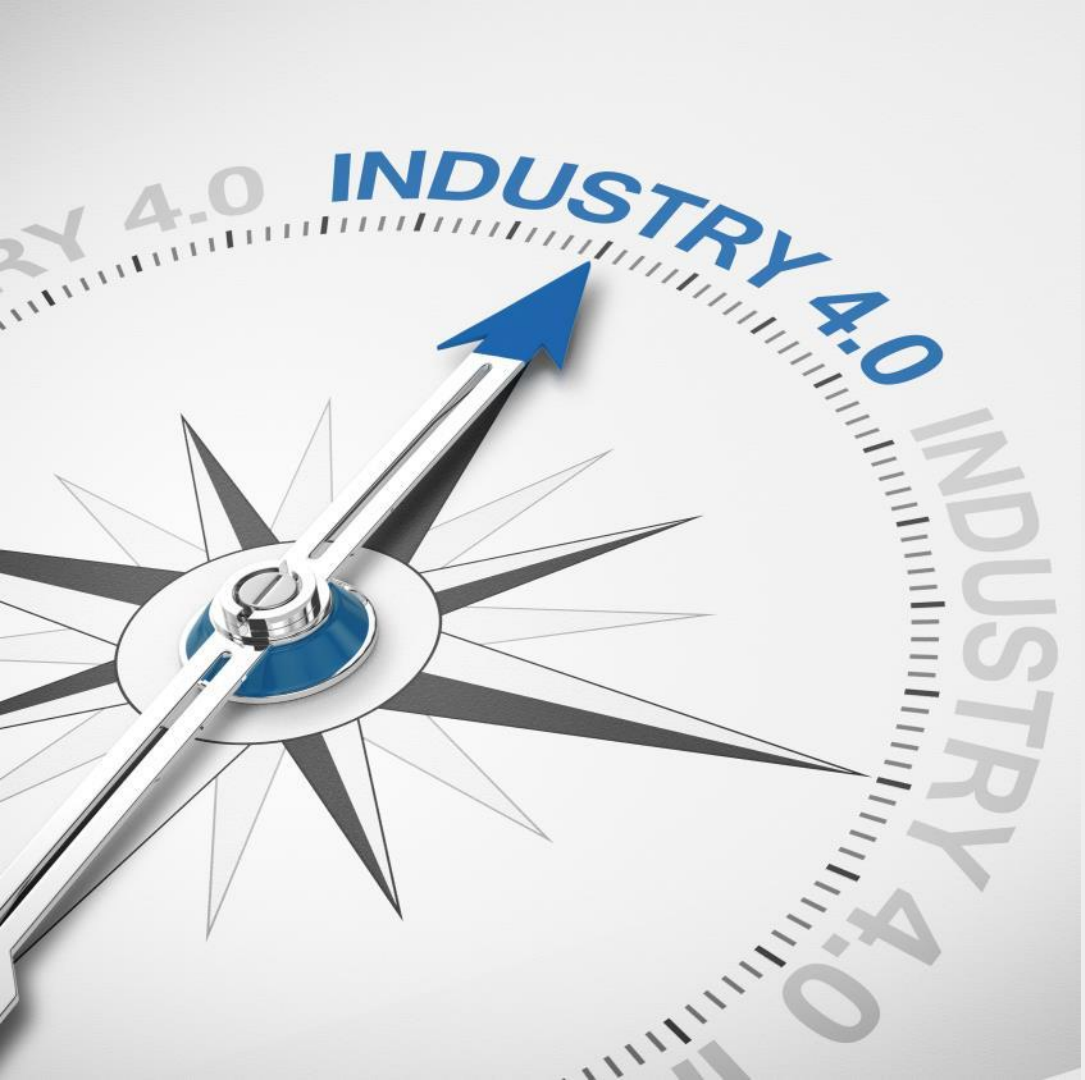


Cybersecurity e Industry 4.0: Le nuove sfide

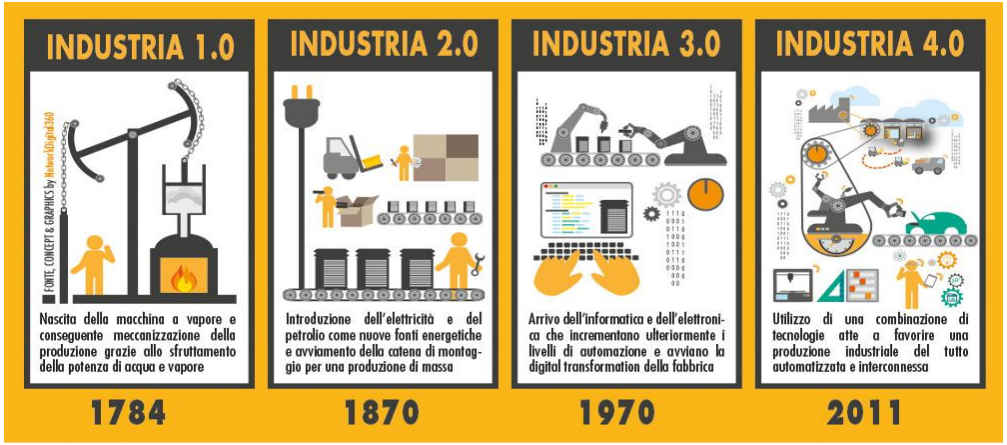
Paolo Maccarrone

Politecnico di Milano
School of Management

Organizzato da

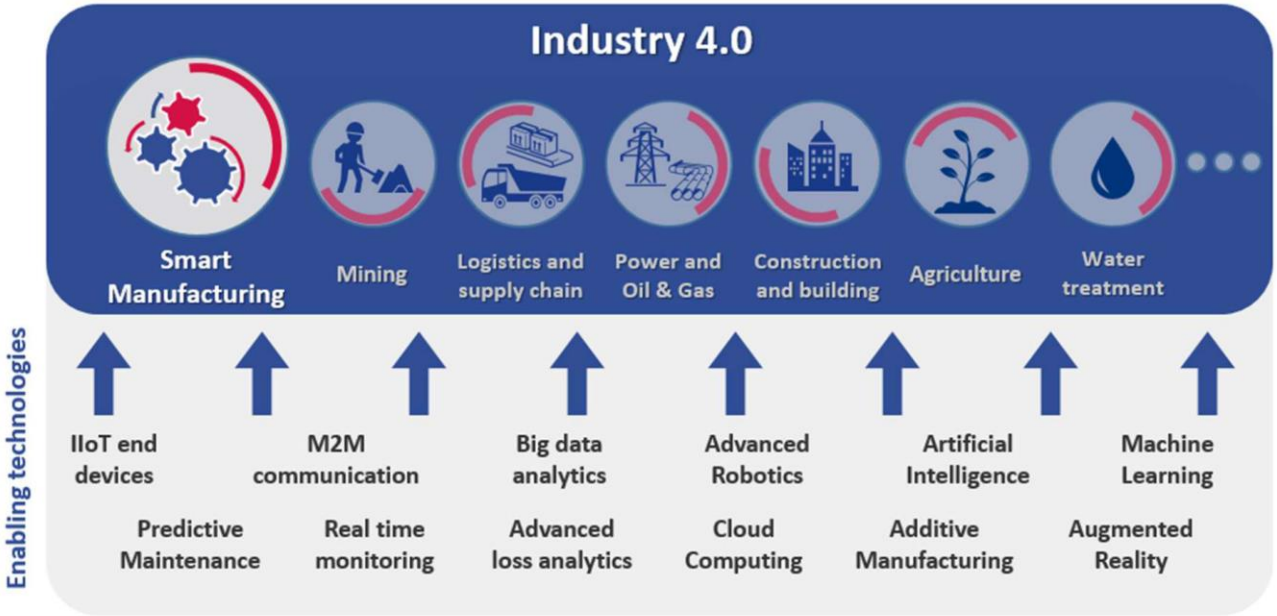
Industry 4.0

- La «quarta rivoluzione industriale»:



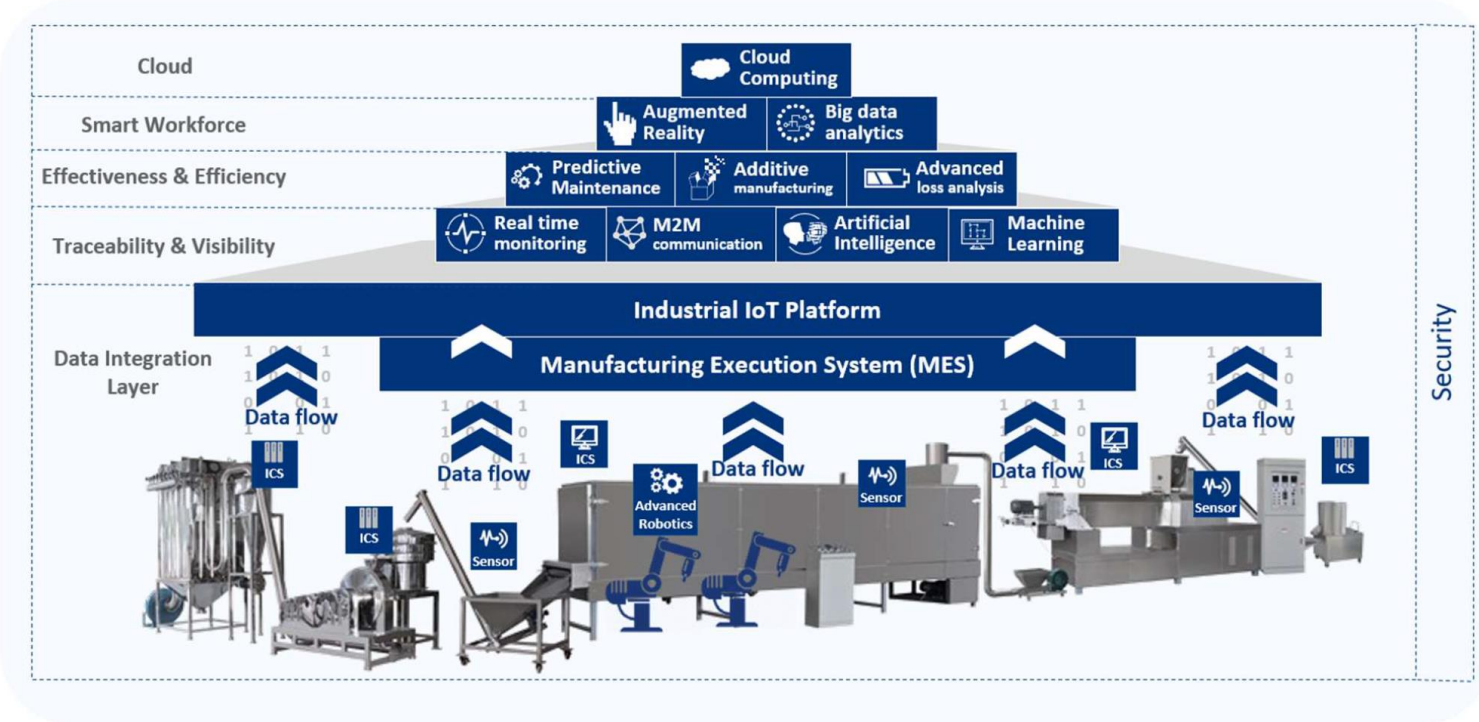
- Può essere vista come un'evoluzione dell'**automazione industriale**, caratterizzata da una marcata **interconnessione** tra sistemi fisici e digitali e dall'utilizzo (anche **real time**) di una mole sempre più ampia di **informazioni** provenienti da un numero crescente di **fonti**

