UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Cybersecurity:
- Tecnologia abilitante per industry 4.0

Mario Esposito

Matr. 1108742

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Gli argomenti

- **Premessa**
- **I principi fondamentali dell'organizzazione Industria 4.0**
- **Le quattro macro-direttrici di sviluppo della Smart Factory**
- **The Industrial Internet of things (IoT)**
- **Cloud**
- **Interconnessione**
- **Cybersecurity**
- **Conclusioni**

Premessa

- Una società nel settore metallurgico, dal 2018, per migliorare le proprie performance produttive, ridurre i propri consumi energetici e rimodernare la propria struttura, attua un piano di investimenti. Le innovazioni apportate, evidenziano la necessità di avere un fornitore unico, che garantisse, all'interno del sito stesso, la disponibilità di una produzione ossigeno, adeguata per quantità/qualità ed efficienza energetica.

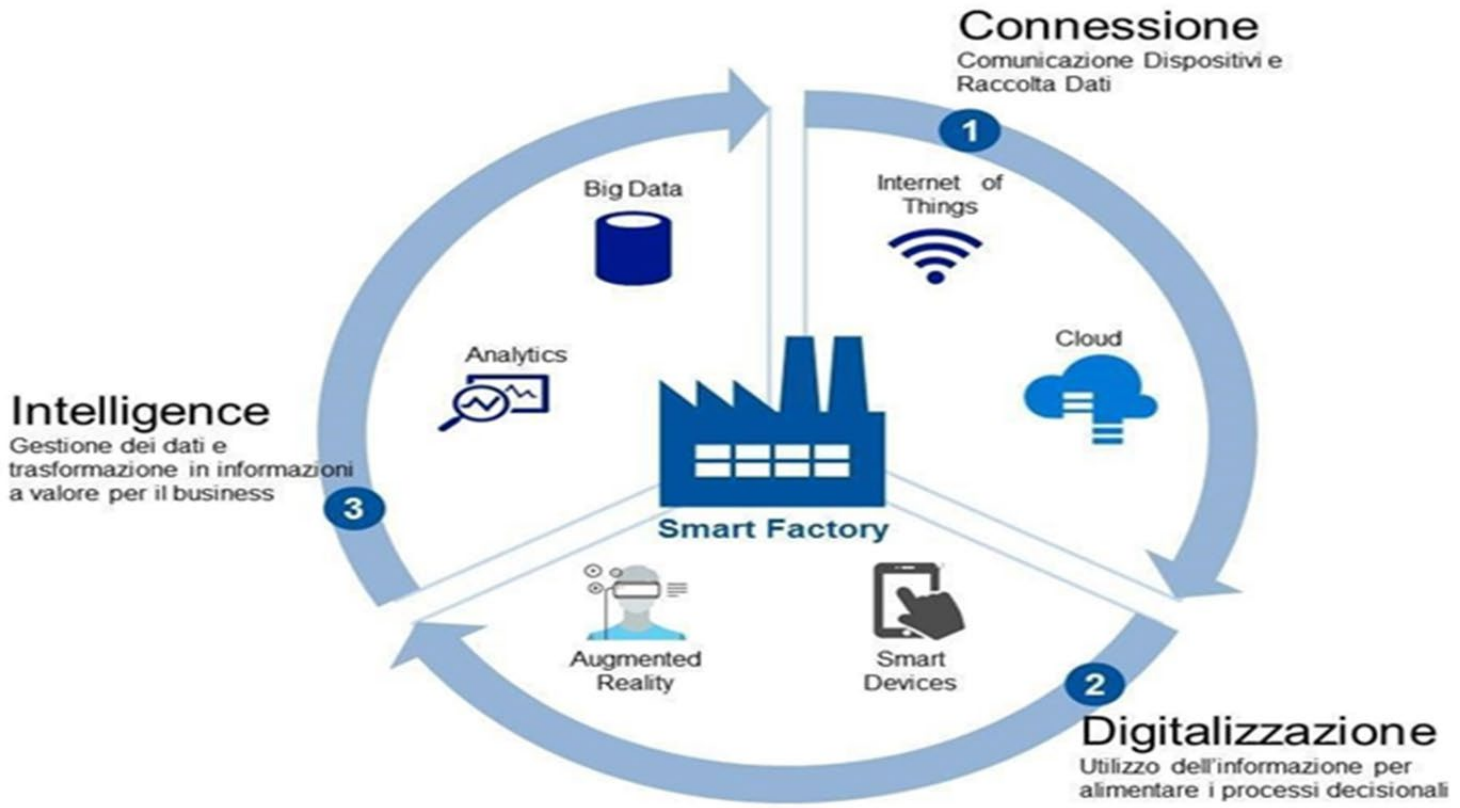
- Il fornitore, società del settore gas tecnici, già titolare del contratto di fornitura di prodotti gassosi on-site, presente all'interno del sito, con un proprio impianto di produzione , ha risposto a questa esigenza con la realizzazione e installazione un nuovo impianto di maggior capacità.

