono in città in cui sono presenti specifiche strategie di pianificazione urbanistica con l'obiettivo di migliorare la qualità della vita degli abitanti, utilizzando dispositivi IoT che permettono di gestire efficacemente le risorse, in modo intelligente e sostenibile.
Le smart city hanno alla base infrastrutture di reti wireless o in fibra per il broadband (ovvero banda larga, che sfruttano un'ampiezza di banda maggiore), reti di trasporto, energia e per l'ambiente, e utilizzano la tecnologia per i servizi di mobilità, scuola, turismo, sanità e gestione delle città stesse e, ovviamente, col tempo le smart city saranno sempre più popolate da smart building.
Le tecnologie adottate permettono quindi di relazionare le infrastrutture con gli abitanti della città.
Un esempio sono i semafori intelligenti, che diventano verdi quando non passano veicoli nel senso opposto, oppure sistemi innovativi per la gestione e lo smaltimento dei rifiuti, altre innovazioni ambientali, energetiche, di mobilità, comunicazione, e urbanistiche.

Smart Health

Un ambito di applicazione dei dispositivi IoT su cui si sta investendo molto e in rapida crescita è sicuramente l'ambito medicale e dell'healthcare, chiamato anche **Internet of Medical Things** (**IoMT**) o **Healthcare Internet of Things** (**HIoT**).
In questo contesto, i dispositivi IoT vengono utilizzati come dispositivi medici che raccolgono dati, i quali vengono poi forniti ai sistemi sanitari attraverso reti informatiche, permettendo quindi di monitorare e tenere traccia delle prestazioni vitali, e anche di attivare delle azioni successive (come, ad esempio, la somministrazione di farmaci).

I principali benefici dell'applicazione dell'IoT nell'ambito medicale e dell'healthcare comprendono:

- diagnosi più rapide, poiché la possibilità di monitorare e tenere sotto controllo i pazienti in tempo reale, in modo continuativo e anche da remoto, aiuta a diagnosticare più velocemente eventuali malattie o complicazioni di quelle esistenti;

- riduzione degli errori, poiché i dati raccolti tramite dispositivi IoT aiutano lo svolgimento di operazioni sanitarie con la riduzione di sbagli, sprechi e costi dei sistemi;
- trattamento proattivo, poiché la possibilità di monitorare i pazienti in tempo reale e in modo continuativo permette di prendere decisioni efficaci e di fornire cure mediche proattive, come la somministrazione di farmaci e anche la fornitura di assistenza nel caso in cui insorgano problematiche;
- riduzione dei costi, poiché l'utilizzo di dispositivi IoT permette di monitorare i pazienti in tempo reale, e permette di ridurre visite e ricoveri.

Figura 3: *Scenario di Smart Health*

I dispositivi IoMT si possono suddividere in tre categorie:

- in-body: dispositivi indossabili che integrano sensori per il monitoraggio dei parametri vitali, dotati di funzionalità di comunicazione remota che possono essere utilizzate per il monitoraggio. A questa categoria appartengono anche i dispositivi impiantati nel corpo del paziente, che sostituiscono una struttura biologica mancante, supportano una struttura biologica danneggiata, o migliorano una struttura biologica esistente;
- in-home: dispositivi utilizzati per il monitoraggio a casa dei pazienti, che necessitano di essere monitorati per malattie croniche oppure per il decorso post-ricovero;
- in-clinic: sistemi utilizzati all'interno di un'organizzazione sanitaria per attività di controllo e amministrative, come ad esempio dispositivi legati alla gestione del personale sanitario, dell'impiego di asset della struttura, del flusso dei pazienti, delle forniture di farmaci, e dell'ambiente.

Esempi di dispositivi IoMT per il monitoraggio della salute di un paziente sono:

- bracciali e applicazioni per il monitoraggio del battito cardiaco e del livello di ossigeno del sangue;
- dispositivi IoT che permettono di monitorare costantemente i livelli di glucosio nel sangue nei pazienti affetti da diabete, effettuando rilevamenti a intervalli regolari, interagendo con un'applicazione che memorizza i dati a lungo termine;
- dispositivi simili a "penne intelligenti" che permettono la somministrazione di insulina nei pazienti affetti da diabete, in grado di registrare in modo automatico l'ora, la quantità e la tipologia di insulina somministrata, e di consigliare l'iniezione di insulina al momento giusto, in base ai dati rilevati, e interagendo con un'applicazione che memorizza i dati a lungo termine;
  bracciali bluetooth e applicazioni per il monitoraggio degli effetti collaterali delle chemioterapie, i cui dati vengono inviati quotidianamente al medico di riferimento. Nel giugno 2018, ASCO (American Society of Clinical Oncology) ha presentato i dati di uno studio clinico su pazienti in terapia per neoplasie maligne all'area della testa e del collo, i quali utilizzavano dispositivi IoT per il monitoraggio degli effetti collaterali delle terapie chemioterapiche.
  Lo studio ha dimostrato che i pazienti che utilizzavano questo sistema di monitoraggio basato su dispositivi IoT hanno manifestato sintomi meno gravi, correlati al cancro e al suo trattamento, rispetto ai pazienti che svolgevano le classiche visite mediche regolari.
  Questo perché i dispositivi IoT hanno permesso una più rapida identificazione e un più puntuale trattamento degli effetti collaterali nel momento in cui si presentavano.
- pacemaker "intelligente", in grado di regolare automaticamente i loro parametri di funzionamento sulla base delle informazioni che raccolgono e analizzano dal cuore del paziente. Questi dispositivi sono in grado di variare automaticamente il ritmo cardiaco sulla base dell'attività fisica del paziente, permettendo quindi il giusto ritmo in ogni momento della vita quotidiana, rilevando eventuali aritmie e reagendo per fornire la migliore terapia;
- inalatori "intelligenti" per il controllo dei sintomi e del trattamento dei pazienti asmatici, che utilizzano un sensore collegato ad un inalatore bluetooth, entrambi connessi ad un'applicazione. Questi inalatori permettono di capire la causa delle crisi asmatiche, di tenere traccia dell'uso dei farmaci e di fornire anche previsioni sugli allergeni;
- lenti a contatto "intelligenti" che hanno l'obiettivo di monitorare e trattare alcune condizioni dell'occhio o alcune malattie, come ad esempio il glaucoma. In particolare, queste lenti a contatto sono in grado di monitorare e registrare automaticamente i cambiamenti nei parametri degli occhi, segnali che possono evidenziare il rischio di glaucoma.

Sono poi in fase sperimentale alcune lenti a contatto per i pazienti affetti da glaucoma che, oltre a misurare costantemente il livello della pressione dell'occhio, saranno in grado di somministrare un medicinale a livello corneale in caso di necessità. Essendo i dispositivi IoT così diffusi e così utilizzati in diversi ambiti che riguardano la vita quotidiana di tutti noi, risulta quindi di fondamentale importanza proteggere e mantenere sicuri sia i dispositivi stessi che i dati da essi trattati.

Big data e analisi tramite tecniche di intelligenza artificiale

Rosa Fiorenza

La società in cui viviamo è sempre più dipendente dalla tecnologia, dagli strumenti e dai servizi digitali che sono resi disponibili dalla tecnologia stessa.
Il numero di oggetti digitali connessi cresce in modo esponenziale, grazie alla diminuzione dei costi IT e all'aumento del valore che si ricava dalla connessione, archiviazione ed elaborazione dei dati forniti da tutti questi oggetti.
Tutti questi dati sono funzionali a uno scopo, ma una volta raccolti possono essere utilizzati per molte altre forme di analisi, correlazione e modellazione ed è evidente per tutti come questi abbiano assunto una rilevanza fondamentale per la nostra società.
Analizzare grandi moli di dati, i cosiddetti Big Data, permette di generare nuova conoscenza utile per prendere decisioni più consapevoli, in ambito business e non solo.

Figura 4: *Le fonti dei Big data*

Partiamo dalla definizione. Cosa si intende per Big Data?
L'espressione Big Data indica una raccolta di dati informativi così estesa in termini di **volume**, **velocità** e **varietà** da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza.

Questa definizione dei Big data attraverso le tre V - volume, velocità e varietà - è stata coniata nel 2001 da Doug Laney, allora Vicepresidente e Service Director dell'azienda Meta Group.
Vediamo nello specifico cosa si intende:

Volume

Si riferisce alla grandissima quantità di dati. Più dati riusciamo a collezionare, più informazioni interessanti e utili ai nostri scopi riusciremo a trarne.
Questo aspetto è cresciuto vertiginosamente nel tempo grazie ai costi sempre più bassi dei data storage, ossia i contenitori in cui i dati sono memorizzati e per l'altrettanta consistente riduzione dei costi per estrarre i dati ed elaborarli.

Varietà

Si riferisce all'eterogeneità delle sorgenti e della natura dei dati che possono essere raccolti.
Le categorie principali sono:

- *Dati Strutturati* ossia dati organizzati quali i fogli di calcolo e i database, che nel passato erano quasi le uniche fonti di dati analizzate e sono relativamente semplici da acquisire, conservare, interrogare e analizzare;
- *Dati Non Strutturati* quali e-mail, foto, video, dispositivi di monitoraggio, audio, post dei social media ecc. che sono più complessi da ordinare e analizzare per ricavarne informazioni utili.

Velocità

Si riferisce alla velocità di elaborazione dei dati, che è aumentata esponenzialmente negli ultimi decenni, permettendo elaborazioni quasi in tempo reale ("near real-time") e amplificando così le potenzialità dei Big data.
La definizione di Laney è stata poi arricchita nel tempo e sono state aggiunte altre tre V, meno tecniche e più orientate al business:

Veridicità

Si riferisce all'accuratezza dei dati e alla loro affidabilità.
Molti fattori possono influenzare la veridicità di un insieme di dati, e con i Big Data, ovviamente, le difficoltà aumentano a causa della molteplicità e numerosità delle sorgenti e delle tecnologie in uso e anche per la velocità di raccolta dei dati.
È evidente come la qualità, l'integrità e la correttezza dei dati utilizzati sia un aspetto critico e fondamentale perché i risultati delle analisi sui dati siano effettivamente utili ed efficaci. Se i dati di origine non sono corretti, le analisi saranno inutili.

Mentre il mondo si muove verso un processo decisionale automatizzato, in cui i computer fanno scelte al posto degli esseri umani, diventa imperativo che le organizzazioni siano in grado di fidarsi della qualità dei dati.

Variabilità

Si riferisce al fatto che, poiché i dati sempre più provengono da contesti variegati e arrivano in formati anche molto diversi tra loro, il loro significato può cambiare anche significativamente in funzione del contesto.

Valore

Si riferisce al valore intrinseco di tutti i dati. Senza analisi non è possibile evincere il tipo di informazione che i dati contengono e a cosa e a chi potrebbero essere utili. Per trovare il valore è quindi necessario analizzare i dati, ma non bastano gli strumenti computazionali, è necessario avvalersi anche di professionisti, gli "scienziati dei dati" (*data scientists*), che devono saper porre le giuste domande e interpretare le informazioni che i sistemi che elaborano i dati restituiscono.

Il termine Big Data non identifica, quindi, solo una grande quantità di dati, ma soprattutto dati utili a costruire un insieme di informazioni in grado di alimentare molte forme di generazione di conoscenza.
I Big Data consentono alle aziende di sfruttare al meglio sia i dati storicizzati nel tempo che i dati generati in tempo reale dalle catene di approvvigionamento, dalla produzione, dai processi e dai comportamenti dei clienti.
Le aziende che sono in grado di individuare i modi migliori per sfruttare gli impatti dei Big Data hanno sicuri benefici in termini di aumento dell'innovazione, competitività sul mercato e crescita finanziaria.
Riportando la definizione nella nostra vita quotidiana, possiamo immaginare i Big Data come un enorme insieme di informazioni su tutti noi e sulle attività che facciamo ogni giorno e nelle situazioni più disparate.

Ad esempio, dati relativi a dove facciamo shopping, a quali prodotti acquistiamo, ai siti web che visitiamo, alle mete dei nostri viaggi, ai nostri post sui social media ecc. Le aziende utilizzano i Big Data per estrarre informazioni vitali per il loro business e i loro scopi, con obiettivi molteplici, ossia migliorare la propria efficienza, offrire servizi migliori, creare campagne pubblicitarie più efficaci o sviluppare prodotti che siano di maggiore interesse per i propri clienti.

Intelligenza Artificiale

Che cosa si intende per Intelligenza Artificiale?
"L'Intelligenza Artificiale studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi hardware e sistemi di programmi software atti a fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana." (Enciclopedia Treccani)
L'obiettivo di questa disciplina è quello di emulare l'intelligenza umana, affinché alcune prestazioni dell'intelligenza umana (per esempio la capacità di risolvere problemi con procedimenti inferenziali) possano essere fornite da una macchina.

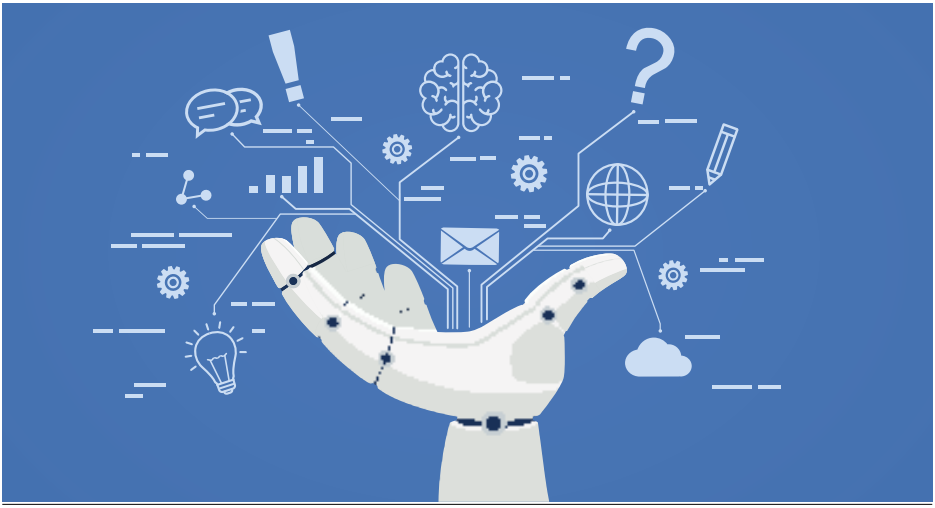


Figura 5: *L'intelligenza artificiale*

L'idea nasce dal matematico Alan Turing che, dopo aver decodificato Enigma[15], la macchina per cifrare e decifrare messaggi usata dai nazisti, e aiutato le Forze Alleate a vincere la Seconda guerra mondiale, ha cambiato la storia una seconda volta ponendosi una semplice domanda: le macchine possono pensare?
Il documento di Turing "Computing Machinery and Intelligence"[16] e il suo "Turing Test"[17] hanno definito l'obiettivo fondamentale e la visione dell'Intelligenza Artificiale.

[15] https://it.wikipedia.org/wiki/Enigma_(crittografia)

[16] https://en.wikipedia.org/wiki/Computing_Machinery_and_Intelligence

[17] Test di Turing, https://it.wikipedia.org/wiki/Test_di_Turing

Il Test di Turing è un test per verificare la capacità di una macchina di esibire un comportamento intelligente equivalente o indistinguibile da quello di un essere umano.

Turing propose che un valutatore umano giudicasse le conversazioni in linguaggio naturale tra un essere umano e una macchina progettata per generare risposte simili a quelle umane. Il valutatore è consapevole che uno dei due partner nella conversazione è una macchina e tutti i partecipanti sono separati.
La conversazione è limitata a un canale di solo testo come la tastiera e lo schermo di un computer. Se il valutatore non è in grado di distinguere in modo affidabile la macchina dall'uomo, si conclude che la macchina ha superato il test.
I risultati dei test non dipendono dalla capacità della macchina di dare risposte corrette alle domande, ma solo da quanto le sue risposte assomigliano a quelle che un essere umano darebbe.
L'Intelligenza Artificiale è la branca dell'informatica che cerca di rispondere affermativamente alla domanda di Turing, ossia è l'impresa di replicare o simulare l'intelligenza umana nelle macchine.
Per comprendere meglio l'evoluzione e l'applicazione dell'Intelligenza Artificiale dobbiamo partire dalla sua classificazione definita sulla base delle capacità.

In particolare, distinguiamo tre tipi di Intelligenza Artificiale, che ne identificano l'applicabilità tecnica:

- Narrow AI (IA debole): è la forma di Intelligenza Artificiale più utilizzata e di maggior successo. Simula l'intelligenza umana per eseguire un singolo compito specifico all'interno di un contesto limitato. Implementa un singolo insieme di abilità cognitive per eseguire una sola particolare funzione, operando in un intervallo predefinito limitato, e non può essere generalizzata per eseguire altre attività.
- Alcuni esempi di Narrow AI sono gli assistenti personali virtuali (come Siri[18], Alexa, ecc.), i programmi di riconoscimento delle immagini, le auto a guida autonoma, l'algoritmo di ranking delle pagine di Google, Google Translate[19], i motori di raccomandazione, le chatbot[20], i filtri antispam, ecc.
- Ad esempio, il software di riconoscimento facciale può riconoscere un volto familiare, ma non può rispondere a un comando vocale. Allo stesso modo, un assistente personale virtuale può rispondere a un comando vocale, ma non può rispondere ad un gesto o un'espressione del volto.

---

[18] Siri, https://it.wikipedia.org/wiki/Siri

[19] https://translate.google.com/

[20] Chat bot o chatbot, https://it.wikipedia.org/wiki/Chat_bot

- L'implementazione del machine learning (modello basato sull'apprendimento dai dati storici, identificando modelli di dati e correlazioni tra dati e risultati) e del deep learning (modello basato sull'estrazione di concetti rappresentativi dai dati stessi) rientra in questa tipologia di IA.
- General AI (IA forte): implementazione di un insieme completo di abilità cognitive non limitato da alcun contesto. L'obiettivo è rendere le macchine in grado di applicare l'intelligenza a qualsiasi compito. I ricercatori non sono ancora stati in grado di realizzare un General AI e in teoria, questo, per essere definito tale, dovrebbe superare il test di Turing di cui abbiamo parlato prima. I ricercatori oggi lavorano alacremente in questo campo con l'obiettivo di riuscire a creare un primo esempio reale di General AI e alcuni ambiti di sviluppo sono: la visione artificiale, l'elaborazione del linguaggio naturale, la robotica, machine learning e deep learning, ecc. Comunque, considerando che si stima che un cervello umano faccia un miliardo di calcoli al secondo mentre il supercomputer più veloce impiega molti minuti per eseguire lo stesso numero di calcoli, possiamo dedurre che non vedremo risultati tangibili presto.
- Super AI: si riferisce all'Intelligenza Artificiale che può essere superiore all'intelligenza umana, ossia macchine in grado di apprendere, ragionare e risolvere i problemi meglio degli umani.