Le «key enabling technologies»



Fonte: ENISA

La *smart factory*



Fonte: ENISA

La rilevanza strategica della cybersecurity

- La **cybersecurity** viene spesso considerat come un'altra componente essenziale di industry 4.0

- Questo perché solo un **adeguato livello di protezione** nei confronti degli attacchi di natura digitale può assicurare il **corretto funzionamento** dei sistemi industriali «digitali», nonché prevenire pericolosi **furti di dati** «mission critical»

Una definizione di cybersecurity

L'insieme di **strumenti, procedure e sistemi** che consente a una entità (ad esempio, una nazione, una organizzazione, un cittadino) la ***protezione dei propri asset fisici*** e della ***confidenzialità, integrità e disponibilità delle proprie informazioni*** attraverso un'attività di **prevenzione, rilevazione e risposta** agli attacchi provenienti d**al «cyberspazio»**

- Alcune considerazioni:
  - Gli attacchi provengono dal **«cyberspazio»:** con questo termine si intende il dominio virtuale costituito dall'insieme di PC, sistemi informativi e reti di telecomunicazione interconnessi a livello globale
  - Due tipologie di **asset sotto attacco**: **dati** e **infrastrutture fisiche** → i confini tra sicurezza **logica** e sicurezza **fisica** sono sempre **meno definiti**

Gli elementi di complessità della cybersecurity

La complessità della cybersecurity dipende da molteplici fattori:

- **differenti target**
- **differenti finalità degli attacchi**
- **pluralità di attacker**

- Questo implica che la stessa vulnerabilità possa essere sfruttata per portare attacchi molto diversi fra loro, a seconda della natura dell'attaccante e della finalità
- Le tre dimensioni sopra riportate verranno illustrate più dettagliatamente nel seguito

- La cybersecurity può riguardare:

AMBITO	DESCRIZIONE
TELECOMMUNICATIONS (o NETWORK) SECURITY	Protezione nei confronti delle **minacce all'infrastruttura di telecomunicazione**
INFORMATION (o DATA) SECURITY	Protezione contro la minaccia di **furto, cancellazione o alterazione di dati** memorizzati o trasmessi all'interno di un sistema informativo (o su altro supporto)
(CRITICAL) INFRASTRUCTURE SECURITY	**Protezione contro attacchi (di natura sia digitale che fisica)** che possono provocare danni ad asset fisici strategici, come nel caso delle infrastrutture critiche di un Paese

- Un paio di considerazioni:
  - attenzione alle possibili conseguenze di una attacco «cyber» sull'**operatività** di sistemi/apparati/infrastrutture (→ ottica «di processo»)
  - Gli attacchi provenienti dal cyberspazio possono provocare danni anche agli **asset fisici** (ex: le infrastrutture critiche), anche in combinazione con attacchi di natura fisica

La cybersecurity: le differenti finalità

- Gli attacchi cibernetici sono perpetrati con finalità differenti. Si distingue generalmente tra **Cyber Crime**, **Cyber Terrorism** e **Cyber Warfare:**