- Il Project Work elaborato nasce dall'esigenza di migliorare e rendere sicuro, un sistema di interconnessione, di raccolta e di elaborazione dei dati, controllato a distanza.

Premessa

PIANO NAZIONALE INDUSTRIA 4.0

I principi fondamentali dell'organizzazione Industria 4.0



"L'industria 4.0 fornisce le risposte pertinenti alla quarta rivoluzione industriale. ... L'industria 4.0 sottolinea l'idea di una digitalizzazione coerente e del collegamento di tutte le unità produttive in un'economia".

(Roland Berger Strategy Consultants)

I principi fondamentali dell'organizzazione Industria 4.0

- ***Interconnessione****: capacità da parte degli asset e delle risorse, di interagire e di scambiare informazioni con i sistemi interni ed esterni mediante l'utilizzo di una rete di scambio dati;*
- ***Virtualizzazione:*** *consiste in una riproduzione virtuale dell'azienda, che sta alla base del concetto di Industria 4.0;*
- ***Decentralizzazione****: capacità che hanno i sistemi intelligenti,* ***di assumere delle decisioni*** *autonomamente e di agire senza un intervento umano;*
- ***Interazione da remoto:*** *con questa funzione si è in grado* ***di interagire, a distanza****, con il sistema, di monitorare i processi o di intervenire;*
- ***Elaborazione in tempo reale:*** *per essere più produttivi ed efficaci, e per risolvere qualsiasi problema nel tempo più breve possibile, viene richiesta la presenza di funzioni che permettano di raccogliere rapidamente informazioni, trarne un valore utile in modo da esercitare azioni immediate;*
- ***Modularità:*** *permette, tramite l'integrazione della catena del valore con il sistema informativo, di modificare i meccanismi di produzione in* ***risposta alla domanda di mercato;***
- ***Orientamento al servizio:*** *il ruolo della tecnologia è stato ed è tuttora quello di contribuire non solo a creare un prodotto o un processo nuovo ma a* ***offrire dei servizi sfruttabili a proprio vantaggio dall'impresa****.*
- ***Sostenibilità****: consiste* ***nell'ottimizzazione del consumo di risorse energetiche*** *per valorizzare l'aspetto ambientale e sociale, migliorando anche le condizioni lavorative;*
- ***Interoperabilità:*** *capacità di due o più sistemi appartenenti ad imprese diverse* ***di scambiarsi dati al fine di creare delle reti di aziende che possano estendersi anche oltre i confini del territorio nazionale*** *in modo da consentire anche alle imprese medio-piccole di incrementare la propria competitività.*

Le quattro macro-direttrici di sviluppo della Smart Factory

- ***Dati, potenza di calcolo, connettività spinta****: unificazione in impresa dei dati e loro conservazione mediante* ***Big Data****, ossia una raccolta di dati sviluppata in termini di portata, varietà e rapidità con strumenti molto complessi, in grado di gestire, estrapolare e processare informazioni nel minor tempo possibile (Cloud Computing).*

- ***Analytics:*** *essere in grado* ***di riconoscere il valore dei dati raccolti*** *in termini di produttività, efficienza. Focalizzazione su dati meritevoli di analisi e di sviluppo.*

- ***Interazione tra uomo e macchina****: resa possibile grazie ai sempre più innovativi e diffusi dispositivi hardware e software, che garantiscono una* ***riduzione degli errori, dei tempi e dei costi*** *e un miglioramento della sicurezza dei processi;*

- ***Il ponte tra digitale e reale:*** *una volta raccolti i dati, analizzati, processati e codificati nelle macchine, è necessario trovare gli strumenti per produrre beni e servizi.*

The Industrial Internet of things (IoT)