Questa classificazione è stata definita da Arend Hintze, un assistente di biologia integrata e informatica presso la Michigan State University, in un suo articolo del 2016.

Sulla base di queste funzionalità, sono state definite quattro tipologie di IA:

1. Macchine Reattive (Reactive Machine): come si evince dal nome, sono macchine in grado di usare intelligenza solo nel percepire e reagire al mondo di fronte a loro.
   - Una macchina reattiva non ha memoria, e non può fare affidamento su esperienze passate per prendere decisioni nel presente.
   - Percepire il mondo direttamente significa che le macchine reattive sono disegnate per completare solo un numero limitato di compiti specializzati.
   - Limitare intenzionalmente la visione del mondo di una macchina reattiva non è una scelta per ridurre i costi, ma ha l'obiettivo di renderla più affidabile e attendibile, facendo in modo che reagisca sempre allo stesso modo verso gli stessi stimoli.
   - Un esempio famoso è "*Deep Blue*"[21], un supercomputer progettato da IBM negli anni '90 per giocare a scacchi e che riuscì, nel 1997 a sconfiggere il grande maestro internazionale Garry Kasparov (anche se Kasparov sollevò il

[21] IBM Deep Blue, https://it.wikipedia.org/wiki/IBM_Deep_Blue

dubbio che ci fosse stato un intervento umano durante la partita per aiutare il supercomputer a non cadere nelle trappole che il grande campione gli tendeva durante il gioco ed effettivamente, dopo molti anni, diversi testimoni confermarono la sua tesi). Deep Blue vedeva i pezzi sulla scacchiera e reagiva sulla base delle regole impostate, senza poter usare le esperienze precedenti e, quindi, senza migliorare con la pratica.

2. Memoria Limitata (Limited Memory): macchine che hanno l'abilità di conservare dati e predizioni precedenti quando raccolgono informazioni e di ponderare potenziali decisioni; essenzialmente sono macchine che guardano nel passato per trovare indizi su cosa potrebbe accadere dopo.
   - Questa intelligenza è più complicata e presenta possibilità maggiori delle macchine reattive.
   - Per realizzare una macchina LM si deve creare un insieme di dati di allenamento e definire il modello di machine learning da utilizzare, il modello deve essere in grado di creare previsioni e deve essere in grado di ricevere feedback umani o ambientali, questi feedback devono essere conservati come dati e questi passaggi vanno ripetuti ciclicamente.
   - Un esempio di applicazione del modello di Memoria Limitata sono le automobili a guida autonoma. Le auto hanno una memoria statica per identificare segnali stradali, semafori e indicatori di corsia e hanno una memoria dinamica in cui memorizzano la velocità e le direzioni delle auto circostanti. Utilizzando regole e conoscenze dalla memoria statica e percependo il loro ambiente attuale sotto forma di ricordi a breve termine, riescono a guidare autonomamente insieme ad altri veicoli e conducenti umani. Tuttavia, la loro memoria della percezione della velocità e delle direzioni di altre auto è di breve durata, solo sufficiente per completare il loro viaggio attuale.
   - Non possono imparare o eccellere nella guida dalle loro esperienze di guida autonoma nel tempo.
   - L'Intelligenza Artificiale a memoria limitata è utilizzata per l'apprendimento automatico (machine learning). La maggior parte delle attuali applicazioni di machine learning si basa su un'Intelligenza Artificiale a memoria limitata e l'uso del machine learning sta portando un cambio di paradigma in ogni settore dell'industria tecnologica.
3. Teoria della mente (Theory Of Mind): è solo teorico, non abbiamo ancora sviluppato capacità tecnologiche e scientifiche necessarie per realizzare questo tipo di modello.
   - Il concetto è basato sul fatto che gli esseri viventi hanno pensieri ed emozioni che influenzano il proprio comportamento.
   - In termini di IA, questo significa che una macchina potrebbe comprendere cosa umani e animali provano e come prendono decisioni attraverso autori-

flessione e determinazione, e che poi utilizzerà questa informazione per prendere le proprie decisioni.
- Essenzialmente le macchine sarebbero in grado di capire e processare, in tempo reale, il concetto di "mente" e le variazioni delle emozioni nel prendere decisioni.

4. Auto-coscienza (Self-Awareness): in questo caso parliamo di Intelligenze Artificiali che diventano consapevoli di sé stesse, ossia l'obiettivo ultimo dell'Intelligenza Artificiale.
   - Questo tipo di IA possiede coscienza ad un livello umano e capisce la sua stessa esistenza nel mondo, così come la presenza e lo stato emotivo degli altri. Sarebbe in grado di capire di cosa gli altri hanno bisogno non solo da ciò che viene comunicato ma anche da come viene comunicato. E soprattutto le macchine sarebbero consapevoli dei loro tratti, della loro condizione e dei propri stati interni inclusi sentimenti, fede e credenze.
   - Una macchina autocosciente non avrebbe bisogno di prendere in prestito la coscienza da un modello, ma avrebbe la sua coscienza, sapendo cosa vuole e cosa deve fare. Una tale macchina sarebbe di fatto una creatura vivente.
   - Chiaramente oggi, allo stato dell'arte dell'evoluzione scientifica, parliamo di fantascienza e, trattando di auto-coscienza e consapevolezza, anche di filosofia.

Big data e Intelligenza Artificiale

Un fattore che ha contribuito alla crescita e all'importanza dell'IA nell'ultimo decennio è il risultato dei Big data.
I motori di ricerca, i social media, l'e-commerce, l'Internet delle cose (IoT) e le analisi aziendali hanno evidenziato l'importanza stessa dei dati. Internet ha reso i dati disponibili in tempo reale da qualsiasi luogo e ovunque, e le organizzazioni hanno bisogno di informazioni rapide da quell'enorme quantità di dati.
Gli esseri umani non riescono a gestire attività così massive, ridondanti e pesanti di analisi dei dati, mentre i computer mancano di funzioni cognitive simili a quelle umane per elaborare i dati in modo indipendente. L'unica alternativa è "infondere intelligenza umana" nei computer, facendo sì che imparino dai dati invece di agire sulla base di una programmazione esplicita.
Big data e IA hanno una relazione sinergica. IA richiede un'enorme quantità di dati per imparare e migliorare i processi per prendere decisioni e l'analitica dei Big data sfrutta la IA per migliorare l'analisi dei dati.

Con questa convergenza, è possibile sfruttare più facilmente avanzate capacità analitiche come "**augmented analytics**" (analisi che applica in modo esplicito l'apprendimento automatico e i processi del linguaggio naturale per identificare i modelli che gli esseri umani potrebbero perdere nei dati; "impara" mentre analizza,

rendendo più veloce e più potente l'analisi, e lasciando agli esseri umani il compito di convalidarla e correggerla lungo la strada) oppure "**predictive analytics**" (funziona allo stesso modo dell'augmented analytics ma concentrandosi su tecniche di apprendimento automatico che prevedono i risultati futuri in base ai dati storici).

Figura 6: *L'Intelligenza artificiale usa i Big data*

Inoltre, facilita ovviamente il recupero più efficace di informazioni utili e utilizzabili nella grande riserva di dati. Un esempio banale potrebbe essere quello di una grande catena di supermercati che, basandosi sui dati storici degli acquisti, può essere in grado di prevedere quante confezioni di barattoli di pelati verranno acquistate in un dato giorno della settimana e assicurarsi che gli scaffali contengano scorte sufficienti. Analizzare grandi moli di dati permette di generare nuova conoscenza utile per prendere decisioni più consapevoli, in ambito business e non solo.
I Big Data Analytics hanno un impatto in tutti i processi, dalla personalizzazione della comunicazione con il cliente all'efficientamento dei processi produttivi, passando per la gestione dei flussi e delle emergenze.

Con le analisi di Big data alimentate da Intelligenze Artificiali, è possibile oggi per le aziende migliorare le prestazioni e l'efficienza aziendale:
- anticipando e sfruttando l'industria emergente e i trend del mercato;
- analizzando il comportamento del consumatore e automatizzando la profilazione del cliente;
- personalizzando e ottimizzando la prestazione delle campagne di marketing digitale;

• usando un sistema di supporto decisionale intelligente.
L'IA può supportare in tutte le fasi del ciclo di vita dei Big Data, può identificare tipi di dati, trovare possibili connessioni ed estrarre conoscenza e valore.
Può essere usata per automatizzare e velocizzare le attività sui dati, comprese la produzione di modelli di dati.
Può riconoscere pattern comuni di errori umani, trovando e risolvendo possibili difetti nelle informazioni.
Può imparare guardando come l'utente interagisce con un programma di analisi, trovando velocemente informazioni inaspettate da grandi insiemi di dati, e può anche imparare a riconoscere leggere differenze nei significati, o sfumature in specifici contesti.
Può segnalare agli utenti anomalie o modelli inaspettati nei dati.
Un esempio di utilizzo virtuoso dei Big data e dell'IA è quello nell'ambito della gestione della pandemia COVID-19.
I Big data e gli strumenti analitici, in questo caso, hanno fornito varie soluzioni come il rilevamento di casi COVID-19 esistenti, la previsione di future epidemie, l'anticipazione di potenziali agenti preventivi e terapeutici e l'assistenza nel processo decisionale informato.
Nell'ambito specifico della Cyber Security, la combinazione dei Big data con l'Intelligenza Artificiale ha assunto un ruolo cruciale, ossia sta sempre più diventando un'arma usata dagli attaccanti per far evolvere le tecniche di attacco ma allo stesso tempo è sempre più usata per far evolvere la capacità di predizione e di rilevamento delle minacce.
I dati che fluiscono all'interno degli ambienti aziendali contengono informazioni preziose che possono essere utilizzate, attraverso l'uso di strumenti analitici corretti, per identificare e mitigare le minacce, di fatto riducendo i rischi all'interno delle aziende.

Quindi applicando le capacità dei Big Data alle sfide della sicurezza, si passa da un approccio alla sicurezza reattivo a uno più proattivo, ottenendo visibilità sui dati non strutturati che costituiscono oggi la percentuale maggiore delle informazioni che un'azienda riceve.
Le tecnologie di Big Data Analytics possono consentire l'individuazione di comportamenti potenzialmente fraudolenti o rischiosi, correlando segnali deboli, ossia che non presentano singolarmente elementi chiari di rischio, provenienti da fonti multiple ed eterogenee (log, transazioni, social media etc.).
Facciamo un esempio su un potenziale uso fraudolento di un conto.
Se un conto per le buste paga registra improvvisamente dei trasferimenti di denaro verso un Paese con il quale non era mai stata precedentemente effettuata alcuna operazione, il conto deve essere monitorato poiché c'è il rischio che venga utilizzato, ad esempio, per il finanziamento di organizzazioni illegali. L'azione in sé stessa del trasferimento di soldi non è indicativa di un'azione illegale, ma se questa, ana-

lizzandola rispetto a tutti i dati sull'uso del conto negli anni, si discosta da quanto fatto precedentemente, allora può indicare un potenziale rischio.
Come abbiamo già detto, il ruolo crescente che la tecnologia ha nelle nostre vite quotidiane e nei luoghi di lavoro, la crescita del cloud e delle tecnologie IoT e mobili hanno innescato una sorta di reazione a catena in termini di rischi per la sicurezza.
La capacità di riconoscere e identificare le diverse fasi di un attacco informatico è un fattore chiave nella protezione degli asset informatici. Tradizionalmente il riconoscimento di un attacco viene effettuato per mezzo di sistemi in grado di individuare alcuni tipi di minaccia, bloccandoli, per mezzo di "sensori" o sonde che rilevano le attività in corso sui sistemi e identificano le anomalie, e da personale altamente specializzato in grado di interpretare i segnali provenienti dai sistemi per riconoscere potenziali situazioni di rischio, indagarle e, nel caso, reagire per arrestare l'attacco.
Questo modo, per così dire "tradizionale", di procedere sta però entrando in crisi a causa dell'enorme aumento dei sistemi da proteggere e della crescente sofisticazione dei mezzi a disposizione degli attaccanti, che possono usare numerose tecniche per superare le barriere tradizionali fornite ad esempio dagli antivirus.
Quindi fronteggiarle con gli strumenti tradizionali rischia di essere proibitivo, in termini di risorse economiche e umane necessarie.
In questo scenario, l'introduzione di sistemi basati sull'Intelligenza Artificiale comporta evidenti benefici, legati alla capacità di trattare volumi di dati più elevati e alla maggiore velocità nell'esecuzione di attività di risposta all'attacco.

Possiamo identificare due aree principali in cui l'impiego di metodi basati su algoritmi di Intelligenza Artificiale può aiutare a rinforzare la gestione della sicurezza informatica.
La prima area è costituita dai sistemi di rilevazione di situazioni anomale potenzialmente pericolose. La sicurezza informatica è un settore nel quale la mole di dati generati è elevatissima, e contiene informazioni su chi o che cosa si collega ai sistemi da proteggere, sugli accessi ai dati, informazioni sulle connessioni verso siti esterni, sui cambiamenti apportati ai sistemi, e informazioni o segnalazioni generate dagli stessi sistemi di sicurezza.

Insomma, una mole vastissima di dati eterogenei, che vanno interpretati e confrontati tra loro per individuare quelle situazioni "anomale" che possono indicare un potenziale attacco in corso, ovvero stiamo parlando di Big Data che necessitano di algoritmi di Intelligenza Artificiale per estrarre conoscenza dai dati.

Ci sono già diverse soluzioni sul mercato realizzate per identificare quegli eventi, o insiemi di eventi, che costituiscono una deviazione rispetto ai comportamenti "medi" rilevati.

Con il loro impiego è possibile aiutare gli esperti umani a tenere sotto controllo un numero di sistemi molto più elevato di quanto sarebbe possibile ricorrendo solo a tecniche tradizionali.
Una seconda area è quella del supporto decisionale per mezzo dei sistemi esperti, quali ad esempio quelli usati negli help desk telefonici per aiutare gli operatori a fornire risposte ai problemi degli utenti, e che, quindi, possono essere impiegati con successo anche nell'ambito della sicurezza informatica. Grazie a loro, è possibile velocizzare e standardizzare l'analisi di determinati eventi, per stabilire se si tratti o meno di incidenti di sicurezza, e mettere in atto delle procedure uniformi di risposta, rendendo più veloci ed efficaci le attività di rilevazione e risposta agli incidenti.
Un esempio rappresentativo potrebbe essere l'uso di tecniche di Machine Learning su Big Data per supportare gli utenti in modo semplice, veloce ed efficace nel riconoscere le e-mail di phishing.
Il phishing è un tipo di truffa attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. Il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi.
All'interno di una e-mail di phishing nella maggior parte dei casi si trova un link, il cui testo a supporto di esso, inviterà l'utente a usarlo. Molte soluzioni utilizzano punteggi di reputazione per stabilire la rischiosità del link, che non garantiscono la tempestività necessaria perché richiedono che quella minaccia sia già conosciuta.
Invece, una piattaforma di machine learning addestrata per riconoscere un link malevolo da uno benevolo permetterebbe di calcolare la reputazione di una URL in pochi secondi, gestendo in modo efficace anche gli attacchi 0-day, ossia gli attacchi nuovi non ancora conosciuti.
È molto facile immaginare come queste tecnologie possano, d'altro canto, essere usate per migliorare i metodi e aumentare l'estensione degli attacchi informatici.
La riduzione dei costi grazie all'uso della IA permette l'aumento della numerosità e della velocità degli attacchi, comportando di fatto una crescita degli attacchi esistenti.
Le potenzialità dell'IA potrebbero agevolare la creazione di nuove minacce e rendere le minacce già esistenti più efficaci, più specifiche e molto meno rilevabili.

Rischi legati all'uso di Big data e Intelligenza Artificiale

Impatti sulla privacy

Gran parte dell'analisi dei dati personali oggi, come l'uso di algoritmi di ricerca, motori di raccomandazione e la tecnologia pubblicitaria, sono guidate dall'apprendimento automatico e dalle decisioni degli algoritmi.
Man mano che l'Intelligenza Artificiale si evolve amplifica la capacità di utilizzare le informazioni personali in modi che possono interferire con la privacy delle persone.

L'Intelligenza Artificiale, così come purtroppo molte delle tecnologie IT, nella maggioranza dei casi non rispetta il principio della **privacy by design** poiché la privacy non è solitamente al primo posto tra i requisiti nello sviluppo delle tecnologie di Intelligenza Artificiale.
C'è un alto rischio per i diritti e le libertà degli individui nel trattamento dei dati personali da parte dell'IA. Alcune delle sfide più importanti per la privacy legate all'uso della IA includono:

- dati esistenti più a lungo rispetto ai soggetti umani che li hanno creati, dovuto ai bassi costi di archiviazione dei dati;
- dati utilizzati oltre il loro scopo originariamente immaginato;
- dati raccolti su persone che non sono l'obiettivo dell'analisi.

I dati raccolti tramite l'Intelligenza Artificiale sollevano anche problemi di privacy come il consenso informato liberamente dato, la possibilità di rinunciare, limitare la raccolta dei dati, descrivere la natura del trattamento dell'IA e persino essere in grado di eliminare i dati su richiesta. Il problema principale è che i soggetti umani dei dati raccolti, spesso potrebbero non sapere che sono stati raccolti dati su di loro e di conseguenza non hanno la possibilità di esercitare i propri diritti.
Mentre la maggior parte delle organizzazioni lavora costantemente per raggiungere e mantenere la conformità alla privacy e ai principi etici nell'uso di informazioni personali sensibili, nell'Intelligenza Artificiale le sfide possono essere significativamente diverse sia nel contenuto che nelle dimensioni.

