CAMERA DI COMMERCIO
DEL MOLISE

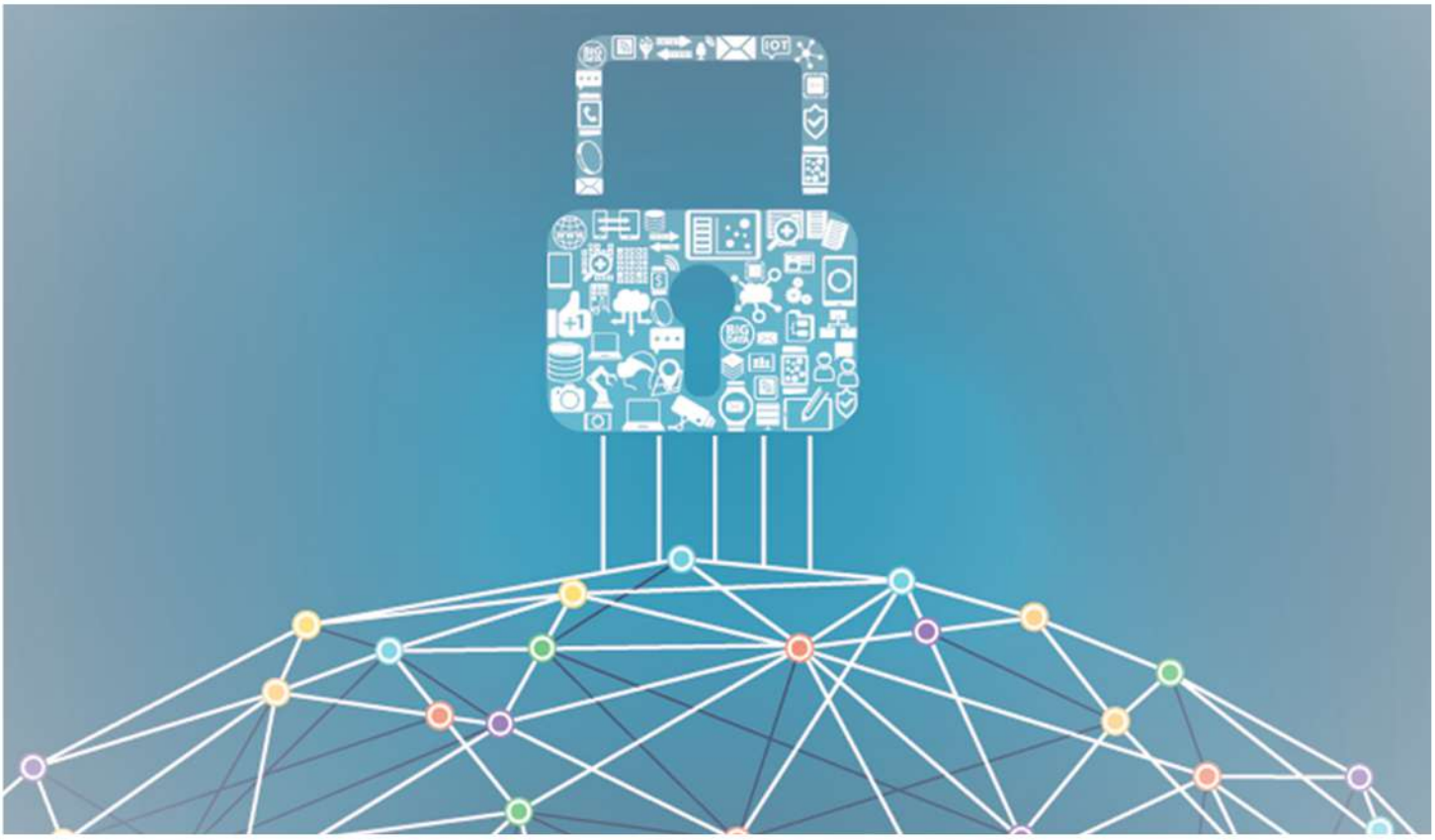
punto
impresa
digitale

Le guide
per l'innovazione
digitale

numero 2

Cybersecurity & Cloud

Scopri di più sulla Cybersecurity e il Cloud



Cybersecurity: proteggere il cyberspazio dai cyber attacchi. Consigli e soluzioni per individuare minacce, vulnerabilità e rischi informatici ed essere in grado di proteggere i dati da possibili attacchi.