AMBITO	DESCRIZIONE	FINALITA'/ DETERMINANTI
CYBER CRIME	**Atti criminali** commessi **usando sistemi informativi o reti di comunicazione** elettroniche **al fine di perseguire vantaggi di tipo economico**	**Economiche**
CYBER TERRORISM	**Attacchi** che, attraverso l'utilizzo e lo sfruttamento di computer o reti di comunicazione, sono **volti** a generare incidenti tali da **generare paura o danni** nei soggetti «target»	**Ideologiche**
CYBER WARFARE	**Attacchi**, che fruttando computer o le reti di comunicazione, sono **volti a danneggiare gli asset fisici o digitali di una nazione** al **fine di comprometterne l'operatività**	**Politiche/ Militari**

La cybersecurity: le tipologie di attacker

Le minacce di tipo cyber possono essere apportate da soggetti diversi, generalmente raggruppati in due macro-categorie:

- Attaccanti **esterni all'impresa**,
- Attaccanti **interni all'impresa**

- Va poi distinto tra i «mandanti» ed esecutori materiali dell'attacco

- Alcuni soggetti possono essere «veicoli» inconsapevoli (o strumentalmente utilizzati da terzi per condurre l'attacco)

	FONTE MINACCIA	DESCRIZIONE
ESTERNI	**Nazioni**	In un contesto di evoluzione del concetto di «warfare» gli stati si stanno dotando di capacità offensive volte a **generare attacchi nei confronti di «nazioni nemiche»** finalizzati a impossessarsi di dati sensibili, proprietà intellettuali o a bloccarne l'operatività
	(Black) hackers	Soggetti che cercano di **ottenere il controllo o bloccare** i sistemi ICT per poi chiedere un riscatto, o sfruttano le vulnerabilità per **rubare dati** (che poi rivendono nel «dark web»)
	(Cyber) terroristi	Individui o organizzazioni interessate a effettuare **attacchi volti a generare paura all'interno di comunità/gruppi/nazioni**
	Competitor industriali	I competitor industriali possono essere **interessati a ottenere informazioni** (quali ad esempio dati o proprietà intellettuali) o a **compromettere le attività operative dei rivali**
	Fornitori	**I fornitori** possono costituire per le imprese **una minaccia** non solo come veri e propri **attaccanti,** ma soprattutto **come veicoli privilegiati per avere accesso alle reti e alle infrastrutture aziendali,** sfruttando ad esempio i canali/strumenti che le imprese lasciano a disposizione dei propri fornitori al fine di fare telecontrollo e manutenzione da remoto degli impianti
INTERNI	**Dipendenti / manager**	I dipendenti possono essere **autori di azioni volontarie volte ad arrecare danni alla propria azienda**, ma **nella maggior parte** sono sfruttati da altre tipologie di attaccanti, quali **veicoli per ottenere l'accesso alle reti aziendali** attraverso tecniche quali il phishing e social engineering.

IT e OT: due mondi «storicamente» distinti

- Per decenni **Information Technology** e **Operation Technology** sono rimasti sostanzialmente **separate**:

	Operation technology	Information technology
Hardware/ software	**Hardware e software sviluppati ad hoc** per lo specifico utilizzo	Utilizzo di **soluzioni off-the-shelf** sia per quanto riguarda la componente hardware sia per la componente software
Protocolli di comunicazione	**Dispositivi stand–alone**, la cui comunicazione con altri apparati avviene con **protocolli proprietari**	**Dispositivi interconnessi** la cui comunicazione avviene attraverso **protocolli standard**
Sicurezza	Garantita dall'isolamento **dei dispositivi**	Garantita da una **continua implementazione di patch software** e dall'applicazione degli ultimi **standard/policy di sicurezza**
Ciclo di vita	Quantificabile in **decenni**	Quantificabile in **anni**
Responsabilità Gestione	La responsabilità della gestione di queste infrastrutture OT è tipicamente a carico delle **business unit operative**	La responsabilità della gestione delle infrastrutture IT è a carico del **reparto ICT**

ALE NICHE

CONFINDUSTRIA

… ma adesso non è più così!

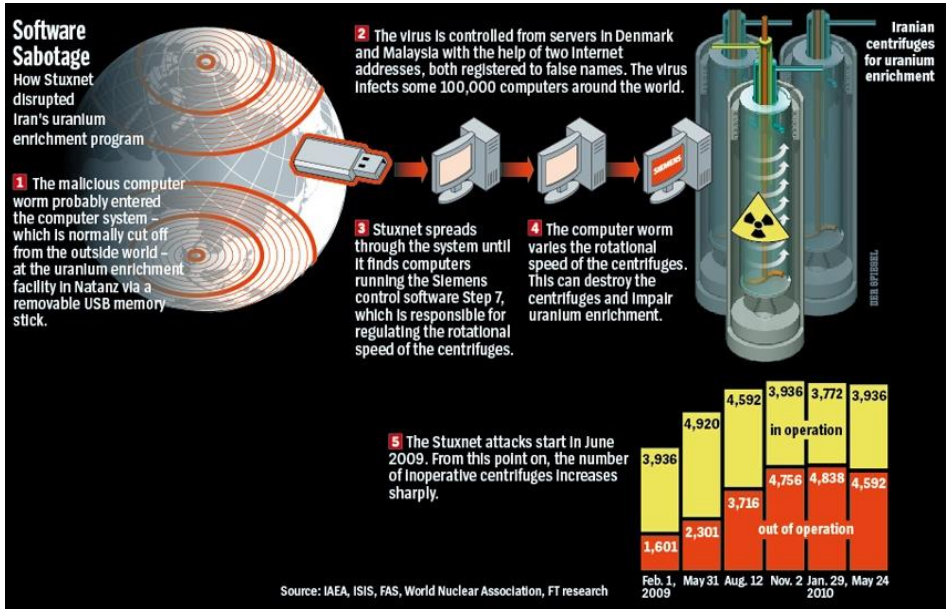
- La crescente diffusione delle tecnologie digitali nell'ambito dei processi produttivi e industriali «at large» ha portato all'**abbattimento delle barriere** tra IT e OT