Deepfake

I deepfake[22] sono video, immagini o file audio creati artificialmente utilizzando modelli di deep learning. Ad esempio, le sequenze video esistenti vengono utilizzate e falsificate sostituendo i volti. Sono destinati ad apparire il più realistici possibile, anche se sono stati generati da un modello ML.
Oltre a utilizzare i deepfake per i video privati, possono anche essere utilizzati per diffondere disinformazione mirata.
La fase di "learning" di questi modelli e di conseguenza la creazione di buoni deepfake costituiscono un passaggio molto dispendioso in termini di tempo e calcolo. Grazie però ai grandi progressi nel campo dell'elaborazione grafica (GPU), questa tecnica è diventata accessibile a tutti, poiché i costi sono diminuiti significativamente.

Molti file deepfake rientrano in una delle seguenti categorie:

- **Face Swapping:** il volto e le espressioni facciali della persona A devono essere proiettati sul corpo della persona B. Questo può anche arrivare a sostituire l'intero

[22] Deep fake, https://it.wikipedia.org/wiki/Deepfake

corpo della persona B in un video o in un'immagine con il corpo della persona A.
- **Body Puppetry:** i movimenti, i gesti o le espressioni facciali della persona A vengono registrati e questi devono poi essere artificialmente posti sulla persona B.
- **Voice Swapping:** un testo scritto viene letto nel modo più autentico possibile con la voce di una persona. Questo metodo può anche essere combinato con il Body Puppetry, per esempio.

I deepfake possono rappresentare una minaccia in molte aree della vita quotidiana. Ad esempio, è possibile che questi file artificiali vengano utilizzati per perpetrare frodi in azienda. Si può ricevere, ad esempio, una chiamata dal superiore o anche dalla direzione nel modo più realistico possibile, con lo scopo di ottenere trasferimenti di denaro.
Quando sentiamo le voci reali di colleghi o superiori, è improbabile che siamo sospetti come quando riceviamo un'e-mail di phishing con un link dannoso allegato.
Oltre a ciò, ci sono pericoli molto più gravi legati alla diffusione di deepfake di alta qualità che possono essere utilizzati per diffondere disinformazione mirata colpendo non solo singoli individui, ma nel peggiore dei casi arrivando a portare sconvolgimenti nella società.

Perdita dei posti di lavoro

Come detto, l'uso dei Big Data può fornire un numero significativo di vantaggi per le aziende che desiderano che le loro strategie e decisioni siano supportate dall'enorme quantità di dati a disposizione. Di conseguenza, il mercato dei Big Data è cresciuto rapidamente negli ultimi anni, ma nonostante il grande entusiasmo non tutti hanno una visione positiva della tecnologia.
Alcuni temono che i Big Data, specialmente in combinazione con altre tecnologie come l'Intelligenza Artificiale, possano costare il lavoro ai lavoratori nel prossimo futuro, se non sta già accadendo.
In realtà, come riportato anche in una ricerca svolta da Eurofound (European Foundation for the Improvement of Living and Working Conditions)[23] sull'impatto occupazionale della digitalizzazione in generale, se, dal punto di vista dell'occupazione, la perdita di posti di lavoro legata all'automazione quando le macchine sostituiscono l'input umano è ampiamente discussa, allo stesso tempo, la creazione di posti di lavoro è innescata dall'emergere di nuovi profili professionali adattati allo sfruttamento delle nuove tecnologie, nonché dall'aumento della domanda di prodotti e servizi basati sulla tecnologia a causa di prezzi più bassi o di nuovi mercati, gruppi di clienti o aree di domanda.

[23] European Foundation for the Improvement of Living and Working Conditions https://en.wikipedia.org/wiki/European_Foundation_for_the_Improvement_of_Living_and_Working_Conditions

Chiaramente però i lavoratori che svolgono attività poco qualificate rischiano di perdere il lavoro e devono gestire la transizione verso l'era digitale.
Questa è una sfida non solo per i lavoratori interessati, ma anche per i datori di lavoro, che si trovano di fronte alla carenza di competenze e alla necessità di supportare i lavoratori nell'adattamento ai processi di produzione e fornitura di servizi differenti, e per le istituzioni.

Bias algoritmico causato da dati errati

Quando parliamo di pregiudizio dell'IA ci riferiamo a una IA che prende decisioni che sono sistematicamente ingiuste per determinati gruppi di persone.

In generale, il pregiudizio algoritmico deriva dalle scelte che gli sviluppatori fanno nella creazione dell'algoritmo, piuttosto che da un esplicito motivo discriminatorio. Una delle scelte critiche nella costruzione di un algoritmo è decidere quale risultato deve prevedere. La scelta di un risultato richiede giudizi di valore soggettivi su come definire concetti come, ad esempio, produttività o affidabilità creditizia in modi misurabili e quantificabili. Questa è una scelta chiave perché modella ciò che l'algoritmo farà e i tipi di dati che considererà quando prende una decisione.
Dopo aver scelto un risultato, i progettisti selezionano gli input o le variabili predittive che un algoritmo deve considerare quando tenta di prevedere il risultato.

La scelta su quali dati di "learning" usare e a quali variabili un algoritmo ha accesso può introdurre pregiudizi se i progettisti forniscono solo i dati che sono più favorevoli a un gruppo rispetto a un altro o utilizzano dati soggettivi che sono distorti.
Un altro problema è che gli input di dati che sono rilevanti per prendere decisioni accurate possono riguardare attributi come razza o genere a causa di pregiudizi strutturali e storici.
Ad esempio, i dati sul reddito possono mostrare che gli uomini guadagnano più delle donne e i dati sugli arresti possono rivelare che gli uomini neri vengono arrestati a tassi più elevati rispetto agli uomini bianchi. Questi dati non sono imprecisi nel senso che travisano la realtà, ma piuttosto non riescono a tenere conto dei pregiudizi sistemici che hanno dato origine alle differenze nei dati.
Gli algoritmi che utilizzano ciecamente questi dati senza comprendere il contesto intorno a particolari disparità statistiche possono rafforzare e replicare modelli di discriminazione nelle decisioni che prendono.

Diversi studi hanno anche evidenziato il rischio che questi pregiudizi possano causare danni reali.
Uno studio pubblicato dal Dipartimento del Commercio degli Stati Uniti, ad esempio, ha rilevato che l'IA di riconoscimento facciale identifica erroneamente le persone di colore più spesso dei bianchi. Questa scoperta solleva preoccupazioni sul

fatto che, se utilizzato dalle forze dell'ordine, il riconoscimento facciale potrebbe aumentare il rischio che la polizia arresti ingiustamente le persone di colore. E in effetti, si sono già verificati arresti illeciti dovuti a una corrispondenza errata da parte del software di riconoscimento facciale.
Un altro studio pubblicato da Georgia Tech, ha scoperto che le auto a guida autonoma guidate dall'Intelligenza Artificiale hanno ottenuto risultati peggiori nel rilevare le persone con la pelle scura, il che potrebbe mettere a rischio la vita dei pedoni dalla pelle scura.
Per tutti questi motivi, oggi c'è una forte spinta perché ci sia un'azione legale che possa rappresentare un'opportunità non solo per sviluppare politiche che riducano al minimo questo tipo di discriminazione, ma anche per creare un sistema in cui i decisori ottimizzino gli algoritmi per l'equità e l'inclusione e li progettino in modo da indirizzare azioni e investimenti verso le comunità più vulnerabili e utilizzarli per costruire una società migliore e più equa.

Diseguaglianza socio-economica

La trasformazione dell'economia grazie alle tecnologie digitali, in particolare nell'Intelligenza Artificiale, sta ponendo un enigma preoccupante: queste tecnologie nella realtà sembra che non stiano facendo molto per far crescere l'economia, ma anzi che in qualche modo la disuguaglianza sociale e di reddito stia peggiorando.
In un saggio intitolato "The Turing Trap: The Promise & Peril of Human-Like Artificial Intelligence"[24], Erik Brynjolfsson, direttore dello Stanford Digital Economy Lab, cerca di rispondere alla seguente domanda: perché queste tecnologie non riescono a produrre una maggiore crescita economica e non stanno alimentando una prosperità più diffusa?

Secondo Brynjolfsson, il problema principale è che, nel tentativo di imitare l'intelligenza umana, ci si è concentrati solo sull'aspetto dell'automazione, che di fatto porta solo alla sostituzione dei lavoratori, piuttosto che estendere le capacità umane e consentire alle persone di svolgere nuovi compiti.
Quello che sta accadendo, quindi, è che i salari per la maggior parte delle persone si sono abbassati, mentre si è amplificato il potere di mercato di pochi che possiedono e controllano le tecnologie.

[24] https://digitaleconomy.stanford.edu/news/the-turing-trap-the-promise-peril-of-human-like-artificial-intelligence/

IoT e rischi di Cyber Security

Sofia Scozzari

La diffusione dell'*"Internet delle Cose"* è un fenomeno sempre più esteso che vede connessi a Internet oggetti, sensori e dispositivi disparati.
È stato previsto che entro il 2025 nel mondo ci saranno quasi 75 miliardi di dispositivi IoT connessi[25].
Un numero esorbitante di "oggetti", quindi, spesso definiti "*smart*" per indicare le loro capacità estese dal digitale, che, se da una parte comportano notevoli vantaggi, dall'altra espongono anche a numerosi rischi.

La minaccia principale deriva dalla percezione di questi dispositivi, che nella concezione generale sono solamente "cose", con lo stesso livello di trust riservato agli elettrodomestici di uso comune.
Certamente non ci aspettiamo di subire un cyber attacco dalla smart tv di casa!
Al contrario, essendo connessi in rete, questi oggetti andrebbero considerati alla stregua dei computer, soprattutto per quanto riguarda i rischi cyber che comportano.
Ogni dispositivo connesso in rete, infatti, è potenzialmente compromissibile.
Un cyber attacco a un dispositivo IoT, quindi, non è affatto una remota possibilità, anzi, è un'eventualità relativamente comune.
E qui di seguito esponiamo alcuni dati al riguardo.

Lo scenario dei Cyber attacchi in ambito IoT

Nel periodo dal 2018 al 2021 abbiamo classificato 45 cyber attacchi globali e di pubblico dominio incentrati sull'IoT[26], con una media di quasi un attacco al mese.
Questi rappresentano solo gli incidenti andati a buon fine e che hanno avuto risonanza mediatica, il che ci fa dedurre che il numero di attacchi totali avvenuti nella realtà sia certamente maggiore.

Prendendo in ogni caso in esame questo campione, notiamo che oltre due terzi degli attacchi (62%, vedi **Figura 7**) ha una gravità alta, ovvero ha comportato ripercussioni notevoli alle vittime e/o ad ulteriori entità coinvolte a causa dell'incidente.

Il restante terzo si divide tra eventi con severity media (20%), critica (13%) e bassa (5%).

---

[25] Statista: Iot number of Connected devices worldwide, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/#statisticContainer

[26] Fonte: Hackmanac Global Cyber Attacks Report 2018 – 2021, https://hackmanac.com

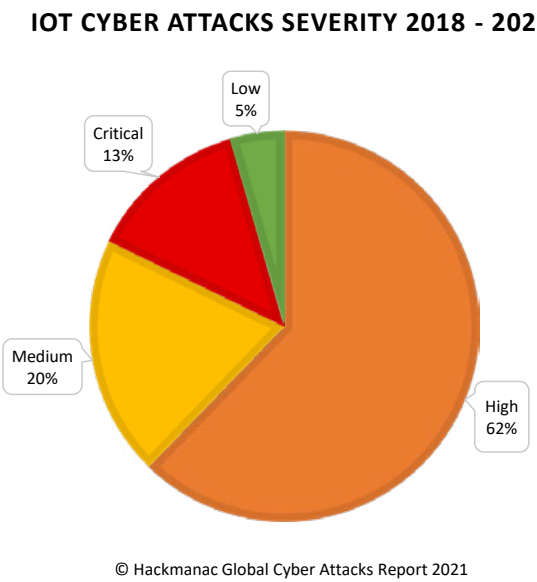


Figura 7: *Severity dei cyber attacchi in ambito IoT*

La motivazione principale dei cyber attacchi è il Cybercrime[27] (84% degli attacchi totali, vd. Fig. 8), in perfetta simbiosi con la tendenza globale: nel 2021 il crimine informatico causa, infatti, l'86% degli attacchi mondiali.
Un aspetto interessante riguarda però altre motivazioni che causano incidenti all'ambito IoT, anche se in misura minore: nel 7% dei casi lo spionaggio o il sabotaggio sono all'origine di questi eventi e, data la loro natura altamente riservata, probabilmente il dato è sottostimato rispetto alla realtà.
Un ulteriore 7% è causato da attività di *Hacktivism*[28], un fenomeno che globalmente tende invece a sparire (1% degli attacchi totali nel 2021).
Infine, una minoranza degli attacchi (2%) deriva da operazioni di Information Warfare / Cyber Warfare[29], ovvero tutte le attività correlate con i conflitti armati nel mondo cyber.

[27] https://it.wikipedia.org/wiki/Crimine_informatico
[28] https://it.wikipedia.org/wiki/Hacktivism
[29] https://it.wikipedia.org/wiki/Guerra_dell%27informazione

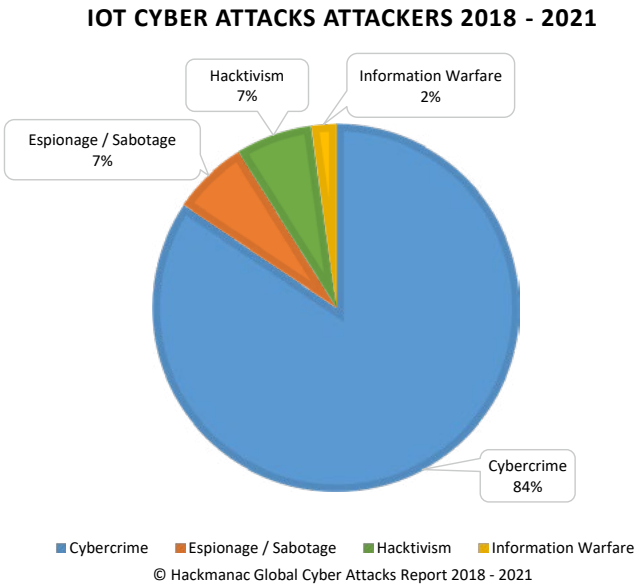


Figura 8: *Motivazione principale dei cyber attacchi in ambito IoT*

Il malware[30] è la tecnica di attacco utilizzata in quasi la metà dei cyber attacchi (49%, vd Fig. 9), un dato che si rispecchia anche nei trend globali, dove, di norma negli ultimi anni l'adozione di questa tipologia di minaccia si attesta sul 40% del totale.
Ne esistono diverse tipologie, dal worm[31], in grado di propagarsi autonomamente nelle reti, al trojan[32] (da "*trojan horse*", il rinomato cavallo di Troia), che fornisce accesso al criminale, fino al ransomware[33], in grado di cifrare tutti i sistemi colpiti in modo che il cyber criminale possa chiedere un riscatto (dall'inglese "*ransom*") per fornire la chiave di cifratura che consente di recuperare i dati.
Ma la variante che mette più a rischio i dispositivi IoT è certamente la botnet[34], un malware in grado di infettare sistemi smart che possono successivamente essere controllati per lanciare attacchi di tipo DDoS (Distributed Denial of Service).

[30] https://it.wikipedia.org/wiki/Malware
[31] https://it.wikipedia.org/wiki/Worm
[32] https://it.wikipedia.org/wiki/Trojan_(informatica)
[33] https://it.wikipedia.org/wiki/Ransomware
[34] https://it.wikipedia.org/wiki/Botnet

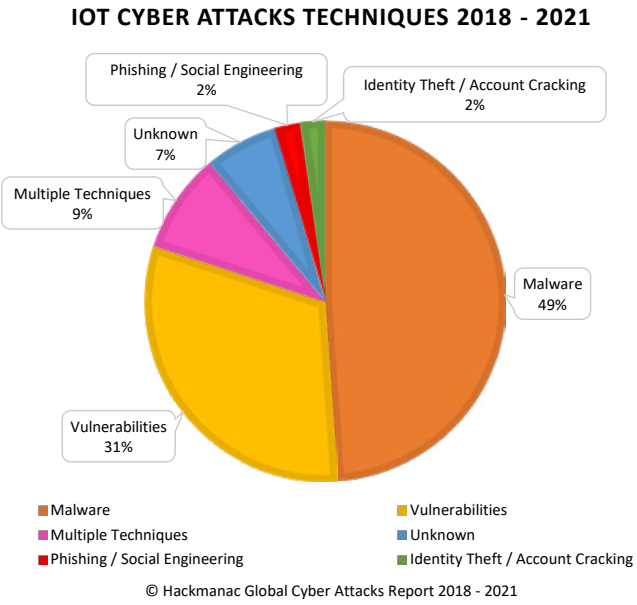


Figura 9: *Principali tecniche utilizzate nei cyber attacchi in ambito IoT*

Questi attacchi permettono di saturare la banda di comunicazione rendendo così irraggiungibili e inutilizzabili server, servizi web e perfino interi data center.
Lo sfruttamento (in gergo "exploit") delle vulnerabilità dei dispositivi, che siano note o meno note (come nel caso degli 0-day[35]), viene utilizzato in un terzo degli attacchi (31%).
Ci riferiamo in questo caso a problematiche varie come configurazioni errate, carenza di aggiornamenti e patch di sistema, bug nel software di sistemi e applicativi, ecc...

Le vulnerabilità non gestite (o, peggio ancora, non note) rappresentano un grosso pericolo per le infrastrutture informatiche in quanto possono essere "*exploitate*" appunto per penetrare nei sistemi e consentire ai cyber criminali di portare a termine le loro operazioni.
In quasi un decimo dei casi (9%), invece, viene utilizzata più di una tecnica per perpetrare gli attacchi verso questi dispositivi, mentre nel 7% le tecniche sono addirittura sconosciute.

[35] https://it.wikipedia.org/wiki/0-day

In minoranza si fa invece ricorso a phishing[36] o tecniche di ingegneria sociale[37] (2%).