La Cybersecurity è tra le tecnologie abilitanti previste dal Piano Impresa 4.0 ed è focalizzata principalmente sulla protezione dei sistemi informatici (computer, reti di telecomunicazione, smartphone, ecc…) e dell'informazione in formato digitale da attacchi interni e, soprattutto esterni. Altri termini utilizzati in alternativa e precedentemente sono IT security, ICT security, sicurezza informatica e sicurezza delle informazioni.
Al di là della terminologia, la cyber security è una disciplina molto pratica. Si occupa di proteggere i sistemi informatici da minacce concrete che hanno una probabilità significativa di realizzarsi, fra le tante che sarebbero concepibili. In questo, la si può vedere come uno strumento di gestione dei rischi.

Mettere al sicuro i nostri dati è possibile?
Proteggere i sistemi informatici adottando misure di sicurezza.

I rischi non sono praticamente mai nulli: le misure di sicurezza sono utilizzate per ridurre i rischi, quasi mai per eliminarli.
Tecnicamente, gli strumenti sono principalmente due: abbandonare la semplice password a favore di meccanismi di autenticazione forte e monitorare gli accessi per rilevare anomalie (accessi da posti inusuali, utilizzo di strumenti diversi dal solito e simili). La profilazione del comportamento abituale dell'utente permette di rilevare quando viene fatto qualcosa di strano, un po' come avviene con gli utilizzi anomali della carta di credito. I due meccanismi possono essere messi insieme per utilizzare la sola password quando si tratta di accessi "normali" o per operazioni poco critiche, utilizzando invece l'autenticazione forte per accessi ad operazioni "delicate e sensibili": si tratta della cosiddetta autenticazione adattiva, utilizzata dalle banche e dai fornitori di servizi in cloud più evoluti.
Utilizzare password robuste, sicure e attraverso sistemi a due fattori: questo tipo di meccanismo fa sì che non basti conoscere la password per avere accesso ad un particolare portale o account, ma serva anche un altro fattore come può essere un token fisico o l'accesso ad un determinato numero telefonico.

I tre parametri fondamentali per la sicurezza delle informazioni sono:
RISERVATEZZA: ad un'informazione può accedere solo chi è autorizzato a farlo.
I rischi sono:
• Accessi non autorizzati per errori di configurazione o perdita chiavi (password)
• Perdite accidentali supporti
• Furto

INTEGRITÀ: il contenuto delle informazioni può essere modificato solo da chi è autorizzato a farlo.
I rischi sono:
• Guasti e relativa corruzione dei dati
• Modifiche accidentali errate

DISPONIBILITÀ: la proprietà di un dato di poter esser raggiungibile in qualsiasi momento.
I rischi sono:
• Eventi naturali che compromettano il servizio di accesso
• Intrusioni/Attacchi (Ransomware)
• Blocco/Guasti dei sistemi

Phishing e messaggistica: facciamo chiarezza.

PHISHING: Il phishing è un tipo di frode ideato allo scopo di rubare importanti informazioni sensibili come numeri di carta di credito, password e dati relativi al conto bancario.
E' uno stratagemma per indurre gli utenti a rivelare, con l'inganno, informazioni personali o finanziarie attraverso un'email o un sito Web, ma sempre più spesso anche tramite messaggi in arrivo da applicazioni molto usate come Whatsapp o Facebook.
Un tipico attacco di phishing inizia con un messaggio di posta elettronica, un link che compare dal nulla in Facebook, o un banner pubblicitario in qualche applicazione molto usata dagli utenti. Si presenta come una notifica ufficiale proveniente da una fonte attendibile, per esempio una banca, ma anche da amici.

II messaggio invita a collegarsi a un sito Web graficamente molto simile a quello originale e a inserire alcune informazioni personali come, per esempio, il numero di conto corrente o la password. Queste informazioni vengono poi utilizzate per appropriarsi dell'identità di chi cade nella truffa.
Questo tipo di attacco è sempre più sofisticato e realistico e per questo riconoscere una mail di phishing è molto difficile.
A volte si tratta di falsi messaggi che sembrano arrivare da un sito affidabile, e che ti spingono, per cause tecniche, a comunicare nuovamente i tuoi dati personali.

Come evitare l'attacco Phishing?

