Scheda didattica

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Titolo | Mantieni i tuoi dati al sicuro: Sicurezza informatica per le MPMI | | | |
| Parole chiave | Sicurezza dei dati, Sicurezza informatica, Protezione dei dati, Sicurezza delle informazioni, Minacce informatiche, Violazioni dei dati, Sicurezza della rete, Gestione dei rischi, Migliori pratiche di sicurezza, Consapevolezza informatica | | | |
| Fornito da | Soluzioni IT per tutti | | | |
| Lingua | Italiano | | | |
| Area formativa | ☐ Fondamenti dell’imprenditorialità digitale in contesti di microimprese  ☐ Comunicazione digitale e marchio  ☐ Finanza digitale  ☒ Sicurezza informatica | | | |
| Risultati formativi | EntreComp | | | |
| ☐ Idee e opportunità  ☒ Risorse  ☒ In azione  Competenze specifiche affrontate:  Mobilitare le risorse, mobilitare gli altri, pianificare e gestire, far fronte all’incertezza, all’ambiguità e al rischio, apprendere attraverso l’esperienza | | | |
| DigComp | | | |
| ☐ Informazioni e alfabetizzazione e dei dati  ☐ Comunicazione e collaborazione  ☐ Creazione di contenuti digitali  ☒ Sicurezza  ☒ Risoluzione di problemi  Competenze specifiche affrontate:  Protezione dei dispositivi, protezione dei dati personali e della privacy, identificazione delle esigenze e delle risposte tecnologiche | | | |
| Livello di competenza | | | |
| ☐ livello 1  ☐ livello 2 | ☐ livello 3  ☐ livello 4 | ☒ livello 5  ☐ livello 6 | ☐ livello 7  ☐ livello 8 |
| Fondazione | Intermedio | Avanzato | Esperto |
| Descrizione | Nell’era digitale di oggi, i dati sono una risorsa preziosa per ogni organizzazione, comprese le micro, piccole e medie imprese (MPMI). Tuttavia, con la crescente dipendenza dalla tecnologia, il rischio di minacce informatiche e violazioni dei dati non è mai stato così elevato.  Il nostro corso di formazione, “Mantieni i tuoi dati al sicuro: La sicurezza informatica per le MPMI” è specificamente progettato per dare ai proprietari, ai manager e ai dipendenti delle MPMI le conoscenze e le competenze necessarie per proteggere i loro dati preziosi e le informazioni sensibili. | | | |
| Obiettivi formativi | * Acquisire una comprensione completa delle minacce alla sicurezza informatica e delle misure necessarie per proteggere le loro MPMI. * Essere dotati delle conoscenze e delle competenze necessarie per creare un’infrastruttura informatica sicura. * Essere in grado di gestire la sicurezza delle informazioni e rispondere efficacemente agli incidenti di sicurezza informatica. | | | |
| Indice (3 livelli: Modulo-Unità-Sezione) | Modulo: Mantieni i tuoi dati al sicuro: Sicurezza informatica per le MPMI  **Unità 1**: Introduzione alla sicurezza informatica per le MPMI  Sezione 1.1. Comprensione della sicurezza informatica: definizione e importanza delle politiche di sicurezza  Sezione 1.2. Minacce comuni alla sicurezza informatica cui devono far fronte le MPMI  **Unità 2**: Creazione di un’infrastruttura TIC sicura  Sezione 2.1. Valutazione delle vulnerabilità della sicurezza informatica  Sezione 2.2. Utilizzo efficace di soluzioni antivirus e antimalware  **Unità 3**: Gestione della sicurezza delle informazioni  Sezione 3.1. Pratiche e linee guida | | | |
| Contenuti sviluppati | Modulo: Mantieni i tuoi dati al sicuro: Sicurezza informatica per le MPMI  Unità 1: Introduzione alla sicurezza informatica per le MPMI  **Sezione 1.1.** Comprensione della sicurezza informatica: definizione e importanza delle politiche di sicurezza  Una politica di sicurezza per le micro, piccole e medie imprese (MPMI) è un documento formale che delinea l’approccio dell'organizzazione alla sicurezza delle informazioni. Stabilisce le regole, le linee guida e le responsabilità per proteggere le risorse, i dati e i sistemi dell’azienda da potenziali minacce e accessi non autorizzati. La politica dovrebbe essere completa, chiara e adattata alle esigenze e ai rischi specifici cui devono far fronte le MPMI. Comprendere la sicurezza informatica e l’importanza delle politiche di sicurezza per le micro e piccole medie imprese dopo il COVID-19 è fondamentale per diversi motivi:  **Consapevolezza delle minacce informatiche**: Comprendere la sicurezza informatica consente **alle persone di essere consapevoli delle varie minacce informatiche e dei rischi esistenti nel panorama digitale.** **Li aiuta a riconoscere potenziali vulnerabilità** e debolezze nei loro sistemi, reti e pratiche.  **Protezione dei dati sensibili**: Le misure di sicurezza informatica proteggono i dati sensibili e riservati da accessi, furti o abusi non autorizzati. Ciò è particolarmente **importante per le MPMI, in quanto spesso gestiscono preziose informazioni sui clienti,** dati finanziari e proprietà intellettuale.  **Prevenzione delle violazioni dei dati**: Le politiche di sicurezza svolgono un ruolo significativo nella prevenzione delle violazioni dei dati e degli attacchi informatici. Delineano **procedure e linee guida per garantire che i dati siano gestiti in modo sicuro** e che i potenziali punti di ingresso per gli aggressori siano ridotti al minimo.  **Mantenimento della Continuità Aziendale**: La sicurezza informatica è essenziale per il **buon funzionamento di una MPMI**. Le politiche di sicurezza **aiutano a identificare potenziali rischi** che potrebbero interrompere le operazioni aziendali e aiutare nello sviluppo di strategie per mantenere la continuità di fronte agli incidenti informatici.  **Conformità e requisiti giuridici**: Molti settori hanno normative e requisiti legali specifici in materia di protezione dei dati e sicurezza informatica. **Comprendere la sicurezza informatica aiuta le MPMI ad aderire a queste normative, evitare sanzioni** e mantenere la fiducia di clienti e partner.  **Costruire la fiducia dei clienti**: Dimostrare l’impegno a favore della sicurezza informatica e avere solide politiche di sicurezza in atto **può migliorare la fiducia dei clienti in una MPMI**. I clienti hanno maggiori probabilità di fare affari con organizzazioni che danno priorità alla protezione dei loro dati e della loro privacy.  **Prevenire perdite finanziarie: Gli attacchi informatici possono comportare perdite finanziarie significative per le MPMI**. La comprensione della sicurezza informatica e l’attuazione di politiche di sicurezza efficaci **possono contribuire a mitigare i rischi finanziari associati alle violazioni dei dati e ad altri incidenti informatici**.  **Gestione della reputazione**: Un attacco informatico di successo può **danneggiare la reputazione di una MPMI**, portando a **una perdita di clienti e opportunità**. Le politiche di sicurezza aiutano a prevenire gli incidenti e dimostrano la dedizione dell’organizzazione alla salvaguardia delle informazioni.  **Preparazione alle crisi**: Le politiche di sensibilizzazione e sicurezza in materia di sicurezza informatica aiutano le MPMI a **prepararsi a potenziali crisi** riducendo i tempi di ripresa.  **Formazione e sensibilizzazione** **dei dipendenti**: Comprendere la sicurezza informatica consente alle organizzazioni di fornire una formazione adeguata ai propri dipendenti. **Educare il personale** sulle migliori pratiche, sulle potenziali minacce e sulle politiche di sicurezza **aiuta a creare una forte cultura della sicurezza** all’interno dell’organizzazione.  **Vantaggio competitivo**: L’enfasi sulla sicurezza informatica e l’adozione di politiche di sicurezza efficaci possono **fornire a una MPMI un vantaggio competitivo**. **I clienti e i partner spesso danno priorità alla sicurezza** quando scelgono i partner commerciali, rendendo la sicurezza informatica un valido elemento di differenziazione.  In conclusione, comprendere la sicurezza informatica e l’importanza delle politiche di sicurezza è fondamentale per le MPMI per proteggere i propri dati, mantenere la continuità operativa, rispettare le normative e costruire fiducia nei confronti di clienti e stakeholder. Affrontando in modo proattivo le minacce informatiche, le MPMI possono rafforzare la loro resilienza e garantire un ambiente digitale sicuro per le loro operazioni.  **Sezione 1.2.** Minacce comuni alla sicurezza informatica cui devono far fronte le MPMI  Le micro, piccole e medie imprese (MPMI) stanno diventando sempre più i bersagli dei criminali informatici a causa dei loro preziosi dati e delle difese potenzialmente più deboli della sicurezza informatica rispetto alle organizzazioni più grandi. Alcune minacce comuni alla sicurezza informatica affrontate dalle MPMI includono:  **Attacchi di phishing**: Il phishing è una tecnica in cui i criminali informatici inviano e-mail, messaggi o siti Web ingannevoli per indurre i dipendenti a divulgare informazioni sensibili come credenziali di accesso, dati finanziari o informazioni personali.  **Ransomware**: Ransomware è un tipo di malware che crittografa i dati di un’organizzazione, rendendoli inaccessibili fino al pagamento di un riscatto. Le MPMI possono essere mirate a causa di misure di sicurezza percepite come più deboli.  **Infezioni malware**: Le MPMI sono esposte a vari tipi di malware, tra cui virus, trojan e spyware. Questi programmi dannosi possono interrompere le operazioni, rubare dati o ottenere l’accesso non autorizzato ai sistemi.  **Minacce interne**: Le minacce interne comportano azioni dannose o errori non intenzionali commessi da dipendenti o individui con accesso ai sistemi, ai dati o alle reti di un’organizzazione.  **Attacchi di ingegneria sociale**: L’ingegneria sociale prevede la manipolazione delle persone per rivelare informazioni riservate, come password o credenziali di accesso. Ciò potrebbe avvenire tramite telefonate, interazioni di persona o social media.  **Dispositivi IoT non protetti**: Molte MPMI utilizzano dispositivi IoT (Internet of Things), come telecamere intelligenti o sensori. Se non correttamente protetti, questi dispositivi possono diventare punti di ingresso per gli aggressori e possono infiltrarsi nella rete.  **Password deboli e autenticazione**: Pratiche di password inadeguate, come l’uso di password facilmente indovinabili o il loro riutilizzo su più account, possono rendere le MPMI vulnerabili agli attacchi di forza bruta o al riempimento delle credenziali.  **Violazioni dei dati**: Le MPMI spesso raccolgono e memorizzano preziosi dati dei clienti. Se non adeguatamente protetta, una violazione dei dati potrebbe portare a danni alla reputazione, perdite finanziarie e conseguenze legali.  **Attacchi Negazione del Servizio (DoS):** Gli attacchi DoS travolgono i sistemi o la rete di un’organizzazione con un’ondata di traffico, causando interruzioni e tempi di inattività.  **Mancanza di aggiornamenti software e patch regolari**: La mancata applicazione di aggiornamenti tempestivi e patch di sicurezza a software e sistemi operativi può lasciare le MPMI esposte a vulnerabilità note.  **Preoccupazioni per la sicurezza** **nel cloud**: L’archiviazione di dati e applicazioni nel cloud può essere conveniente per le MPMI, ma può anche introdurre rischi per la sicurezza se non configurata e gestita in modo appropriato.  **Attacchi della catena** **di fornitura**: I criminali informatici possono prendere di mira le MPMI come mezzo per ottenere l’accesso alle organizzazioni più grandi sfruttando le vulnerabilità nella catena di fornitura.  **Impostazioni di sicurezza mal** **configurate**: Impostazioni di sicurezza configurate in modo errato su sistemi, applicazioni o dispositivi di rete possono creare lacune di sicurezza non intenzionali.  **Mancanza di consapevolezza sulla sicurezza informatica dei dipendenti**: La consapevolezza e la formazione insufficienti in materia di sicurezza informatica tra i dipendenti possono aumentare la probabilità di cadere vittima di varie minacce informatiche.  Per mitigare tali minacce, le MPMI dovrebbero investire in misure di sicurezza informatica, come la formazione regolare dei dipendenti, solidi controlli degli accessi, solidi metodi di autenticazione, infrastrutture TIC sicure, gestione della sicurezza delle informazioni, software di sicurezza aggiornato e un piano di risposta agli incidenti ben definito. Le pratiche proattive di sicurezza informatica possono ridurre significativamente il rischio di cadere vittima di attacchi informatici e proteggere le preziose risorse e la reputazione dell’organizzazione.  Unità 2: Creazione di un’infrastruttura TIC sicura  **Sezione 2.1.** Valutazione delle vulnerabilità della sicurezza informatica  La valutazione delle vulnerabilità in materia di sicurezza informatica è essenziale per le MPMI per individuare potenziali punti deboli nei loro sistemi, infrastrutture TIC, reti e pratiche. Ecco i passi che una MPMI può adottare per valutare le vulnerabilità della sicurezza informatica:  **Identificare le risorse e i dati**: Iniziare identificando tutte le risorse, le infrastrutture ICT, i sistemi, i dispositivi e i dati che la tua MPMI utilizza o memorizza. Ciò include hardware, software, server, dispositivi di rete, servizi cloud e informazioni sensibili.  **Condurre una valutazione dei rischi**: Eseguire una valutazione completa dei rischi per identificare potenziali minacce, vulnerabilità e il potenziale impatto di un incidente informatico sulla tua organizzazione. Questa valutazione contribuirà a dare priorità agli sforzi per affrontare in primo luogo i rischi più critici.  **Test di penetrazione**: Prendi in considerazione la possibilità di condurre test di penetrazione (hacking etico) per simulare attacchi informatici reali sui tuoi sistemi e reti. Questo aiuta a identificare potenziali punti di ingresso e aree deboli nelle tue difese di sicurezza.  **Revisione della sicurezza di rete**: Valutare la sicurezza dell’infrastruttura di rete, inclusi firewall, router, switch e reti wireless. Assicurarsi che questi dispositivi siano configurati in modo appropriato e che siano predisposti controlli di accesso.  **Valutare Software e Applicazioni**: Verificare regolarmente la presenza di aggiornamenti e patch di sicurezza per tutti i software e le applicazioni utilizzati nella tua organizzazione. Il software obsoleto può creare vulnerabilità che gli aggressori informatici possono sfruttare.  **Valutare la sicurezza** **degli endpoint**: Valutare le misure di sicurezza sui dispositivi endpoint (ad esempio laptop, smartphone, tablet) utilizzati dai dipendenti. Implementare software antivirus, crittografia e applicare politiche per l’accesso ai dati aziendali sui dispositivi personali.  **Controllare la sicurezza fisica**: Non trascurare la sicurezza fisica. Valutare i controlli fisici di accesso ai locali dell’ufficio, alle sale server e alle aree sensibili in cui i dati e le apparecchiature sono archiviati.  **Esaminare la consapevolezza dei dipendenti**: Valutare il livello di consapevolezza della sicurezza informatica tra i tuoi dipendenti. Condurre corsi di formazione e workshop per istruirli sulle minacce informatiche comuni e sulle migliori pratiche per la sicurezza dei dati.  **Rivedere le politiche della password**: Assicurati che siano in vigore criteri di password efficaci, tra cui la necessità di password complesse, modifiche regolari della password e il non riutilizzo delle password su più account.  **Servizi cloud sicuri**: Se utilizzi servizi cloud, valuta le loro caratteristiche di sicurezza e assicurati che soddisfino i requisiti della tua organizzazione. Implementare l’autenticazione e la crittografia a più fattori per i dati sensibili memorizzati nel cloud.  **Analizzare le politiche di sicurezza**: Rivedere e aggiornare regolarmente le politiche di sicurezza. Assicurarsi che siano allineate agli standard del settore e ai requisiti di conformità. Queste politiche dovrebbero riguardare settori come la protezione dei dati, i controlli di accesso, la risposta agli incidenti e l’uso accettabile.  **Verifica dei fornitori di terze parti**: Se lavori con fornitori o fornitori di servizi di terze parti, valuta le loro pratiche di sicurezza informatica e le misure di protezione dei dati per garantire che non introducano rischi aggiuntivi.  **Preparazione alla risposta agli incidenti**: Valuta il piano di risposta agli incidenti della tua organizzazione per assicurarti che sia completo e copre le misure appropriate da adottare in caso di incidente informatico.  **Revisioni periodiche di sicurezza:** Condurre revisioni e valutazioni periodiche di sicurezza per mantenere una comprensione continua della posizione della sicurezza informatica dell’organizzazione.  **Garantire la sicurezza della rete wi-fi:** Proteggere le reti Wi-Fi è fondamentale per prevenire l’accesso non autorizzato e proteggere i dati sensibili.  Essa può essere ottenuta mediante:   * modifica delle credenziali predefinite * utilizzo di crittografia avanzata * abilitazione dell’accesso protetto da Wi-Fi 3 (WPA3) o WPA2 con AES (standard di crittografia avanzata) per una crittografia avanzata * evitare l’uso di metodi di crittografia obsoleti e vulnerabili come WEP (wired equivalente privacy) * modifica dell’identificatore predefinito del set di servizi (SSID) a un nome univoco che non rivela informazioni sulla tua azienda o organizzazione * disattivare la trasmissione SSID per rendere la rete meno visibile ai potenziali aggressori * configurazione di una rete ospite separata per visitatori o clienti che li isola dalla rete interna principale, utilizzando password complesse * abilitare il filtraggio degli indirizzi Mac per consentire solo a dispositivi specifici con indirizzi Mac pre-approvati di connettersi alla rete wi-fi * mantenere aggiornato il firmware * disabilitare la gestione remota sul router per impedire l’accesso non autorizzato dall’esterno della rete * abilitare firewall e crittografia di rete * disattivare il plug and play universale (UPNP) sul router, in quanto può essere sfruttato dagli aggressori per aprire porte ed esporre la rete a potenziali minacce * monitoraggio dell’attività della rete * garantire l’accesso fisico * educare i dipendenti.   **Sezione 2.2.