Queste tecniche sfruttano lo studio del comportamento umano per riuscire a carpire informazioni o convincere l'utente a compiere azioni convenienti all'attaccante (come, ad esempio, infettarsi con un malware aprendo un allegato in un'email, visitando un sito compromesso o installando un software all'apparenza legittimo).
Infine, le tecniche correlate con i furti di identità digitale e la compromissione degli account vengono utilizzate in egual misura nel 2% dei casi per portare a termine attacchi contro i dispositivi IoT.
Per quanto riguarda la distribuzione geografica dei cyber attacchi in ambito IoT, in larga maggioranza questi vanno a colpire località multiple (62%, vd. Fig. 10), come ad esempio nel caso di vittime distribuite in diversi paesi.

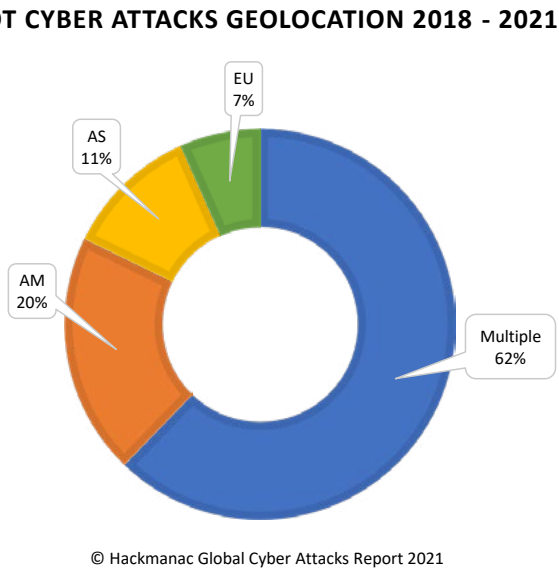


Figura 10: *Distribuzione geografica dei cyber attacchi in ambito IoT*

[36] https://it.wikipedia.org/wiki/Phishing

[37] https://it.wikipedia.org/wiki/Ingegneria_sociale

Un quinto degli attacchi (20%) si verifica invece sul continente americano, meno della metà di quanto avviene nel trend globale, dove la percentuale si attesta sul 45-47% del totale.
Una minoranza di incidenti, infine, avviene in Asia (11%) e in Europa (7%).

I rischi cyber in ambito IoT

I dispositivi IoT nascono spesso come oggetti di uso comune, a volte anche di dimensioni molto ridotte, che successivamente vengono adattati per essere connessi in rete nel modo più conveniente possibile.
Questo comporta che le preoccupazioni inerenti alla sicurezza informatica vengano prese in considerazione di rado in fase di progettazione, esponendo a notevoli minacce non solo i dispositivi stessi, ma anche tutti i sistemi e le informazioni che si verranno a trovare nella stessa rete.

I rischi aumentano tanto più è critico l'ambito di applicazione degli IoT, come ad esempio nel settore industriale (si parla in questi casi di IIoT, Industrial Internet of Things), negli ospedali, nel settore energetico, ecc.
In molti di questi casi, inoltre, gli IoT vengono forniti con un servizio di manutenzione incluso gestito in toto dal fornitore.
Questo, se da una parte può apparentemente semplificare le cose, dall'altra impedisce di avere il pieno controllo sulla gestione dei dispositivi e di verificare che le misure messe in atto siano adeguate.

In generale, i rischi cyber dell'IoT possono essere suddivisi in tre categorie, di seguito prese in esame.

Rischi di percezione

I dispositivi IoT vengono generalmente considerati come semplici oggetti e non come elementi connessi in rete, che andrebbero protetti al pari di computer e smartphone.
Questo genera un'errata valutazione dei rischi in quanto non vengono percepiti come potenziali vettori di attacco.
Eventuali incidenti, invece, potrebbero non solo compromettere le loro funzioni ma anche consentire l'accesso ad altri sistemi sulla stessa rete.
I rischi cyber in questo caso vengono totalmente ignorati, a causa di una forma di trust eccessiva ed è bene ribadire che ogni dispositivo connesso in rete è potenzialmente a rischio e va protetto adeguatamente.

Rischi di connessione

Gli IoT possono connettersi ad Internet o ad altri dispositivi con diverse modalità: Ethernet[38] (tramite il comune cavo di rete), WiFi o altri protocolli come il Blue-

[38] https://it.wikipedia.org/wiki/Ethernet

tooth, sono tutte opzioni valide che vengono scelte in base alla natura del dispositivo, alla convenienza o alle necessità tecniche.
Sarebbe bene che i dispositivi adottassero metodi di connessione sicuri e di ultima generazione, oltre che sistemi di trasmissione dei dati su Internet in grado di proteggere la privacy dei propri utenti (ad esempio tramite l'utilizzo di VPN o cifrando i dati prima di trasmetterli).
Ma non sempre gli utenti dispongono di sufficiente controllo sulla tipologia di connessione o sulla configurazione degli IoT, in quanto queste decisioni vengono prese in fase di design e non necessariamente le interfacce consentono alternative.
Può rivelarsi difficile, quindi, anche solo verificare la sicurezza dei protocolli utilizzati, non solo modificarne la configurazione.
Le connessioni di questi dispositivi possono inoltre essere affette da ulteriori problematiche come l'autenticazione assente o insufficientemente robusta, la carenza di verifica e controllo degli accessi o l'assenza di segmentazione delle reti.
Queste problematiche espongono al rischio di compromissione non solo gli IoT ma anche tutto ciò si trova sulla stessa rete.

Rischi applicativi

I dispositivi IoT sono progettati con sistemi operativi e firmware soggetti a vulnerabilità come tutti i software.
Mentre nel caso di sistemi informatici convenzionali i processi di verifica e gestione degli aggiornamenti sono ormai una prassi rodata, nel caso degli IoT invece l'applicazione di update e patch di sicurezza a software, firmware e sistemi correlati possono risultare difficili, quando non impossibili in quanto non previsti dall'interfaccia utente.
Anche ove l'aggiornamento sia previsto, l'errata percezione di questi dispositivi non agevola il processo.
Ad esempio, potrebbe non venirci in mente di appurare periodicamente la presenza di aggiornamenti per la smart TV di casa o per il termostato smart, seppure consapevoli di quanto questa verifica sia importante per i computer e gli applicativi che usiamo di frequente.

I 10 cyber incidenti più gravi (finora) in ambito IoT

Come abbiamo visto in precedenza, i cyber attacchi che coinvolgono l'IoT sono numerosi e si stima che siano in continuo aumento.
Sebbene quindi l'IoT comporti evidenti rischi per la sicurezza e la privacy dei suoi utenti, la loro diffusione d'altra parte pare inarrestabile ed è impensabile a questo punto rinunciare a questa evoluzione tecnologica.

Alcuni incidenti, tuttavia, si sono trasformati in veri e propri incubi per gli effetti, le implicazioni e i pericoli che hanno comportato.

Ne abbiamo selezionato dieci, descritti qui di seguito, insieme ai preziosi insegnamenti che ci hanno fornito.

1. **Stuxnet**

   Questo particolare incidente, avvenuto tra il 2010 e il 2014, è forse quello che ha fatto comprendere più di tutti i potenziali pericoli derivanti dall'adozione di tecnologie IoT non sufficientemente protette, specialmente nell'ambito di applicazione industriale o energetico.

   Lanciato per sabotare l'impianto di arricchimento dell'uranio a Natanz, in Iran, lo scopo principale dell'attacco era disabilitare le centrifughe impedendo la rilevazione dei malfunzionamenti e della presenza del malware.

   Stuxnet[39], il famoso malware utilizzato in questo attacco, ha stupito per il suo livello di sofisticatezza, che ha dimostrato quanto chi lo ha progettato avesse una buona conoscenza della rete informatica dell'impianto.

   Si stima che siano state distrutte fino a 1.000 centrifughe.

   La lezione da trarre da questo incidente è che i dispositivi mission-critical non devono essere raggiungibili da una rete esterna, a meno che non sia strettamente necessario e, in quest'ultimo caso, è bene assicurarsi che l'accesso sia opportunamente protetto.

2. **La botnet Mirai**

   Nel 2016 la botnet Mirai[40] ha infettato numerosi dispositivi IoT, principalmente router e telecamere IP datate o con software non aggiornati.

   Successivamente i dispositivi infettati sono stati utilizzati per inondare con un attacco DDoS (Distributed Denial of Service) Dyn, una società che controllava gran parte dell'infrastruttura del sistema dei nomi di dominio (DNS) di Internet.

   Mirai ha in questo modo messo in ginocchio gran parte delle reti Internet in Europa e negli Stati Uniti, arrecando danni e rendendo indisponibili per ore una serie di importanti siti web come Twitter, the Guardian, Netflix, Reddit, CNN, GitHub, Shopify, SoundCloud, Spotify, Etsy e molti altri.

   Il malware ha compromesso dispositivi progettati con versioni obsolete del sistema operativo Linux e che utilizzavano credenziali predefinite.

   La lezione imparata riguarda l'importanza di progettare dispositivi IoT che prevedano l'aggiornamento del sistema operativo per essere sicuri di poter mitigare le vulnerabilità.

   Inoltre, è fondamentale modificare le credenziali predefinite degli IoT per non consentire un facile accesso ai criminali informatici.

3. **I dispositivi cardiaci del St. Jude**

   Nel 2017, l'americana FDA (Food and Drug Administration)[41] ha confermato

[39] https://it.wikipedia.org/wiki/Stuxnet

[40] https://it.wikipedia.org/wiki/Mirai_(malware)

[41] https://it.wikipedia.org/wiki/Food_and_Drug_Administration

che i dispositivi cardiaci impiantabili del St. Jude Medical erano affetti da una vulnerabilità che avrebbe potuto consentire ad un cyber criminale di accedere e compromettere gli strumenti, esaurendo la batteria o, peggio, somministrando al paziente stimolazioni o shock.
I dispositivi, con funzionalità di pacemaker e di defibrillatori, vengono tutt'ora utilizzati per monitorare e controllare le funzioni cardiache dei pazienti e prevenire gli infarti.
La vulnerabilità è stata rilevata nel sistema che questi strumenti utilizzavano per leggere i dati e condividerli da remoto con i medici, consentendo al tempo stesso l'accesso al dispositivo ad un cyber criminale con intenti malevoli.
La lezione? L'importanza di proteggere correttamente le connessioni dei dispositivi connessi, in particolare in ambito medicale dove un cyber attacco di questa portata potrebbe costare vite umane.

4. I condomini in Finlandia

Nel novembre 2016, i criminali informatici hanno interrotto il riscaldamento di due condomini nella città di Lappeenranta, in Finlandia.
L'attacco è stato portato a termine con un DDoS che, andando a colpire i regolatori smart del riscaldamento degli edifici, li obbligava a riavviarsi continuamente, impedendo di fatto di erogare il riscaldamento.
L'aspetto più preoccupante della questione è che l'attacco è avvenuto in un periodo dell'anno in cui le temperature in Finlandia scendono ben al di sotto dello zero, creando non pochi disagi ai residenti.
La situazione è stata ripristinata solo interrompendo la connessione a Internet degli edifici.
La lezione appresa è che è necessario monitorare e implementare sistemi di protezione da minacce come i DDoS, in particolare in ambiti di applicazioni civili così critici.

5. La Jeep Cherokee

Nel 2015 un team di ricercatori è stato in grado di assumere il controllo totale di un SUV Jeep Cherokee.
Sfruttando una vulnerabilità dell'aggiornamento del firmware, i ricercatori hanno dirottato il veicolo sulla rete cellulare Sprint, riuscendo in seguito a modificare il funzionamento di diversi sistemi, dall'aria condizionata ai tergicristalli.
Il test ha dimostrato, inoltre, che un attaccante sarebbe in grado di manomettere il veicolo facendolo accelerare, rallentare e persino virare fuori strada, potendo così causare gravi incidenti.
Sebbene in questo caso si sia trattato solo di una dimostrazione, è evidente che un cyber attacco di questa portata potrebbe comportare la perdita di vite umane.
La lezione in questo caso riguarda la necessità di progettare adeguatamente i

veicoli connessi per metterli al riparo dal rischio di accessi malevoli e manomissioni da remoto.

6. La webcam TRENDnet

Dal 2010 al 2012 l'azienda TRENDnet ha commercializzato le sue telecamere SecurView pur affette da una grave vulnerabilità.

L'azienda trasmetteva le credenziali degli utenti in chiaro su Internet, senza utilizzare alcuna protezione per proteggere l'invio dei dati.

Inoltre, le telecamere memorizzavano in chiaro le informazioni di accesso, perfettamente leggibili da qualsiasi dispositivo mobile.

Questo avrebbe potuto permettere a un cyber criminale (e non siamo certi che non sia accaduto) di poter accedere alle webcam e al contenuto salvato nei dispositivi.

L'incidente ha quindi rappresentato un enorme rischio per la privacy dei suoi ignari utenti.

E ha insegnato che un IoT deve essere in grado di crittografare sia le credenziali di accesso che i dati salvati nel dispositivo, così come le informazioni trasmesse su Internet.

Queste funzionalità dovrebbero essere tra le prime discriminanti nella selezione del prodotto più adatto alle proprie esigenze.

7. Il baby cardiofrequenzimetro Wi-Fi Owlet

Nel 2016 un ricercatore ha scoperto una grave vulnerabilità nel cardiofrequenzimetro Wi-Fi Owlet, un sensore che i bambini indossano in un calzino che monitora il battito cardiaco, in grado di inviare un avviso agli smartphone dei genitori se qualcosa non va.

Mentre la stazione base del dispositivo crittografava i dati inviati e ricevuti dai server del produttore, che, in caso di necessità, contattava i genitori, il ricercatore ha scoperto che la rete Wi-Fi ad hoc che collegava la stazione base al sensore era completamente non crittografata e non richiedeva alcuna autenticazione per accedervi.

Questo comportava la possibilità di spiare la connessione e perfino prendere il controllo del dispositivo impedendo l'invio di avvisi.

Ancora una volta i rischi che comportano l'utilizzo di un dispositivo IoT non efficacemente protetto sono inquietanti al punto da poter mettere a repentaglio vite umane.

La lezione è certamente quella di verificare la protezione delle connessioni di questi dispositivi, sia per quando riguarda le modalità con cui si connettono ad Internet, sia per le comunicazioni tra i vari componenti del sistema.

8. Il baby monitor

Nel 2014 una coppia ha sentito una voce maschile nella camera del figlio di 10 mesi. La voce proveniva dal baby monitor che i genitori utilizzavano per monitorare il bambino, evidentemente hackerato da uno sconosciuto.

L'attaccante era stato anche in grado di muovere la telecamera a suo piacimento.
L'incidente ha mostrato quanto questi dispositivi possano rivelarsi pericolosi per la privacy se connessi a Internet senza le adeguate protezioni.
Sebbene sia passato diverso tempo dall'incidente e nel frattempo i baby monitor connessi ad Internet siano stati dotati di sistemi di appositi sistemi di protezione, questo incidente ha insegnato l'importanza di valutare attentamente i rischi di privacy che questi apparati comportano e di verificare con attenzione che siano protetti in modo corretto.

9. Il sensore del Casinò

Nel 2018, un casinò americano è stato hackerato tramite un termometro smart installato nell'acquario della hall.
Per quanto possa apparire ridicolo, i criminali informatici sono stati in grado di sfruttare una vulnerabilità nel termostato per violare la rete del casinò e da qui accedere al database ad alto rischio dei giocatori d'azzardo per poi esportarlo e pubblicarlo in Internet.
La lezione appresa? Anche un sistema apparentemente insignificante come il sensore di un acquario può mettere a rischio dati molto sensibili.
È bene verificare le risorse potenzialmente raggiungibili dagli IoT e, quando possibile, isolarli dalle porzioni di rete contenenti computer, server e database.

10. I dispositivi Nest

Nel 2019 una coppia ha sorpreso con un orrore uno sconosciuto parlare al figlio di 7 mesi dalla webcam Nest che utilizzavano per monitorare il bambino.
Come se non bastasse, successivamente i genitori hanno scoperto che anche il loro termostato Nest era stato compromesso e non erano più in grado di impostare la temperatura desiderata in casa.
Tutti i loro dispositivi Nest erano stati evidentemente *hackerati*.
Successivamente ulteriori clienti di Nest hanno segnalato incidenti simili, ma la società, posseduta da Google, ha continuato a negare di aver ricevuto un data breach sui propri sistemi.
Al contrario, Nest ha inizialmente insistito sul fatto che era responsabilità delle vittime proteggere meglio i loro dispositivi, mettendo a disposizione una serie di suggerimenti per migliorare la sicurezza degli apparati.
Successivamente la società ha finalmente distribuito una patch per risolvere la problematica.
Ma l'incidente ha chiarito inequivocabilmente che, sebbene i produttori abbiano le loro responsabilità nel progettare apparati IoT più sicuri già in fase di design, gli utenti non possono permettersi di ignorare come configurarli al meglio e di verificare gli aspetti di sicurezza.

Aspetti di Compliance e Privacy

Beatrice Ridolfi

Come abbiamo visto nel capitolo introduttivo, i dispositivi IoT sono molto diffusi e utilizzati in diversi ambiti che riguardano la vita quotidiana di tutti noi, non solo per migliorare la qualità della vita delle persone nella gestione quotidiana della casa, degli edifici e delle città, ma anche come dispositivi medici.
Per questo motivo e per evitare possibili rischi di sicurezza come descritto nel paragrafo precedente, è di fondamentale importanza proteggere e mantenere sicuri sia i dispositivi stessi che i dati da essi trattati, considerando sempre centrale il ruolo dell'utente.
Per garantire la protezione e la messa in sicurezza sia dei dispositivi IoT sia dei dati da essi trattati, e per minimizzare il rischio di abusi, ci si può affidare anche a norme internazionali e a regolamenti, quali ad esempio la norma tecnica ISO/IEC 27400 e il Regolamento Generale per la Protezione dei Dati personali (GDPR).