• Riconoscere il mittente della e-mail: il primo consiglio da seguire quando si riceve una e-mail è controllare chi l'ha inviata. Gli hacker sono bravissimi a creare account e-mail molto simili, quasi identici a quelli dei vostri amici: a cambiare è solamente un punto o una lettera. Se si è poco attenti, non si ha scampo: si scarica l'allegato e il pirata informatico ha accesso a tutti i vostri dati, anche quelli bancari. Un piccolo trucco per riconoscere le e-mail pishing è di studiare e analizzare le lettere e i punti con cui è composto l'indirizzo di posta elettronica. Solitamente gli hacker invertono nome e cognome o spostano il punto di qualche lettera.
• Social engineering: Gli hacker sono diventati anche degli abili psicologi e hanno iniziato a studiare le abitudini degli utenti per riuscire a rubare le loro credenziali. La pratica prende il nome di social engineering e riesce a convincere anche l'utente più scaltro a cadere nelle trappole dei pirati informatici che conoscono alla perfezione le necessità delle loro vittime e giocano sulla stan chezza causata da ritmi di lavoro molto spesso insostenibili. Più si lavora veloce e più si è portati a cliccare sui link senza nemmeno leggere il contenuto del messaggio. Anche un piccolo errore grammaticale è sintomo che sia opera di un hacker. Quindi massima attenzione e occhi sempre ben aperti: gli hacker scommettono proprio sulla distrazione degli utenti.

• Cosa possono fare gli utenti per bloccare gli attacchi phishing: non solo machine learning e intelligenza artificiale. Grazie ad alcuni accorgimenti fatti direttamente dagli utenti è possibile bloccare gli attacchi phishing e mettere un bastone tra le ruote degli hacker. In primis è necessario effettuare gli aggiornamenti di sistema ogni volta che se ne ha la possibilità.
Le software house rilasciano update continuamente per bloccare i nuovi pericoli hacker. Altro accorgimento da prendere è utilizzare password diverse e difficili per ogni account. Se avete problemi nel ricordare le chiavi d'accesso è possibile utilizzare uno dei tanti password manager presenti sugli store online.
• Autenticazione in due passaggi: l'autenticazione a due fattori è tra le misure di sicurezza più avanzate per proteggere i propri account online, in quanto richiede all'utente di indicare due forme di autenticazione. Il primo fattore in genere è la password. Il secondo può essere un SMS o un codice email.
Quindi cosa è importante fare quando ci arriva una mail? Controllare sempre: il mittente, il dominio mittente, l'allegato, il link e le credenziali.

Come contrastare le minacce ai dati di tipo fisico e di tipo logico?

La sicurezza fisica riguarda il preservare l'integrità dei sistemi quali il computer, le reti ecc…, assicurando la sorveglianza e quindi la sicurezza dell'edificio che ospita il sistema informativo, controllando l'accesso delle persone all'edificio, predisponendo sistemi di antincendio e antiallagamento e utilizzando sistemi di business continuity e di disaster recovery. Con il termine business continuity ci si riferisce ad una soluzione globale, che comprende tutte le procedure e i processi che hanno lo scopo di garantire la continuità del business e di evitare l'interruzione delle attività, sia dovute a disservizi del reparto IT che a cause di altra natura. Il termine disaster recovery indica tutte le misure tecniche utili per affrontare un eventuale disastro che colpisce i sistemi in formativi aziendali e che può avere diversa origine: catastrofi naturali come alluvioni o terremoti, errori umani, furti o attacchi hacker.

La sicurezza logica si riferisce alla sicurezza perimetrale (attacchi informatici dalla rete); alla sicurezza end-point (virus e malware) e alla sicurezza applicativa, sistemi AAA e crittografia dei dati (accesso non autorizzato ad applicazioni e dati; furto di informazioni).

Come utilizzare la Cybersecurity nella tua PMI?

- Usare software di protezione aggiornati e completi, sia per l'ambiente di ufficio sia per quello di produzione. Per soddisfare le normative in tema di sicurezza delle informazioni (cyber security e protezione dei dati), le organizzazioni devono investire per adeguarsi ai relativi standard costantemente aggiornati con l'evolversi degli aspetti tecnologici e delle vulnerabilità informatiche.
- Investire sulla formazione. L'unica soluzione per le PMI per difendersi dagli attacchi cyber-fisici dei pirati informatici è investire nella formazione dei propri dipendenti. Potrà sembrare banale, ma sono pochissime le aziende che spendono per la cybersicurezza: preferiscono assumere un esperto piuttosto che formare tutti i dipendenti, mettendo, però, in pericolo tutti i dati dell'azienda.
- Ridurre il rischio di errore umano e furto dei dati personali con soluzioni come il cloud o la firma digitale.