- ***L'Industrial Internet of Things (IoT)*** *può essere considerato come* ***uno dei driver principali dell'Industry 4.0****. Esso* ***indica l'utilizzo della rete Internet per connettere dispositivi diversi e creare un sistema totalmente integrato di tecnologie****, ha assunto un ruolo centrale nella realtà industriale per via della crescente complessità dei sistemi industriali;*
- ***L'Internet of Things*** *comporta una serie di* ***vantaggi economici*** *poiché migliora l'efficienza operazionale e, conseguentemente, la produzione in quanto si ottiene* ***un risparmio in termini di costi e di tempi****, avendo una coordinazione più efficiente e veloce* ***dove l'analisi delle attività e dei processi di decision making*** *sono decentralizzate.*
- ***L'interconnessione*** *adoperata dall'Internet of things tra tutte le tecnologie e devices permette di fornire delle* ***soluzioni tempestive e rapide*** *qualora ci si trovi dinanzi a mutamenti all'interno dei processi operazionali.*
- *L'IoT ha avuto un impatto molto rilevante, condizionando la* ***creazione o la modifica di interi modelli di business****.*

Cloud

Tutto ciò ha comportato la necessità della nascita del ***cloud computing*** *cioè un accentramento dell'archiviazione presso le aziende di dati ed informazioni fondamentali.*

Il ***Cloud Computing:*** *gli utenti rinunciano al possesso di proprie risorse hardware e software acquisendole attraverso la semplice connessione internet secondo i propri bisogni.*

La ***principale criticità*** *derivante dall'adozione di un'infrastruttura Cloud riguarda sicuramente* ***la sicurezza dei dati.*** *L' utilizzo dei servizi cloud dovrà essere fatto ponderando prioritariamente, rischi e benefici, dei servizi offerti, l'affidabilità del fornitore e del servizio, oltre ad analizzare e prestare attenzioni alle clausole contrattuali, in particolare, le opportune cautele per* ***tutelare la confidenzialità dei dati.***

Le operation *di un'impresa prevedono numerose attività richiedenti una quantità di informazioni e una capacità di calcolo sempre maggiore, che richiede spesso di immobilizzare risorse finanziare.*

Le aziende 4.0, possono avere attività che richiederanno ***una maggiore condivisione dei dati*** *tra i siti e i confini aziendali.*

L’interconnessione

L’impianto normativo del Piano Industria 4.0, ruota intorno al ***concetto di interconnessione****, che ha suscitato dubbi e perplessità, chiarite con due circolari ai requisiti obbligatori, dapprima* ***la Circolare 23 maggio 2018, n. 177355 e successivamente con la Circolare 01 agosto 2018, n. 295485*** *del MISE.*

Affinché tale requisito possa considerarsi soddisfatto è necessario che il bene strumentale sia in grado di scambiare informazioni, attraverso un collegamento basato su protocolli di comunicazione, documentati, ***disponibili pubblicamente e internazionalmente riconosciute (TCP/IP, HTTP, MQTT, ecc****.) con:*

- *sistemi interni quali* ***gestionali****, sistemi di pianificazione, sistemi di progettazione e sviluppo del prodotto,* ***monitoraggio locale e remoto****, altre macchine dello stabilimento, etc.;*
- ***sistemi esterni*** *come i clienti, i fornitori, i partner nella progettazione e sviluppo collaborativo, altri siti di produzione, supply chain.*

Altro requisito obbligatorio ***prevede l’identificazione univoca del bene strumentale****, al fine di riconoscere l’origine delle informazioni, mediante l’utilizzo di standard di indirizzamento internazionalmente riconosciuti.*

L’interconnessione

- *Va però ricordato che, con riferimento ai "Beni strumentali il cui funzionamento è controllato da sistemi computerizzati o gestito tramite opportuni sensori e azionamenti” –* ***il requisito dell’interconnessione viene ulteriormente a specificarsi sotto un duplice profilo.***
- *In primo luogo, caratteristiche obbligatorie richieste per tali beni figura anche quella della “****interconnessione ai sistemi informatici di fabbrica con caricamento da remoto di istruzioni e/o part program****”; detta caratteristica si considera soddisfatta, se “…****il bene scambia informazioni con sistemi interni*** *(es: sistema gestionale, sistemi di pianificazione, sistemi di progettazione e sviluppo del prodotto, monitoraggio, anche in remoto, e controllo, altre macchine dello stabilimento, ecc.) per mezzo di un collegamento basato su specifiche documentate, disponibili pubblicamente e internazionalmente riconosciute.*
- *In secondo luogo, la citata circolare n. 4/E del 2017 ha previsto che i beni devono soddisfare anche al requisito della “****integrazione automatizzata con il sistema logistico della fabbrica o con la rete di fornitura e/o con altre macchine del ciclo produttivo****”.*