- Questo però ha fatto sì che apparati e sistemi industriali fossero esposti a **nuove vulnerabilità**

Il primo caso di attacco ai sistemi industriali

- **Stuxnet** è un virus informatico appositamente creato e diffuso dal Governo statunitense nell'ambito dell'operazione "Giochi Olimpici", promossa da Bush nel 2006 (operazione che consisteva in un'ondata di "attacchi digitali" contro l'Iran in collaborazione col governo israeliano)

- Lo scopo del software era il sabotaggio della **centrale nucleare** iraniana di Natanz. In particolare, il virus doveva disabilitare le centrifughe della centrale, impedendo la rilevazione dei malfunzionamenti e della presenza del virus stesso



L’attacco alla power grid ucraina

Hackers behind Ukraine power cuts, says US report

26 February 2016

Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

Hackers were behind an attack that cut power to 225,000 people in Ukraine, a US report has concluded.

The December 2015 incident is thought to be the first known successful hack aimed at utilities.

- Nella vigilia del Natale 2015 venne perpetrato un attacco ai danni della compagnia ucraina di **distribuzione elettrica** Kyivoblenergo

- L’attacco fu realizzato attraverso un’**intrusione** da parte di un soggetto terzo **all’interno del network aziendale** e all’interno dei **sistemi SCADA** destinati al **monitoraggio delle cabine elettriche,** determinando la disconnessione dalla rete di 30 cabine elettriche (7 cabine a 110 kV e 23 a 35 kV) e la mancata fornitura di energia elettrica per tre ore a più di 225.000 utenti sul territorio ucraino

ANIE FEDERAZIONE
FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Gli attacchi si fanno più frequenti…

CYBERSECURITY

Maxi attacco hacker al big dell'alluminio, ferme in tutto il mondo le fabbriche di Norsk Hydro

Home > Cyber Security

Condividi questo articolo

Presi di mira i sistemi IT del gruppo utilizzando un ransomware: parte degli stabilimenti costretta a operare manualmente, chiusi molti degli impianti di estrusione. L'azienda: "Ripercussioni difficili da valutare"

19 Mar 2019

Patrizia Licata
giornalista

- Attacco condotto tramite **cryptovirus LockerGoga**
- Obiettivo: **bloccare i sistemi IT** e chiedono un **riscatto** per il ripristino
- L'azienda è stata costretta a **fermare diverse fabbriche di estrusione del metallo**, che trasformano l'alluminio grezzo in componenti per clienti che vanno dai costruttori d'auto alle aziende dell'edilizia
- Gli impianti che si occupano di fusione (in Norvegia, Qatar e Brasile) sono stati costretti a operare **manualmente**
- Esclusi solamente le centrali idroelettriche (gestiti con sistemi IT **indipendenti**)

ANIE FEDERAZIONE
FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

… anche in Italia:

«Nel Nordest un attacco informatico blocca le linee di produzione: tutti i lavoratori a casa. La stabilimento della società **Costan** (gruppo Epta) leader nell'allestimento di impianti frigoriferi per supermercati e ipermercati è chiuso da mercoledì 8 Maggio e i vertici sperano di poter riaprire lunedì 13. A casa quindi centinaia di lavoratori. Quando gli operai sono arrivati nello stabilimento si sono resi conto che era impossibile lavorare: la rete aziendale era «out of service». Stiamo parlando di una società da 1.140 dipendenti, ovvero una delle principali aziende metalmeccaniche della provincia di Belluno» (*Il Gazzettino*, 9 maggio 2019)

L’escalation continua…

LA STAMPA TECNOLOGIA

SEGUICI SU ACCEDI

NewsGuard, una squadra di giornalisti recensisce i siti di informazioni per ...

Il fondatore di Amazon presenta il modulo lunare "Blue Moon", ma Elon ...