** Utilizzo efficace di soluzioni antivirus e antimalware:  L’uso efficace di soluzioni antivirus e antimalware è fondamentale per le micro, piccole e medie imprese (MPMI) per proteggere le loro infrastrutture, sistemi, reti e dati ICT da varie minacce informatiche.  Ecco alcune migliori pratiche per l’uso efficace di soluzioni antivirus e antimalware:  **Scegli una soluzione completa**: Seleziona un software antivirus e antimalware affidabile e completo che offre protezione in tempo reale, aggiornamenti regolari e scansioni frequenti per rilevare e rimuovere software dannoso.  **Mantieni aggiornato il software**: Assicurati che l’antivirus e il software antimalware siano aggiornati con le ultime definizioni dei virus e gli aggiornamenti del database. Ciò è essenziale per individuare e proteggere dalle minacce nuove ed emergenti.  **Abilita la scansione in tempo** **reale:** Attiva le funzionalità di scansione in tempo reale nel software antivirus per controllare automaticamente i file, i download e gli allegati e-mail per individuare malware appena vi si accede.  **Scansioni regolari**: Impostare scansioni programmate da eseguire in tempi convenienti quando il sistema ha meno probabilità di essere in uso intenso, ad esempio al di fuori dell’orario di lavoro.  **Abilita gli aggiornamenti automatici**: Abilita gli aggiornamenti automatici sia per il software antivirus che per il sistema operativo per garantire una protezione continua contro le minacce più recenti.  **Eseguire scansioni di sistema complete**: Eseguire periodicamente scansioni di sistema complete per controllare a fondo tutti i file, compresi quelli nelle aree meno frequentemente accessibili.  **Quarantena e isola le minacce**: Configurare il software antivirus per mettere in quarantena o isolare le minacce rilevate, impedendo loro di diffondersi o causare ulteriori danni.  **Scansiona i dispositivi esterni**: Eseguire la scansione di tutti i dispositivi esterni, come unità USB o dischi rigidi esterni, prima di accedere ai file per impedire l’introduzione di malware nella rete.  **Educare i dipendenti**: Educare i dipendenti sull’importanza della protezione antivirus e antimalware e addestrarli ad essere cauti con allegati e-mail, download e link per evitare inavvertitamente l’introduzione di malware.  **Implementare la protezione degli endpoint**: Prendere in considerazione l’utilizzo di soluzioni di protezione degli endpoint che forniscono una difesa a più livelli contro vari tipi di minacce, tra cui ransomware e exploit zero-day.  **Gestione centralizzata**: Se si gestiscono più sistemi, utilizzare strumenti di gestione centralizzati per monitorare e controllare software antivirus e antimalware su tutti i dispositivi da un’unica interfaccia.  **Manutenzione regolare del sistema:** Eseguire regolarmente attività di manutenzione del sistema, come la pulizia e la deframmentazione del disco, per ottimizzare le prestazioni del sistema e migliorare l’efficacia delle scansioni antivirus.  **Monitorare e rispondere alle segnalazioni**: Configurare il software antivirus per inviare avvisi per le minacce rilevate e rispondere prontamente e esaminare eventuali avvisi per intraprendere le azioni appropriate.  **Valutazioni periodiche di sicurezza**: Condurre valutazioni e controlli di sicurezza periodici per valutare l’efficacia delle soluzioni antivirus e antimalware e identificare le aree di miglioramento.  **Strategie di backup e ripristino dei dati:** Implementare una strategia regolare di backup dei dati per garantire che i file importanti siano sicuri in caso di grave infezione da malware o attacco ransomware. Stabilire una pianificazione di backup di routine per garantire che i dati critici siano regolarmente sottoposti a backup. A seconda del volume di dati e della frequenza delle modifiche, i backup giornalieri, settimanali o mensili possono essere appropriati. Inoltre, la MPMI può utilizzare soluzioni di backup automatizzate per ridurre il rischio di errori umani e garantire che i backup siano eseguiti in modo coerente senza intervento manuale. Non dimenticare di archiviare i dati di backup in più posizioni fisiche per mitigare il rischio di perdita di dati a causa di furti, incendi o altri disastri che colpiscono una singola posizione. Considera i backup basati sul cloud oltre ai backup in loco come una soluzione economica e affidabile. I backup nel cloud offrono una facile scalabilità, accessibilità e ridondanza dei dati.  Ricorda che la sicurezza informatica è un processo continuo. Valutazioni periodiche, monitoraggio continuo e azioni rapide per affrontare le vulnerabilità sono essenziali per proteggere le MPMI dalle minacce informatiche in continua evoluzione.  