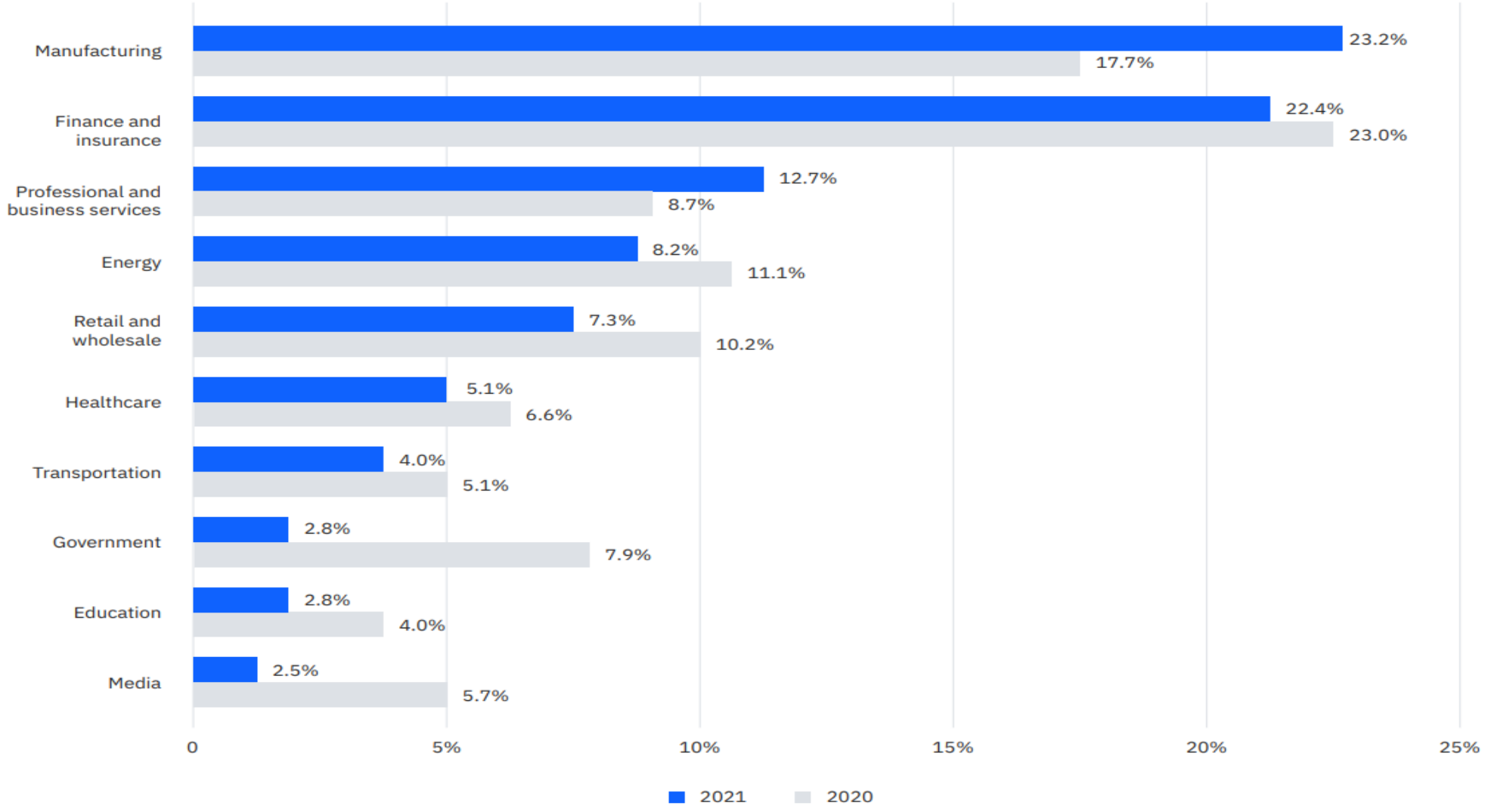
Cybersecurity

- *L'aumento della connettività comporta l'aumento anche dell'esigenza di **proteggere i sistemi di produzione e la rete informatica** da potenziali minacce, e conseguentemente aumenta per l'Industria 4.0 il rischio di attacchi informatici.*
- *La **cybersecurity** raggruppa tutte quelle tecnologie che aiutano a proteggere il sistema informativo da attacchi che possono causare la perdita o la compromissione di dati sensibili.*
- *La frequenza di tali attacchi è sempre più elevata. Gli hacker professionisti riescono con l'utilizzo di un qualsiasi device ad entrare nelle reti, potendole alterare. Questa situazione crea disordine e dissesto poiché consegue una perdita a danno dell'azienda.*
- *C'è necessità di **considerare la sicurezza una priorità**, insieme ad altri indicatori, tra cui la definizione dei ruoli e di metriche chiare, così come la **valutazione del rischio informatico**.*
- *Tuttavia, la trasformazione digitale rappresenta un'opportunità anche per i responsabili della sicurezza e per il settore IT poiché possono sfruttare il suo utilizzo per essere maggiormente competitivi.*

Cybersecurity

- La crescita esponenziale dell'integrazione tra il mondo OT (Operational Technology) e il mondo IT (Information Technology), ha contribuito a migliorare e snellire la gestione dei processi industriali, ma dall'altro sono aumentati i rischi e le possibilità di subire attacchi informatici.
- In ambito industriale, particolarmente a rischio sono i **sistemi ICS *(Industrial Control Systems)*** che si occupano di gestire **l'interazione e l'interconnessione** tra i macchinari industriali di un'azienda.
- I sistemi di controllo spesso si interfacciano con dispositivi esterni tramite la rete web, di conseguenza l'intera infrastruttura viene esposta ad attacchi informatici che possono provocare gravi danni alla **safety** fino a comportare l'interruzione dei processi industriali, e la conseguente **Business Interruption** con gravi perdite economiche.
- Secondo l'IBM X-Force's ranking, *l'industria manifatturiera è uno dei settori più colpiti da attacchi di tipo ransomware nel 2021.*
