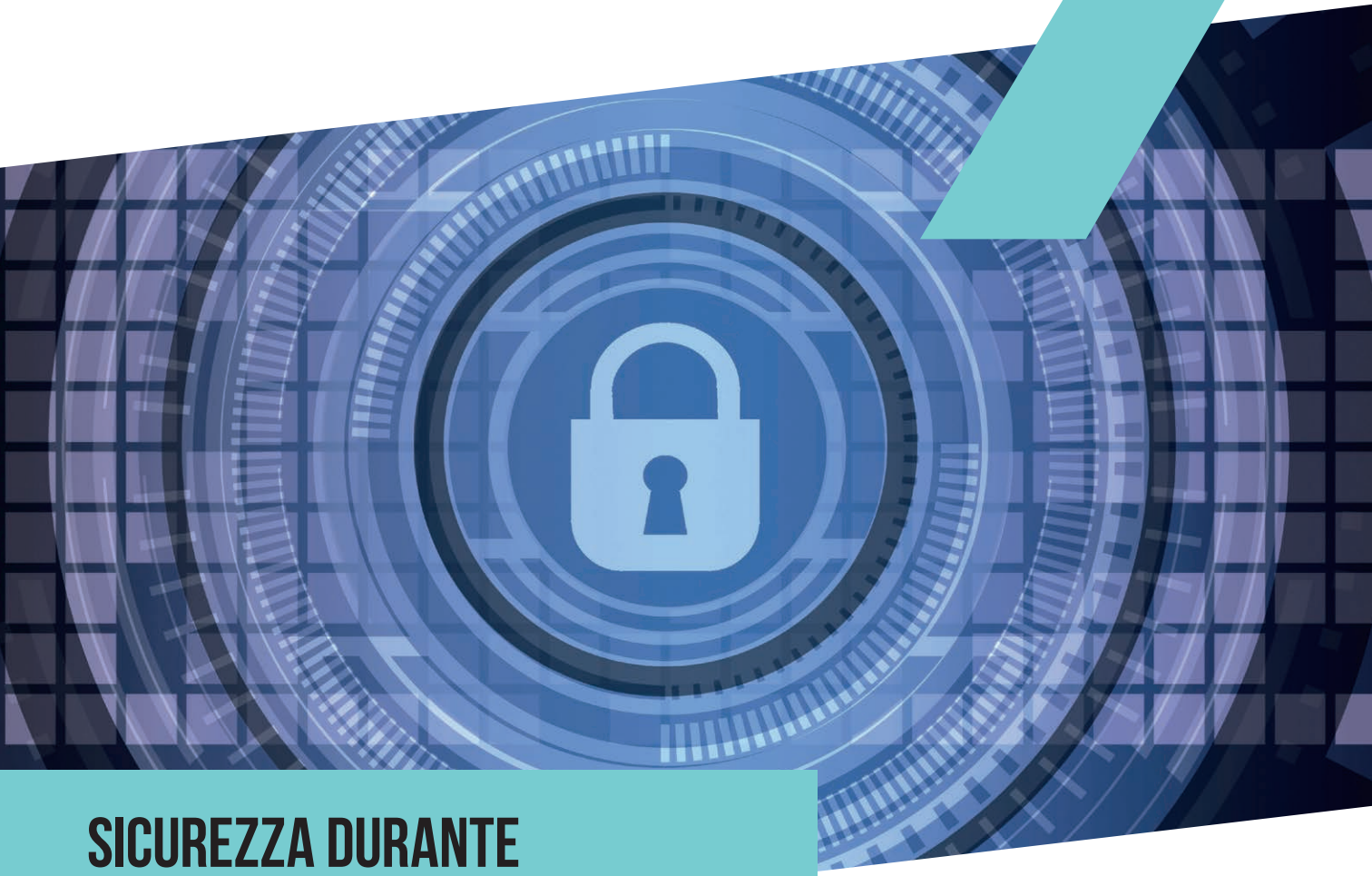
CYBER SECURITY



SICUREZZA DURANTE LE OPERAZIONI IN RETE E SU SISTEMI APERTI

punto
impresa
digitale

La Camera di Commercio di Cagliari ha aderito al Network Nazionale Impresa 4.0 costituendo il Punto Impresa Digitale (PID) attraverso la sua Azienda Speciale Centro Servizi Promozionali per le Imprese.

Il PID di Cagliari offre numerosi servizi di informazione, formazione e orientamento alle proprie imprese che vogliono cogliere le opportunità offerte dalla IV Rivoluzione Industriale e più in generale dalla digitalizzazione.