Individuare malware e programmi dannosi: cos'è il malware?

• Per malware (contrazione dell'inglese "malicious software", ossia software dannoso) si intende qualsiasi tipo di software dannoso o fonte di disturbo, creato per accedere segretamente a un dispositivo senza che l'utente ne sia a conoscenza. I tipi di malware includono spyware, adware, phishing, virus, trojan, worm, rootkit, ransomware e dirottamenti del browser.

Ecco come accorgersi se sei vittima di un attacco hacker:
- Avendo un antivirus sul tuo PC, ti sarà facile riconoscere l'aspetto dei veri messaggi, quindi non cliccare su quelli che potrebbero essere truffe.
- Se compaiono toolbar vicino alla barra degli indirizzi, che non hai installato, che potrebbero riportare messaggi di "aiuto", fai attenzione, di certo è un campanello di allarme.
- Quando sul tuo PC c'è un programma che provoca POP-UP frequenti e casuali.
- Se i tuoi contatti ricevono mail mai inviate da te.
- Se ricevi fatture di acquisti on line che non hai effettuato.

Suggerimenti per una navigazione sicura su internet.

- Accedere possibilmente solo a siti via https
- Utilizzare password robuste, sicure e attraverso sistemi a due fattori (una buona password deve avere almeno 10-12 caratteri alfanumerici, che non siano un'intera parola del dizionario)
- Non utilizzare MAI la stessa password per autenticazioni diverse
- Limitare e mantenere a un livello professionale le informazioni personali
- Continuare ad usare le impostazioni sulla privacy
- Assicurarsi che la connessione Internet sia sicura
- Fare acquisti online da siti sicuri
- Prestare attenzione a ciò che si posta e a ciò che si scarica
- Mantenere aggiornato il programma antivirus.

Cloud: i tuoi dati, i tuoi programmi disponibili ovunque!

Che cosa è il Cloud Computing?

E' l'insieme di risorse hardware e software che forniscono servizi su richiesta attraverso la rete internet.
Cloud è un termine inglese che significa nuvola. Non è altro che uno spazio di archiviazione personale, chiamato talvolta anche cloud storage che risulta essere accessibile in qualsiasi momento ed in ogni luogo utilizzando semplicemente una qualunque connessione ad Internet. Bisogna comunque precisare che con il termine cloud, oltre che a riferirsi al cloud storage, a volte ci si potrebbe riferire anche ad altri servizi offerti dal cloud computing.
Il "cloud storage", dunque, non fa altro che sincronizzare tutti i propri file preferiti in un unico posto, con il conseguente vantaggio di riscaricarli, modificarli, cancellarli e/o aggiornarli, senza avere quindi più il bisogno di portare con sé hard disk esterni, pen drive USB, ecc.. Oltre a questo, volendo, ci sarà anche la possibilità di fare delle preziose copie di backup, nonché di condi videre tutti i propri file preferiti con chi si vorrà, e per quanto tempo si vorrà, con indubbi vantaggi in termini di tempo e praticità.

Il NIST (National Institute of Standards and Technology) definisce le principali caratteristiche del cloud:
• On-demand self service: il consumatore utilizza il cloud in base alle sue necessità.
• Broad network access: funzionalità in rete e accessibilità da qualsiasi device (pc, mobile, tablet ecc).
• Resource pooling: le risorse di calcolo del provider del cloud sono gestite per garantire i livelli di servizio a tutti i clienti.
• Rapid elasticity: tutte le funzionalità possono essere velocemente adeguate in funzione della domanda dei client del cloud.
• Measure service: i cloud controllano automaticamente ed ottimizzano l'utilizzo delle risorse più appropriate misurando costantemente il livello di servizio richiesto dai client del cloud.

Quali sono i vantaggi nell'adozione del Cloud per la tua PMI?

