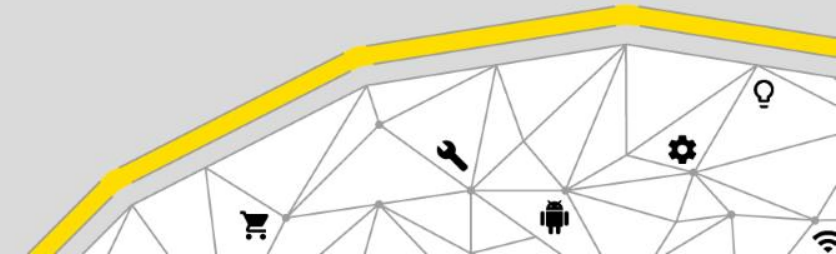
CONFINDUSTRIA

PROGETTO FORMATIVO
INDUSTRY 4.0
PREPARATI AL FUTURO

NETGROUP
SOFTWARE & NETWORK ENGINEERING

Cybersecurity in Industry 4.0: quali rischi e come affrontarli

IN COLLABORAZIONE CON
SISTEMI FORMATIVI CONFINDUSTRIA



Cyber Security: una definizione

Cyber Security - *insieme delle tecnologie utili a proteggere un computer o un insieme di computer (sistema informatico) da attacchi che possono portare alla perdita o compromissione di dati ed informazioni.*

Per valutare la sicurezza è solitamente necessario individuare le **minacce**, le **vulnerabilità** e il **rischio** associato agli asset informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una determinata soglia di tollerabilità (es. economico, politico-sociale, di reputazione, etc.) ad una organizzazione aziendale.

Industria 4.0 – ampliamento rischi Cyber Security

«connessione tra sistemi fisici e digitali, analisi complesse attraverso Big Data e adattamenti real-time» [rif. MISE]

Industry 4.0 significa innovazione di processo, di prodotto, di servizi, di gestione, con impatti significativi sugli impianti, sui prodotti, sulle informazioni. Tutto questo oggi è reso possibile grazie alla **pervasività delle tecnologie ICT**, alla interconnessione tra migliaia di reti dati e alla integrazione di software che interconnettono uomini e cose in giro per il mondo.

Con **Industry 4.0**, si applica il concetto di Always-on a tutto il mondo manifatturiero, con adozione completa del paradigma **Internet of Things** all'Industria.

Bisogna includere nuovi requisiti a livello di safety e di security

Cyber Security - un primo rischio

Con il diffondersi dell'**IIoT** (Industrial Internet of Things) ogni dispositivo, sensore, server, client di visualizzazione o periferica è un potenziale punto di accesso.

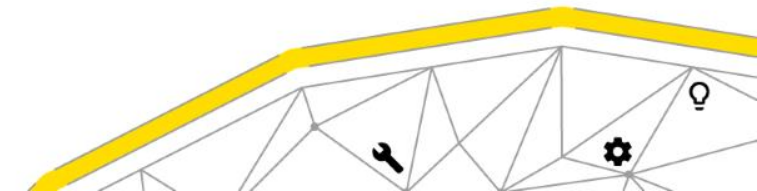
È infatti incrementata a dismisura quella che gli esperti chiamano la **superficie di attacco**, vale a dire le opportunità di sferrare attacchi malevoli e devastanti da parte di cyber criminali.

Soprattutto nelle architetture non presidiate non si può rischiare che un "single point of failure", l'anello debole della catena, comprometta la sicurezza dell'intero sistema.

È importante notare inoltre come, nel caso di **Industria 4.0**, i rischi siano di diverso tipo rispetto a quelli presenti nell'IT tradizionale.

Secondo rischio della Cyber Security

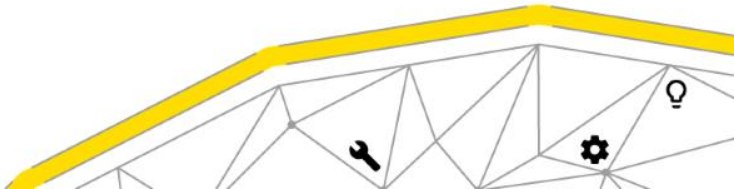
Un altro rischio, spesso meno evidente, ma con effetti altamente critici, è legato al fatto che i sistemi informativi, le soluzioni applicative, i middleware, soprattutto se non adeguatamente progettati, **diventano punti di stazionamento degli attaccanti, sia per generare criticità a livello locale, sia per attivare attacchi verso sistemi esterni**.
All'identificazione di una vulnerabilità in un software segue normalmente il rilascio di un aggiornamento da parte del produttore.
I sistemi possano essere compromessi o violati anche nel caso di applicazione degli aggiornamenti. In questo caso, la vulnerabilità prende il nome di **0-day**, e risulta particolarmente pericolosa, proprio per l'assenza di una chiara strategia di protezione



Cyber Security – rischio sulla conoscenza

Altro importante rischio della cyber security è la mancanza di conoscenza e sensibilità al problema della cyber security.
Mentre il progresso tecnologico mette oggi a disposizione strumenti avanzati per proteggere dati e sistemi, il fattore umano continua a costituire il punto debole della sicurezza. È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere a dati o ad altre risorse attraverso l'uso dei vari dispositivi.