Con Android Q arrivano le emoji gender fluid

Arriva la bicicletta elettrica superveloce

Aston Martin ritorna al 4 cilindri, per ora per il campionato DTM

Triton, il malware più pericoloso di sempre

Un virus in grado di manomettere impianti industriali e mettere in pericolo vite umane: è il primo di questo tipo

LEGGI ANCHE

ZIONE NAZIONALE
E ELETTROTECNICHE
TRONICHE

CONFINDUSTRIA

… e non è solo «terrorismo psicologico»

WIRED .IT Sezioni Wired Next Fest Gallery Wired Next

HOT TOPIC WIRED NEXT FEST 2019 GAME OF THRONES FACEBOOK TRAILER ELEZIONI EUROPEE SMARTPHONE AVENGERS GOOGLE VEDI TUTTI

HOME INTERNET WEB

di **Gabriele Porro**
Contributor
11 APR, 2019

Chi si rivede: Triton, il malware che provoca danni catastrofici, torna all'attacco

Mancano 11 giorni al Wired Next Fest. Scopri il programma

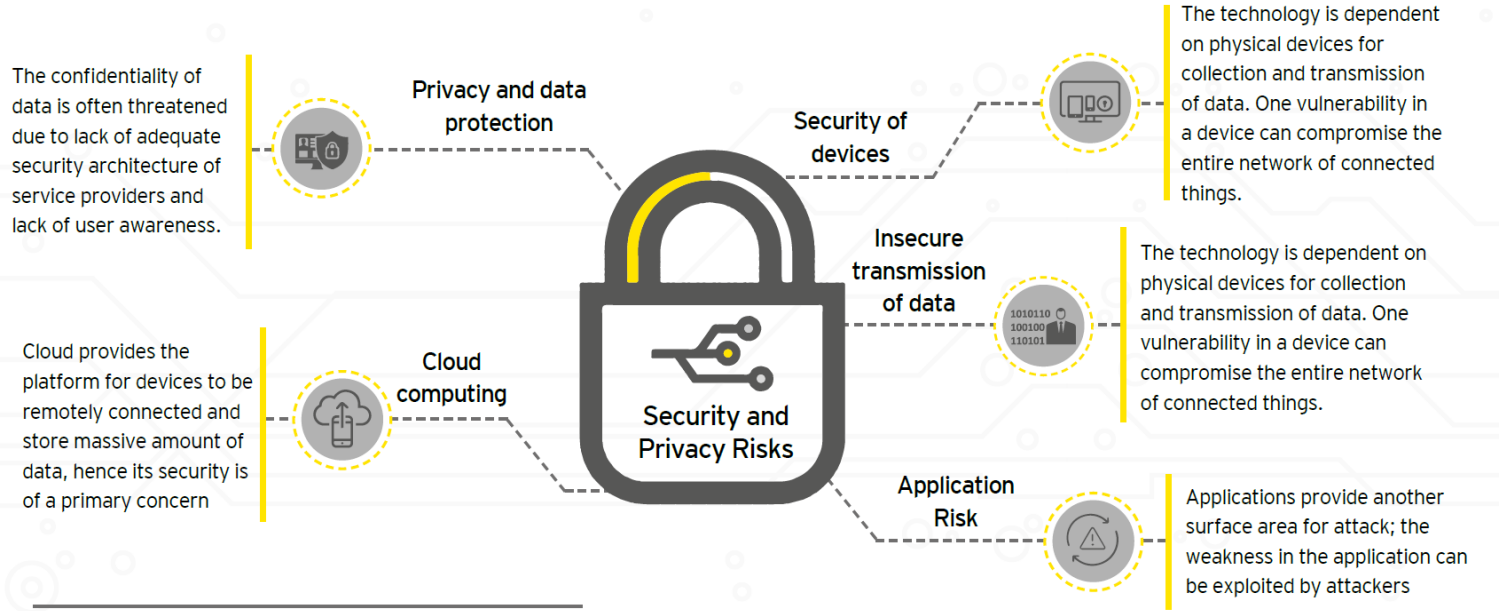
Scoperto un attacco con un impianto critico in Arabia Saudita. Il malware consente agli hacker di prendere il controllo di infrastrutture pericolose e di condizionarne l'attività. Il primo colpo nel 2017

Malware (Getty Images)