ISO/IEC 27400

Con l'obiettivo di fornire delle linee guida per la sicurezza informatica e la privacy dei sistemi IoT, a giugno 2022 è stata pubblicata la norma tecnica ISO/IEC 27400:2022[42] nella sua prima versione.
ISO (International Organization for Standardization)[43] è un'organizzazione internazionale di organismi nazionali di normazione di oltre 160 paesi, i cui risultati finali sono pubblicati come norme internazionali e che dal 1947 ad oggi ha pubblicato oltre 22.000 norme.
I principi chiave nello sviluppo delle norme ISO sono il fatto che rispondono alle esigenze di mercato, sono basate sull'opinione di esperti a livello globale, sono sviluppate attraverso un processo che coinvolge diversi stakeholders e sono basate sul consenso.
IEC (International Electrotechnical Commission)[44] è un'organizzazione internazionale di normazione che prepara e pubblica standard internazionali per tutte le tecnologie elettriche, elettroniche e affini, note come "elettrotecnica".
Fanno parte di questa organizzazione internazionale oltre 170 Paesi, e dal 1906 ad oggi ha pubblicato oltre 10.000 norme.

ISO e IEC costituiscono, quindi, il sistema specializzato di riferimento per la normazione mondiale. Gli organismi nazionali membri di ISO e IEC partecipano allo

[42] https://www.iso.org/standard/44373.html

[43] https://www.iso.org/home.html

[44] https://iec.ch/homepage

sviluppo di norme internazionali attraverso i comitati tecnici istituiti dalle rispettive organizzazioni, per occuparsi di particolari settori di attività tecnica, collaborando negli ambiti di interesse reciproco.
In particolare, il sottocomitato 27 (SC 27), da cui nascono tutte le norme della famiglia 27000 e anche altre degne di nota, è delegato ad occuparsi, in seno al Joint Technical Committee (JTC 1) di ISO/IEC, della sicurezza delle informazioni. Il suddetto sottocomitato il cui nome completo è ISO/IEC JTC 1 SC 27 *"Information security, Cyber Security and privacy protection"* sviluppa quindi norme per la protezione delle informazioni e dell'ICT, includendo metodologie, tecniche e linee guida per indirizzare gli aspetti di sicurezza delle informazioni e di privacy.
È proprio da questo sottocomitato che è stata sviluppata la norma tecnica ISO/IEC 27400 in quanto, come tutti i sistemi ICT, essendo largamente distribuiti e coinvolgendo un vasto numero di entità, anche per i sistemi IoT risulta essere di fondamentale importanza la gestione della sicurezza delle informazioni e la protezione dei dati personali da essi trattati.
E per questo motivo è stato considerato necessario definire delle linee guida che permettessero di individuare i rischi a cui sono sottoposti i sistemi IoT e i controlli di sicurezza e privacy che sono raccomandati.
Questa norma non contiene requisiti, e quindi la sua applicazione non può essere resa obbligatoria, però fornisce delle linee guida utili per garantire la sicurezza informatica e la privacy dei sistemi IoT.

Secondo la norma, esistono diverse categorie di sorgenti di rischio che possono avere un effetto sui sistemi IoT, tra cui:
- le vulnerabilità dei sistemi IoT;
- la qualità dei sistemi IoT e delle loro componenti;
- la mancanza di competenze e conoscenze, e anche l'errore umano, nelle persone che forniscono o che usano sistemi IoT;
- l'esistenza di specifiche persone che hanno l'intento malevolo di attaccare un sistema IoT;
- l'esistenza di sistemi e dispositivi esterni che possono essere utilizzati per generare degli attacchi ai sistemi IoT;
- l'esistenza di fenomeni naturali;
- la mancanza di una governance organizzativa all'interno degli stakeholder dei sistemi IoT.

A partire dai rischi a cui sono sottoposti i sistemi IoT, vengono quindi definiti controlli raccomandati per la sicurezza e la privacy, suddividendoli in base ai destinatari di riferimento, considerando non solo i fornitori di servizi IoT e gli sviluppatori di sistemi IoT, ma anche gli utenti e chi usufruirà di tali sistemi.
I controlli proposti sono stati pensati per essere utilizzati anche in congiunzione con altri controlli, come ad esempio quelli definiti nella norma tecnica ISO/IEC

27002[45], che definisce un insieme di controlli per trattare i rischi relativi alla sicurezza delle informazioni.

Controlli di sicurezza per i fornitori di servizi IoT e per gli sviluppatori di sistemi IoT

Sono innanzitutto indicati controlli a livello organizzativo che hanno l'obiettivo di dare supporto alla direzione aziendale per la gestione della sicurezza dei sistemi IoT, come la definizione di politiche aziendali specifiche e la definizione di specifici ruoli e responsabilità all'interno dell'azienda, controlli che sono raccomandati per tutti i sistemi informatici, come il monitoraggio del funzionamento del sistema stesso, la creazione e la protezione dei log che tengono traccia degli eventi e l'acquisizione di informazioni derivanti da eventuali incidenti. In aggiunta, vengono indicati alcuni controlli specifici riguardo lo sviluppo e la costruzione dei sistemi IoT.
È importante definire i principi di ingegneria sicura dei sistemi IoT, che indirizzino la progettazione e l'implementazione di funzioni di sicurezza, la difesa in profondità e la messa in sicurezza di sistemi e software utilizzati per lo sviluppo di sistemi IoT, in modo tale da garantire la progettazione e l'implementazione della sicurezza dello sviluppo di sistemi IoT.
Adeguate misure di sicurezza dovrebbero essere implementate durante tutte le fasi del ciclo di vita dei sistemi IoT, a partire dalla progettazione e dallo sviluppo, fino alla messa in opera, alla manutenzione e alla dismissione.
Oltre all'implementazione di misure di sicurezza durante tutte le fasi del ciclo di vita dei sistemi IoT, è importante anche utilizzare tecnologie di rete e di comunicazione adatte per questi sistemi, in modo tale che soddisfino le esigenze di sicurezza, in termini di riservatezza e integrità delle informazioni, performance e le altre necessità dei sistemi IoT, come la mobilità e la localizzazione geografica.
Infine, risulta essere importante per i fornitori di servizi IoT e per gli sviluppatori di sistemi IoT, fornire agli utenti dei dispositivi stessi una guida sull'uso corretto, evidenziando i rischi e gli effetti indesiderati di servizi o sistemi IoT che possono derivare da un uso improprio dei dispositivi, in modo tale da rendere gli utenti consapevoli dei rischi per la sicurezza nel loro uso e garantire l'attuazione delle misure di sicurezza.

Controlli di sicurezza per gli utenti di sistemi IoT

Anche gli utilizzatori dei sistemi IoT possono adottare controlli di sicurezza che permettono di utilizzare i dispositivi in modo sicuro, dal momento della scelta fino alla dismissione.
Al momento dell'acquisto, è buona prassi che gli utenti scelgano dispositivi e sistemi IoT che forniscono informazioni di contatto per il supporto, in modo tale da avere una garanzia sull'uso sicuro dei dispositivi.

[45] https://www.iso.org/standard/75652.html

Dopo avere acquistato un dispositivo o un sistema IoT, l'utente dovrebbe applicare in modo corretto le impostazioni iniziali, per garantire il corretto funzionamento anche dal punto di vista della sicurezza.

Infine, quando un dispositivo IoT non viene più utilizzato, è importante disattivarlo e revocare tutte le credenziali, per evitare possibili rischi di sicurezza, e quando un dispositivo deve essere smaltito o riutilizzato, devono essere rimossi tutti i dati sovrascritti in modo sicuro, per garantire la protezione delle informazioni.

Controlli sulla privacy per i fornitori di servizi IoT e gli sviluppatori di sistemi IoT

Oltre ai controlli legati alla sicurezza, nei contesti IoT viene raccomandata anche l'implementazione di controlli sulla privacy per la gestione sicura dei dati personali trattati.
Fra i controlli che possono essere applicati da fornitori di servizi IoT e sviluppatori di sistemi IoT vi sono la prevenzione degli eventi invasivi sulla privacy, mediante l'integrazione di funzionalità per il miglioramento della privacy all'interno di dispositivi e servizi IoT, e l'adeguata gestione dei controlli sulla privacy, riesaminandone in modo continuativo l'efficacia ed identificando quelli che potrebbero essere nuovi rischi, tenendo sempre in considerazione l'evoluzione delle esigenze di privacy degli utenti e i requisiti normativi.
Inoltre, è importante ridurre al minimo la raccolta di dati da fonti indirette, o ancora meglio non raccoglierli affatto, per impedire la raccolta di dati senza il consenso degli utenti dei sistemi IoT. Per garantire la protezione dei dati personali è importante anche gestire in modo appropriato le misure di protezione dei dati personali e comunicarle solo alle parti interessate, e garantire che i dati raccolti non possano permettere l'identificazione dell'utente, al fine di impedirne la raccolta attraverso il monitoraggio di un dispositivo IoT.
Infine, all'utente IoT dovrebbe essere comunicata un'informativa sulla privacy, che indichi in primis quali dati personali verranno raccolti e lo scopo del loro utilizzo.

Controlli sulla privacy per gli utenti di sistemi IoT

Anche gli utenti e quindi gli utilizzatori dei sistemi IoT possono adottare controlli sulla privacy che permettono di proteggere i propri dati personali.
Innanzitutto, è importante ricordarsi di fornire il consenso all'uso dei propri dati personali per i dispositivi e servizi IoT solo dopo averne valutato la reale necessità e il possibile impatto in caso di violazione dei dati, revocando il consenso se non più necessario o se si manifestano dei problemi con il dispositivo o il servizio IoT, in modo tale da impedire un uso improprio dei propri dati personali.
Inoltre, è importante verificare la reale necessità di connessione da parte dei dispositivi e servizi IoT con altri dispositivi o servizi e consentirla solo in caso di una valida necessità, per garantire un uso mirato di dispositivi o servizi IoT.

Infine, è buona prassi richiedere la certificazione o la validazione delle funzionalità per la protezione della privacy dei sistemi e servizi IoT, per assicurarsi che tali funzionalità siano affidabili.

GDPR

Essendo i dispositivi IoT dei dispositivi che trattano dati personali, ad essi si applica ovviamente anche il Regolamento Generale per la Protezione dei Dati personali (GDPR)[46].
Il GDPR è un regolamento europeo divenuto operativo nel maggio 2018, che disciplina il modo in cui le aziende e le organizzazioni trattano i dati personali, con l'obiettivo di dare ad ogni individuo il controllo sull'utilizzo dei propri dati, stabilendo requisiti precisi e rigorosi per il trattamento dei dati, la trasparenza, la documentazione da produrre e conservare e il consenso degli utenti.
Uno dei principi fondamentali introdotti dal GDPR è il principio di *privacy by design*, ovvero il fatto che la tutela dei dati personali degli utenti deve iniziare dalle prime fasi di progettazione del dispositivo o del servizio, in modo tale da garantire la protezione dei dati e degli utenti fin dall'inizio, prevenendo il verificarsi dei rischi privacy e di sicurezza.

Alla base del principio di privacy by design vi sono quindi i seguenti concetti:

- prevenire e non correggere: gli eventuali problemi devono essere valutati nella fase di progettazione e si deve prevenire il verificarsi dei rischi, evitando di effettuare valutazioni di conformità solo a seguito della produzione di un dispositivo o di un servizio, o addirittura a seguito di un evento che potrebbe avere un impatto sui dati personali;
- sicurezza durante tutto il ciclo di vita del dispositivo o del servizio;
- visibilità e trasparenza del trattamento, per garantire la tutela dei dati;
- centralità dell'utente, ovvero il rispetto dei diritti.

Un altro principio fondamentale è il principio di *privacy by default*, che prevede la tutela della privacy come impostazione di default e incorporata nel progetto.
Secondo questo principio le misure di protezione dei dati personali dovrebbero essere attive a prescindere e non dovrebbero quindi essere attivabili o disattivabili a discrezione. Inoltre, il titolare del trattamento per impostazione predefinita dovrebbe trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste per il funzionamento del dispositivo o del servizio e per il periodo strettamente necessario a tali fini.

[46] https://gdpr-info.eu/

Anche per questo principio, è necessario agire già dalle prime fasi di progettazione del dispositivo o del servizio, per garantire che non vengano raccolti dati non necessari e per garantire un elevato livello di protezione per quelli raccolti.

L'introduzione di questi due principi porta il Titolare del trattamento, che normalmente coincide con chi sviluppa o acquista i dispositivi o i servizi, ad effettuare una valutazione di impatto privacy ogni volta che il trattamento di dati operato dal dispositivo o dal servizio potrebbe comportare rischi elevati per la privacy degli utenti. Nell'ambito IoT è quindi necessario effettuare la valutazione di impatto privacy, in quanto il trattamento può presentare un rischio elevato per i diritti e le libertà degli utenti e, se svolta in maniera corretta e responsabile, offre garanzie necessarie per un trattamento corretto dei dati anche in situazioni di emergenza.
Se da un lato è indubbio il vantaggio che i sistemi IoT hanno nella gestione quotidiana della vita di chi li utilizza, dall'altro lato è da considerare il fatto che tale utilizzo sempre più frequentemente espone l'utente finale ad un maggior numero di rischi e attacchi informatici, che possono compromettere anche la sicurezza fisica dell'utente stesso (basti pensare ai dispositivi medici e sanitari).
Il quantitativo di informazioni e dati personali condivisi (anche inconsapevolmente) dall'utente finale nell'utilizzo di sistemi IoT e la possibilità di ricavare informazioni sulle sue abitudini, espongono quest'ultimo a sempre più possibili data breach (da intendersi non solo come furto di dati, ma nella accezione più ampia prevista da GDPR come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati").
Le notifiche di data breach e più in generale di attacchi informatici legati all'utilizzo dei dispositivi IoT sono in forte aumento negli ultimi anni, tanto da mantenere costante l'attenzione dell'Autorità Garante della Protezione dei Dati Personali.
Il Garante Privacy invita infatti i Titolari del trattamento a predisporre misure tecniche e organizzative adeguate e ad avere maggiore consapevolezza sull'importanza di proteggere i dati personali trattati.
Solo in questo modo è possibile garantire un livello di sicurezza adeguato commisurato al rischio a cui sono esposti i dati personali.

Threat Intelligence

Giorgia Dragoni

Abbiamo ormai ben compreso la tendenza a connettere in rete sempre più oggetti di uso comune, che accompagnano le nostre attività quotidiane a livello privato e professionale. Abbiamo esaminato i rischi legati al mondo dell'Internet of Things sia in ambito domestico sia nel mondo industriale e l'aumento, preoccupante, degli incidenti che sfruttano come punto di ingresso proprio i device connessi.
Come fare quindi per contrastare e soprattutto prevenire possibili attacchi da parte dei criminali informatici?
Uno degli approcci che possono aiutare le aziende a mettere in atto meccanismi di difesa è quello basato sulla Threat Intelligence. Si tratta di un metodo proattivo, fondato sulla ricerca e sull'elaborazione di informazioni al fine di identificare possibili minacce di sicurezza e di implementare opportune azioni di mitigazione prima che una vulnerabilità possa essere effettivamente sfruttata.
Con il termine Threat Intelligence – o Cyber Threat Intelligence (CTI) – si fa riferimento alla conoscenza che deriva da un processo analitico basato su prove e ipotesi, sviluppato a partire da una varietà di fonti di dati che riguardano contesto, meccanismi, implicazioni e possibili conseguenze di una minaccia o un pericolo esistente o emergente.
Le informazioni vengono raccolte da fonti diversificate, che possono includere per esempio i log dei sistemi informatici (ovvero i file che registrano le operazioni effettuate da un utente o da una macchina), statistiche e portali di vendor di strumenti tecnologici di Cyber Security (da cui reperire per esempio indirizzi IP dannosi, domini e hash di file), fonti giornalistiche, ma anche ricerche nel dark web e nel deep web.
In pratica, l'attività di Cyber Threat Intelligence è molto simile a quello che nel mondo reale definiremmo "controspionaggio", per contrastare le azioni malevole messe in atto dai pirati informatici.
È uno strumento che permette di individuare eventuali punti deboli all'interno della rete e di condividere poi il patrimonio conoscitivo acquisito con tutti gli stakeholder coinvolti nei processi di sicurezza, in modo da poter attuare strategie di prevenzione e protezione efficaci a partire da una base di conoscenza collettiva.
L'obiettivo della Threat Intelligence è quello di fornire supporto ai processi decisionali, aiutando gli esperti di Cyber Security a predisporre le misure di protezione più opportune per far fronte ai possibili nuovi attacchi.

Il ciclo di vita della Cyber Threat Intelligence

Fare Threat Intelligence non significa semplicemente raccogliere dei dati grezzi: per far sì che le informazioni raccolte siano davvero utili a incrementare le proprie

strategie di difesa, è necessario seguire una serie di passaggi sequenziali, all'interno di un ciclo iterativo.

Il ciclo prevede le seguenti fasi:

1. **Pianificazione e direzione:** è la fase in cui vengono posti gli obiettivi e vengono definite le domande a cui il processo di Threat Intelligence dovrà dare risposta. In questo passaggio vanno identificati gli asset da proteggere e stabilite le priorità d'azione, in base agli impatti che un potenziale incidente di sicurezza potrebbe generare sull'organizzazione.
2. **Raccolta:** è la fase in cui si raccolgono e aggregano i dati grezzi provenienti dalle diverse fonti informative, interne ed esterne. Nella raccolta, è fondamentale diversificare le fonti utilizzate, dai colloqui con gli stakeholder al già citato dark web, e prestare attenzione alla qualità dei dati, per evitare di non cogliere eventi minacciosi rilevanti o – al contrario – di essere fuorviati da falsi positivi.
3. **Elaborazione e trattamento:** è il passaggio in cui vengono riordinati i dati raccolti, riportandoli in un formato leggibile e utilizzabile. Diverse fonti e diversi metodi di raccolta dei dati richiedono infatti differenti strumenti di trattamento e un processo di armonizzazione delle informazioni, che vengono riorganizzate con metadati.
4. **Analisi:** quando i dati raccolti sono stati processati in un formato utilizzabile arriva il momento di analizzarli, al fine di estrarne insight realmente utili. Si tratta della fase di intelligence vera e propria, in cui le informazioni vengono interpretate per essere trasformate in report, raccomandazioni e conclusioni, in un formato capace di guidare le decisioni aziendali.
5. **Diffusione:** è la fase in cui le analisi elaborate vengono diffuse tra gli stakeholder coinvolti nel processo di sicurezza, facendo attenzione a veicolare l'intelligence richiesta, con un opportuno linguaggio e con un focus specifico, a seconda delle esigenze dei diversi interlocutori.
6. **Feedback:** è il passaggio in cui gli stakeholder esaminano il prodotto di intelligence, valutando se risponde alle richieste e agli obiettivi iniziali. Questo processo è fondamentale per definire eventuali nuove esigenze, che daranno il via a un nuovo ciclo avviando la fase iniziale di pianificazione e direzione.