Unità 3: Gestione della sicurezza delle informazioni  **Sezione 3.1.** Pratiche e linee guida  La gestione della sicurezza delle informazioni è fondamentale per le micro, piccole e medie imprese (MPMI) per **proteggere i loro dati sensibili**, **mantenere la fiducia dei clienti** e **salvaguardare le loro operazioni aziendali**.  Ecco alcune linee guida e pratiche chiave che le MPMI possono seguire per gestire efficacemente la sicurezza delle informazioni:  **Valutazione del rischio**: Condurre una valutazione approfondita dei rischi per identificare potenziali vulnerabilità e minacce alla sicurezza delle informazioni. Comprendere i tipi di dati che l’organizzazione gestisce, i rischi associati a ciascun tipo e l’impatto di una violazione della sicurezza.  **Politiche e procedure di sicurezza**: Sviluppare e implementare politiche e procedure complete per la sicurezza delle informazioni che coprono aree come la gestione dei dati, i controlli di accesso, la gestione delle password, il backup dei dati e la risposta agli incidenti.  **Formazione dei dipendenti**: Formare tutti i dipendenti sulle migliori pratiche sulla sicurezza delle informazioni, sui protocolli di protezione dei dati e su come riconoscere e rispondere alle minacce alla sicurezza come gli attacchi di phishing. Educare i dipendenti alla sicurezza informatica è fondamentale per una strategia di difesa globale. Gli attacchi di ingegneria sociale e il phishing sono minacce prevalenti rivolte alle MPMI, i dipendenti devono essere in grado di identificare e mitigare i loro rischi riconoscendo le e-mail di phishing, gestendo allegati sospetti e implementando protocolli di autenticazione e-mail. In questo senso, la sicurezza delle password svolge un ruolo cruciale nella protezione dei dati sensibili. I dipendenti devono essere consapevoli delle pratiche per creare password complesse, implementare l’autenticazione a più fattori (MFA) e gestire i criteri di password all’interno dell’organizzazione.  **Controlli** **di accesso**: Attuare controlli di accesso per garantire che solo il personale autorizzato abbia accesso ai dati sensibili. Utilizzare il controllo dell’accesso basato sui ruoli per limitare l’accesso in base a ruoli e responsabilità professionali.  **Trattamento sicuro dei dati**: Stabilire linee guida per la gestione sicura dei dati, sia in formato digitale che fisico. Ciò include una corretta memorizzazione, crittografia e smaltimento sicuro delle informazioni sensibili.  **Aggiornamenti e patch del software regolari**: Mantieni tutti i software, inclusi i sistemi operativi, le applicazioni e gli strumenti di sicurezza, aggiornati con le ultime patch e aggiornamenti per affrontare le vulnerabilità note.  **Firewall e software antivirus**: Distribuisci firewall e software antivirus/anti-malware affidabili per proteggerti da minacce esterne.  **Configurazione sicura della rete**: Configurare le reti in modo sicuro, comprese le reti Wi-Fi, per impedire l’accesso non autorizzato e l’intercettazione dei dati.  **Backup e ripristino** **dei dati:** Eseguire regolarmente il backup dei dati critici e testare il processo di ripristino dei dati per garantire la continuità operativa in caso di perdita di dati o di un attacco informatico.  **Piano di risposta agli incidenti**: Sviluppare un chiaro piano di risposta agli incidenti che delinea le misure da adottare in caso di violazione della sicurezza o di violazione dei dati. Assegnare ruoli e responsabilità al personale chiave per una gestione efficace degli incidenti. La preparazione e la risposta efficace agli incidenti di sicurezza informatica è essenziale per ridurre al minimo i danni e attenuare i rischi.  **Gestione dei fornitori**: Se la MPMI utilizza fornitori o fornitori di servizi di terze parti, condurre la dovuta diligenza per garantire che le loro pratiche di sicurezza delle informazioni siano in linea con gli standard dell’organizzazione.  **Monitoraggio e controlli continui**: Implementare monitoraggio continuo e controlli di sicurezza periodici per rilevare e affrontare potenziali problemi di sicurezza in modo proattivo.  **Conformità alla privacy dei** **dat**i: Rimani aggiornato con le leggi e i regolamenti sulla privacy dei dati pertinenti che si applicano alle operazioni della MPMI. Rispettare i requisiti di protezione dei dati e informare i clienti sulle pratiche di gestione dei dati.  **Sensibilizzazione e cultura in materia di sicurezza**: Promuovere una cultura di sensibilizzazione e responsabilità in materia di sicurezza tra i dipendenti. Incoraggiare la segnalazione di incidenti e preoccupazioni di sicurezza.  **Revisioni di sicurezza regolari**: Condurre revisioni periodiche della sicurezza e valutazioni dei rischi per identificare le minacce emergenti e le potenziali aree di miglioramento.  Gestendo in modo proattivo la sicurezza delle informazioni, le MPMI possono ridurre il rischio di violazioni dei dati, proteggere le informazioni sensibili e creare fiducia con clienti e partner, contribuendo in ultima analisi al successo a lungo termine dell’azienda. | | | |