Si colloca all'interno di questo insieme di strumenti la presente collana di brochure per le imprese che affrontano le tecnologie previste dal Piano Impresa 4.0.

punto
impresa
digitale

Realizzato con collaborazione tecnica di Dintec

DESCRIZIONE DELLA TECNOLOGIA

Nel Piano Impresa 4.0 si fa riferimento alla sicurezza informatica (o “Cyber Security”) come a quei “software, sistemi, piattaforme e applicazioni per la protezione di reti, dati, programmi, macchine e impianti da attacchi, danni e accessi non autorizzati”; in tal senso si riportano come esempi i sistemi di controllo degli accessi al sistema informatico, i sistemi di monitoraggio del traffico dati, i sistemi di criptazione dei dati e dei canali di trasmissione, i sistemi di gestione della privacy e sicurezza dei dati sensibili, i sistemi per l’interazione sicura degli oggetti. Anche in questo caso con il termine “Cyber Security” ci si riferisce ad un insieme di tecnologie, processi e pratiche progettati per proteggere reti, dispositivi, programmi e dati da attacchi, danni o accessi non autorizzati.

CYBER SECURITY

Parlare di Cyber Security vuol dire prendere in considerazione diversi aspetti, i principali possono essere riassunti in:

1. **sicurezza della tecnologia:** dai controlli di accesso all'installazione di software antivirus, la tecnologia può essere utilizzata per ridurre i rischi informatici.
2. **sicurezza dei processi:** i processi devono definire chiaramente ruoli, responsabilità e procedure. Le minacce informatiche sono in continua evoluzione, quindi i processi devono essere rivisti regolarmente.
3. **comportamento delle persone:** ogni dipendente deve essere consapevole del proprio ruolo nella prevenzione delle minacce informatiche. Il personale di sicurezza informatica deve rimanere aggiornato con gli ultimi rischi e soluzioni.

In generale la cyber security si concentra sulla "prevenzione" delle minacce e quindi a cercare di evitare che si subisca un qualsiasi danno o alterazione dei normali processi desegnati attraverso procedure che evitino malfunzionamenti o perdita di informazioni; tuttavia non deve essere trascurata la possibilità di "minimizzare" danni eventualmente avuti: in tal senso si parla di "disaster recovery" o "business continuity".
Questi termini "disaster recovery" o "business continuity" fanno riferimento a soluzioni che permettono il recupero delle informazioni eventualmente perse o di errori di sistema a seguito di un attacco informatico (o più in generale di un malfunzionamento); queste soluzioni, come gli altri aspetti che compongono la cyber security, fanno affidamento sulle tecnologie e/o su processi che si attivano nel momento in cui serve "minimizzare i danni".
È certo che questi sistemi non hanno alcuna efficacia in termini di competenze perse o di "segreti aziendali" trafugati che potrebbero conseguire ad un attacco informatico.

In generale un attacco informatico avrà come obiettivo i dati e di alterarne le principali caratteristiche che sono:

Riservatezza: una minaccia è tale quando non permette di proteggere le informazioni aziendali dagli accessi da parte di soggetti non autorizzati.

Integrità: una minaccia potrebbe modificare un dato e quindi cambiare l'autenticità e il valore che esso ha e la relativa informazione. Ad esempio, se un sito vende prodotti e un malvivente ha la possibilità di modificare i prezzi, questo potrebbe far sì che possano acquistare quel che vogliono a prezzi non corrispondenti a quelli reali.

Disponibilità: una minaccia potrebbe negare l'accesso all'informazione agli utenti autorizzati.

CYBER SECURITY: LE PRINCIPALI MINACCE

PHISHING

Il phishing è la pratica di inviare email fraudolente da fonti affidabili che assomigliano a email normalmente utilizzate dagli utenti. L'obiettivo è quello di rubare dati sensibili come dati personali, numeri di carta di credito e/o informazioni di accesso. È il tipo più comune di attacco informatico. Puoi proteggerti attraverso un comportamento corretto e una soluzione tecnologica che filtra le email dannose.

RANSOMWARE

Il ransomware è un tipo di software malevolo. È progettato per estorcere denaro bloccando l'accesso ai file o al sistema informatico fino al pagamento del riscatto. Il pagamento del riscatto, tuttavia, spesso non garantisce il ripristino dei file o del sistema.

MALWARE

Il malaware è un tipo di software progettato per ottenere accessi non autorizzati (e quindi per poter accedere a informazioni che possono essere “sensibili” o “riservate”) o per danneggiare un computer.

