CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Ministero delle Imprese
e del Made in Italy

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

VADEMECUM SULLA CYBERSECURITY

per le Piccole e Medie Imprese

SOMMARIO

PREFAZIONE PRES. CYBER 4.0, LEONARDO QUERZONI

L'avvento della digitalizzazione ha aperto nuovi orizzonti per le imprese di tutte le dimensioni, offrendo opportunità senza precedenti di crescita, innovazione e connettività. Tuttavia, con questa crescita digitale sono emerse anche minacce insidiose che possono mettere a rischio la sicurezza delle aziende. In questo scenario è essenziale che anche le piccole e medie imprese siano consapevoli dei pericoli legati alla cyber security e adottino misure appropriate per proteggere i propri dati e le proprie operazioni.

In Italia, come nel resto del mondo, gli attacchi informatici sono in costante aumento e hanno raggiunto proporzioni allarmanti. Nel corso dell'ultimo anno, sono stati registrati numerosi casi di violazioni della sicurezza informatica, con conseguenze finanziarie e reputazionali significative per le imprese coinvolte.

Secondo recenti studi condotti da esperti del settore (Rapporto Clusit 2023), nel 2022 gli attacchi in Italia sono stati 188, in crescita del 169% rispetto all'anno precedente. Di questi, il 7,6% è andato a segno (contro il 3,4% del 2021). A completare il quadro, la gravità, che è risultata elevata o critica nell'83% dei casi. Il settore più attaccato in Italia nel 2022 è quello governativo, con il 20% degli attacchi, seguito a brevissima distanza dal comparto manifatturiero (19%), che rappresenta il 27% del totale degli attacchi censiti nel settore livello globale.

Gli attacchi nel nostro Paese sembrano andare di pari passo con il grado di maturità tecnologica negli specifici ambiti: i settori dei servizi professionali, e tecnico-scientifico vedono un incremento del 233,3% di incidenti gravi, l'industria manifatturiera il +191,7%. Essendo tra le più colpite, è rilevante anche la crescita per le organizzazioni del comparto informatico, (+100%) e governativo-militare (+65,2%).

Questi dati mettono in luce l'importanza di affrontare la questione della cyber security con serietà e urgenza. Le piccole e medie imprese, che nel nostro Paese rappresentano oltre il 99% del sistema economico imprenditoriale, sono spesso considerate bersagli più facili dagli attaccanti, poiché possono avere risorse limitate e misure di sicurezza meno robuste rispetto alle grandi aziende. Tuttavia, nonostante le criticità e le sfide, è possibile adottare un approccio proattivo e mitigare i rischi associati agli attacchi informatici.

A partire dal lavoro realizzato dall'Agenzia Europea di Cybersecurity (ENISA) nell'identificazione delle buone pratiche per la cybersecurity nelle PMI, Cyber 4.0, il Centro di Competenza nazionale sulla cybersecurity, insieme ad Unindustria – Unione degli Industriali e delle imprese Roma, Frosinone, Latina, Rieti, Viterbo, ha proseguito nella direzione della definizione e finalizzazione di un vero e proprio Vademecum sulla Cyber Security per le Piccole e Medie Imprese.

Lo scopo di questo piccolo manuale promosso anche dal Ministero delle Imprese e del Made in Italy è proprio quello di fornire una guida chiara e pratica su come proteggere le aziende dalle minacce cibernetiche. Attraverso una serie di linee guida, raccomandazioni e strumenti, il Vademecum aiuterà le PMI a comprendere le principali vulnerabilità e a mettere in atto misure preventive efficaci.

Leonardo Querzoni
Presidente CYBER 4.0

PREFAZIONE PRES. UNINDUSTRIA, ANGELO CAMILLI

In un'epoca in cui la tecnologia digitale ha permeato ogni aspetto delle attività aziendali, la sicurezza informatica è diventata una priorità fondamentale per il successo e la sopravvivenza delle imprese.

Ormai è evidente che il tema della cyber security non riguarda solo le grandi imprese multinazionali o le istituzioni governative; tutti noi, indipendentemente dalle dimensioni o dal settore di appartenenza, siamo potenziali bersagli. Un singolo attacco informatico può causare danni finanziari significativi e mettere a rischio la continuità delle nostre attività. Pertanto, è fondamentale adottare una mentalità proattiva e fare della sicurezza informatica una priorità aziendale.

Siamo ben consapevoli dei numerosi ostacoli e delle sfide che le piccole e medie imprese affrontano quotidianamente, tuttavia, è fondamentale ricordare che investire nella protezione dei dati e nella sicurezza digitale rappresenta un investimento a lungo termine per la sostenibilità e la competitività delle imprese.

La crescente minaccia degli attacchi informatici e delle violazioni della sicurezza rappresenta un rischio significativo per le attività, minacciando non solo la reputazione, ma anche la capacità di operare in modo efficiente e di mantenere la fiducia dei clienti e dei partner commerciali.

La sfida che ci attende è determinante per la difesa dell'economia del territorio.

Da qui nasce l'idea di promuovere e realizzare il Vademecum sulla Cyber Security per le Piccole e Medie Imprese in seno al Gruppo Tecnico Cyber Security di Unindustria, espressione della realtà industriale del Lazio grazie alla partecipazione di esperti in materia di sicurezza informatica presieduti dall'Ing. Lorenzo Benigni.

Collaborare con il Competence Center Cyber 4.0 rappresenta un primo passo verso un ecosistema in cui le competenze e il know-how sono messe a fattor comune a beneficio della grande forza del Paese: le nostre PMI.

È importante sottolineare che il Vademecum è un modo per offrire una guida pratica non solo agli imprenditori, ma anche ai collaboratori e a tutti coloro che operano o interagiscono con i sistemi informatici, poiché spesso le principali vulnerabilità si trovano proprio nelle azioni che il singolo compie talvolta distrattamente. Dodici passi per un business più sicuro, guideranno le PMI attraverso le migliori pratiche per proteggere i dati sensibili, garantire la privacy dei clienti e mettere in atto una strategia di gestione dei rischi che si adatti alle specifiche esigenze aziendali.

Siamo fiduciosi che attraverso l'applicazione di queste linee guida, sarà possibile migliorare la resilienza cibernetica delle nostre imprese contribuendo allo sviluppo competitivo, sano e duraturo del tessuto economico regionale.

Angelo Camilli
Presidente Unindustria

1 SVILUPPARE UNA SOLIDA CULTURA SULLA CYBERSECURITY

1.1 ATTRIBUIRE LA RESPONSABILITÀ DELLA GESTIONE

Una solida sicurezza informatica è essenziale per il successo duraturo di ogni PMI. All'interno dell'organizzazione si dovrebbe affidare la responsabilità di questa funzione cruciale a una persona avente il compito di garantire che siano destinate alla cybersecurity risorse appropriate, quali impegno in termini di tempo da parte del personale, acquisto di software, servizi e hardware per la sicurezza informatica, formazione del personale e sviluppo di politiche efficaci.

Contesto

È necessario identificare (o introdurre) in azienda professionalità specializzate in grado di affrontare le tematiche di cybersecurity con visione strategica e capaci al contempo di interfacciarsi con le funzioni tecniche, sia a supporto di processi e procedure aziendali, sia per implementare i requisiti normativi e di compliance relativi agli aspetti di protezione dei dati e delle informazioni – in ambito nazionale, europeo e internazionale, sia per supporto e guida del processo di digitalizzazione e transizione verso l'adozione di nuove soluzioni tecnologiche e organizzative. Figure, quindi, specializzate nei processi di governance e che parlino anche la lingua del top-management.

IDENTIKIT DEL RESPONSABILE CYBERSECURITY

ATTIVITÀ

La figura responsabile della sicurezza informatica riporta al senior management aziendale e solitamenta si occupa di:

- Definire, verificare, sviluppare e comunicare la visione e la strategia di cybersecurity aziendale, ivi comprese le policy e le procedure, in accordo con la normativa cogente
- Implementare programmi per la protezione del patrimonio informativo, comprese le azioni di risposta a possibili incidenti o attacchi agli archivi informativi aziendali;
- Disegnare e attuare processi per mitigare i rischi correlati all'adozione delle tecnologie digitali;
- Gestire il flusso informativo verso le autorità, in merito ad eventuali obblighi in ambito cybersecurity;
- Sviluppare iniziative di awareness e formazione per promuovere e sviluppare una cultura aziendale consapevole degli aspetti di cybersecurity;
- Dialogare ad intervalli regolari sia con il top-management sia con il servizio IT, Amministrazione e Controllo, Ricerca & Sviluppo, Responsabili delle varie Unità operative;
- Definire, in accordo con i vertici aziendali, il budget in ambito cybersecurity e monitorare l'utilizzo delle risorse. Suggerire policies e soluzioni ai manager dell'organizzazione.

CONOSCENZE

- Conoscenza dei principali standard, normative, best practices in ambito cybersecurity e protezione dei dati;
- Conoscenza del business, dell'architettura e della tecnologia dell'organizzazione in oggetto per stabilire con oculatezza le politiche di sicurezza volte a proteggerla di fronte ai cyber rischi;
- Conoscenza dei principi e delle tecniche di security e privacy by design;
- Comprensione delle contromisure tecniche ed organizzative in ambito cybersecurity;
- Modelli di analisi del rischio cybersecurity;
- Modelli di valutazione della maturità cyber;
- Pratiche di sicurezza, principali tool per la difesa e protezione dei sistemi informatici.

COMPETENZE

- Comunicare l'importanza di un'efficace gestione della cybersecurity all'interno dell'organizzazione, anche attraverso informazioni documentate, e rendere disponibile, per quanto appropriato, la politica cyber alle parti interessate;
- Analizzare e comprendere i processi aziendali critici dell'organizzazione e valutare possibili conseguenze che risulterebbero se i rischi si concretizzassero;
- Misurare e analizzare gli scenari di rischio cyber, definire criteri per l'accettazione e priorità per il trattamento del rischio;
- Valutare e migliorare la maturità cybersecurity dell'organizzazione attraverso l'implementazione di presidi tecnici e organizzativi;
- Progettare, applicare, monitorare meccanismi e strumenti per la protezione dei sistemi informatici;
- Richiedere e disporre di expertise, risorse, processi in linea con la politica cyber adottata;
- Valutare potenziali impatti (benefici e rischi) dell'innovazione digitale;

Raccomandazioni utili

- **Cybersecurity integrata con il core business aziendale:** Il responsabile cybersecurity deve essere coinvolto nei processi aziendali (core e di supporto) non solo per identificare e valutare i rischi di cybersecurity, ma anche per verificare la conformità alle normative cogenti in materia. Deve comprendere l'organizzazione e il suo contesto, considerando i possibili fattori interni ed esterni che influenzano la sua capacità di conseguire gli esiti previsti nonché le interfacce e le interdipendenze tra le attività svolte dall'organizzazione e quelle svolte da altre organizzazioni. La cybersecurity deve essere considerato un obiettivo programmatico da parte dell'organizzazione;
- **Responsabilità "integrata":** nel contesto delle PMI non è raro trovare risorse che integrano sotto le proprie responsabilità anche quella della sicurezza informatica (tipicamente in un'unica funzione di responsabile sistemi informativi). In tali casi si raccomanda comunque di tenere una linea gestionale dedicata che riporti periodicamente al top management aziendale circa lo stato corrente dei rischi cyber e l'avanzamento delle iniziative in corso;
- **Il responsabile della sicurezza informatica "as a service":** qualora non sia disponibile personale interno preparato a ricoprire tale ruolo, si può ricorrere ad un fornitore esterno. Tuttavia, è opportuno monitorare l'operato del fornitore al fine di garantire coerenza con la strategia di digitalizzazione e sviluppo attraverso l'identificazione di un focal point interno (preferibilmente con almeno competenze di base in ambito cybersecurity).