| 5 voci del glossario | **Internet delle cose (IoT).** L’internet delle cose, o IoT, è un sistema di dispositivi informatici interconnessi, macchine meccaniche e digitali, oggetti, animali o persone che sono dotati di identificatori univoci (UID) e la capacità di trasferire dati su una rete senza richiedere l’interazione umana o uomo- computer.  Fonte: TechTarget <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>  **Negazione del servizio (DoS).** La Negazione del servizio (DoS) è un tipo di attacco informatico progettato per disabilitare, chiudere o interrompere una rete, un sito web o un servizio. In genere, un malware viene utilizzato per interrompere o inibire il normale flusso di dati dentro e fuori un sistema per rendere l’obiettivo inutilizzabile o inaccessibile per un certo periodo. Un esempio di attacco DoS: quando si accede a un sito Web in modo massiccio e ripetuto da luoghi diversi, impedendo ai visitatori legittimi di accedere al sito Web.  Fonte: Trend Micro <https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos>  **Autenticazione multi-fattore.** L’autenticazione a più fattori (MFA) è un metodo di autenticazione che richiede all’utente di fornire due o più fattori di verifica per ottenere l’accesso a una risorsa come un’applicazione, un account online o una VPN. L’AMF è una componente fondamentale di una forte politica di gestione dell’identità e degli accessi (IAM). Piuttosto che chiedere semplicemente un nome utente e una password, l’AMF richiede uno o più fattori di verifica aggiuntivi, il che riduce la probabilità di successo di un attacco informatico.  Fonte: OneLogin <https://www.onelogin.com/learn/what-is-mfa>  **Identificatore del set di servizi (SSID).** (Service Set IDentifier) Il nome assegnato a una rete Wi-Fi (wireless). Tutti i dispositivi della rete devono utilizzare questo nome con distinzione tra maiuscole e minuscole per comunicare tramite Wi-Fi, che è una stringa di testo fino a 32 byte di lunghezza. Fuori dalla scatola, i router wireless e i punti di accesso hanno un SSID predefinito, che può essere il nome del produttore, come "linksys" o "netgear" o semplicemente "default". Alcuni dispositivi usano il loro numero di modello come SSID. Utilizzando un browser Web, l’SSID (e la password) possono essere modificati manualmente nelle impostazioni di configurazione del dispositivo.  Fonte: PCMAG <https://www.pcmag.com/encyclopedia/term/ssid>  **Plug and Play universale (UPnP).** UPnP (Universal Plug and Play) è un protocollo di rete che consente ai dispositivi di scoprirsi e connettersi senza la necessità di configurazione manuale o intervento dell’utente. Il protocollo automatizza tutti i passaggi necessari per il riconoscimento e la comunicazione tra dispositivi sulla stessa rete.  Fonte: **FeniceNAP** <https://phoenixnap.com/blog/what-is-upnp>  **Exploit zero-day**: Un exploit zero-day (0day) è un attacco informatico che prende di mira una vulnerabilità del software che è sconosciuta al fornitore di software o ai fornitori di antivirus. L’aggressore individua la vulnerabilità del software prima di qualsiasi parte interessata a mitigarla, crea rapidamente un exploit e lo usa per un attacco. È molto probabile che tali attacchi abbiano successo perchè le difese non sono in atto. Ciò rende gli attacchi zero-day una grave minaccia per la sicurezza.  Fonte: **Imperva** <https://www.imperva.com/learn/application-security/zero-day-exploit/>  **Ransomware**: Ransomware è un tipo di malware che impedisce o limita gli utenti di accedere al loro sistema, sia bloccando lo schermo del sistema o bloccando i file degli utenti fino al pagamento di un riscatto. Famiglie di ransomware più moderne, collettivamente classificate come cryptoransomware, crittografano determinati tipi di file sui sistemi infetti e costringono gli utenti a pagare il riscatto attraverso determinati metodi di pagamento online per ottenere una chiave di decrittazione.  Fonte: **Trend Micro** [**https://www.trendmicro.com/vinfo/us/security/definition/ransomware**](https://www.trendmicro.com/vinfo/us/security/definition/ransomware) | | | |