- Quindi la Sicurezza Informatica, o Cyber Security, non deve essere sottovalutata ma, al contrario, deve essere parte integrante delle strategie aziendali; perché i danni che un attacco provoca all'azienda non si limita soltanto all'ambito operativo.

Cybersecurity



Cybersecurity

Quindi la Sicurezza Informatica, o Cyber Security, non deve essere sottovalutata ma, al contrario, deve essere parte integrante delle strategie aziendali; perché i danni che un attacco provoca all'azienda non si limita soltanto all'ambito operativo.

Incidenti relativi alla Cyber Security all'interno di un ICS possono:

- *diffondere informazioni riguardo processi e progetti mettendo a rischio il segreto aziendale;*
- *diffondere informazioni sensibili e dati riservati appartenenti a dipendenti o persone esterne all'azienda;*
- *comportare l'incorrere in sanzioni per la trapelazione delle informazioni in base a quanto stabilito dalla GDPR;*
- *provocare danni con impatto sull'ambiente a causa del malfunzionamento dei processi;*
- *compromettere o arrestare la produzione per periodi medio-lunghi;*
- *danneggiare le strutture a causa di una cattiva gestione dell'attacco.*

Cybersecurity

I principali tipi di attacchi informatici ai sistemi di controllo industriale:

• attraverso un malware, che riesce a penetrare all'interno della rete aziendale grazie ad una disattenzione di un utente che naviga in siti non protetti oppure apre un'email di phishing con allegati malevoli (ad esempio gli attacchi ransomware quali Cryptolocker e simili);
• a causa di attacchi specifici rivolti agli ICS,
• tramite configurazione errata di alcuni componenti hardware o software dell'ICS;
• a causa di attacchi interni, per mano di dipendenti (o ex-dipendenti) con intenzioni fraudolente allo scopo di danneggiare di proposito il sistema di controllo;
• Denial-Of-Service: Un attacco denial-of-service invia grandi flussi di traffico al sistema informatico bersaglio per esaurire le risorse, fino a renderlo indisponibile.
• Sql Injection: Sfrutta i difetti di progettazione di un'applicazione web, iniettando un codice che forza la condivisione di informazioni che dovrebbero invece restare riservate.