1.2 COINVOLGERE IL PERSONALE

Coinvolgere i dipendenti:

- mediante un'efficace comunicazione in ambito cybersecurity da parte della dirigenza e, ove previsto, dal Responsabile Cyber,
- sostenendo apertamente le iniziative per la cybersecurity,
- offrendo formazioni appropriate ai dipendenti, e
- definendo regole chiare e specifiche al riguardo nelle politiche in materia cybersecurity, in compliance alle normative vigenti

Contesto di riferimento

Il vettore maggiormente utilizzato per attacchi di tipo cyber che coinvolgono le PMI è il fattore umano. Sempre più spesso i criminali fanno leva sull'inconsapevolezza o su una conoscenza comunque parziale dei rischi informatici da parte dei dipendenti, per garantirsi un primo varco all'interno dei sistemi informativi aziendali.

Come creare una consapevolezza in merito ai rischi informatici? [12]

Per aumentare la propria sicurezza aziendale, un meccanismo fondamentale di prevenzione è creare una conoscenza diffusa delle minacce cyber e incentivare lo sviluppo di comportamenti consapevoli nell'utilizzo del web e dei dispositivi mobili. I dipendenti devono inoltre essere sempre al corrente sia delle politiche di cyber sicurezza della propria azienda sia del valore del contributo di ciascuno all'efficacia del sistema aziendale.

Raccomandazioni utili

Il primo passo per aumentare la consapevolezza dei propri dipendenti è sempre una valutazione organica del livello di conoscenza delle principali tematiche di cybersecurity e del grado di resilienza rispetto a potenziali minacce. Esistono numerose iniziative in proposito.

Coerentemente con le proprie esigenze ed il contesto organizzativo, ecco alcune buone pratiche per stimolare l'attenzione e la crescita di consapevolezza tra i dipendenti:

- È opportuno che la leadership aziendale guidi e promuova, anche attraverso l'allocazione di risorse adeguate, corsi di formazione e altre iniziative di sensibilizzazione volte al potenziamento di una cultura della cybersicurezza.
- È opportuno considerare sia iniziative di awareness passiva (es. materiale multimediale a disposizione dei dipendenti tramite intranet o cartelle di rete, video e webinar) sia iniziative di awareness attiva (es. role play, simulazioni);
- La strategia di formazione e awareness in ambito cybersecurity deve essere indirizzata a diverse categorie di utenti aziendali (top management, staff, amministrativi, operatori e tecnici, utenti dei sistemi informativi);
- È buona pratica attivare un canale informativo periodico per il personale (es. newsletter, pillole informative tramite video e canali multimediali aziendali).

Risorse utili

- L'Agenzia Europea di Cybersecurity (ENISA) ha sviluppato un numero di risorse gratuite per aumentare la consapevolezza sui temi di cybersecurity, e mette a disposizione risorse specifiche dedicate al contesto delle PMI [1] [2];
- L'Agenzia per la Cybersicurezza Nazionale (ACN, [7]) pubblica periodicamente informazioni sui principali temi di cybersecurity che interessano la nazione, in particolare attraverso il canale del Computer Incident Response Team [8], o tramite la newsletter periodica intitolata "La settimana cibernetica";
- Si raccomanda di monitorare il sito del Centro di Competenza Nazionale Cyber 4.0 , oppure la pagina LinkedIn, per rimanere aggiornati in merito ad opportunità di formazione, seminari e webinar in materia cybersecurity. Cyber 4.0 inoltre pubblica una newsletter quindicinale [9];
- Per rimanere aggiornato in merito alle ultime novità normative e prassi in materia di protezione dei dati personali, consulta il sito dell'Autorità Garante per la Protezione dei Dati Personali [10].

1.3 PUBBLICARE POLITICHE IN MATERIA DI CIBERSICUREZZA

È importante che siano definite, distribuite, e periodicamente riviste e aggiornate, le politiche di cybersicurezza aziendali, che identifichino anche i comportamenti da seguire quando i dipendenti usano l'ambiente, le attrezzature e i servizi informatici aziendali. Tali politiche dovrebbero altresì evidenziare le conseguenze in casi di loro violazione.

Contesto di riferimento

Il riferimento nazionale in materia di politiche di cybersicurezza è il Framework Nazionale di Cybersecurity e la Data Protection [12], che definisce un elenco di controlli da attuare per assicurare una protezione adeguata di processi, infrastrutture tecnologiche e dati.

Buone pratiche

Le politiche che descrivono le regole ed i comportamenti da seguire in ambito cybersecurity e protezione dei dati:

- devono essere scritte, mantenute e aggiornate periodicamente;
- comunicate, in modo chiaro, tramite specifici canali di comunicazione;
- disponibili e idonee all'uso, dove e quando necessario;
- condivise con la Direzione e tutti gli utenti interni dei sistemi informatici;
- conosciute e comprese da parte dei fornitori (es. sottoscrizione delle politica cybersecurity da parte del fornitore in fase di apertura rapporto);
- riesaminate per valutare i risultati delle azioni correttive intraprese e le opportunità per il miglioramento continuo.

ESEMPIO DI UN INDICE DI UNA POLITICA CYBERSECURITY

- Obiettivi
- Quadro normativo (interno ed esterno)
- Perimetro di applicazione
- Il modello organizzativo (ruoli e responsabilità)
- Gestione, sicurezza e classificazione delle informazioni
- Regole in ambito ICT asset management
- Gestione del rischio informatico
- Gestione degli aspetti di sicurezza informatica nei rapporti con i fornitori
- Gestione degli aspetti di sicurezza fisica
- Gestione degli accessi logici
- Regole per l'utilizzo dei dispositivi informatici da parte del personale
- Change management
- Acquisizione, sviluppo e manutenzione dei sistemi informatici
- Regole per la protezione della rete
- Gestione degli incidenti di sicurezza informatica
- Gestione della continuità operativa (es. conformità alla ISO 22301)
- Monitoraggio e miglioramento continuo (KPI, KRI, obiettivi e strumenti)
- Regole per revisione ed aggiornamento della politica

Cosa deve contenere una politica di cybersecurity ed information security?

Una politica deve:

- definire i fattori esterni ed interni che impattano sulla definizione e sul governo della cybersecurity;
- descrivere il modello organizzativo in ambito cybersecuirity e protezione dei dati;
- definire ad alto livello le regole per l'implementazione dei "Controlli essenziali" (definiti dal Framework Nazionale di Cybersecurity e Protezione dei Dati Personali) [12].

Risorse utili

- Framework Nazionale Cybersecurity e Data Protection [12], con particolare riferimento alla sezione 2.3 "Integrazione dei controlli essenziali".
- In materia di processi e procedure per la protezione del patrimonio informativo aziendale, il riferimento internazionale è la norma ISO/IEC 27001 [28] che inquadra le azioni necessarie per garantire la tutela, integrità e disponibilità dei dati e dei sistemi informativi
- Per informazioni aggiuntive consultare:
  - Norma internazionale ISO 22301 [35] relativa alla gestione della continuità operativa, che definisce i requisiti necessari a pianificare, stabilire, attuare, rendere funzionante un sistema di gestione documentato, e per monitorare, mantenere attivo e migliorare in continuo il sistema di gestione finalizzato a proteggere, ridurre le possibilità di accadimento, preparare, dare risposte e ripristinare eventi destabilizzanti per un'organizzazione, quando questi si manifestarsi.
  - European Cyber Resilience Act [36], proposta di regolamento sui requisiti di sicurezza informatica per i prodotti digitali, volta a garantire prodotti hardware e software più sicuri, maggiore trasparenza verso l'utente e tutela dei suoi diritti.
  - Direttive NIS [30] e NIS2.

1.4 ESEGUIRE AUDIT PER LA CYBERSICUREZZA

È necessario svolgere periodicamente audit sulla protezione di dati e sistemi, da affidare a persone in possesso di conoscenze, competenze ed esperienze appropriate. I revisori dovrebbero essere indipendenti, che si tratti di contraenti esterni o di personale interno all'azienda, non coinvolto nelle operazioni informatiche quotidiane.

Contesto

È opportuno che l'organizzazione pianifichi, stabilisca, attui e mantenga uno o più programmi di audit comprensivi di frequenze, metodi, responsabilità, processi coinvolti e reporting, anche considerando i risultati degli audit precedenti.

Parole chiave [13]:

- Audit: processo sistematico, indipendente e documentato, volto ad ottenere prove, relativamente a un determinato oggetto, e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno. Un audit può essere "interno" svolto da parte della Società stessa al fine di verificare la propria conformità a norme e/o regolamenti, oppure può essere di tipo esterno (seconda o terza parte), ad esempio svolto da parte di un cliente su un proprio fornitore;
- La figura dell'auditor cybersecurity: l'auditor in ambito cybersecurity conduce revisioni indipendenti per valutare la conformità dei controlli e dei processi, considerando il framework normativo interno ed esterno all'organizzazione.

Raccomandazioni

- Nel contesto delle PMI una valutazione della postura di cybersecurity e delle azioni prioritarie da intraprendere può essere conseguita anche tramite attività che in termini di risorse e strumenti siano più semplici di un audit, come le attività di assessment (valutazione e verifica di determinati processi, considerando le normative applicabili esterne e le regole aziendali).

L'ASSESSMENT DI CYBERSECURITY

Cyber 4.0 ha sviluppato insieme alla rete dei Digital Innovation Hub di Confindustria un modello di assessment cybersecurity specifico per il contesto organizzativo e tecnologico tipico di una PMI. Il modello di assesment si base sul Framework Nazionale Cybersecurity e prende in considerazione tutti i controlli definiti "essenziali" [12]. Tramite l'implementazione del modello di assessment è possibile:

- comprendere le vulnerabilità e le debolezze del governo cybersecurity dell'organizzazione;
- identificare i principali sistemi informatici a supporto dei processi dell'organizzazione;
- identificare e descrivere le azioni di rimedio prioritarie per diminuire i rischi cybersecurity applicabili all'organizzazione.

Per saperne di più contatta Cyber 4.0 all'indirizzo: cyber@cyber40.it.

Inoltre, ENISA ha rilasciato sul proprio sito il "Cybersecurity Maturity assessment for Small and Medium Enterprises". Lo strumento disponibile gratuitamente online valuta il livello di maturità aziendale attraverso una serie di domande accentrate in tre aree chiave per il governo della sicurezza informatica (persone, tecnologie, processi). Considerando lo specifico contesto aziendale, viene fornito anche un piano d'azione personalizzato per la sicurezza informatica.

1.5 TENERE A MENTE LA PROTEZIONE DEI DATI

A norma del Regolamento Generale dell'Unione Europea sulla Protezione dei Dati [14] (nota come GDPR), ogni PMI che tratta o conserva dati personali appartenenti a residenti UE/ SEE deve garantire che vengano svolti adeguati controlli della sicurezza ai fini della protezione dei dati e che anche qualsiasi terzo che lavora per conto della PMI abbia attuato idonee misure di sicurezza.

Parole chiave [14]

- Dato personale: Qualsiasi informazione concernente una persona fisica identificata o identificabile
- Trattamento di dati personali: Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- Titolare del trattamento: Una persona fisica o giuridica o un altro organismo responsabile del trattamento dei dati personali e che ne determina le finalità e i mezzi.
- Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
- Trattamento su larga scala: Il Regolamento Generale sulla protezione dei dati non fornisce una definizione precisa di larga scala; tuttavia, le linee guida in materia [14] indicano i seguenti fattori caratterizzanti i trattamenti effettuati su larga scala:
  - numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
  - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
  - la durata, ovvero la persistenza, dell'attività di trattamento;
  - la portata geografica dell'attività di trattamento.

- Monitoraggio sistematico: secondo in linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" [16] si tratta di trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" . Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, si tratta di quei contesti nei quali può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).

Per tutti i termini ed i concetti previsti normativa in materia di protezione dei dati personali, consulta il testo in italiano del GDPR [11], in particolare art. 4 "Definizioni".

Contesto di riferimento

Dal 25 maggio 2018 è divenuto pienamente applicabile in tutti gli Stati membri il Regolamento UE 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

In data 19 settembre 2018 è entrato in vigore il D.lgs. 10 agosto 2018, n. 101 [17] che ha introdotto disposizioni per l'adeguamento della normativa nazionale italiana (D.lgs. 196/2003) alle disposizioni del GDPR, recependo le regole europee nell'ambito del contesto giuridico nazionale. Il D.lgs. ha l'obiettivo di armonizzare le norme del Codice della Privacy al GDPR ed è entrato in vigore il 19 settembre 2018.