Cyber Threat Intelligence "for Things"

La CTI per le "cose" mira a creare consapevolezza situazionale tra gli stakeholder e a supportare il processo decisionale per adottare misure tattiche, operative e strategiche legate alla gestione dei dispositivi connessi, che rientrano nel grande mondo che abbiamo definito Internet of Things.

Tali misure riguardano il miglioramento della sicurezza dei prodotti e dei sistemi cloud, la correzione delle vulnerabilità o investimenti nella protezione di aree specifiche ritenute a rischio, come per esempio interfacce Bluetooth o Wi-Fi.

In sostanza, la Cyber Threat Intelligence delle cose è un'estensione del processo più tradizionale, che si focalizza sugli ambienti fisici e sui prodotti hardware come punti di ingresso delle minacce.
Guardando alle fasi di raccolta e analisi dei dati, tra le varie fonti utili che possono confluire in una piattaforma per la Threat Intelligence in ambito IoT possiamo annoverare le honeypot, ovvero sistemi software o hardware che simulano un prodotto, caratterizzati da vulnerabilità progettate appositamente per renderli appetibili per gli hacker. Le honeypot vengono mantenute isolate, ovvero non collegate con la rete a cui sono associati gli altri dispositivi, e sottoposte a un controllo costante. Se un hacker dovesse provare a sfruttare le vulnerabilità per eseguire i suoi attacchi, quindi, non riuscirebbe a guadagnare l'accesso a dati critici, ma verrebbe immediatamente rilevato e identificato dal sistema di controllo, lasciando tracce rilevanti ai fini di threat intelligence, per esempio rispetto ai metodi e alle tecniche di attacco utilizzabili.
Anche l'intelligence del dark web può contribuire ad arricchire le informazioni utili in ambito IoT. Nel dark web si possono infatti rintracciare per esempio gli attacchi pianificati a un'organizzazione, i documenti segreti che sono stati scoperti e trafugati dai malintenzionati o le vulnerabilità zero-day condivise nei prodotti.

Un'altra fonte di informazioni utile è rappresentata dai penetration test, che permettono di testare la sicurezza dei device. Tramite l'analisi è possibile riscontrare vulnerabilità che devono poi essere corrette e comunicate anche agli stakeholder che possiedono o producono lo stesso prodotto o prodotti simili, come ad esempio telecamere IP, CPU o microcontrollori.
Esistono inoltre degli specifici feed di dati rilasciati da diversi vendor di Cyber Security, che raccolgono tutte le informazioni relativi alle minacce IoT.
All'interno di un feed è possibile, ad esempio, trovare dati sui siti web (che vengono detti maschere) che sono stati utilizzati per scaricare un malware che ha attaccato i dispositivi IoT, protocolli, indirizzi IP, hash e nomi dei file che gli hacker tentano di lanciare dall'URL (coperti appunto dalla maschera) sui dispositivi IoT.
Come detto, le analisi di Threat Intelligence devono poi essere distribuite all'interno dell'organizzazione ai soggetti interessati.
Una volta ricevute le CTI pertinenti, gli stakeholder possono iniziare a implementare le azioni correttive, riparando eventuali aree di vulnerabilità emerse a livello di hardware, software o infrastrutture.
Cambiando prospettiva e allargando il punto di vista sulla sicurezza di un'organizzazione nel suo complesso, gli stessi device IoT possono costituire una fonte utile da utilizzare ai fini di Cyber Threat Intelligence.
Come visto, infatti, l'IoT descrive un mondo in cui qualsiasi cosa può essere connessa e comunicare in modalità "intelligente", combinando dati per produrre intelligenza utilizzabile.

Anche i dati trasmessi dai device connessi, quindi, possono essere analizzati ed elaborati proprio al fine di identificare possibili minacce di sicurezza. Non dobbiamo infatti dimenticare che l'IoT ha trasformato il mondo fisico in un unico grande sistema informativo, con l'obiettivo finale di migliorare la qualità della vita e abilitare nuovi modelli di business.

L'informazione è potere: se è collegato, deve essere protetto

Manuela Santini

L'adozione di dispositivi IoT, grazie ad iniziative incentivanti (es. Piano Nazionale di Ripresa e Resilienza, PNRR), sta vivendo un momento particolarmente favorevole. Tuttavia, almeno fino ad oggi, nella progettazione e nell'installazione di molti di questi dispositivi non è stata posta sufficiente attenzione agli aspetti di sicurezza, introducendo in molti contesti **rischi non noti e non adeguatamente gestiti.**
Ad esempio, i dispositivi IoT sono spesso presi di mira per essere inseriti all'interno di botnet, reti di dispositivi connessi alla rete utilizzati per effettuare operazioni a loro insaputa, come eseguire attacchi di tipo DdoS (Distributed Denial of Service)[47]. Questo tipo di attacco consiste nel tempestare di richieste di dati un servizio, finché non si riesce a renderlo irraggiungibile.

Come ricorderete dagli incidenti che abbiamo descritto in precedenza, nel settembre 2016 una serie di attacchi DDoS Mirai ha scosso Internet.
Mirai, software dannoso sviluppato al solo scopo di infettare un dispositivo, è stato progettato per prendere di mira principalmente dispositivi domestici come termostati, videocamere, frigoriferi, baby monitor. Sfruttandone le vulnerabilità, il malware Mirai è stato in grado di collegarli in una rete di dispositivi infetti, conosciuta come botnet Mirai, e utilizzarli per condurre attacchi su larga scala col solo fine di rendere irraggiungibile un servizio o un dispositivo.
Purtroppo, la compromissione dei dispositivi IoT è possibile perché la maggior parte sono protetti da sistemi di sicurezza domestici, acquistati solitamente sotto forma di programmi e installati sui computer di casa o, peggio ancora, sono privi di protezione.
In molti casi, i dispositivi IoT vengono installati utilizzando solo le credenziali predefinite o pensando che i produttori del dispositivo abbiano già effettuato tutte le attività di *hardening* necessarie, cioè quell'insieme di configurazioni dei dispositivi che mirano a rafforzare la sicurezza dei dispositivi stessi, quali arresto dei servizi non necessari, disabilitazione di privilegi e/o account amministrativi o di assistenza, limitazioni a connessioni di rete, etc.
Fortunatamente, a causa del fatto che la maggior parte degli utenti domestici non dispone di una larghezza di banda elevata, l'utilizzo di reti residenziali per attacchi di botnet DDoS ha un'efficacia limitata, tuttavia questi tipi di attacchi possono essere utilizzati come amplificazione rispetto ad attacchi diretti.
Ci sono, inoltre, dei rischi legati alle componenti hardware. I dispositivi IoT sono spesso basati su chipset utilizzati in diversi contesti.

[47] https://it.wikipedia.org/wiki/Denial_of_service#DDoS

Per chipset si intende l'insieme delle componenti di un apparato elettronico adibite a specifiche funzionalità quali la gestione dell'Hard Disk, la gestione dei BUS, la gestione della memoria, etc..
Tali componenti si trovano installati su dispositivi aventi sia funzionalità che marche diverse come router e lavatrici. Oltre a comportare un vantaggio economico per il produttore del dispositivo, questo può rendere più semplice la ricerca di vulnerabilità, non avendo necessità di strumenti specifici per l'ambito IoT.

OSINT

La ricerca delle vulnerabilità dei dispositivi IoT è spesso il punto di partenza di un attacco informatico.
Prima di sferrare un attacco, gli attaccanti eseguono una fase di ricognizione e "*footprinting*"[48] dove si occupano di raccogliere tutte le informazioni utili rispetto all'obiettivo dell'attacco, quali ad esempio versioni dei firmware, account di default, indirizzi IP, posizione geografica.
La raccolta delle informazioni da parte dell'attaccante dipende dal livello di interesse che può trarre dall'attacco stesso, il quale può variare nel corso del tempo: ciò che è privo di valore oggi non è detto che lo sia anche domani.
Analogamente, un dispositivo ubicato in una certa area geografica può avere un valore diverso rispetto ad un dispositivo situato altrove. L'attaccante avrà quindi necessità di localizzare il dispositivo.
Gli obiettivi del "footprinting" sono quindi la raccolta di informazioni di rete, la raccolta di informazioni di sistema e la raccolta di informazioni sulle organizzazioni. Più informazioni vengono raccolte sul target, maggiore è la probabilità di ottenere risultati rilevanti per un potenziale attacco ma anche per definire la propria strategia di difesa.

La raccolta di queste informazioni può avvenire in modalità passiva, senza una diretta interazione con l'infrastruttura o il dispositivo target, oppure in modalità attiva con diretta interazione con l'oggetto dell'analisi.
Per eseguire attività di "ricognizione" o Cyber-Threat Intelligence (CTI), cioè la ricerca di vulnerabilità tramite risorse online quali motori di ricerca, siti governativi, siti web di aziende pubbliche o private, quotidiani online, immagini satellitari, social media, si possono utilizzare diversi servizi online in grado di fornire informazioni relative alla rete, ai sistemi e alle organizzazioni semplicemente perché sono presenti sul Web.
Le tecniche utilizzate per la ricerca e raccolta di tali informazioni sono dette di OSINT (Open Source Intelligence).

[48] Footprinting, https://hacktips.it/footprinting/

Proprio i social media, e in particolare Twitter, costituiscono una delle fonti di CTI più popolari utilizzate per raccogliere informazioni su vulnerabilità, minacce e incidenti.

Nello studio "*Social Media Monitoring for IoT Cyber-Threats*"[49], finanziato dal programma di ricerca dell'Unione Europea nell'ambito del programma di ricerca e innovazione Horizon 2020, è analizzato il contenuto dei tweet raccolti, al fine di individuare le principali categorie di vulnerabilità di specifici software, per capire quali sono i fattori che influenzano il retweet dei post sulle vulnerabilità di tali software.
Per le organizzazioni ma anche per i singoli cittadini diventa quindi importante comprendere come un uso corretto di questi servizi e, in particolare, un'adeguata attenzione alle informazioni che si sceglie di condividere, possa aiutare a prevenire furti di identità, perdite di dati nonché a tutelarsi da futuri attacchi informatici.
Ne è un esempio il difetto di iParcelBox[50] scoperto attraverso tecniche di OSINT dai ricercatori di McAfee, che proprio grazie alle ricerche di informazioni pubblicamente disponibili sono stati in grado di trovare e abusare di vulnerabilità del software presente sul dispositivo IoT.

Per conoscere le risorse OSINT sono disponibili diverse fonti che ne spiegano o supportino nella ricerca.
Un esempio è l'OSINT Framework[51], predisposto da Justin Nordine e concentrato proprio sulla raccolta di informazioni da strumenti o risorse gratuiti.
Il framework fornisce collegamenti ad una vasta gamma di risorse, utili anche per ricerche nel dark web.

Come è possibile notare da **Figura 11**, esistono numerose fonti OSINT e numerosi strumenti per il monitoraggio di dispositivi e reti.

[49] Social Media Monitoring for IoT Cyber Threats, https://www.researchgate.net/publication/354493500_Social_Media_Monitoring_for_IoT_Cyber-Threats

[50] https://portswigger.net/daily-swig/iot-security-iparcelbox-flaw-uncovered-through-open-source-intelligence

[51] https://osintframework.com/

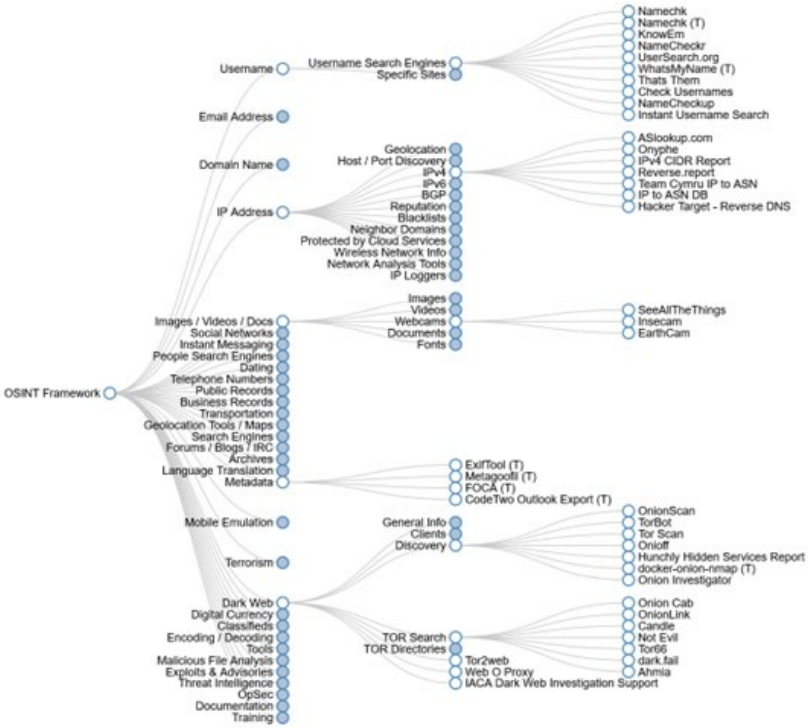


Figura 11: *OSINT Framework*

Nel documento "COMPARATIVE STUDY OF OSINT TOOL FOR IOT"[52] redatto da Journal of Emerging Technologies and Innovative Research (JETIR) viene descritto in modo esaustivo cosa si intende per OSINT e i tipi di strumenti adottabili, confrontandoli tra di loro, indicando pro e contro di ogni strumento, evidenziando come la combinazione di strumenti come Shodan con NMap e molti altri forniscono informazioni dettagliate sul dispositivo IoT in analisi, mettendo gli utenti in grado di ottenere risultati più accurati ed efficaci nel contrastare le minacce a cui i dispositivi sono esposti.
Vediamo di seguito, più nel dettaglio, alcuni di questi strumenti.

Shodan

Come abbiamo visto, nel documento comparativo redatto dal JETIR, tra gli strumenti utili alla ricerca di informazioni in ambito IoT troviamo Shodan.[53]

[52] https://www.jetir.org/papers/JETIR2106084.pdf

[53] https://www.shodan.io/

Shodan è un motore di ricerca utile a individuare dispositivi connessi a Internet, con semplici ricerche e l'utilizzo di filtri tra i quali:
- "city:" per la ricerca di dispositivi per città specifiche,
- "os:" per la ricerca di determinati sistemi operativi,
- "port:" per la ricerca di una specifica porta aperta,
- "hostname:" per cercare host che corrispondono ad una determinata stringa,
- "product:" per la ricerca di prodotti specifici è possibile trovare router, webcam, pannelli di amministrazione di stazioni idriche o sciistiche ed in via più generale dispositivi industriali gestibili da remoto, utilizzando Internet non solo per i siti web ma per scoprire di tutto.

I dati vengono raccolti World-Wide e il suo database è aggiornato costantemente.
I banner, cioè le informazioni che descrivono un servizio su un dispositivo, sono l'informazione di base che può essere reperita tramite Shodan.
È bene precisare che a differenza dei banner per i siti web, i banner degli Industrial Control System (di seguito, ICS) forniscono informazioni sul firmware, serial number e altri dettagli più tecnici che descrivono il dispositivo.
Queste informazioni sono raccolte indipendentemente dal protocollo utilizzato per l'attribuzione di indirizzi IP ai dispositivi connessi a una rete.

Si riporta un esempio di banner relativo a una IP Camera:

```
HTTP/1.1 200 Ok¶
Server: mini_httpd/1.21 18oct2014¶
Date: Wed, 01 Sep 2021 16:15:18 GMT¶
Content-Type: text/html; charset=UTF-8¶
Content-Length: 375¶
Last-Modified: Wed, 27 Apr 2016 07:02:43 GMT¶
Connection: close¶
 ¶
IP Camera:¶
Model: APM-H803-MPC¶
Alias Name: IROAD CP¶
Client Version: 75.1....¶
```

Se volessimo per esempio sapere se vi sono vulnerabilità presenti su quello specifico modello, potrebbe essere utile una ricerca nell'elenco delle CVE (Common Vulnerabilities and Exposures)[54] che fornisce identificatori comuni per le vulnerabilità di sicurezza informatica note pubblicamente.

[54] https://www.cve.org/

L'elenco delle CVE è una vera e propria base dati nella quale sono censite vulnerabilità in modo tale che chiunque possa avervi accesso. L'elenco è costantemente aggiornato e, oltre ad essere utilizzato come standard in vari istituti di ricerca, è molto utile per individuare vulnerabilità e conoscerne la gravità. Infatti, ogni vulnerabilità è classificata in base al Common Vulnerability Scoring System (CVSS)[55], standard che assegna un valore di gravità da 1 a 10.

I parametri presi in considerazione sono: Vettore di Attacco (AV) ovvero la modalità, complessità dell'attacco (AC), permessi richiesti (PR), necessità di interazioni da parte dell'utente (UI) e infine l'impatto in termini di riservatezza, integrità e disponibilità dei sistemi o delle loro funzionalità.
Nel caso in oggetto, la ricerca per modello ha identificato una vulnerabilità CVE-2017-17101 la cui descrizione riporta:
"È stato scoperto un problema nel software Apexis APM-H803-MPC, utilizzato con molti modelli diversi di telecamere IP. Un metodo CGI non protetto all'interno dell'applicazione web consente a un utente non autenticato di bypassare la schermata di accesso e accedere ai contenuti della webcam, tra cui: streaming video in diretta, file di configurazione con tutte le password, informazioni di sistema e molto altro. Con questa vulnerabilità, chiunque può accedere a una webcam vulnerabile con privilegio di 'super amministratore'".
Già dalla descrizione possiamo notare come questa vulnerabilità sia pericolosa per l'utente, ma se volessimo ulteriori informazioni è possibile consultare il National Vulnerability Database (NVD)[56], l'archivio governativo statunitense che consente di automatizzare la gestione delle vulnerabilità.