Cybersecurity

Le contromisure fondamentali per mitigare e ridurre i danni:

• sensibilizzare e formare il personale dipendente sulle tematiche della Cyber Security e sui rischi che l'azienda corre;
• migliorare la protezione dell'ICS integrando le soluzioni di sicurezza IT con misure di difesa hardware, quali la firma digitale e le tecniche di crittografia;
• affidarsi a specialisti di Cyber Security che permettano di migliorare la sicurezza complessiva attraverso attività di prevenzione, rilevazione e infine gestione degli attacchi informatici.

Cybersecurity

- Con la legge di conversione n. 91 del 15 luglio 2022 in G.U. n. 164 del 15 luglio 2022, il credito d'imposta sulla **formazione** passa al 70% per le piccole imprese e al 50% per le medie imprese.
- E' necessario, per ottenere il credito d'impsta, che le attività formative siano erogate da soggetti che verranno individuati con decreto del ministro dello Sviluppo economico e che i risultati relativi all'acquisizione o al consolidamento delle suddette competenze siano certificate.
- Massimali di spesa: 300mila euro per le piccole imprese e a 250mila euro per le medie imprese. E resta invariato anche il credito d'imposta per le grandi imprese, al 30% fino al limite massimo annuale di 250mila euro.
- Tra le spese ammesse (comma 48 legge 205/2017): *big data e analisi dei dati; cloud e fog computing; cyber security; integrazione digitale dei processi aziendali*;….

Conclusioni

• È possibile tentare di salvaguardare le proprie informazioni usando password complesse e diversificate, non cliccando su link contenuti in messaggi e-mail provenienti da indirizzi sconosciuti o su siti non affidabili o evitando di accedere a reti Wi-Fi pubbliche libere. Ma queste semplici regole non sono sufficienti ed è indispensabile utilizzare software antivirus all'avanguardia per avere un grado di protezione più elevato.

Con il GDPR, il regolamento generale per la protezione dei dati, l'Unione Europea ha inoltre notevolmente rafforzato la tutela dei dati personali e della privacy dei cittadini europei, prevedendo una serie di obblighi per i titolari del trattamento dei dati, aumentando la sensibilità delle organizzazioni rispetto ai temi della cybersecurity.

Maggiore incentivo è stato dato inserendo la sicurezza informatica tra le tecnologie abilitanti del Piano Nazionale Transizione 4.0. Le imprese che intendano proteggere il proprio sistema informativo potranno pertanto adottare soluzioni di cybersecurity avvalendosi della consulenza di esperti del settore e beneficiare al contempo del credito d'imposta.

Conclusioni

Si può intervenire per la protezione in molti modi.
Dallo sviluppare ed installare nei propri sistemi dei software sempre più avanzati che permettano di rilevare eventuali attacchi esterni e soprattutto bloccarli.
Un esempio possono essere i sistemi di rilevamento delle intrusioni. Software di sicurezza progettati per allertare automaticamente gli amministratori quando qualcuno o qualcosa sta tentando di compromettere il sistema informativo attraverso attività dannose o violazioni delle politiche di sicurezza.
Altra soluzione è il ricorso ad una Vpn, che consente alle aziende di estendere la propria rete privata, creando una "rete privata virtuale" che permette agli utenti di collegarsi alla "rete principale".
La crittografia rende invisibili i dati dell'utente, nascondendo i dati scambiati tra PC e server, estendendo una rete privata in una rete pubblica. I protocolli per creare Vpn utilizzano algoritmi crittografati molto robusti, ideali per la protezione dei dati.
L'autenticazione dell'utente, può avvenire con metodi classici, come nome utente e password, ma anche tramite smartcard, riconoscimento biometrico o altri metodi.

Conclusioni

• Nei prossimi anni assisteremo ad una sempre più crescente evoluzione tecnologica finalizzata all'implementazione dei processi produttivi.

I dati e le informazioni rivestono importanza fondamentale. Sono fonte di controllo e verifica oltre ad essere requisito imprescindibile per il funzionamento delle nuove tecnologie dell'Industria 4.0.

Le imprese che operano in un ambiente sempre più cooperativo, devono fronteggiare uno dei problemi organizzativi per eccellenza:

- la scelta dei livelli di apertura e segretezza da adottare per non incorrere in eventi spiacevoli che possano pregiudicarne l'operato.

Bisogna necessariamente pensare di dare ampio spazio all'innovazione ed allo sviluppo di nuove tecnologie.

L'aumento della competizione con altri soggetti è sì un rischio, ma rappresenta anche uno stimolo a migliorarsi e a migliorare.