Il quadro normativo introduce il concetto di "responsabilizzazione" di titolari e responsabili del trattamento: è richiesta infatti l'adozione da parte di titolari e responsabili di comportamenti proattivi al fine di dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (per maggiori informazioni consulta gli artt. 23-25, in particolare, e l'intero Capo IV del Regolamento [14]).

I titolari hanno il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

IDENTIKIT DEL "RESPONSABILE DELLA PROTEZIONE DEI DATI" (DATA PROTECTION OFFICER)

Il responsabile della protezione dei dati personali (di seguito "RPD"; o anche conosciuto come Data Protection Officer) è una figura prevista dall'art. 37 del GDPR. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento, ed ha il compito di supportare, controllare, fornire consulenza, formare ed informare l'organizzazione in merito all'applicazione del GDPR. A tal fine, deve essere "tempestivamente e adeguatamente" coinvolto in tutte le questioni riguardanti la protezione dei dati personali anche con riferimento ad attività di interlocuzione con l'Autorità.

Coopera, inoltre, con l'Autorità e costituisce il punto di contatto rispetto a quest'ultima e agli interessati, in merito alle questioni connesse al trattamento dei dati personali (artt. 38 e 39 del GDPR)

Il Responsabile della Protezione dei dati può essere un "dipendente" del titolare o del responsabile del trattamento (secondo quanto previsto dall'art. 37, par. 6, del GDPR) in grado di svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

Qualora il Responsabile della Protezione dei Dati sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (es. una Società che fornisce servizi di DPO as a service, come uno studio legale), purché sia comunque identificata una persona fisica atta a fungere da punto di contatto con gli interessati e con l'Autorità di controllo.

È obbligatorio nominare un Responsabile della Protezione dei dati?

Sono tenuti alla designazione del RPD il titolare o il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lettere b) e c), del GDPR, ossia soggetti che:

- svolgono attività di core business che consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati (es. attività di marketing profilato, gestione reti di telecomunicazioni) su larga scala (per tale concetto, fare riferimento alla sezione "parole chiave"); o
- Svolgono attività di core business in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (es. azienda ospedaliera).

Tutti gli altri enti non sono tenuti a designare un DPO.

In ogni caso, resta comunque fortemente raccomandata la designazione di tale figura.

Per maggiori informazioni puoi consultare l'art. 37, par. 1, lettere b) e c), del GDPR oppure le linee guida in materia emanate dal Gruppo di Lavoro "Articolo 29"[1] [15].

Risorse utili:

- Visita la sezione web del sito del Garante Privacy italiano, dedicata agli obblighi posti a capo dei titolari del trattamento[2];
- Consulta le iniziative formative in materia privacy organizzate dal Garante Privacy[3];
- Utilizza e diffondi le infografiche del Garante Privacy per accrescere la consapevolezza e la formazione in materia di dipendenti e fornitori [4];
- Si può inoltre consultare la Norma ISO/IEC 27701 che tiene conto della protezione della Privacy delle entità potenzialmente coinvolte dal trattamento dei dati personali e la Norma ISO/IEC 27702 che fornisce linee guida per l'implementazione dei controlli descritti dalla ISO/IEC 27001.

1 "Il Gruppo di lavoro "Articolo 29" (Art. 29 WP) era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del RGPD) aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali". Per maggior informazioni visita la pagina: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_it

2 https://www.garanteprivacy.it/home/doveri

3 https://www.garanteprivacy.it/home/attivita-e-documenti/iniziative

4 https://www.garanteprivacy.it/infografiche

2 FORNIRE UNA FORMAZIONE APPROPRIATA

Fornire a tutti i dipendenti formazioni periodiche di sensibilizzazione alla cybersecurity in modo che possano riconoscere e affrontare le varie minacce alla cybersecurity. I corsi di formazione dovrebbero essere personalizzati per le PMI e concentrarsi su situazioni di vita reale. Fornire ai responsabili della gestione della cybersecurity in seno all'impresa formazioni specifiche sulla cybersecurity in modo che abbiano le capacità e le competenze necessarie per svolgere il loro lavoro.

Contesto

La formazione in ambito cybersecurity è divenuta elemento essa stessa di protezione e gestione del rischio cyber. La Strategia Nazionale di Cybersecurity [18] identifica la formazione e promozione della cultura della sicurezza cibernetica come un fattore abilitante alla realizzazione degli obiettivi della strategia stessa, in quanto correlati in maniera trasversale agli obiettivi di protezione, risposta, sviluppo.

Il contesto tecnologico attuale comporta la necessità da parte delle organizzazioni di costruire o aumentare la consapevolezza collettiva dei rischi derivanti dall'utilizzo di strumenti informatici. La formazione dei dipendenti risponde alla duplice esigenza di:

- creare consapevolezza diffusa a livello aziendale delle minacce e dei rischi cyber, fornendo le nozioni in merito ai presidi ed alle buone pratiche che ciascun utente deve mettere in pratica per prevenire o reagire ad incidenti informatici;
- rafforzare, integrare o creare in azienda nuove competenze – manageriali e specialistiche – per gestire consapevolmente la sicurezza degli asset tecnologici.

La formazione è da considerarsi parte integrante del programma di mitigazione dei rischi cyber e di gestione della sicurezza delle informazioni.

Raccomandazioni utili

A prescindere dallo strumento formativo scelto, vi sono dei fattori critici di successo da tenere in considerazione nella definizione ed implementazione delle iniziative di formazione:

- Comprendere le esigenze: identificare le esigenze di formazione e le peculiarità del contesto organizzativo e tecnologico dell'organizzazione;
- Disegnare una strategia di formazione: un documento approvato dal management che preveda interventi periodici e aggiornamento continuo dei contenuti in linea con l'evoluzione delle minacce cyber, con revisione almeno annuale;
- Programmare interventi almeno su due livelli: awareness diffusa per tutti i dipendenti, con interventi brevi e possibilmente frequenti, in parallelo a formazione specifica sia per personale tecnico-operativo che per il livello manageriale, con contenuti e linguaggi da adattare al target di riferimento;
- Monitorare i risultati attraverso strumenti quantitativi e qualitativi volti al miglioramento continuo dell'efficacia delle iniziative formative.

Strumenti per campagne di awareness – AR-in-a-Box

AR-in-a-Box è uno strumento gratuito pubblicato ed aggiornato in continuo da parte di ENISA, che fornisce buone pratiche su come progettare e implementare efficaci programmi di sensibilizzazione sulla sicurezza informatica, anche per PMI.

Sono messi a disposizione in maniera strutturale metodologie e risorse necessarie per aumentare efficacemente la consapevolezza della sicurezza informatica all'interno della propria azienda. Per ulteriori informazioni su AR-in-a-Box, è possibile consultare la pagina del sito web dedicata [4], oppure contattare ENISA a: arinabox@enisa.europa.eu

Risorse utili

- Strategia Nazionale di Cybersecurity [18]
- ENISA, AR-in-a-Box [4]
- Sito web Cyber 4.0: www.cyber40.it.

IL RUOLO DEL CENTRO DI COMPETENZA NAZIONALE CYBER 4.0

Cyber 4.0 supporta le PMI erogando formazione in ambito cybersecurity per una molteplicità di target: manageriale, giuridico e tecnico, con una focalizzazione specifica sul contesto delle PMI.

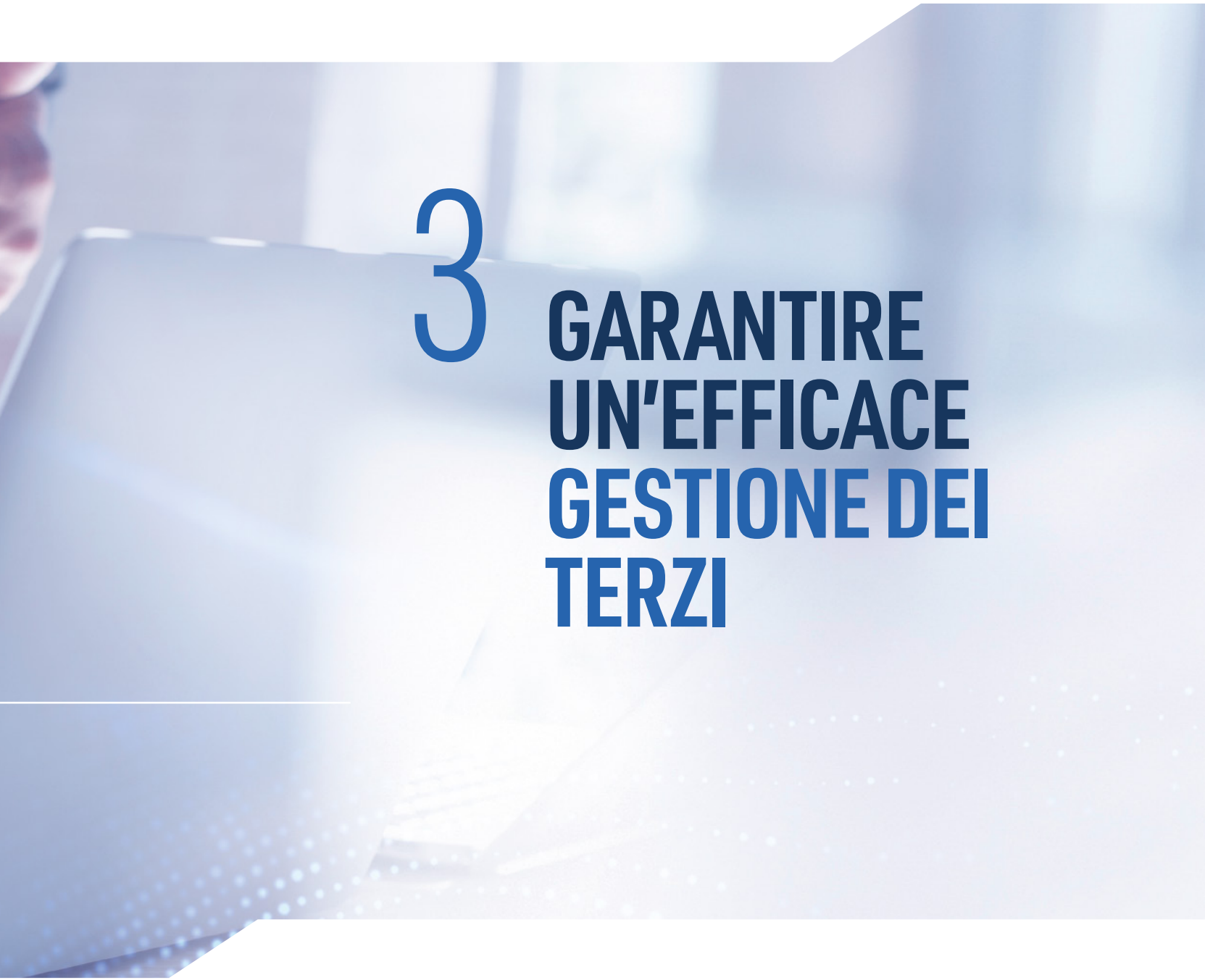
Il Centro, promosso dal Ministero delle Imprese e del Made in Italy, è un partenariato pubblico-privato altamente rappresentativo del contesto nazionale di cybersecurity e mette a fattor comune le competenze dei propri partner per sviluppare iniziative a supporto di imprese e Pubblica Amministrazione.

Le attività che realizza Cyber 4.0 sono, principalmente, di orientamento e advisory su innovazione tecnologica in ambito cybersecurity, di formazione e awareness, di promozione di iniziative di ricerca industriale e dello sviluppo sperimentale attraverso appositi bandi.

In merito alla formazione, a corsi standard a catalogo si affiancano percorsi formativi disegnati sulla base delle esigenze dei singoli. I percorsi sono rivolti tanto a manager, che a esperti cyber e operatori informatici, e sono fruibili sia in aula, che in modalità e-learning o presso l'organizzazione.