La componente umana, il **Man-in-the-middle** è l'anello debole della catena e una delle porte di accesso più facili da utilizzare da parte di un attaccante malevolo.



Controlli di Cyber Security

L'innalzamento dei livelli di sicurezza delle piccole e micro imprese diventa un passaggio fondamentale per la messa in sicurezza delle filiere produttive. Un numero sempre maggiore di attacchi a grandi imprese capo-filiera viene infatti realizzato grazie a vulnerabilità presenti nelle imprese parte delle loro filiere.

Questo innalzamento è particolarmente importante in questo momento di forte trasformazione digitale del settore industriale.

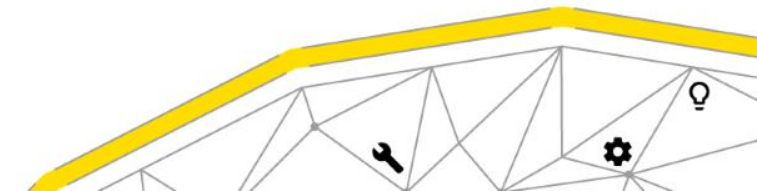
Il Cybersecurity Report 2016, realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di Cybersecurity presenta **15 Controlli Essenziali di Cybersecurity**, destinati principalmente a piccole e micro imprese italiane.

15 Controlli Essenziali di Cyber Security

1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc…) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, …). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

Come affrontare i rischi – alcuni esempi metodologici

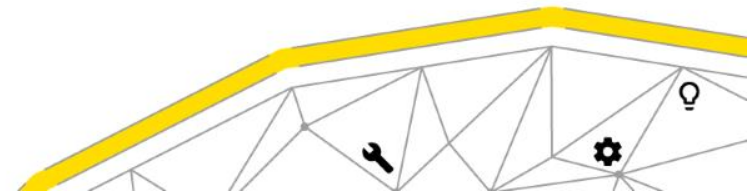
- ✓ Nella **redazione dei progetti** occorre prendere in considerazione le **esigenze di sicurezza** (il passaggio progettuale è obbligatorio, ma la sua qualità e approfondimento sono sostanzialmente una decisione dell'azienda).
- ✓ **Coinvolgere** nella fase di progetto, anche se normalmente non si occupa del processo produttivo, **il personale IT**.
- ✓ Verificare la sicurezza dell'infrastruttura a termine del progetto, eseguendo un **security assessment** specializzato nel mondo dei sistemi industriali.
- ✓ Sviluppare una corretta **cultura della sicurezza** in tutto il personale, indipendentemente dalle sue responsabilità.
- ✓ Coniugare la cybersecurity con il concetto di **cyber-resilience**.



Tecniche di remediation

Modello "**security by design**": progettare il sistema, l'impianto e l'infrastruttura tenendo presenti le questioni rilevanti per la cyber security, mettendo al primo passo proprio una attenta analisi e valutazione del rischio: questo consente di concentrare gli sforzi nei punti in cui si riterranno le contromisure e gli interventi più efficaci ed urgenti.

Adozione di tecnologie come la **virtualizzazione**, il **Cloud**, i **Virtual desktop** e i **thin client** che hanno mostrato come lavorare su credenziali e controllo accessi, sul traffico dati in entrata e in uscita, sulla possibilità di eseguire backup temporizzati e ravvicinati sia strada assai più sicura di quella di creare un "perimetro invalicabile".



Focus on … soluzioni pensate per il mondo industriale

Quando si parla di industria la parola chiave è **OT, Operational Technology**, che rappresenta l'insieme di tutti i "sistemi intelligenti" che gestiscono informazioni dell'impianto, sistemi che hanno esigenze primarie di "**Disponibilità**" ed "**Integrità**", mentre la **Riservatezza** è quasi un parametro accessorio.
In ambito industriale vanno quindi utilizzate soluzioni espressamente pensate per questo scopo. Il mercato propone oggi dispositivi intelligenti con funzioni **IPS/IDS**, **Firewall**, **Antimalware** e soprattutto dotate di avanzate funzioni di filtraggio, application/protocol/datapackage **White-Listing** ed **Anomaly detection**: le uniche tecniche che si sono dimostrate veramente efficaci nel contrastare problemi di security su reti e sistemi di controllo e telecontrollo in molti settori industriali.

Azioni in corso per la Cyber Security in Industria 4.0

- ✓ **Norme e misure più stringenti** - normative internazionali come il GDPR, oltre alla Direttiva NIS, dovrebbero progressivamente limitare la frequenza e la virulenza delle minacce, imponendo obblighi e pesanti sanzioni alle imprese
- ✓ **Aumento dell'automazione** di strumenti per individuare le minacce tramite l'utilizzo di tecniche *machine-learning*, con una crescente applicazione della *Big Data Analytics* alla sicurezza cibernetica.
- ✓ **Maggiore consapevolezza** - l'informatizzazione della società ha allargato il concetto di sicurezza ICT per includervi persone (**safety**) e cose (**security**). Sarà sempre più necessario tenere uniti i due concetti.

CONFINDUSTRIA

PROGETTO FORMATIVO
INDUSTRY 4.0
PREPARATI AL FUTURO

Grazie

www.sfc.it/preparatialfuturo

www.netgroup.it
info@netgroup.it

IN COLLABORAZIONE CON
SISTEMI FORMATIVI CONFINDUSTRIA