| 5 domande di autovalutazione a scelta multipla | Quesito n. 1. Cos’è una politica di sicurezza?  Opzione a: Si tratta di un documento informale che delinea l’approccio dell’organizzazione alla sicurezza delle informazioni  Opzione b: Si tratta di un documento formale che stabilisce le regole, le linee guida e le responsabilità per proteggere le risorse, i dati e i sistemi dell’azienda da potenziali minacce e accesso non autorizzato  Opzione c: Una politica per proteggere solo i beni dell’azienda  Opzione d: Le opzioni dell’albero sono corrette  Opzione corretta: b  Quesito n. 2. Perchè è importante comprendere la sicurezza informatica e le politiche di sicurezza?  Opzione a: Comprendere la sicurezza informatica consente alle persone di essere consapevoli delle varie minacce informatiche e rischi esistenti nel panorama digitale  Opzione b: Le misure di sicurezza informatica proteggono i dati sensibili e riservati da  accesso non autorizzato, furto o uso improprio  Opzione c: Le politiche di sicurezza svolgono un ruolo significativo nella prevenzione delle violazioni dei dati e degli attacchi informatici  Opzione d: Le tre risposte sono corrette  Opzione corretta: d  Quesito n. 3. Si prega di indicare quale risposta è vera:  Opzione a: Gli attacchi informatici possono causare perdite finanziarie trascurabili alle MPMI  Opzione b: Un attacco informatico di successo può danneggiare la reputazione di una MSME, portando a una perdita di clienti e opportunità  Opzione c: Educare il personale sulle migliori pratiche, potenziali minacce e sicurezza  le politiche aiutano a creare una forte cultura della sicurezza all’interno dell’organizzazione  Opzione d: Clienti e partner spesso non danno priorità alla sicurezza quando si scelgono partner commerciali, rendendo la sicurezza informatica un valido fattore di differenziazione  Opzione corretta: b & c  Quesito n. 4. Si prega di sottolineare le minacce comuni alla sicurezza informatica per le MPMI  Opzione a: Trattamenti interni, infezioni e impostazioni di sicurezza ben configurate  Opzione b: Violazioni dei dati, password deboli e autenticazione, infezioni da malware  Opzione c: Attacchi di phishing, attacchi alla catena di fornitura, dispositivi IoT non protetti  Opzione d: Tutte le risposte sono errate  Opzione corretta: b & c  Quesito n. 5. Quali misure una MPMI può adottare per valutare la sua vulnerabilità in sicurezza informatica?  Opzione a: Controllare la sicurezza fisica, esaminare la consapevolezza dei dipendenti e la revisione delle politiche della password  Opzione b: Identificare risorse e dati, condurre una valutazione dei rischi e controllare la sicurezza dei dati fisici  Opzione c: Garantire la sicurezza della rete wi-fi, il test di penetrazione e la valutazione di Software e applicazioni  Opzione d: Le tre risposte sono corrette  Opzione corretta: d | | | |
| Bibliografia e ulteriori riferimenti | Consiglio tecnico di Forbes. (2023, 25 maggio). Piccolo ma potente: Migliori pratiche in materia di cibersicurezza per le PMI. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/?sh=44510c371a33>  Devonshire Green (n.d.). L’importanza della cibersicurezza per le PMI. Devonshire Green. <https://www.devonshiregreen.uk/the-importance-of-cybersecurity-for-smes/>  Agenzia dell’Unione europea per la cibersicurezza (ENISA). (2021). Cibersicurezza per le PMI: Sfide e raccomandazioni. ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes/@@download/fullReport>  Agenzia dell'Unione europea per la cibersicurezza (ENISA). (2021). Guida alla cibersicurezza per le PMI. ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport>  Ministero dell’Economia e della Competitività (Spagna). (2021). Piano di digitalizzazione per le PMI [PDF]. Governo spagnolo. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210902-digitalisation-smes-plan.pdf>  Yerik Afrianto Singgalen. (2021, agosto). Esplorare la sensibilizzazione e la gestione dei rischi delle PMI in materia di cibersicurezza: Sensibilizzazione alla sicurezza delle informazioni. ResearchGate. <https://www.researchgate.net/publication/353622348_Exploring_MSMEs_>  Cybersecurity\_Awareness\_and\_Risk\_Management\_Information\_Security\_Awareness | | | |
| Materiale correlato | DREAM\_WP3\_Cybersecurity\_ITSFA\_ITSFA | | | |
| Video (se presente) | [link] | | | |