I corsi erogati da Cyber 4.0 beneficiano di incentivi specifici per il contesto delle Piccole e Medie Imprese. Per saperne di più entra in contatto con il Centro di Competenza:

https://www.cyber40.it



3 GARANTIRE UN'EFFICACE GESTIONE DEI TERZI

Garantire che tutti i fornitori, in particolare quelli che hanno accesso a dati e/o sistemi sensibili, siano gestiti attivamente e soddisfino i livelli di sicurezza concordati. Dovrebbero essere attuati accordi contrattuali per definire le modalità di soddisfacimento di tali criteri di sicurezza da parte dei fornitori.

Contesto

Gli attacchi alla supply chain (o catena di approvvigionamento) sono in continuo aumento per numero e sofisticatezza. Per approfondire le diverse tipologie degli attacchi informatici derivanti dalla supply chain, è possibile consultare la sezione "Tecniche di attacco utilizzate per compromettere la filiera di fornitura" del report in materia pubblicato da ENISA [22]

COME PRESIDIARE ADEGUATAMENTE I PROPRI FORNITORI?

Raccomandazioni utili

- Al momento dell'esternalizzazione di un servizio o dell'acquisto di un prodotto ICT, identificare i dati, le informazioni ed i processi impattati, al fine di valutare adeguatamente i rischi di natura cyber ed eventuali vincoli normativi applicabili
- Mappare le relazioni commerciali dei fornitori lungo la catena di approvvigionamento, con l'obiettivo di identificare e tracciare le subforniture e gli eventuali accessi alle informazioni ed ai dati dell'organizzazione
- Valutare l'affidabilità in ambito cybersecurity del fornitore, prima della stipula del contratto, anche al fine di definire clausole contrattuali adeguate al livello di sicurezza da garantire
- Richiedere al fornitore l'implementazione di processi di verifica tecnici periodici (es. vulnerability assessment e penetration test) al fine identificare prontamente eventuali vulnerabiltà dei sistemi informatici
- Monitorare il livello di affidabilità del fornitore in ambito cybersecurity e protezione dei dati, anche tramite audit o attività di assessment, dando priorità ai fornitori che hanno accesso ad informazioni critiche o dati sensibili
- Richiedere al fornitore periodicamente aggiornamenti in merito a rischi cybersecurity/ tentativi di attacchi informatici o aggiornamenti in merito alle vulnerabilità
- Coinvolgere/ informare i fornitori in merito ad attività di awareness e formazione in ambito cybersecurity

CHE OBBLIGHI SE LA PMI È FORNITORE?

Istituito con il D.L. 105/2019, il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) [23] è il framework normativo che identifica le infrastrutture critiche, pubbliche e private, del Sistema Paese e definisce quali misure di sicurezza devono essere adottate per proteggere dati e sistemi informativi ritenuti gestite dalla stesse.

Tra tali misure, anche specifici controlli volti a garantire la sicurezza delle attività attuate da parte dei fornitori.

Nel caso in cui una PMI sia fornitore di un'organizzazione inserita nel PSNC (o sia essa stessa nel PSNC) sono definiti i seguenti controlli da effettuare obbligatoriamente sui fornitori [24]:

- adottare un processo di valutazione del rischio dei fornitori di sistemi informativi, componenti e servizi;
- scegliere fornitori che abbiano la capacità di garantire la continuità dell'approvvigionamento, l'assistenza e la manutenzione nel tempo;
- per acquisire componenti software, verificare l'applicazione di pratiche di sviluppo sicuro e l'utilizzo di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware che sarà installato all'interno dei beni e dei sistemi ICT;
- utilizzare pratiche, tecniche e procedure per verificare l'adeguatezza del codice sorgente;
- svolgere audit periodici sui fornitori e mantenere adeguate evidenze;
- con particolare riferimento alla minaccia ransomware, è utile valutare con eventuali fornitori di storage remoto le politiche di backup e ripristino dei dati e tenerne conto in fase di analisi dei rischi derivanti da ransomware.

Per l'elenco completo delle misure di sicurezza da implementare per le infrastrutture critiche del PSNC, è disponibile l'allegato B del DPCM 81/2021 [25], uno dei decreti attuativi del Perimetro di Sicurezza Nazionale Cibernetica, istituito dal D.L. 105/2019.

Altre risorse utili

- un efficace sistema di gestione della supply chain può essere definito considerando quanto previsto dalla ISO 28000 [26], norma certificabile riconosciuta a livello internazionale, che definisce i requisiti per l'implementazione di un sistema di gestione della sicurezza lungo la catena di fornitura (Supply Chain Security);
- NIST - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (pubblicazione speciale NIST 800-161 Revisione 1), fornisce indicazioni sull'identificazione, la valutazione e la risposta ai rischi di sicurezza informatica lungo la filiera di approvvigionamento [27]

4 SVILUPPARE UN PIANO DI RISPOSTA AGLI INCIDENTI

Elaborare un piano formale di risposta agli incidenti che contenga orientamenti, ruoli e responsabilità chiari e documentati per garantire che tutti gli incidenti a livello della sicurezza siano affrontati in modo tempestivo, professionale e appropriato. Per rispondere prontamente alle minacce per la sicurezza, studiare gli strumenti che potrebbero monitorare e creare allerta in caso di attività sospette o di violazioni della sicurezza

Parole chiave

Riportiamo le definizioni pubblicate dal Computer Security Incident Response Team Italia [21]:

- Incidente informatico: ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, l'indisponibilità, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici;
- Violazione dei dati (Data Breach): nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone;
- Indicatori di Compromissione (IoC): Indicatori impiegati per la caratterizzazione e la rilevazione di una minaccia nota (es. indirizzi IP coinvolti nell'esecuzione di un malware);
- Polizia Postale: La polizia postale e delle comunicazioni è una delle unità della polizia di Stato italiana, il cui compito è quello di reprimere i reati che sono legati all'utilizzo dei mezzi di comunicazione, come per esempio Internet;
- CSIRT Italia: Il CSIRT Italia (Computer Security Incident Response Team) è un team di esperti in cybersecurity che agisce in chiave di prevenzione e tempestiva individuazione delle minacce, di ricezione di notifiche e supporto nella gestione degli incidenti segnalati da soggetti pubblici e privati nazionali. Istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN) con D.L. n. 82/2021, lo CSIRT Italia emette preallarmi, allerte, bollettini e divulga informazioni alle parti interessate in merito a rischi e incidenti, anche per supportare le attività di sensibilizzazione, prevenzione e gestione del rischio cyber. Effettua inoltre un costante monitoraggio degli incidenti a livello nazionale, ne riceve notifica da parte dei soggetti coinvolti, li analizza e fornisce supporto alla risposta, al contenimento dei danni e al ripristino della normale operatività.

Buone pratiche

Le attività essenziali che caratterizzano un efficace modello di gestione per la risposta agli incidenti sono solitamente raggruppate nelle seguenti fasi [28][29]:

1. PIANIFICAZIONE E PREPARAZIONE:

- Identificare dei ruoli e delle relative responsabilità per la gestione degli incidenti;
- Comprendere le normative applicabili in materi di notifica incidenti (es. obbligo notifica di una violazione dei dati personali [14], obbligo notifica incidente ad impatto rilevante secondo la normativa NIS [30]);
- Sviluppo e formalizzazione del modello di gestione degli incidenti, che specifichi ruoli e responsabilità in azienda, fasi del processo di gestione degli incidenti, follow up dell'incidente;
- Pubblicazione del modello di gestione degli incidenti alle parti interne (dipendenti) ed esterne (fornitori, stakeholder), limitatamente alle aree di interesse rilevanti per le diversi parti.

2. IDENTIFICAZIONE E VALUTAZIONE DELL'EVENTO

- Identificare ed implementare gli strumenti tecnici per la rilevazione e valutazione di minacce informatiche (es. Intrusion Detection Systems, Intrusion Prevention Systems, antivirus, etc.);
- Qualora l'evento interessi strutture e sistemi che trattano dati personali o dati particolari, si tratta di una violazione di dati personali, per la quale il Regolamento Europeo e la sua traslazione nel contesto nazionale pongono obblighi di notifica (per approfondimenti consultare il punto 4 del presente documento, oppure visita la pagina informativa del Garante Privacy [1]).

3. GESTIONE DELL'INCIDENTE:

- Rilevamento e Analisi;
- Contenimento;
- Eliminazione; Remediation e Recovery.

4. NOTIFICA DELL'INCIDENTE

1 https://www.garanteprivacy.it/regolamentoue/databreach

- In caso di data breach, è necessario procedere ad una valutazione dell'impatto dell'incidente per i diritti e le libertà dei soggetti interessati, al fine di comprendere la necessità di notifica al Garante Privacy, oppure anche ai soggetti interessati. Consulta la pagina del Garante Privacy dedicata alla notifica di un data breach [2], dove è disponibile "L'autovalutazione per la notifica di una violazione di dati personali" ed il template per la compilazione della notifica;
- In caso di eventi informatici, è mandatorio formalizzare denuncia presso la sede più vicina della Polizia Postale e delle Comunicazioni (ogni capoluogo di provincia è dotato di una sede). In alternativa, la Polizia Postale mette a disposizione il Commissariato Online [19]. Tramite la sezione "Segnalazioni online" è possibile compilare un format dedicato agli eventi informatici che potrebbero derivare da fattispecie criminosa.
- È possibile segnalare volontariamente un evento tramite il sito web dello CSIRT nazionale [3], sezione "Segnalazioni", tramite il portale dedicato alla PA / Amministrazione / Impresa / Cittadino [20]. Ai sensi dell'art. 18 del D.Lgs. 65/2018 [30], tutti i soggetti, indipendentemente dalla loro identificazione quali Operatori di Servizi Essenziali o Fornitori di Servizi Digitali, possono inoltrare allo CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati, in modo da contribuire alla raccolta di dati relativi alle minacce che insistono sul cyberspazio nazionale. Allo stesso modo, al di fuori degli obblighi derivanti dalla normativa di riferimento, qualunque soggetto pubblico o privato può segnalare incidenti di sicurezza in forma volontaria. La notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica. Successivamente, il soggetto notificante potrebbe essere contattato a scopo informativo, qualora le informazioni fornite allo CSIRT siano poco chiare o incomplete.

5. MIGLIORAMENTO CONTINUO (LESSON LEARNED):

- il modello di gestione degli incidenti deve essere revisionato ed aggiornato qualora necessario (es. cambiamenti organizzativi, cambiamenti derivanti dallo sviluppo digitale e cybersecurity dell'azienda, cambiamenti normativi), così da garantire continua idoneità, adeguatezza, efficacia. In caso di aggiornamento, il piano va comunicato e reso disponibile ai dipendenti;
- si raccomanda di censire gli incidenti informatici e tutte le informazioni note correlate, in un apposito registro degli incidenti. Qualora si sia trattano di data breach, la normativa privacy richiede obbligatoriamente al titolare del trattamento di registrare formalmente le tentate o accadute violazioni dei dati personali;
- creare un repository degli attacchi/vulnerabilità noti, delle successive azioni intraprese e dei risultati di ogni azione correttiva.

2 https://servizi.gpdp.it/databreach/s/

3 https://www.csirt.gov.it/segnalazione

Riferimenti utili

Di seguito l'elenco delle normative, a livello nazionale ed europeo, con impatto sulla gestione degli incidenti informatici ed in particolare in merito agli obblighi di notifica degli incidenti:

- Regolamento Generale sulla Protezione dei Dati [14], che introduce l'obbligo per i titolari del trattamento di notificare un incidente con impatto sui diretti e le libertà dei soggetti interessati al Garante per la Protezione dei Dati nazionale, ed in alcuni casi anche ai soggetti interessati;
- D. Lgs. 65/2018 che recepisce la Direttiva Europea recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, che introduce l'obbligo di notifica degli incidenti informatici ad impatto rilevante per gli Operatori di Servizi Essenziali ed i Fornitori di Servizi Digitali;
- PSD2, che introduce l'obbligo di notifica degli incidenti per i soggetti che emettono strumenti di pagamento [31];
- Decreto in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inseriti all'interno del Perimetro di Sicurezza Nazionale Cibernetica [24]

5 RENDERE SICURO L'ACCESSO AI SISTEMI

Incoraggiare tutti a utilizzare una frase d'accesso, composta da almeno tre parole comuni scelte a caso che forniscano un'ottima combinazione facilmente ricordabile e sicura.