Nella **Figura 12** riportata nella pagina seguente, è possibile reperire la classificazione della vulnerabilità CVE-2017-17101, che in base ai parametri precedentemente descritti, ottiene un punteggio di 9.8 - Critico.

[55] https://it.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

[56] https://nvd.nist.gov/vuln

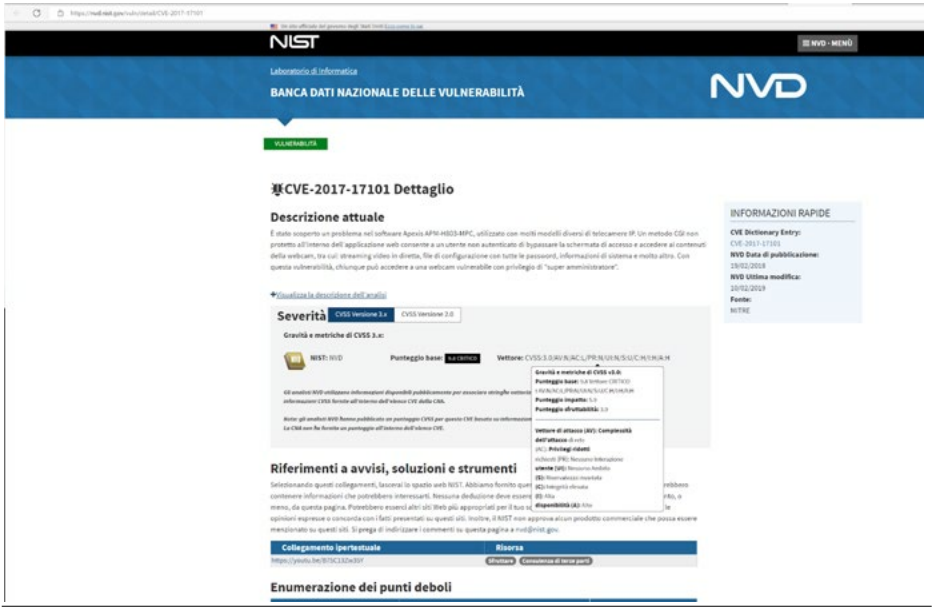


Figura 12: *NVD*

Come è possibile notare, con due semplici ricerche è stato possibile recuperare informazioni che potrebbero essere utili per un potenziale attacco.
Ovviamente nel caso di specie non abbiamo ancora la certezza che la vulnerabilità sia sfruttabile sul dispositivo individuato tramite Shodan, ma facendo ulteriori ricerche e utilizzando diversi tool potrebbe essere possibile costruire un attacco mirato.
Oltre al banner, Shodan acquisisce anche i meta-dati sul dispositivo, come la posizione geografica, l'hostname, il sistema operativo e tante altre informazioni, alcune delle quali a disposizione solo per sviluppatori che utilizzano le API (Application Programming Interface)[57] messe a disposizione, per l'integrazione di Shodan nelle loro applicazioni.
Molto più semplice, sempre tramite Shodan, è verificare quanti e quali dispositivi connessi hanno per esempio impostate le credenziali di default (e quali sono).
Per supportare gli utenti nella verifica di sicurezza dei dispositivi presenti in casa e connessi a Internet è sufficiente eseguire un test tramite scanner gratuiti online appositamente creati per IoT come per esempio Bullguard IoT Scanner[58].
Questo servizio automatizza la ricerca su Shodan, verificando se i dispositivi presenti nella rete casalinga sono pubblici, quindi accessibili al pubblico.

[57] https://it.wikipedia.org/wiki/Application_programming_interface

[58] https://iotscanner.azurewebsites.net/

Google Dorking

L'attività di "Footprinting" può essere svolta anche con altri metodi come il "Google Dorking", che prevede una conoscenza avanzata dei comandi, chiamati operatori, di Google e l'inserimento di particolari stringhe (Google Dorks o Google Hacks) all'interno della ricerca di Google.
Tramite Dork semplici (utilizzo di un solo operatore) o Dork avanzati (utilizzo di più operatori all'interno della stessa stringa) è possibile trovare siti web, database vulnerabili e dispositivi IoT. La sintassi risulta molto semplice e intuitiva: operatore:stringa da cercare.
Ad esempio, se volessi cercare le pagine di login di IP Camera potrei utilizzare l'operatore "intitle" per restringere i risultati della ricerca ai documenti contenenti la parola chiave "Login" nel titolo e poi cercare tramite l'operatore "intext" tutte le occorrenze della parola chiave "IP camera":

```
intitle:"Login" intext:"IP camera"
```

I risultati potrebbero condurre a siti di produttori o forum con le indicazioni di accesso a IP Camera, o portare direttamente a pagine di login.

A semplificare ulteriormente l'utilizzo di Google, nel 2000 Johnny Long ha creato il Google Hacking Database[59], o GHDB.
Il suo utilizzo così come l'utilizzo di Shodan o altri sistemi analoghi, se utilizzati per controllare lo stato di sicurezza del proprio sito o dispositivo non sono illegali, ed è bene conoscerli per individuare errori di impostazione dei propri sistemi.

Nel sito Exploit Database, dove una sezione è proprio dedicata ai Google Dork, si possono trovare diversi modi di sfruttare vulnerabilità (codice exploit) o dimostrazioni di fattibilità dell'attacco ovvero le proof-of-concept (PoC).
Conoscere se vi sono exploit, cioè modalità di sfruttamento di una vulnerabilità mediante percorsi noti e definiti, è un altro elemento essenziale per conoscere i rischi del connettere i propri dispositivi su Internet.

Ricerca di vulnerabilità ed NMAP

La ricerca di vulnerabilità, come già descritto in apertura, non è limitata alla modalità passiva ma può essere svolta anche in modalità attiva.
Gli strumenti a disposizione per la ricerca attiva di vulnerabilità in ambito IoT sono i medesimi di quelli che potremmo utilizzare in ambito IT. Tuttavia, i rischi di blocco di dispositivi a causa degli scan sono elevati.

[59] https://www.exploit-db.com/google-hacking-database

Quindi, soprattutto se i dispositivi devono essere sempre attivi, è opportuno utilizzare metodologie di ricerca passive, dove vengono solo rilevate le vulnerabilità o problematiche di aggiornamento.
Con le modalità di ricognizione attiva, si possono rilevare in modo più rapido le medesime informazioni rilevabili in modalità passiva quali indirizzi IP dei dispositivi IoT, servizi TCP/UDP attivi, porte aperte, protocolli utilizzati, password di default, etc. mediante attività di network scan o vulnerability scan.
In particolare, le porte consentono ad app e programmi di comunicare con la rete. Alcuni dispositivi IoT, richiedono che vengano aperte delle specifiche porte per il controllo remoto del dispositivo, col rischio di esporre pubblicamente delle vulnerabilità sfruttabili per attaccare la rete, aziendale o domestica.
In generale tramite gli IOT Network Security Scanner è possibile rilevare i dispositivi presenti nella rete Wi-Fi degli utenti raccogliendo informazioni sui dispositivi rilevati, individuare eventuali vulnerabilità, eseguire scansioni di porte aperte,etc.
Strumenti come Nmap [60] permettono di creare una mappatura della rete ed è estremamente utile per la configurazione dei dispositivi IoT o per un malintenzionato per reperire informazioni circa le porte da cui il dispositivo può accedere al mondo esterno e gli indirizzi IP associati.

```
Nmap scan report for **.**.**.**¶
Host is up (0.063s latency).¶
MAC Address: nn:nn:nn:nn:nn:nn (Technicolor CH USA)¶
```

La ricerca di porte aperte sui router può essere eseguita anche mediante servizi online come_Hide My Name[61], basato su Nmap, inserendo il proprio indirizzo IP pubblico.
Per conoscere il proprio indirizzo pubblico, ancora una volta la ricerca su web ci viene in aiuto. Basta inserire come stringa di ricerca "my IP" e, a seconda del motore utilizzato, può venire visualizzato direttamente l'indirizzo IP o i siti da cui è possibile recuperare l'informazione. Sempre tramite questi siti, oltre a sapere il proprio indirizzo IP è possibile reperire per qualsiasi indirizzo IP informazioni quali ISP (Internet Service Provider)[62] e dati di geolocalizzazione come latitudine e longitudine.
A livello aziendale, esistono diverse soluzioni che possono identificare comportamenti anomali della rete e tenere traccia delle modifiche locali sui dispositivi.
Le organizzazioni possono quindi proteggersi dalle vulnerabilità dei dispositivi IoT, identificando e seguendo le best practice che garantiscono la sicurezza dell'Internet of Things.

---

[60] https://nmap.org/

[61] https://hidemy.name/en/port-scanner/

[62] https://it.wikipedia.org/wiki/Internet_service_provider

Tuttavia, le vulnerabilità IoT devono essere prevenute da tutte le parti interessate.
I produttori dei dispositivi, devono essere in grado di mettere in sicurezza tutto il processo produttivo effettuando vulnerability assessment e penetration test in laboratorio per limitare la possibilità che vi siano vulnerabilità in fase di produzione, rilevare e risolvere nel più breve tempo possibile le vulnerabilità note nei loro prodotti, rilasciando patch, segnalando in modo proattivo quando il supporto termina.

Protezione dei dispositivi

Gli utenti devono comprendere i rischi per la sicurezza dell'IoT e sapere che è necessario modificare le password predefinite, rimanere aggiornati su quando il dispositivo entra in "end-of-life", mantenere aggiornato il firmware e il software del dispositivo abilitando gli aggiornamenti automatici ove possibile, e quali siano le impostazioni sicure da implementare sul dispositivo.
Tra le impostazioni di sicurezza che possono aiutare a non essere censiti nei database di Shodan o servizi simili vi è l'adozione di un server VPN (Virtual Private Network)[63] all'interno della propria rete locale, sia questa una rete domestica o aziendale.

La VPN è il modo migliore per nascondere il proprio indirizzo IP in quanto permette la creazione di canale privato di comunicazione, detto tunnel, che permette il transito di informazioni in modo completamente "invisibile" a soggetti non autorizzati, nonostante venga sfruttata una connessione pubblica su Internet.
Oltre all'adozione di una VPN per l'accesso alle interfacce di amministrazione dei dispositivi, è opportuno assicurarsi che sul router siano aperte solo le porte necessarie al funzionamento del dispositivo.
In conclusione, l'aggiornamento periodico del firmware dei dispositivi e l'utilizzo di VPN, sono le migliori soluzioni per limitare l'esposizione a rischi.

[63] https://it.wikipedia.org/wiki/Rete_privata_virtuale

Case Study

Disclaimer

Quanto segue è una simulazione realistica, a mero scopo dimostrativo e didattico, di ciò che è possibile fare ed ottenere utilizzando tecniche di hacking, social engineering e OSINT.
Tutti gli output sono frutto di test realizzati in ambienti controllati e privati. Inoltre, personaggi e i luoghi sono puramente casuali.
Nessun reato, dunque, è stato commesso per effettuare la simulazione che segue. Ciononostante, ti ricordiamo che realizzare condotte di questo tipo nella vita reale costituisce una fattispecie di reato e può essere perseguito penalmente. Ti invitiamo, quindi, caldamente a non replicare le tecniche esposte.

Lo stalker

Quante volte per strada ci sentiamo osservati? Siamo in un luogo pubblico, frequentato da migliaia di persone, eppure non ci sentiamo al sicuro, vogliamo tornare a casa.
A casa nostra ci sentiamo protetti, ma in un mondo ormai interconnesso, è davvero così?
Di solito lo stalker è un collega, un conoscente, un ex partner che non si rassegna ad una storia finita, o anche uno sconosciuto. Per il nostro esempio prendiamo un conoscente.
Bob, così lo chiamiamo, vuole sapere tutto di Alice.
Di lei sa solo nome e cognome ma è già tantissimo. Si ricorda di aver letto dei suoi commenti e dei suoi post in alcuni gruppi su Facebook, che lo avevano affascinato, ma purtroppo non sono amici.
Bob inizia a cercarla su Facebook, escono tante ragazze con lo stesso nome e cognome. Non la trova, forse ha cambiato nome e relativo avatar.
Poco male, il Facebook ID non cambia.
Il Facebook ID è un numero formato da diverse cifre che permette di riconoscere l'utente in modo univoco all'interno di Facebook. Vedremo poi come questa informazione sarà utile a Bob.
Bob, decide quindi di registrarsi con un account fasullo e per farlo utilizza una mail temporanea, così sarà più difficile risalire a lui.
Esistono diversi servizi che offrono questa possibilità, uno di questi è "*10 minutes mail*"[64], un sito molto utile quando ci si vuole registrare ad un servizio senza fornire il proprio indirizzo e-mail e limitare il rischio di finire in chissà quale mailing list di spam.

[64] https://10minutemail.com/

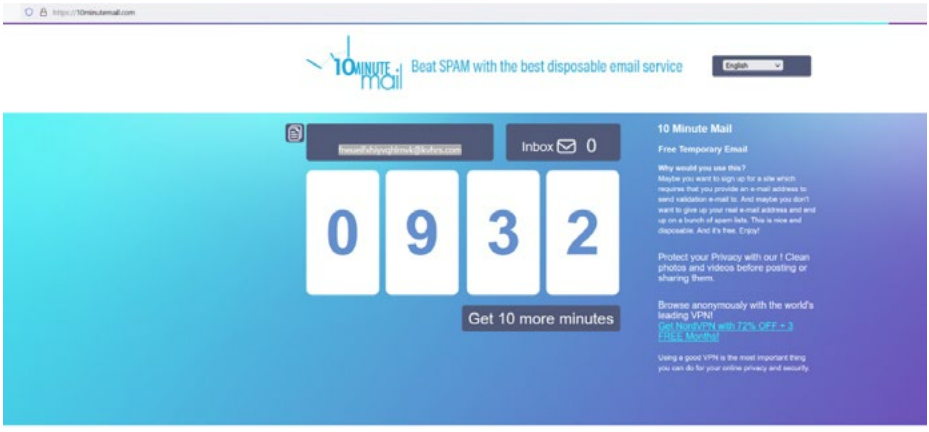


Figura 13: *10 Minute Mail*

Come sempre, siti nati con le migliori intenzioni, possono essere utilizzati per altri scopi.
Bob crea la sua e-mail temporanea e procede con la creazione del proprio account Facebook, iscrivendosi al social network.

Figura 14: *Iscrizione a Facebook*

Nella casella di posta temporanea ecco che arriva il codice di verifica.

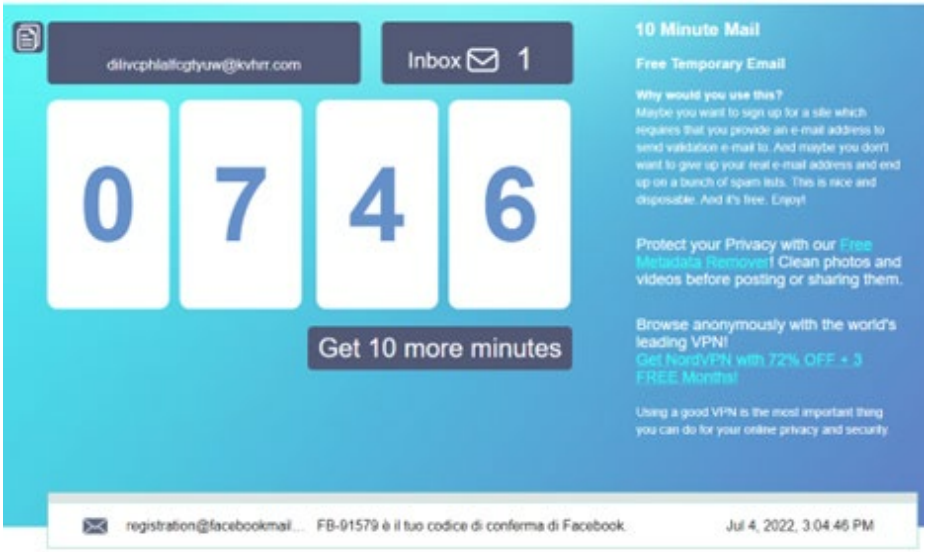


Figura 15: *Codice di verifica per l'iscrizione a Facebook*

Bob ora può terminare l'iscrizione, e procedere con la creazione del profilo. Per destare meno sospetti, configura un profilo femminile e un avatar carino e coccoloso come un gattino di pochi mesi. Inizia a postare foto, iscriversi a gruppi, chiedere amicizie, ecc. Nel giro di poco tempo, l'account ha diversi contatti e foto prese dal web.

Ora è il momento di trovare Alice.
Tramite la ricerca, trova il post che Alice aveva pubblicato nel gruppo, e così risale al nuovo nome e al suo profilo.

Vi ricordate che prima avevamo detto che ci sarebbe servito il Facebook ID?
Ecco, tramite questo ID, Bob potrà effettuare delle ricerche in Facebook per vedere quali gruppi segue Alice, su quali foto ha messo i like e quindi recuperare tante informazioni sulla povera malcapitata.

Bob si collega quindi al sito "Lookup-ID"[65] che permette, tramite la URL di un profilo facebook, di risalire al Facebook ID associato.

[65] https://lookup-id.com/

Figura 16: *Lookup-ID*

Inizia quindi a cercare nei gruppi e i like:
https://www.facebook.com/search/1449054229/groups
https://facebook.com/search/1449054229/stories-liked

Fortunatamente Alice non è una sprovveduta, conosce i pericoli dei social media, quindi ha impostato correttamente la privacy del proprio account, permettendo solo ai suoi contatti di vedere le sue attività sul social.
Bob, non si arrende, proverà a recuperare le informazioni che gli interessano, come ad esempio l'indirizzo di casa, in altro modo.
Alice lavora, quindi avrà sicuramente un profilo su LinkedIn. Bob cerca su Google "Linkedin nome cognome Milano" e oltre ai profili Linkedin, Google mostra anche le foto.
Eccola, trovata!