li hacker che nel 2017 ha manovrato il malware **Triton ha**

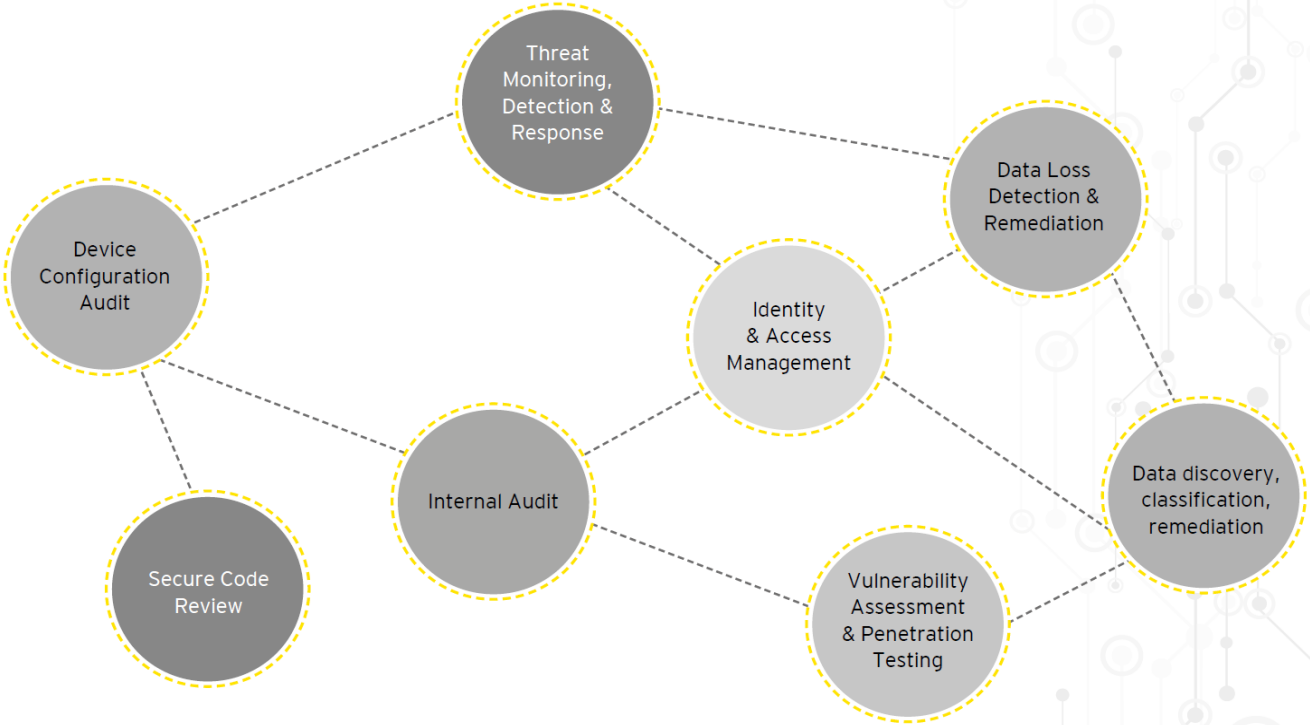
https://www.wired.it/internet/web/2019/04/11/triton-malware-arabia-saudita/

I rischi legati all'IOT



Fonte: E&Y

AI e cybersecurity: le potenzialità…



Fonte: E&Y

… e i rischi:

Data manipulation
AI and Machine learning systems make better predictions by analysing huge amounts of data. But if the learning data sets or algorithms can be manipulated, it can lead to potentially disastrous results for sectors specifically in healthcare, finance, etc.

Unauthorized access
Lack of strong access control, credential management and privilege account administration can lead to abuse of system functionalities and system availability by accessing the Machine learning algorithm data source and training method.

Protection of training data
Majority of the training data fed into a system consists of sensitive personal information for services like e-governance, healthcare, finance etc. Hackers can gain access to such confidential data by utilizing reverse engineering.

Unmasked PII
Personally Identifiable Information in unmasked form being used in an AI platform can lead to compromise of the data. Hence organizations need to ensure masking/ encryption of the PII.

Regulatory and compliance issues
Although analysis of huge amounts of data leads to more accuracy in providing core services, but getting adequate consent for data collection, processing and storage in order to comply to regulations pose a challenge.

Fonte: E&Y

La direttiva NIS

- La **direttiva NIS** – Network and Information Security – (EU 2016/1148) rappresenta, in ambito europeo, il **primo insieme di regole** relative alla **sicurezza delle reti e dei sistemi informativi**

- La **direttiva prescrive** agli stati membri dell'UE l'implementazione di **piani strutturati** volti a impedire che le reti e i sistemi informativi, a causa della loro importanza per il corretto funzionamento delle attività economiche e sociali, possano diventare facile bersaglio di **azioni tese a danneggiare o interromperne la loro operatività**

- In particolare la direttiva NIS si prefigge i seguenti obiettivi:
  - L'istituzione per ciascuno stato membro di un'**autorità nazionale competente per la sicurezza informatica** e di un **Computer Security Incident Response Team (CSIRT)**
  - L'istituzione di un **gruppo di cooperazione,** al fine d'agevolare il coordinamento strategico e lo scambio di informazioni inerenti ai rischi e alla gestione degli incidenti di sicurezza informatica
  - L'applicazione di **obblighi di cybersecurity** in capo agli **operatori di servizi essenziali (OSE)**

Gli obblighi per gli OSE

- Gli Operatori di Servizi Essenziali individuati in Italia sono 465, appartenenti a 8 settori strategici: **energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile** e **infrastrutture digitali**.