Se si sceglie una password tipica: deve essere lunga e avere caratteri minuscoli e maiuscoli, possibilmente anche numeri e caratteri speciali; evitare ovvietà, ad esempio «password», sequenze di lettere come «abc» o di numeri come «123»; evitare di usare informazioni personali reperibili online.

Comunque, che si tratti di frasi d'accesso o di password: non riutilizzarle altrove; non condividerle con i colleghi; attivare l'autenticazione a più fattori; utilizzare un gestore di password dedicato.

Contesto

Non è mai scontato sottolineare l'importanza della password come prima difesa contro data breach, data leakage o minacce all'integrità ed alla disponibilità dei dati.

Ogni anno viene realizzata una classifica delle password più diffuse nei principali mercati mondiali, valutando anche il rischio di violazione connesso all'utilizzo di password facilmente identificabili.

L'Italia, come la maggior parte d'Europa, presenta un indice di rischio elevato, con oltre 4 password trafugate e divulgate online pro capite. Secondo la ricerca , tra le password più comuni in Italia ci sono ancora semplici serie numeriche come "123456", "123456789", 12345", "12345678", "000000".

Ma si trovano anche nomi comuni di persona, animali, o riferimenti a squadre di calcio come "juventus", "password", "andrea" e "napoli".

Buone pratiche

A livello aziendale è essenziale [7][29]:

- Forzare l'utilizzo di caratteri speciali nella definizione della password del dipendente, congiuntamente all'utilizzo di numeri, punteggiatura, presenza di lettere maiuscole e minuscole,nonchè di una lunghezza minima di almeno 8 caratteri, pena invalidità della password stessa;
- Impostare il cambio password forzato periodicamente (si raccomanda ogni 3 mesi, a scalare a seconda della criticità delle risorse accedute con quelle credenziali);
- Cambiare sempre la password di default che molti sistemi e dispositivi hanno preimpostata (esempio classico, la coppia user: admin e password: admin per molti dispositivi di rete);
- Definire policy che vietino l'utilizzo di password in condivisione con colleghi, la condivisione delle password utilizzate per l'accesso ai propri dispositivi, la scrittura in chiaro della passwaord su qualsiasi supporto (agenda, lavagna, blocco notes, etc.) lasciato incustodito e a vista in ufficio;
- È buona norma inoltre non utilizzare le stesse password per accedere a servizi differenti, in modo da limitare un possibile effetto a cascata che potrebbe scaturire dalla compromissione di un servizio;
- Inoltre, considerando l'aumentare continuo e l'evolversi dei rischi informatici, è raccomandabile impostare l'autenticazione a più fattori, almeno sui sistemi maggiormente critici: l'autenticazione a più fattori fa riferimento alla necessità di accoppiare qualcosa che si sa (tipicamente le credenziali username e password) con qualcosa che si ha (tipicamente un token o comunque un secondo canale come un sms) o con qualcosa che si è (un elemento biometrico, tipo l'impronta digitale o il riconoscimento del volto).

6 RENDERE SICURI I DISPOSITIVI

6.1 MANTENERE IL SOFTWARE CORRETTO ED AGGIORNATO

Usare preferibilmente una piattaforma centralizzata per gestire gli aggiornamenti.

Si raccomanda vivamente alle PMI di:

- **aggiornare regolarmente tutti i software;**
- **procedere agli aggiornamenti automatici ogniqualvolta possibile;**
- **individuare software e hardware che richiedono aggiornamenti manuali;**
- **tenere conto dei dispositivi mobili e IoT.**

Parole chiave [21]:

- Patch: Aggiornamento del software per eliminare o mitigare vulnerabilità di sicurezza e altri bug generici.
- Penetration Testing (PT): Attività volte a valutare la robustezza di un sistema informatico o di una rete rispetto a potenziali attacchi cyber. Si avvale di strumenti e tecniche volte a verificare l'effettiva possibilità di sfruttare eventuali vulnerabilità presenti nel sistema per penetrare nello stesso, caratteristica questa che lo contrappone a tecniche che si limitano a rilevare la presenza di vulnerabilità senza tentare di sfruttarle.
- Vulnerability Assessment (VA): Attività volta a rilevare l'esposizione di vulnerabilità in un sistema informatico.
- Contesto
- La gestione efficace degli aggiornamenti ai dispositivi informatici (anche denominato "Patch management") rappresenta una contromisura preventiva, al fine di sanare eventuali vulnerabilità che potrebbero venire sfruttate da parte dei criminali informatici.
- Raccomandazioni [7][29]
- La PMI deve dotarsi di personale e procedure per recuperare in maniera tempestiva le informazioni sulle vulnerabilità tecniche dei sistemi informativi; tuttavia, una volta che la patch è resa disponibile da una sorgente legittima, devono essere preliminarmente verificati i rischi che ne derivano dall'installazione.

- Sarebbe opportuno tenere traccia delle patch installate su ciascun dispositivo e della data degli ultimi aggiornamenti effettuati: tale pratica supporta le attività di analisi e recupero a seguito di eventuale attacco. Conseguentemente, un inventario degli asset completo e aggiornato rappresenta un prerequisito per un'efficace gestione delle vulnerabilità tecniche e dei potenziali attacchi informatici correlati.

Per saperne di più

Per rimanere aggiornato sulle vulnerabilità dei sistemi informatici, controlla gli "alert" pubblicati sul sito web del CSIRT (bolletini, news). In alternativa segui la pagina twitter del CSIRT.

Inoltre, assicurati di ricevere periodicamente o in via eccezionale, bollettini da parte dei vendor di software e strumenti informatici, in merito a vulnerabilità rilevate e patch rilasciate.

Cyber 4.0 aggrega competenze di rilievo nazionale e internazionale e può supportare le organizzazioni nell'analisi tecnico-operativo delle vulnerabilità e favorire un contesto di scambio delle informazioni tra imprese, Forze dell'Ordine e technology vendor, per favorire la crescita collettiva del sistema di protezione delle imprese italiane. Per saperne di più visita la pagina del Centro Competenza Cyber 4.0, sezione "Servizi".

6.2 ANTI-VIRUS

Si consiglia di attuare una soluzione antivirus gestita a livello centrale su tutti i tipi di dispositivi e aggiornarla per assicurarne l'efficacia continua e di evitare l'installazione non autorizzata di software malevoli.

Parole chiave [21]:

- Virus: Tipologia di malware capace, una volta attivato, di danneggiare documenti e file eseguibili. Il virus è caratterizzato dalla presenza di istruzioni che ne consentono la replicazione e la conseguente diffusione, che avviene durante il trasferimento del file infetto da un computer a un altro. Si differenzia dal worm, che è in grado di propagarsi autonomamente mediante diffusione dentro reti di computer o tramite email.
- Antivirus: Software che riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli.

Contesto

In caso di minaccia informatica, l'individuazione del codice malevolo permette di intraprendere correttamente e velocemente le opportune contromisure associate alla salvaguardia e all'integrità dei dati e alla disponibilità dei sistemi.

Raccomandazioni

La scelta di un antivirus non può prescindere dalle seguenti valutazioni

- Capacità di protezione da ricorrenti minacce cyber (esempio ransomware);
- funzionalità aggiuntive più adatte per il contesto tecnologico ed organizzativo (es. scansione allegati);
- basso impatto sulle performance del sistema per evitare rallentamenti operativi
- garanzia di affidabilità, grazie a verifiche effettuate da diversi laboratori indipendenti;
- Altre funzionalità aggiuntive come: funzionalità di rilevamento proattivo che identificano le minacce e le anomalie, filtro spam.

ATTENZIONE ALLA SCELTA DELL'ANTIVIRUS

Sulla base del decreto "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina" approvato venerdì 18 marzo 2022 dal Consiglio dei ministri [32], l'Agenzia Nazionale Cybersecurity ha sottolineato la straordinaria necessità e urgenza di assicurare il rafforzamento dei presidi per la sicurezza, la difesa nazionale, le reti di comunicazione elettronica e degli approvvigionamenti di materie prime. In tale contesto l'Agenzia Nazionale propone ha richiesto urgentemente a tutte le organizzazioni nazionali un'analisi del rischio derivante dall'utilizzo di soluzioni di sicurezza informatica di origine russe con riferimento ai dispositivi che si occupano di endpoint security tra cui antivirus, anti malware ed endpoint detection and response; web application firewall, delle seguenti aziende:

- **«Kaspersky Lab»**
- **«Group-IB»**
- **«Positive Technologies»**

In caso di utilizzo di tali dispositivi si richiede di procedere ad una diversificazione. Per saperne di più, è disponibile un approfondimento sul sito web dell'ACN .

Cyber 4.0 offre consulenza specializzata per la scelta e l'implementazione di prodotti antivirus. Visita la pagina dedicata del sito web del Centro di Competenza.

6.3 UTILIZZARE STRUMENTI DI PROTEZIONE PER I MESSAGGI DI POSTA ELETTRONICA E IL WEB

Adottare soluzioni per bloccare messaggi di posta elettronica indesiderati (spam), quelli contenenti link a siti web dannosi o allegati dannosi (virus) nonché messaggi di posta elettronica di phishing.

Parole chiave[21]:

- Phishing: Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.
- Spear Phishing: invio di e-mail mirato. Attacco a un individuo o un'organizzazione specifica, con contenuti personalizzati in base alla vittima.
- Spam/Spamming: Invio indiscriminato e ripetuto di messaggi di comunicazione elettronica verso indirizzi generici e non verificati, perlopiù con finalità commerciali. Le comunicazioni inviate con simili modalità vengono definite spam.

COS'È IL PHISHING

Il phishing è un attacco che rientra tra le tecniche di Social Engineering, ossia l'insieme di tecniche (non solo informatiche) basate sulla manipolazione psicologica per indurre la vittima a commettere errori di sicurezza, fornire informazioni confidenziali o effettuare pagamenti indesiderati ed eseguire azioni desiderati dall'attaccante.

In che modo avvengono gli attacchi informatici tramite posta elettronica?

- File dannosi allegati che, una volta aperti, autorizzano inconsapevolmente l'esecuzione di software malevoli;
- Pagine web fittizie a cui si accede mediante link contenuti nel messaggio e-mail; queste sono spesso riconoscibili dalla presenza di errori ortografici;
- Mittenti mascherati o sconosciuti che propongono operazioni inusuali;
- Mittenti mascherati o sconosciuti che propongono di eseguire operazioni (es. blocco account, pagamenti, rinnovi contrattuali) con un tono allarmistico e di urgenza.
- Come riconoscere un attacco phishing?
- Per riconoscere un attacco di phishing è necessario prestare attenzione a:
- Il mittente (nome e sintassi dell'email);
- Link collegati all'email: è opportuno essere certi dell'affidabilità della pagina web a cui si viene reindirizzati. Appoggiando il cursore sopra il link, senza cliccare, è possibile controllare la pagina web a cui si viene reindirizzati tramite il link;
- Oggetto dell'email e testo (errori di grammatica, frasi sconnesse, carattere / lingue diverse);
- Allegati e rispettivi titoli.

Altre tipologie di phishing

- Whaling: Attacco che prendedi mira un CEO, un CFO o qualsiasi CXX di un settore o di una specifica azienda. Un'email per il whaling potrebbe affermare che l'azienda sta per incorrere in conseguenze legali e che è necessario cliccare sul collegamento per ottenere maggiori informazioni. Il collegamento porta quindi a una pagina che richiede di inserire tutti i dati critici dell'azienda, come CF e numeri dei c/c bancari.
- Smishing: Attacco che, per la sua esecuzione, utilizza i messaggi di testo o SMS. Una tecnica comune di smishing consiste nell'inviare a un telefono cellulare tramite SMS un messaggio che contiene un collegamento cliccabile o un numero di telefono da richiamare.
- Vishing: Gli aggressori sono sempre alla ricerca di informazioni personali o aziendali sensibili. Questo attacco viene però eseguito tramite una chiamata vocale. Da qui la "v" al posto delle lettere "ph" nel nome.