Per fare le ricerche su LinkedIn bisogna essere registrati, poco male Bob procede con la creazione di un account fasullo, come già fatto in precedenza.
Per LinkedIn non basta la mail temporanea, serve anche un servizio di ricezione SMS per l'autenticazione a due fattori.
My Temp SMS[66], servizio che offre numeri di telefono virtuali usa e getta aggiornati mensilmente, nato sempre per finalità di tutela degli utenti da registrazioni e rischi di inserimenti in liste spam, fa al caso suo.

[66] https://fr.mytempsms.com/

Figura 17: *My Temp SMS*

Così Bob, ottiene il suo numero temporaneo su cui riceve il codice LinkedIn.
E, dopo aver completato la registrazione, provvede a cercare Alice, trovandola.

Figura 18: *Ricerca su Linkedin*

A questo punto, Bob sa dove lavora Alice, ma per avere maggiori informazioni deve chiederle il contatto.
Modifica il suo profilo fingendosi un neo assunto della società, inizia a chiedere i contatti ai più giovani, nel giro di qualche ora Bob ha già 5 contatti.
A questo punto, Bob chiede il contatto diretto. Alice, accetta, dopotutto ci sono diversi contatti in comune.
Bob trova solo poche informazioni, quella più interessante è la mail personale, niente cellulare. Guarda su Internet per trovare il numero dell'azienda dove lavora Alice, per provare a farsela passare o meglio ancora a farsi dare il numero di cellulare.

Purtroppo, non riesce nell'intento, la società non fornisce queste informazioni al telefono.
Trascorre qualche giorno nei pressi dell'ufficio per vedere se riesce a incrociarla, capire gli orari, etc.
Finalmente la vede, arriva, prende il caffè al bar all'angolo, torna in ufficio e alle 19:00 esce.
La segue, la vede che sale in auto e si segna il numero di targa.
I giorni seguenti cerca la macchina, in un punto nascosto con il biadesivo Bob attacca un AirTag - Apple[67], un piccolo dispositivo che permette di trovare le cose che perdi. Dove sono le puoi vedere direttamente nell'app "Dov'è" che serve per localizzare i dispositivi Apple e rintracciare amici e familiari.

Ecco, che con una spesa di pochi euro, Bob ha scoperto dove abita.
Inserisce le coordinate su Google Maps, e raggiunge la sua destinazione.
La macchina di Alice è proprio parcheggiata lì.
Bob recupera il suo AirTag e si mette in macchina.
Dal cellulare Bob prova a vedere quali siano le reti Wi-Fi disponibili, su F-Droid[68], repository alternativo e senza tracciamento al Google App Store, ci sono diverse app che analizzano le connessioni Wi-Fi.
WiFiAnalyzer[69], software open source creato per supportare gli utenti nell'ottimizzazione della propria rete Wi-Fi, fa al caso suo: semplice e immediato.
Bob ha rilevato un router Zyxel.

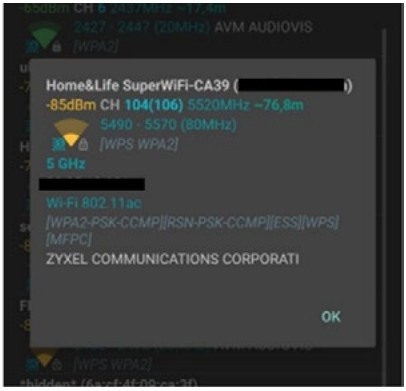


Figura 19: *Rilevazione del router Zyxel*

[67] https://www.apple.com/it/airtag/

[68] https://f-droid.org/

[69] https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer&hl=it&gl=US

Le credenziali amministrative di default di questo tipo di router sono ricostruibili in base al serial number. Se Alice non ha cambiato la password di default, questa è recuperabile.
Non avendo il serial number, Bob usa un programma che gli permette di generare tutti i serial number, e sempre tramite applicazioni create ad hoc e liberamente disponibili sul web, come "zykgen"[70], Bob crea il suo database delle password.

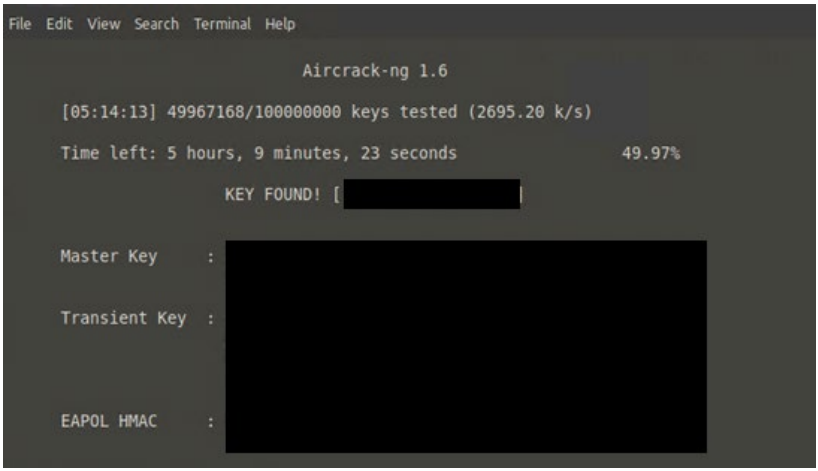


Figura 20: *Aircrack-ng*

In seguito, con un portatile e l'antenna esterna ad alto guadagno, grazie a Aircrack-ng[71], suite completa di strumenti per valutare la sicurezza della rete Wi-Fi, Bob riesce ad individuare l'SSID e ad effettuare tutti i passaggi propedeutici all'attacco Brute Force, che, tramite la lista delle password che aveva generato in precedenza, dopo circa 10 ore di attesa, gli permette di ottenere la password del Wi-Fi di Alice.

A questo punto a Bob non resta altro da fare che collegarsi al Wi-Fi di Alice e tramite Wireshark[72], software nato per supportare nella risoluzione di problemi sulla rete e che permette di intercettare i dati che vi transitano, riesce a capire cosa è connesso alla rete Wi-Fi.

[70] https://geeksrepos.com/luc10/zykgen
[71] https://www.aircrack-ng.org/
[72] https://www.wireshark.org/

In particolare, tramite Fing - Network Tool[73], strumento creato per supportare gli utenti a sfruttare al meglio la propria rete domestica, visualizzando tutti i dispositivi connessi al Wi-Fi, Bob scopre che connessi alla Wi-Fi vi sono una IP Camera, un PC Windows, una tv e un tablet.

Bob ha ottenuto un'informazione importante, c'è una IP Camera connessa, non gli resta che andare a casa a fare una ricerca su Shodan, dove inserisce l'IP della videocamera e ottiene le informazioni per l'accesso, in particolare la pagina di login. Prova diverse combinazioni di user e password, ma senza successo. Alice ha cambiato la password di default.

Bob non si arrende e decide di provare a cercare quale potrebbe essere la password utilizzata. Prova quindi a ricostruire la mail aziendale tramite Google Dorks:
`inurl:https://www.azienda-casestudy.it AND intext:@azienda-casestudy.it`

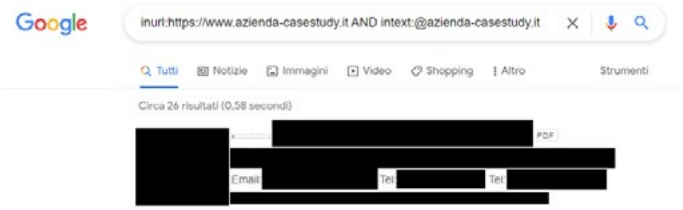


Figura 21: *Google Dorks*

Bob nota che le email sono costruite come nome.cognome@azienda-casestudy.it perciò prova ad inviare una mail così costruita, usando il nome e cognome di Alice. Non è importante il contenuto ma che il server non risponda che la mail non esiste. Nessuna risposta di errore, l'account esiste.
Ora Bob deve verificare se l'account aziendale e/o quello personale è contenuto in qualche breach, così da poter eventualmente recuperare le password associate.
È risaputo, dopotutto, che spesso si usano le medesime password su diversi servizi per essere certi di ricordarle.

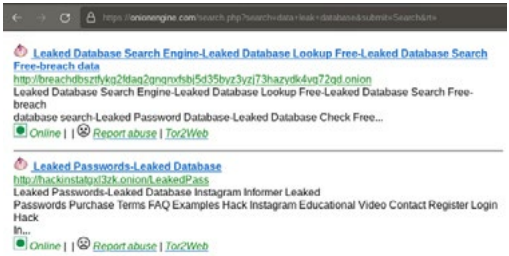
Bob, quindi, cerca i due account su "Have I Been Pwned"[74], sito creato a supporto degli utenti per verificare se i propri account sono stati oggetto di qualche breach. Purtroppo, uno dei due account è presente in diversi leak, alcuni dei quali vedono coinvolti dati come e-mail e password. Esattamente quelli che servivano a Bob.

[73] https://www.fing.com/

[74] https://haveibeenpwned.com/

Figura 22: *Risultati del data breach in "Have I been pwned?"*

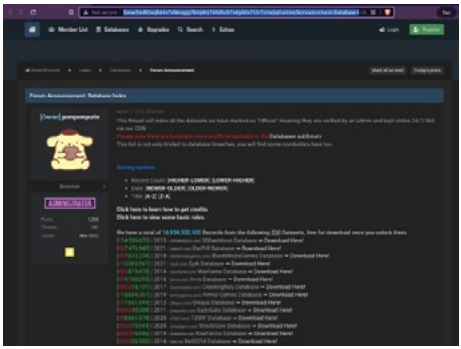
Ora Bob non deve fare altro che cercarli nel Dark Web per reperire le informazioni che gli servono.



¶

Figura 23: *Ricerca sul Dark Web*

Bob inizia quindi la ricerca delle password ed ecco che la password *"Alice_Case-Study2022"* è presente in un leak, associata alla sua email personale e collegata a un numero di cellulare.



¶

Figura 24: *Forum sul Dark Web*

Bob prova a chiamarla nascondendo il suo numero telefonico e utilizzando una linea VOIP[75].
Deve solo assicurarsi che sia il suo numero.
Si finge quindi un addetto del servizio clienti di una nota azienda di servizi e chiama Alice chiedendole di confermare la sua identità.
Alice, scocciata, risponde confermando di essere la persona che stanno cercando, precisando di essere impegnata e chiudendo in fretta la comunicazione.
Per Bob è sufficiente, ora ha anche il numero privato e una serie di password da provare per accedere alla IP Camera.

[75] Voice Over IP, https://it.wikipedia.org/wiki/Voice_over_IP

Ne prova alcune e questa volta ha fortuna.
Alice, come prevedibile, ha riutilizzato la password su altri servizi, noncurante di tutte le raccomandazioni sull'uso corretto delle password che ormai sempre più spesso troviamo nelle pagine di registrazione dei diversi servizi online.

Grazie a questa sua noncuranza, ora Bob può accedere remotamente alla IP Camera, tranquillamente dal suo browser, dove vuole e quando vuole, per spiare Alice nell'intimità delle mura di casa e non solo.

Conclusioni

"Nell'acronimo IoT, la S sta per Sicurezza"
Questa è una delle battute più popolari quando si parla di "*Internet delle Cose*" che ci ricorda come questi dispositivi siano stati adottati e largamente diffusi senza prendere in considerazione gli aspetti di sicurezza ed i rischi di privacy, aggravati ancora di più, come abbiamo visto (*vedi Cap "Big data e analisi tramite tecniche di intelligenza artificiale"*), dalla diffusione dei Big Data ed all'uso sempre più comune di Intelligenza Artificiale.
D'altra parte, i cyber attacchi non concedono tregua (*vedi Cap "IoT e rischi di Cyber Security"*).
Lo scenario risultante è preoccupante: con l'applicazione sempre maggiore di IoT e una altrettanto scarsa attenzione alla sicurezza, la superficie di attacco per i cyber criminali risulterà sempre più ampia.
Come si risolve questa situazione?
Nell'attesa che norme come la ISO/IEC 27400 diventino obbligatorie (*vedi Cap. "Aspetti di Compliance e Privacy"*), l'onere di migliorare la sicurezza dell'ambito IoT spetta sia ai produttori che agli utenti.

Raccomandazioni per i produttori

I produttori di IoT, per quanto esperti nel produrre applicativi standard, mostrano spesso gravi lacune già in fase di design per quanto riguarda la sicurezza degli apparati.
Alla luce di tutti gli aspetti finora presi in esame, è necessario che queste lacune siano colmate nel più breve tempo possibile.
È inderogabile, infatti, sviluppare protocolli, strategie e standard di sicurezza più efficaci per il settore IoT per non compromettere la sicurezza e la privacy degli utenti.
Come stabilito da GDPR, i principi di *privacy by default* e *privacy by design* hanno evidenziato l'importanza di tutelare i dati personali degli utenti e che queste tutele devono iniziare fin dalle fasi di progettazione dei dispositivi, cercando in questo modo di prevenire i rischi di privacy e sicurezza.

Ogni dispositivo IoT dovrebbe quindi prevedere:
- un sistema di cifratura dei dati salvati;
- una modalità sicura di invio dei dati via Internet;
- l'utilizzo di autenticazione e, possibilmente, la modifica obbligatoria delle credenziali di default;
- la verifica periodica di eventuali vulnerabilità e l'invio tempestivo di patch per risolverle;
- la possibilità di aggiornare agevolmente il firmware.

Raccomandazioni per gli utenti

Gli utenti andrebbero scoraggiati dall'utilizzo di dispositivi IoT che non dispongano delle caratteristiche di sicurezza di base appena esposte.
Ma spesso non si dispone della consapevolezza necessaria sui rischi e sulle implicazioni per gli aspetti di sicurezza e di privacy derivanti da un uso poco accorto di dispositivi IoT non *hardenizzati*.
In attesa che i produttori intervengano quanto prima sulla questione di rendere più sicuri gli IoT (già dalla fase di design!), gli utenti possono però intervenire in questi ambiti:

a) Autenticazione: se i dispositivi IoT prevedono un'autenticazione è prioritario modificare le credenziali di accesso di default, o, quantomeno, la password. La nuova password deve essere univoca per dispositivo e sufficientemente complessa.
b) Connessioni sicure: i dispositivi devono essere dotati di sistemi di connessione su Internet sicuri, ad esempio tramite l'adozione di protocolli di rete adeguati e all'avanguardia o l'utilizzo di VPN.
c) Segmentazione: i dispositivi meno sicuri vanno separati dai sistemi più critici (valido in particolare in presenza di applicativi privi di sistemi di autenticazione).
d) Accessi: è necessario verificare le risorse a cui hanno diritto di accesso i singoli dispositivi assicurandosi che, in caso di violazione degli IoT, i sistemi ed i dati più sensibili risultino comunque protetti.
e) Policy: è una buona prassi stabilire politiche per i dispositivi non autorizzati, in modo da consentire, se necessario, un accesso parziale alla rete ed alle risorse, isolando le informazioni ed i sistemi più sensibili.
f) Aggiornamenti: I dispositivi IoT devono essere aggiornati con le ultime patch di sicurezza software e del firmware in modo da mitigare le problematiche che i cyber criminali potrebbero sfruttare per violare i sistemi. È importante verificare con frequenza la disponibilità di eventuali nuovi aggiornamenti e, nel caso siano presenti, applicarli tempestivamente.
g) Vulnerabilità: è fondamentale, infine, che gli IoT siano inclusi nelle normali verifiche di routine dei sistemi informatici per identificare e mitigare periodicamente eventuali vulnerabilità. Come sempre, il consiglio è di eseguire questi controlli regolarmente e di risolvere le problematiche rilevate nel più breve tempo possibile.

Consapevolezza dei rischi

L'Internet delle Cose è ormai una realtà consolidata che avrà applicazioni sempre maggiori (vedi Cap. "Campi di applicazione).
Allo stesso tempo i cyber attacchi verso questi dispositivi saranno sempre più frequenti ed i rischi per la privacy aumenteranno in modo esponenziale.
Essere consapevoli dei rischi e delle minacce che gli IoT comportano è ormai una priorità, così come trovare il giusto compromesso per mitigare questi pericoli.

È indispensabile tenersi sempre aggiornati, le minacce e le tipologie di cyber attacchi sono in continua evoluzione ed anche la tecnologia si evolve rapidamente:

- Il 5G consentirà il collegamento di molti più dispositivi e quindi anche di molti più oggetti intelligenti;
- La sensoristica sta progredendo sia negli ambiti di applicazione sia nell'hardware: i sensori sono sempre più piccoli, più precisi e più raffinati;
- Le tecniche di analisi dei dati raccolti diventano sempre più sofisticate.

La previsione di una maggiore diffusione di oggetti e sensori intelligenti collegati alla rete amplifica notevolmente i rischi legati alla sicurezza; per questo è prioritario sensibilizzare sempre di più gli utenti, fornendo informazioni ed esempi in modo da prevenire i danni derivanti dai rischi più comuni.

Le informazioni che abbiamo raccolto in questa pubblicazione, cercando di dare una prospettiva ampia di questo ambito, vanno esattamente in questa direzione: l'obiettivo è divulgare ad un pubblico più ampio possibile le opportunità del mondo IoT ed i rischi che derivano da un uso poco accorto di questa tecnologia.
Se da una parte, infatti, la tecnologia può avere impatti molto rilevanti sulla società e sul progresso, gli svantaggi possono essere mitigati solo dall'educazione degli utenti alla consapevolezza dei rischi.

Ringraziamenti

Competenze, Condivisione e Crescita:
dalle tre “C” nasce il progetto Women For Security, il presento lavoro è uno degli esempi concreti delle attività della community.

Ringrazio, a nome di tutto il Comitato Direttivo, le Cyber Ladies che hanno dedicato tempo e sforzi alla stesura di questa pubblicazione.

Ringrazio tutti i professionisti che da anni lavorano per sensibilizzare la comunità sui temi della cybersecurity e sulla protezione degli asset.

Noi continueremo ad impegnarci nella diffusione di una corretta cultura digitale con l’auspicio che le nuove generazioni abbiano tutte le informazioni necessarie per poter fare le scelte personali, professionali che sono sul campo, prive di divisioni di genere.

Stay tuned

Cinzia Ercolano
Founder Women For Security

WOMEN
for Security

womenforsecurity.it