SOCIAL ENGINEERING

L’ingegneria sociale è una tattica che i criminali possono usare per indurre una “vittima” a rivelare informazioni sensibili. Possono, ad esempio, sollecitare un pagamento monetario o ottenere l’accesso ai dati riservati. Ad esempio, il criminale potrebbe identificarsi, eventualmente attraverso una società fasulla di supporto tecnico che ha anche un proprio sito web, come appartenenti al supporto tecnico e che stanno chiamando l’utente per fornire il supporto necessario a risolvere un’intrusione... intrusione che invece avviene proprio attraverso la chiamata! È chiaro che il social engineering può essere combinato con una qualsiasi delle minacce sopra elencate per aumentare la probabilità di fare clic su collegamenti dannosi, scaricare malware o fidarsi di una fonte non sicura.

AMBITI APPLICATIVI

L'utilizzo sempre più diffuso di nuove tecnologie di interconnessione e la possibile digitalizzazione di tutti i processi aziendali fanno sì che tutti gli ambiti di impresa possano essere di "interesse" di tecnologie e di pratiche legate alla cyber security, tra queste si possono segnalare:

DIREZIONE E RISORSE UMANE

in particolare nell'adottare misure tecnologiche, formative e procedurali che permettano la tutela dell'integrità dei dati e la privacy delle persone che lavorano in azienda, ma anche di collaboratori e/o fornitori.

PRODUZIONE E ASSEMBLAGGIO

ttraverso la diffusione di sistemi interconnessi e Internet delle cose (IoT), anche i singoli macchinari e oggetti con connessione internet (stampanti ad esempio) possono essere punti di accesso all'intera rete aziendale e devono pertanto essere messi in sicurezza.

SALE EVENTI/RECEPTION

tutti gli ambienti in cui possano entrare fisicamente anche persone e cose che non seguono procedure e/o non hanno tecnologie aziendali devono poter essere messe nelle condizioni di non rappresentare una "minaccia" in termini di sicurezza aziendale.

VANTAGGI

Rendere sicuri i dati e le informazioni aziendali in termini di riservatezza, integrità e disponibilità.

Avere sistemi che permettano di reagire ad attacchi e malfunzionamenti minimizzando le perdite, grazie a sistemi di business continuity e disaster recovery.

Garantire livelli di servizio sempre più alti sui dati sensibili dei clienti, fornitori e collaboratori.

Poter utilizzare consapevolmente nuove tecnologie e poter perseguire politiche di sviluppo in chiave Impresa 4.0

Aumentare la segretezza aziendale e la perdita di informazioni, accidentale o malevola, verso i concorrenti.

PUNTI DI ATTENZIONE

Costi di gestione e mantenimento dei sistemi importanti.

Sistemi costantemente monitorati e migliorati per garantire il più alto livello di efficacia contro gli attacchi informatici.

Competenze IT necessarie molto specialistiche.

Necessità di formazione continua ai dipendenti sui rischi e le nuove metodologie di attacco.

Sistemi mai sicuri al 100%.

Resistenze culturali: spesso connesse all'introduzione di cambiamenti procedurali o di nuove tecnologie di identificazione.

PUNTO IMPRESA DIGITALE - PID
Centro Servizi Promozionali per le Imprese
Azienda Speciale della Camera di Commercio di Cagliari
Largo Carlo Felice, 66
09124 Cagliari

Alessia Bacchiddu
Digital Coordinator / Tel. 070 60512332

Alessandra Dessì
Digital Coordinator / Tel. 070 60512331

email: pidcagliari@csimprese.it
www.ca.camcom.it - www.csimprese.it

Centro Servizi per le Imprese
Camera di Commercio Cagliari

Camera di Commercio Cagliari

SCOPRI IL TUO LIVELLO DI DIGITALIZZAZIONE

SELFI4.0

1 / SOLUZIONI AVANZATE PER LA MANIFATTURA
Robot collaborativi interconnessi e rapidamente programmabili

2 / MANIFATTURA ADDITIVA
Stampanti in 3D connesse a software di sviluppo digitale

3 / REALTÀ AUMENTATA E REALTÀ VIRTUALE
Supporto dei processi produttivi e di erogazione dei servizi

4 / SIMULAZIONE
Simulazione per ottimizzare i processi

5 / INTEGRAZIONE ORIZZONTALE E VERTICALE
Integrazione delle informazioni lungo la catena del valore dal fornitore al consumatore

6 / INTERNET DELLE COSE (IoT)
Comunicazione multidirezionale tra processi produttivi e prodotti

7 / CYBER SECURITY
Sicurezza durante le operazioni in rete e su sistemi aperti

8 / CLOUD
Gestione di dati su sistemi aperti

9 / BIG DATA AND ANALYTICS
Analisi di basi di dati per ottimizzare prodotti e processi produttivi

punto impresa digitale