Contesto

Le minacce che possono avvenire tramite l'utilizzo della posta elettronica hanno l'obiettivo di:

- diffondere virus informatici all'interno della rete aziendale;
- sottrarre informazioni riservate attraverso social engineering

Altri consigli per un uso corretto della posta elettronica

- Per evitare la ricezione di molteplici messaggi di posta indesiderata, tra la quale si può nascondere una comunicazione fraudolenta, verifica l'effettiva necessità di sottoscrizione a molteplici newsletter e altri servizi di marketing;
- In caso di sottoscrizione a newsletter, servizi di campagne commerciali e marketing / profilazione, si raccomanda di non utilizzare mai l'indirizzo di posta elettronica aziendale;
- Verificare l'autenticità del mittente ogni qualvolta viene richiesto di condividere informazioni;
- Non prestare attenzione al "Nome visualizzato" del mittente, ma prestare attenzione all'indirizzo di posta del mittente;
- Verifica l'autenticità del mittente anche nel caso in cui le informazioni arrivino dall'interno dell'azienda; ad esempio, qualora vi siano dei sospetti in merito ad un email, è consigliato chiamare telefonicamente il mittente per chiedere conferma in merito alla comunicazione sospetta;
- Evitare di scaricare gli allegati contenuti nelle e-mail se non si conosce la provenienza, o non è chiaro l'oggetto;
- Non condividere mai informazioni personali o riservate via e-mail (es. carta di credito, numero del documento di identità);
- Leggere attentamente il contenuto di ogni mail in cui siano presenti link e/o allegati. Spesso questo tipo di attacchi sfrutta infatti la fretta e la poca attenzione delle persone.

Per saperne di più

- Visita la pagina informativa del Garante Privacy per formarti ed informarti in merito a questo attacco informatico .
- Al sito web di Cyber 4.0 puoi trovare informazioni utili in merito ad attività di simulazione di attacchi di natura social engineering, come ad esempio il phishing, volta a comprendere il livello di conoscenza e comprensione della minaccia da parte dell'organizzazione, e alla pianificazione di eventuale attività formativa mirata.

6.4 CRITTOGRAFIA

Proteggere i dati criptandoli. Le PMI dovrebbero garantire che i dati conservati su dispositivi mobili quali laptop, smartphone e tablet siano criptati.

Per i dati trasferiti su reti pubbliche, come le reti WIFI di alberghi e aeroporti, assicurarsi che i dati siano criptati utilizzando una rete privata virtuale (VPN) oppure accedendo a siti web con connessioni sicure mediante il protocollo SSL/TLS.

Assicurarsi che i propri siti web utilizzino una tecnologia di crittografia adeguata per proteggere i dati dei clienti mentre viaggiano su internet.

Contesto

La crittografia consente di preservare la confidenzialità delle informazioni aziendali senza imporre restrizioni sull'utilizzo dei dispositivi.

Esistono molte applicazioni della crittografia, la più semplice e nota delle quali è la cifratura dei dati di un dispositivo mobile/ portatile attraverso una chiave di blocco. È questa da considerarsi una pratica fortemente raccomandata, in quanto i dati protetti da crittografia divengono così fruibili solo quando il dispositivo è sbloccato tramite l'inserimento di una chiave (es. password, riconoscimento biometrico, etc.), conosciuta o posseduta solo dall'utente autorizzato.

Ciò consente un primo livello di difesa dei dati aziendali anche nel caso in cui il dispositivo sia smarrito o rubato.

Raccomandazioni per lavoro da remoto tramite VPN [7][28]

In caso di lavoro da remoto si raccomanda di utilizzare, se presente, la VPN messa a disposizione dell'azienda. Durante la connessione alla VPN, è possibile svolgere la propria mansione lavorativa utilizzando i servizi informatici aziendali ad esempio: utilizzare la posta elettronica tramite la intranet o attraverso client di posta; accedere alle cartelle di rete (es. File Server, SharePoint); effettuare l'accesso alle applicazioni tramite la intranet aziendale; accedere ai server di amministrazione dell'Azienda.

Tuttavia, durante la connessione alla VPN, è fortemente sconsigliato: navigare su internet su qualsiasi sito non aziendale; utilizzare strumenti di cooperazione non autorizzati dalla Società (es. piattaforma skype qualora non consentita da parte dell'azienda); condividere documenti tramite piattaforme documentali non autorizzate dalla Società (es. google drive qualora non consentito da parte dell'azienda.

Consigli da tenere a mente durante la navigazione web

- Verificare che l'indirizzo web inizi sempre con https://;
- Verificare la presenza di un lucchetto nella finestra del browser (che indica la crittografia delle comunicazioni). Questa modalità di protezione si rende fondamentale quando il sito richiede modalità di autenticazione tramite utente e password ed impedisce, attraverso il meccanismo della cifratura della comunicazione, che le credenziali vengano intercettate una volta inserite.

Raccomandazioni per l'utilizzo di reti Wi-Fi

- Disabilitare la connessione automatica a reti Wi-Fi aperte sia dal proprio PC che dai dispositivi portatili;
- Utilizzare sempre le reti Wi-Fi aziendali, quando disponibili;
- Diffidare delle rete wi-fi pubbliche – In caso di necessità, qualora si stia navigando tramite rete Wi-Fi aperta, non accedere ad informazioni confidenziali e/o ad informazioni critiche aziendali;
- Non lasciare le modalità di accesso alla rete Wi-Fi aziendale con le impostazioni predefinite dal fornitore.

6.5 ATTUARE LA GESTIONE DEI DISPOSITIVI MOBILI

In caso di lavoro a distanza, molte PMI consentono al personale di utilizzare i propri laptop, tablet e/o smartphone.
Ciò dà adito a diverse preoccupazioni sotto il profilo della sicurezza dei dati commerciali sensibili conservati in quei dispositivi.

È possibile gestire questo rischio con l'impiego di una soluzione di gestione di dispositivi mobili (MDM), che consenta alle PMI di:

- **controllare quali dispositivi sono autorizzati ad accedere ai loro sistemi e servizi;**
- **assicurarsi che nel dispositivo sia installato un software anti-virus aggiornato;**
- **stabilire se il dispositivo debba essere criptato;**
- **confermare se nel dispositivo sono installate patch aggiornate per il software;**
- **assicurarsi che il dispositivo sia protetto da PIN e/o password;**
- **cancellare da remoto i dati delle PMI presenti nel dispositivo qualora il proprietario ne segnali lo smarrimento o il furto, o se il proprietario del dispositivo non ha più un rapporto di lavoro con la PMI.**

Contesto

L'utilizzo del dispositivo mobile per svolgere mansioni aziendali può comportare rischi che la società deve tenere a mente ed affrontare attraverso regole scritte, procedure tecniche ed automatizzate, formazione. I rischi connessi all'utilizzo di dispositivi mobili personali sono di diversa natura:

- Rischi per comportamenti degli utilizzatori (Incuria/imperizia nell'utilizzo dei dispositivi mobili aziendali, Gestione impropria delle credenziali di accesso ai dispositivi/servizi;
- Rischi correlati agli strumenti (Virus informatici, Hacking e Sniffing, Malfunzionamento, Danneggiamento dispositivi);
- Rischi per contesto fisico-ambientale (Furto o smarrimento, Indisponibilità delle infrastrutture centralizzate);
- Rischi di conformità (Acquisizione dati di localizzazione senza opportuna informativa agli utenti, Profilazione utente senza consenso).

Inoltre, si ricordano gli adempimenti più importanti per il datore di lavoro:

- La normativa privacy, per la protezione dei dati personali dei dipendenti [14];
- gli adempimenti della normativa giuslavoristica sui controlli a distanza (art. 4 L.300/70) in caso di attività di raccolta dati e monitoraggio svolta tramite il dispositivo informatico utilizzato dal dipendente.

7 RENDERE SICURA LA PROPRIA RETE

7.1 UTILIZZARE FIREWALL

I firewall gestiscono il traffico in entrata e in uscita da una rete e sono essenziali per proteggere i sistemi delle PMI. Dovrebbero essere impiegati firewall per proteggere tutti i sistemi critici, in particolare dovrebbe essere utilizzato un firewall per proteggere la rete della PMI da internet.

Parole chiave [21]

- Firewall: Sistema di sicurezza perimetrale (ossia collocato nel punto in cui due reti entrano in contatto, tipicamente posto tra la rete esterna/ Internet e quella interna ad una organizzazione) che protegge i dispositivi dislocati a valle del firewall da accessi non consentiti.
- Access Control List: controllo degli accessi alle informazioni, risorse, database, rete, sistemi, ecc. in base al principio del "Need to Know". Questa lista, ovviamente, deve essere tenuta aggiornata.

Contesto

Per proteggere le informazioni ed i servizi esposti ed accessibili tramite internet, è necessario individuare ed implementare controlli tecnici ed organizzativi per prevenire accessi non autorizzati dall'esterno della rete aziendale

Raccomandazioni

- Adottare un firewall che sia adatto alle specifiche caratteristiche aziendali e che fornisca soluzioni avanzate di sicurezza, ad esempio:
  - Supporto per la connessione VPN, se prevista;
  - integrazione con capacità di bloccare applicazioni o intrusioni pericolose (IPS – Intrusion Prevention Systems) e di rilevare le intrusioni (IDS – Intrusion Detection Systems);
  - Filtro e blocco della navigazione internet;

    - Filtro e scansione della posta elettronica;
    - Capacità di ispezionare il traffico HTTPS;
    - Capacità di aggiornamento automatico;
    - Facilità di gestione.
- Il firewall può essere utilizzato anche per segmentare la rete interna, al fine di isolare sistemi e processi più critici, evitando il propagarsi dell'evento e dunque il contagio in caso di incidente informatico.
- Individuare i responsabili della gestione dei firewall e sviluppare procedure per la gestione degli stessi (aggiornamento, impostazione delle regole, monitoraggio).
- Verificare periodicamente l'effettiva necessità di connessione alla rete di dispositivi informatici, al fine di limitarne la connessione ove possibile.

Per saperne di più

Informazioni aggiuntive sulla sicurezza della rete possono essere trovate nella ISO/IEC 27033 - Sicurezza della rete [33].

7.2 ANALIZZARE LE SOLUZIONI DI ACCESSO REMOTO

Le PMI dovrebbero analizzare periodicamente gli strumenti di accesso remoto per garantirne la sicurezza, in particolare:

- assicurarsi che tutti i software di accesso remoto siano corretti e aggiornati;
- limitare l'accesso remoto da luoghi geografici o da indirizzi IP sospetti;
- limitare l'accesso remoto del personale ai soli sistemi e computer necessari per lavorare;
- applicare password forti per l'accesso remoto e, ove possibile, attivare l'autenticazione a più fattori;
- garantire il monitoraggio e l'attivazione di allerta per avvertire di attacchi sospetti o insolite attività sospette.

Inoltre, con particolare riferimento ai fornitori [7] [28]:

- Gli accessi da remoto da parte dei fornitori o di altre parti esterne dovrebbero essere identificati, limitati ai requisiti di business, monitorati. Tale aspetto dovrebbe essere valutato nell'ambito dell'analisi del rischio informatico;
- Gli accessi da remoto da parte dei fornitori dovrebbero essere concordati e formalizzati attraverso i contratti di servizio;
- In caso di accesso da remoto da parte del fornitore per manutenzione, l'organizzazione dovrebbe essere preliminarmente informata. Tale obbligo dovrebbe essere contrattualizzato.

8 MIGLIORARE LA SICUREZZA FISICA

Dovrebbero essere attuati controlli fisici adeguati nei luoghi in cui sono presenti informazioni importanti. I laptop o smartphone aziendali, ad esempio, non dovrebbero essere lasciati incustoditi nel sedile posteriore di un veicolo. Ogniqualvolta un utente si allontana dal computer dovrebbe bloccarlo. Altrimenti, predisporre la funzione di blocco automatico su ogni dispositivo utilizzato a fini aziendali. I documenti sensibili stampati non dovrebbero essere lasciati incustoditi e quando non sono utilizzati andrebbero archiviati in modo sicuro.