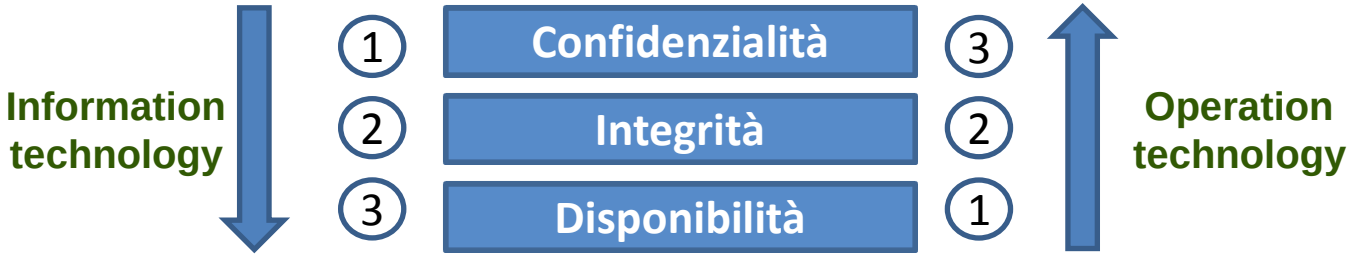
- Tali operatori saranno obbligati a:
  - adottare **misure adeguate atte a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete** e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali
  - **fornire all'autorità competente NIS**:
    - Le **informazioni necessarie a valutare la sicurezza della loro rete** e dei sistemi informativi, compresi i documenti relativi alle politiche di sicurezza
    - La **prova dell'effettiva attuazione delle politiche di sicurezza**, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato
  - **notificare** al Computer Security Incident Response Team (CSIRT) nazionale e per conoscenza alle autorità competenti NIS**, ogni incidente** avente un impatto **rilevante sulla continuità del servizio fornito**

La governance della cybersecurity in ambito industriale

Una corretta gestione della cybersecurity in ambito industriale implica:

- Lo svolgimento sistematico di attività di **risk assessment,** finalizzate a identificare gli asset aziendali a rischio e a monitorare le possibili minacce cui tali asset sono esposti
- La definizione delle **soluzioni** tecnologiche ed organizzative necessarie per garantire un sicurezza adeguato, la loro corretta implementazione e il monitoraggio dei risultati (secondo un classico ciclo Plan-Do-Check-Act)
- La corretta definizione di tutti gli aspetti **macro-organizzativi** (unità coinvolte, ruoli e responsabilità, procedure, flussi di comunicazione, ecc)
- La creazione di una **cultura organizzativa** orientata alla sicurezza informatica anche nell'ambito delle operations (tramite interventi di formazione, sensibilizzazione, ecc)

Le differenze tra IT o OT



Le differenti priorità determinano l'impossibilità di «replicare» semplicemente gli approcci di sicurezza sviluppati nel contesto IT (quale ad esempio l'aggiornamento o «patching» sistematico dei sistemi operativi) all'interno del contesto OT

Gli standard di riferimento

STANDARD	ENTE	DESCRIZIONE
ISA 62443	International Society for Automation (ISA)/ International Electrotechnical Commission (IEC)	Definisce **le linee guida da utilizzare per incrementare la sicurezza informatica degli Industrial Control System**, definendo 5 possibili livelli di sicurezza target da raggiungere.
IEC 62351	International Electrotechnical Commission (IEC)	Lo standard indica **policies, procedure e tecnologie** volte a implementare una **sicurezza di tipo end-to-end** per abilitare uno scambio di informazioni tra un mittente e un destinatario al sicuro da possibili accessi non autorizzati o da modifiche
NIST Cybersecurity Framework	National Institute of Standards and Technology (NIST)	Il Cybersecurity Framework è stato sviluppato come strumento a disposizione delle imprese per confrontare i propri **processi** e la propria **organizzazione**, al fine di evidenziare eventuali carenze e gap nell'approccio alla gestione dei rischi di cybersecurity e sviluppare piani di miglioramento
NIST 800-82	National Institute of Standards and Technology (NIST)	Lo standard **NIST 800-82** rappresenta una **guida volta a migliorare la sicurezza all'interno dei sistemi ICS,** aiutando le imprese a **identificare i possibili attacchi** a cui possono essere soggetti questi sistemi e le **possibili azioni** da adottare al fine di **sviluppare una una «defense-in-depth» strategy**
ISO 27019	International Organization for Standard / (IEC)	Lo standard identifica per il settore energy un **insieme di regole/practice volto a garantire la sicurezza dei sistemi di controllo e delle tecnologie di automazione** utilizzati per controllare e monitorare la produzione, trasmissione/distribuzione dell'elettricità, del gas, del petrolio e del calore.

Alcune considerazioni sugli standard

- Vi è un parziale **overlapping** tra alcuni standard, legata alla diversa origine geografica (tipicamente US vs. Europa), il che non facilita le imprese che operano su scala internazionale
- In ogni caso, pur se in continua evoluzione, gli standard relativi alla tematica della cybersecurity sembrano essere già discretamente maturi e adeguati nel supportare le imprese nella definizione dell'**ambito** («cosa proteggere») che delle **modalità** (il «come»)
- Il problema piuttosto sembra essere il livello di **adozione** di tali standard da parte:
  - degli **operatori** ai vari stadi della filiera (in particolare per gli standard focalizzzati sui sistemi di governance della sicurezza)
  - Dei **fornitori** (nel caso degli standard di prodotto)
- Con riferimento a quest'ultimo punto, le grandi imprese (leader di filiera) sembrano avere un ruolo chiave nell'incentivare i fornitori ad adottare questi standard e a sviluppare i prodotti in base a un approccio **«security-by-design»**