• Maggiore flessibilità, per la crescita del business. La procedura è semplice per aumentare i gigabyte nei server remoti.
• I fornitori dei cloud si occupano di eseguire gli aggiornamenti software regolari, compresi gli aggiornamenti di sicurezza (cybersecurity).
• Il cloud computing riduce l'elevato costo dell'hardware. È sufficiente pagare l'abbonamento in base alle proprie necessità, con un'alta facilità di installazione e gestione.
• Più team possono accedere, modificare e condividere documenti da qualsiasi luogo in qualsiasi momento anche tramite le App.
• Il cloud computing, con una connessione a Internet, permette di lavorare ovunque. E con la maggior parte dei servizi cloud, si hanno applicazioni mobili, e le aziende possono offrire vantaggi di lavoro più flessibili per i dipendenti (smart working).
• Più collaboratori e partner lavorano ai documenti, maggiore è la necessità di un controllo documentale a tenuta stagna. Tutti i file vengono memorizzati centralmente e tutti hanno accesso alla versione corrente portando a una migliore interazione, che in ultima analisi significa un lavoro migliore.
• Il cloud computing offre maggiore sicurezza sulla perdita di dati, poiché i dati vengono archiviati nel cloud. E si può accedere anche in remoto.
• In un mondo completamente interconnesso il vantaggio dell'azienda nell'implementare un approccio strutturato della cybersecurity permette di garantire la sicurezza dei propri dati e di quelli dei suoi clienti.

Le tre grandi categorie del Cloud Computing: IaaS – PaaS – SaaS

IaaS (Infrastructure as a Service): le soluzioni Iaas sono quelle tipiche del cloud computing; con una soluzione IaaS, infatti, si affitta l'infrastruttura IT, ovvero server e macchine virtuali (VM), risorse di archiviazione, connessioni di rete, da un provider di servizi cloud con pagamento in base al consumo. Esempi: Posta elettronica, Intranet, CRM.

PaaS (Platform as a Service): si riferisce a servizi di cloud computing che forniscono un ambiente on demand per lo sviluppo, il test, la distribuzione e la gestione di applicazioni software. In questo modo gli sviluppatori hanno la possibilità di creare in modo più semplice e rapido app Web o per dispositivi mobili, senza doversi preoccupare della configurazione o della gestione dell'infrastruttura sottostante. Esempi: Sviluppo applicazioni linguaggio Java, Python, Net (siti web).
SaaS (Software as a Service): la modalità SaaS tecnicamente può essere intesa come un metodo per la distribuzione di applicazioni software tramite Internet, on demand. Con una soluzione SaaS, i provider di servizi cloud ospitano e gestiscono l'applicazione software e l'infrastruttura sottostante e si occupano delle attività di manutenzione, come gli aggiornamenti software e l'applicazione di patch di protezione. Esempi: Storage (Dropbox).

VANTAGGI:	SVANTAGGI:
Cybersecurity: • Garantire l'operatività dei sistemi contro qualsiasi attacco informatico interno ed esterno • Garantire livelli di servizio sempre più alti sui dati sensibili dei clienti • Consentire alle aziende di rimanere al passo con i tempi e non correre pericoli attraverso un sistema di gestione dei rischi: monitoraggio e protezione dati (senza lasciare gap)	**Cybersecurity:** • Costi di gestione importanti • Competenze IT necessarie molto specialistiche • Sistemi mai sicuri al 100%
Cloud: • Possibilità di archiviare grandi quantità di dati • Possibilità di usare applicazioni sempre aggiornate • Grande spazio di archiviazione senza occupare memoria nei personal computer • Sicurezza nella gestione dei dati sviluppata dalle aziende fornitrici di Cloud • Possibilità di accedere ai dati in qualsiasi situazione • Interfaccia Userfriendly • Maggiore flessibilità anche nei canoni di servizio	**Cloud:** • Sicurezza informatica e Violazione Privacy: il rischio sicurezza aumenta con le reti wireless • Sistema paralizzato in assenza di connessione con la rete Internet • Non conoscenza dell'ubicazione fisica dei dati • Diverse normative nella gestione dei dati (normativa USA vs Europa) • Competenze informatiche necessarie per gli amministratori aziendali (ITC) del Cloud

CAMERA DI COMMERCIO
DEL MOLISE

punto
impresa
digitale

Punto Impresa Digitale

Camera di Commercio del Molise

Piazza della Vittoria, 1 – 86100 Campobasso
Corso Risorgimento, 302 – 86170 Isernia

pid@molise.camcom.it Tel. 0874/4711
www.molise.camcom.gov.it