Contesto

Le regole di cybersecurity previste dall'organizzazione rischiano di non essere efficaci se non combinate con chiare regole in ambito sicurezza fisica. In aggiunta a quanto in premessa, di seguito alcune raccomandazioni da tenere a mente per la sicurezza degli ambienti fisici aziendali

Raccomandazioni

- Prevedere postazione di controllo degli accessi non solo all'ingresso principale dell'azienda ma anche all'interno (es. lungo i corridoi o in specifiche aree) anche per fornire informazioni agli auditor;
- Identificare le aree fisiche interne ed esterne l'organizzazione ove risiedono le informazioni ed i dispositivi informatici critici per l'organizzazione, e renderle accessibili solo al personale autorizzato;
- Definire un sistema per identificare facilmente i dipendenti dell'azienda al fine di riconoscere gli esterni (es. fornitori / visitatori);
- Identificare ed implementare adeguati sistemi di sicurezza fisica per proteggere e monitorare l'accesso ad aree che contengono informazioni / dispositivi informatici (es. accesso tramite tesserino di riconoscimento, accesso tramite tornello);

- identificare i punti di accesso (es. aree di carico e scarico) non adeguatamente presidiati ed attraverso i quali potrebbero accedere persone non autorizzate; implementare adeguate contromisure per prevenire l'accesso non autorizzato (es. videosorveglianza, porte allarmate);
- Verificare che le aree ove sono presenti server ed hardware siano dotati di sistemi di sicurezza ambientale (es. sistemi antincendio);
- Sottoporre a test periodici i sistemi antiintrusione.

9 RENDERE SICURI I BACK UP

Per consentire il recupero di informazioni essenziali, sarebbe opportuno eseguire backup perché costituiscono un modo efficace per il ripristino da disastri, ad esempio un attacco ransomware.
Per il backup dovrebbero applicarsi le seguenti regole:

- **Il backup deve essere regolare e automatico ogniqualvolta possibile;**
- **il backup deve essere tenuto separatamente dall'ambiente di produzione della PMI;**
- **i backup devono essere criptati, soprattutto se saranno spostati tra diversi luoghi;**
- **deve essere verificata la capacità di ripristinare regolarmente i dati dai backup.**
- **Idealmente, andrebbe effettuato un test periodico di un ripristino completo dall'inizio alla fine.**

Parole chiave [21]

- Back up: salvataggio, parziale e totale, dei contenuti di una memoria, assicurando quindi la ridondanza dei dati.
- Ransomware: Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Contesto

Il backup è la copia, parziale o completa, dei dati in uso aziendale e la loro archiviazione separata dall'ambiente operativo.

Un corretto e testato sistema di backup rappresenta una salvaguardia utile in caso di compromissione del patrimonio informativo aziendale, perché consente di ripristinare la situazione operativa al momento in cui è stata effettuata la copia.

IL RANSOMWARE

Il ransomware è un malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. Molto spesso un secondo riscatto viene richiesto anche per non divulgare a terzi i dati che sono stati sottratti prima della cifratura.

I ransomware sono, nella maggioranza dei casi, diffusi tramite siti web malevoli o compromessi, ovvero per mezzo di allegati in posta elettronica apparentemente innocui (es. file PDF) provenienti da mittenti che appaiono legittimi.

Un esempio molto pertinente di attacco che causa compromissione del patrimonio informativo aziendale è rappresentato dal ransomware. Il ransomware è oggi di gran lunga la minaccia più diffusa nel contesto delle PMI.

Raccomandazioni

- Si raccomanda di classificare i dati in base al livello di criticità che questi rivestono all'interno dell'organizzazione consente di ottimizzare le risorse a disposizione; in tal modo è possibile individuare chiaramente quali porzioni di dati sono critiche e necessitano, ad esempio, di backup più frequenti e in siti isolati. Inoltre, in base alla criticità del dato occorre valutare l'opportunità di avere le repliche su siti remoti o comunque su porzioni di rete segmentate.
- Le politiche per svolgere i back up dei dati dovrebbero essere formalizzate tramite procedure documentate, svolte da parte di personale autorizzato e competente.
- È opportuno definire un piano di back up tenendo conto dei seguenti requisiti:
  - l'estensione (back up completo / differenziale) e la frequenza regolare dei backup, dovrebbe essere definito considerando gli obiettivi di business dell'organizzazione ed in linea con il piano di continuità operativa, qualora esistente;
  - eseguire il backup durante le ore notturne o comunque negli slot temporali in cui l'organizzazione non è nel pieno delle attività;
  - documentare e testare le procedure di ripristino;
  - la verifica dei backup permette di garantire l'integrità del dato;
  - i backup dovrebbero essere archiviati in un sito remoto, ad una distanza sufficiente per evitare ogni danno in caso di disastro fisico che interessi il sito principale;
  - garantire la sicurezza fisica ed ambientale dei supporti fisici dei back up;
  - per i dati critici, proteggere le copie di backup attraverso la crittografia;
  - quando le informazioni ed i dati sono gestiti da parte di fornitori, valutare le politiche di backup e ripristino dei dati e tenerne conto in fase di analisi dei rischi di indisponibilità.
- Si raccomanda inoltre di valutare una separazione anche logica dell'ambiente di back-up dall'ambiente operativo, così che la compromissione dell'uno (per esempio per via di un ransomware), non comporti la possibilità di accesso – e compromissione a cascata – anche dell'altro.

10 LAVORARE CON IL CLOUD

Pur offrendo numerosi vantaggi, le soluzioni basate sul cloud presentano alcuni rischi peculiari che le PMI dovrebbero prendere in considerazione prima di impegnarsi con un provider di servizi cloud. L'ENISA ha pubblicato una «Guida alla sicurezza del cloud per le PMI» [6] cui le PMI dovrebbero fare riferimento per la migrazione al cloud. Quando scelgono un provider di servizi cloud, le PMI dovrebbero fare in modo di non violare leggi o regolamenti in caso di conservazione di dati, specialmente dati personali, al di fuori dell'UE/del SEE. Ad esempio, il regolamento generale dell'UE sulla protezione dei dati richiede che i dati personali di residenti UE/SEE non siano conservati o trasmessi al di fuori dell'UE/del SEE, salvo in casi molto specifici.

Contesto

Il cloud computing comporta diversi vantaggi per le organizzazioni: economia nella gestione dei processi; possibilità di "scalare" la soluzione iniziale; flessibilità organizzativa; bassi tempi del "time to market"; efficienza energetica; riduzione dei costi; adeguamento a certificazioni ambientali ed etiche; utilizzare ambienti di collaborazione e comunicazione distribuita in maniera digitale; supporto alla business continuity.

COSA SI INTENDE CON IL TERMINE CLOUD

Il cloud è un paradigma di fruizione, tramite internet, di risorse informatiche a servizio, a partire da un pool di risorse hardware e software disponibili da remoto. Tra i numerosi vantaggi, l'utente non deve configurare e installare alcun software sulla propria macchina.

Per le PMI, inoltre, uno dei benefici più rilevanti dell'utilizzo di risorse cloud è la possibilità di contrattualizzare con il fornitore l'implementazione di presidi di sicurezza dei dati e delle applicazioni generalmente più solidi di quelli che potrebbero essere predisposti per un'infrastruttura completamente ospitata presso la propria organizzazione.

Sono tuttavia da prendere in considerazione misure atte a garantire il pieno controllo dei dati gestiti in cloud.

Tipologie di cloud e di servizi

- **Cloud privato:** Installato dall'azienda nel proprio data center per proprio utilizzo esclusivo. L'azienda detiene controllo e totale responsabilità della gestione dell'infrastruttura e degli aspetti di sicurezza dei dati. Altro scenario di cloud privato è quello in cui l'azienda installa il proprio cloud privato nel data center di un soggetto terzo (es. un fornitore di servizi cloud), dove dispone di macchine dedicate.
- **Cloud pubblico:** Offerto in modo pubblico da fornitori che mettono a disposizione i propri data center ed erogano servizi on demand. Questa logica consente, tra gli altri vantaggi, di utilizzare i servizi cloud limitatamente all'intervallo di tempo necessario, consentendo una riduzione degli investimenti in infrastrutture e risorse interne che le gestiscono, e il conseguimento di importanti economie di scala.
- **Cloud ibrido:** Combinazione dei due precedenti modelli, l'utente utilizza risorse sia del suo cloud privato che di quello pubblico.
- **Multi-cloud:** il modello prevede due o più cloud (dello stesso tipo) messi a disposizione da fornitori differenti. Tale approccio consente, tra gli altri vantaggi, di ridurre la dipendenza da singoli fornitori, aumentando la flessibilità e mitigando l'impatto di eventuali incidenti.

Esistono 3 tipologie di servizi basati sul cloud computing:

- **Software-as-a-Service (SaaS):** distribuzione di applicativi software su richiesta
- **Infrastructure-as-a-Service (IaaS):** risorse infrastrutturali fisiche e virtuali (server, macchine virtuali, risorse di archiviazione e networking) su richiesta
- **Platform-as-a-Service (PaaS):** strumenti e ambienti per lo sviluppo, il test, la distribuzione e la gestione di applicazioni software

Raccomandazioni

- verificare ruoli e le responsabilità affidate al fornitore del servizio cloud, considerando le specifiche tipologie di servizio e di infrastruttura, al fine di assicurare che tali obblighi siano formalizzati adeguatamente tramite contrattualistica (es. risoluzione di vulnerabilità note e rilevate entro determinati SLA).
- verificare le responsabilità e le attività che devono essere attuate da parte del fornitore in caso di incidente. Conseguentemente, identifica chiaramente attraverso procedure interne le responsabilità e le attività che rimangono a capo dell'azienda.
- attuare meccanismi atti a verificare la quantità e la modalità di accesso alle informazioni ed ai dati conservati in cloud da parte del fornitore.
- assicurare che il fornitore cloud abbia individuato adeguate contromisure di tipo fisico ed ambientale in caso di attacchi fisici / disastri ambientali.
- identificare le attività di trattamento svolte dal fornitore del servizio cloud, considerando l'infrastruttura e la tipologia di servizio offerto. Ove necessario procedere con la nomina a responsabile del trattamento dei dati.
- Verificare, ed assicurare, che in caso di trasferimento, o anche solo accesso, dei dati personali all'esterno dell'Unione Europea che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 [14]). In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 [14]). Per maggior informazioni visita la pagina del Garante Privacy dedicata al trattamento dei dati extra UE [1].

1 https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero

11 RENDERE SICURI I SITI ONLINE

È essenziale per le PMI assicurarsi che i loro siti web online siano configurati e tenuti in modo sicuro e che i dati personali o finanziari, come i dati delle carte di credito, siano protetti in modo adeguato. Ciò comporterà la realizzazione di test periodici della sicurezza sui siti web per individuare potenziali carenze a livello di sicurezza e di verifiche periodiche per garantire che il sito sia tenuto e aggiornato correttamente.

Contesto

Il sito web è il canale attraverso cui vengono erogati i servizi dell'azienda, è l'immagine con cui essa si presenta alle proprie controparti ed è un archivio di dati e informazioni essenziali per la conduzione del proprio business. La protezione del sito web è pertanto elemento cruciale per tutte le aziende, e in special modo per le PMI, che spesso lo utilizzano come punto di contatto unico con la propria clientela, B2B o B2C.

Raccomandazioni

Ecco alcuni passi utili per verificare e mantenere la sicurezza del proprio sito web:

- Utilizzare sempre la connessione HTTPS che garantisce la cifratura del traffico, in modo da proteggersi da possibili intercettazioni malevole dei dati scambiati tra client e server;
- Prestare attenzione al rinnovo periodico del certificato digitale associato al proprio sito web, alla registrazione del proprio dominio ed ai servizi collegati (hosting e database);
- Verificare e monitorare i cookie installati sul proprio sito web, al fine di attuare un sistema di gestione conforme alla normativa privacy ed alle linee guida in materia emanate dal Garante privacy italiano. Consulta i materiali informativi presenti alla pagina web dell'Autorità privacy dedica ai cookies [1] ;
- Assicurarsi che il sito web sia dotato di un'adeguata informativa al trattamento dei dati personali, effettuato durante la navigazione dell'utente o per la raccolta di informazioni tramite form, moduli di contatto / moduli di iscrizioni a servizi.

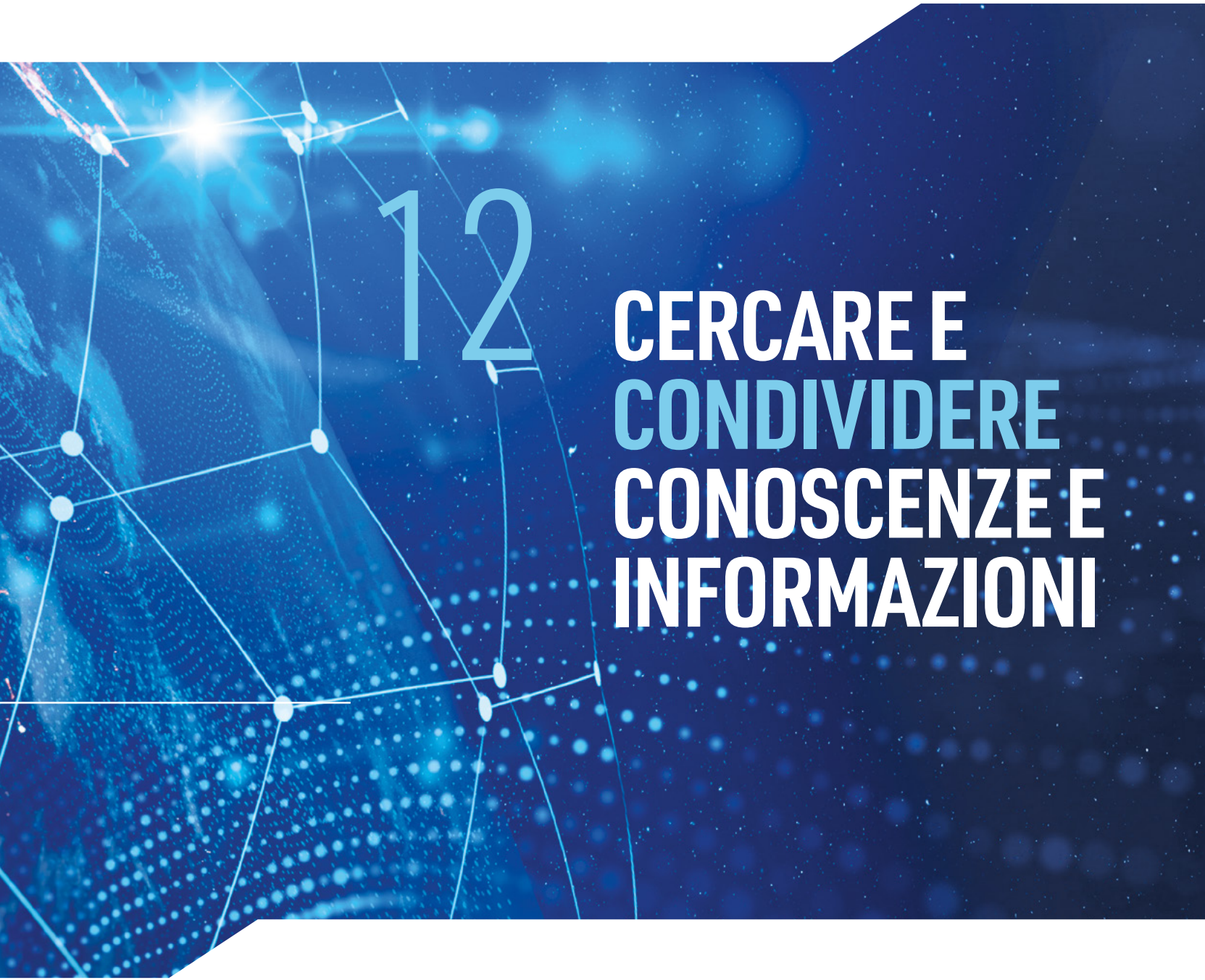
1 https://www.garanteprivacy.it/temi/cookie

BUONE PRATICHE PER L'UTILIZZO DI UN CONTENT MANAGEMENT SYSTEM (CMS)

Se si utilizza un CMS per archiviare, organizzare e pubblicare facilmente i contenuti di un sito web, è necessario fare attenzione agli aspetti di sicurezza: a causa della notevole diffusione di questi sistemi e del loro utilizzo anche da personale non esperto in ambito sicurezza informatica e IT, sono spesso bersagli da parte di hacker informatici.

Per mitigare il rischio di attacco, si raccomanda di seguire alcune buone pratiche:

- Installare il prima possibile gli aggiornamenti disponibili (è possibile attivare la funzionalità di aggiornamento automatico)
- Utilizzare plug-in strettamente necessari
- Oltre all'autenticazione ordinaria (nome utente e password), per l'accesso all'interfaccia di amministrazione è possibile introdurre un'autenticazione a due fattori
- Limitare gli accessi con privilegi di amministratore a determinati indirizzi IP
- Utilizzare web application firewall (WAF) per bloccare gli attacchi provenienti dal web
- Affidarsi ad esperti di sicurezza informatica per sottoporre periodicamente il sito web ad attività di vulnerability assessment e penetration test.



12

CERCARE E CONDIVIDERE CONOSCENZE E INFORMAZIONI

Uno strumento efficace nella lotta contro la criminalità informatica è la condivisione di informazioni. La condivisione di informazioni in relazione alla criminalità informatica è fondamentale per consentire alle PMI di comprendere meglio i rischi cui vanno incontro. È più probabile che le imprese adotteranno misure per rendere sicuri i loro sistemi se sentono parlare dai loro omologhi delle sfide della cybersecurity e di come sono state superate piuttosto che se ne vengono a conoscenza attraverso relazioni del settore o indagini sulla cybersecurity.

Contesto

Come sottolineato anche dalla Strategia Nazionale di Cybersecurity, la condivisione di informazioni in merito ad eventi di natura cyber tra tutti i soggetti, pubblici e privati, è essenziale per costruire un sistema compatto di risposta e prevenzione.

Il punto di riferimento a livello nazionale è lo CSIRT istituito presso l'Agenzia Nazionale di Cybersicurezza, verso il quale è possibile inviare segnalazioni e informazioni su attacchi informatici rilevati o presunti, che non costituiscono atti formali di querela o denuncia, e dal quale è possibile ottenere bollettini informativi su attività malevola monitorata a livello nazionale. Nel caso in cui si volesse segnalare un attacco alle Forze dell'Ordine, si rimanda alla sezione di questo Vademecum relativo alla gestione degli incidenti.

Esistono poi iniziative settoriali per la condivisione di informazioni, alcune già operative, come ad esempio il CERTFin per il settore finanziario, altre progettate e in corso di costituzione, come gli ISAC settoriali (Information Sharing and Analysis Center) previsti dalla Strategia Nazionale.

È allo studio la possibilità di costituire un ISAC per le PMI [1] .

1 https://www.cyber40.it/news/un-isac-per-le-pmi/

Raccomandazioni

- È possibile condividere informazioni in merito ad attacchi informatici presso il sito dello CSIRT Italia, portale segnalazioni, sezione imprese e cittadini. La notizia non costituisce denuncia, querela o esposto, per la cui presentazione si rinvia agli organi di Polizia competenti o Autorità giudiziaria;
- Il Centro di Competenza Cyber 4.0 organizza periodicamente incontri tra istituzioni, mondo accademico e della ricerca ed organizzazione private, e sviluppa un'azione specifica dedicata alle PMI
  - A partire da Ottobre 2022, in collaborazione con la rete dei Digital Innovation Hub, si è sviluppato un percorso nelle Regioni italiane con appuntamenti ricorrenti in cui è prevista la condivisione di esperienze di PMI attaccate e delle azioni messe in campo per ripristinare l'operatività del business;
- È opportuno inoltre monitorare lo scenario delle ulteriori iniziative nazionali di awareness e potenziamento della consapevolezza, anche con l'obiettivo di costruire una rete informale di relazioni di fiducia in ambito cyber, che spesso sono il punto di partenza per una collaborazione fattiva anche a livello operativo.

BIBLIOGRAFIA

[1] European Union Agency for Cybersecurity (ENISA), Cybersecurity for SMEs, challenges and recommendations, 2021
https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

[2] European Union Agency for Cybersecurity (ENISA), Cybersecurity guide for SMEs, 2021
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

[3] European Union Agency for Cybersecurity (ENISA), Cybersecurity Maturity Assessment for Small and Medium Enterprises,
https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/, 2023

[4] European Union Agency for Cybersecurity (ENISA), Cybersecurity Awareness Raising: The ENISA -Do-It-Yourself Toolbox,
https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box, 2023

[5] European Union Agency for Cybersecurity (ENISA), European Cybersecurity Skills Framework, 2022

[6] European Union Agency for Cybersecurity (ENISA), Cloud Security Guide for SMEs,
https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes, 2015

[7] Agenzia Nazionale di Cybersicurezza, **www.acn.gov.it**

[8] CSIRT Italia, Computer Security Incident Response Team, **https://www.csirt.gov.it/**

[9] Cyber 4.0, **www.cyber40.it**

[10] Garante per la Protezione dei Dati Personali, **https://www.garanteprivacy.it/**

[11] Garante per la Protezione dei Dati Personali, Il Testo del Regolamento, **https://www.garanteprivacy.it/il-testo-del-regolamento**

[12] CIS Sapienza Università di Roma, CINI Cybersecurity National Lab, Framework Nazionale per la Cybersecurity e la Data Protection, Versione 2.0, **https://www.cybersecurityframework.it/framework2**, 2019

[13] ISO/IEC 27000:2018 (ISO 27000) Information technology – Security techniques – Information security management systems – Overview and vocabulary.

[14] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, Regolamento Generale sulla Protezione dei Dati,
https://ec.europa.eu/info/law/law-topic/data-protection_en

[15] Gruppo Articolo 29, Linee Guida sui responsabili della protezione dei dati, 2017,
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[16] Gruppo Articolo 29, Linee-guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 (WP248), 2017,
https://ec.europa.eu/newsroom/article29/items/611236

[17] D.lgs. 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE,
https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

[18] Agenzia per la Cybersicurezza Nazionale, Strategia Nazionale di Cybersicurezza 2022 – 2026, **https://www.acn.gov.it/strategia-nazionale-cybersicurezza**, 2022

[19] Polizia Postale e delle Comunicazioni, Commissariato di Polizia Online, **https://www.commissariatodips.it/**

[20] CSIRT Italia, Segnalazione Evento, **https://www.csirt.gov.it/segnalazione**

[21] CSIRT Italia, Glossario, **https://www.csirt.gov.it/glossario**

[22] European Union Agency for Cyber Security, Threat Landscape For supply chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, 2021

[23] DECRETO-LEGGE 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, **https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg**

[24] Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81, **https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg**

[25] Allegato B, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81, **https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg**

[26] ISO/IEC 28000:2007 "Specification for security management systems for the supply chain"

[27] NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations SP 800-161 Rev. 1, 2022

[28] ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements; ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls

[29] ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management

[30] Decreto Legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, **https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg**

[31] Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD 2), **https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L2366&from=LT**

[32] DECRETO-LEGGE 21 marzo 2022, n. 21, Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina, **https://www.gazzettaufficiale.it/eli/id/2022/03/21/22G00032/sg**

[33] ISO/IEC 27033-1:2015: "Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts

[34] CSIRT Italia, Misure di protezione organizzazione dei dati per un ripristino efficace, Agosto 2021, **https://www.csirt.gov.it/contenuti/ransomware-misure-di-protezione-e-organizzazione-dei-dati-per-un-ripristino-efficace**

[35] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

[36] European Commission, Cyber Resilience Act, 2022, **https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act** (draft)