CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SESSIONE FORMATIVA ON LINE CORSO DI PERFEZIONAMENTO

CYBER SECURITY: IL RUOLO DEGLI ADS

Autore Dott.ssa Gloriamaria Paci

Studio Paci & C. Srl
Studio Consulenza Privacy Dott.ssa Gloriamaria Paci
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)

Telefono: 0541 – 1795431
Telefax: 0541 - 1794118
Cellulare: 347-5244264
Mail: info@consulenzepaci.it
Sito web: www.consulenzepaci.it

Seguici sui social!
https://linktr.ee/studiopaci

Associazione Protezione Diritti e Libertà Privacy APS
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)
Tel. 0541-1795431 / Fax 0541-1794118
Cell. Gloriamaria Paci 347-5244264

segreteria@associazionedirittiprivacy.it
posta@pec.associazionedirittiprivacy.it
www.associazionedirittiprivacy.it

Seguici sui social!

https://linktr.ee/apdlp

Gloriamaria Paci

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 Gloriamaria decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela dei dati personali.

L'esperienza di giornalista pubblicista, affiancata a quella di consulente privacy nel settore pubblico e privato, sia sul territorio italiano che in paesi Extra UE (RSM), verrà impiegata per pubblicare numerosi articoli e testi di settore.

Relatrice a convegni, seminari e corsi di formazione, con l'introduzione del Regolamento Europeo 2016/679, oggi ricopre il ruolo di Responsabile per la protezione di dati personali per privati ed enti pubblici.

Presidente dell'Associazione protezione diritti e libertà privacy, porta avanti progetti ed iniziative finalizzate all'aggregazione di quanti sono interessati alla salvaguardia dei diritti e delle libertà personali nell'ambito della protezione dei dati.

Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci & C. Srl
(cda)

Associazione Protezione diritti e libertà privacy APS
(Vice presidente)

Contatti:
dileo@studiopaciecsrl.it
Cell. 3931019939
www.consulenzepaci.it
Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICQ SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

PROGRAMMA DEL CORSO

1. IL RUOLO DELL'AMMINISTRATORE DI SISTEMA

2. GUIDA ALLA CYBERSICUREZZA PER LE PMI

- 12 azioni per rendere sicura la propria Impresa

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

ORGANISMO

L'ENISA, **Agenzia dell'Unione Europea per la Cybersicurezza**, è un centro di competenze in materia di sicurezza informatica in Europa. Aiuta l'UE e i paesi membri dell'UE a essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione.

enisa

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

FUNZIONI

L'Agenzia collabora con le organizzazioni e le imprese per rafforzare la fiducia nell'economia digitale, promuovere la resilienza delle infrastrutture dell'UE e, in ultima analisi, garantire la sicurezza digitale dei cittadini dell'UE. Ciò avviene attraverso la condivisione delle conoscenze, lo sviluppo di personale e strutture e la sensibilizzazione.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

REPORT 2022

Arco temporale analizzato dal report: luglio 2021 – luglio 2022

Il 03 novembre 2022, l'ENISA ha pubblicato **l'ottava relazione annuale "*ENISA Threat Landscape*"** (ETL), identificando e valutando le principali minacce informatiche per il periodo luglio 2021 - luglio 2022.

ENISA

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

REPORT 2022

Sulla base dell'analisi presentata in questo rapporto, l'ENISA identifica e si concentra sui seguenti otto principali gruppi di minacce.

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

RANSOMWARE

Il ransomware **è un programma informatico dannoso che può infettare un dispositivo digitale, bloccando l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto da pagare per liberarli**.

Esistono due tipi principali di ransomware:

1. **i cryptor** → criptano i file contenuti nel dispositivo rendendoli inaccessibili;
2. **i blocker** → bloccano l'accesso al dispositivo infettato.

Questo tipo di software malevoli si diffonde soprattutto attraverso **comunicazioni ricevute via e-mail, sms o sistemi di messaggistica.**

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

PHISHING = PRINCIPALE VETTORE DI ATTACCHI RANSOMWARE

Il phishing è il tentativo fraudolento di rubare i dati degli utenti, come credenziali di accesso, dati della carta di credito o anche denaro, mediante tecniche di ingegneria sociale.

Questo tipo di attacco viene in genere lanciato attraverso messaggi di posta elettronica che sembrano inviati da una fonte attendibile, con l'intento di convincere l'utente ad aprire un allegato malevolo o a seguire un URL fraudolento.

MINACCIA INTERNA

Una minaccia interna **è un'azione che può portare a un incidente, compiuta da una persona o da un gruppo di persone affiliate alla potenziale vittima** o che lavorano per la medesima.

I **cinque tipi di minaccia interna** possono essere definiti secondo le motivazioni e gli obiettivi:

1. **lavoratori negligenti** che trattano impropriamente i dati, violano le politiche di utilizzo e installano applicazioni non autorizzate;
2. agenti interni che rubano informazioni **per conto di terzi**;
3. **dipendenti insoddisfatti** che cercano di danneggiare la loro organizzazione;
4. **insider malintenzionati** che sfruttano i privilegi esistenti per rubare informazioni a scopo di guadagno personale;
5. **terzi irresponsabili** che compromettono la sicurezza attraverso l'intelligence, l'uso improprio o l'accesso a un asset o il suo utilizzo per finalità malevole.

MALWARE

Il malware è un tipo comune di attacco informatico sotto forma di software malevolo. Le famiglie di malware comprendono cryptominer, virus, ransomware, worm e spyware. **Gli obiettivi tipici sono il furto di informazioni o di identità, lo spionaggio e l'interruzione dei servizi**.

I **protocolli web** e di **posta elettronica** sono stati i vettori di attacco iniziali più comunemente utilizzati per diffondere il malware.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SOCIAL ENGINEERING

Il social engineering attacks sono delle vere e proprie strategie basate su interazioni interpersonali finalizzate a carpire informazioni riservate.

Comprendono un'ampia gamma di attività che tentano di sfruttare un errore umano o un comportamento umano con l'obiettivo di ottenere l'accesso a informazioni o servizi.

Utilizza varie forme di manipolazione per indurre le vittime a commettere errori o a consegnare informazioni sensibili o segrete. Nella sicurezza informatica, l'ingegneria sociale induce gli utenti ad aprire documenti, file o e-mail, visitare siti Web o concedere a persone non autorizzate l'accesso a sistemi o servizi.

Tali tipologie di minacce fanno sempre affidamento su un elemento umano per avere successo.

SOCIAL ENGINEERING

Principali vettori

Tra i principali vettori di tale minaccia:

- Phishing
- Spear-phishing
- Smishing
- Vishing
- Whaling
- Business e-mail compromise (BEC)

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SOCIAL ENGINEERING

Spear-phishing

Lo spear-phishing è una versione più sofisticata del phishing che prende di mira organizzazioni o individui specifici. Le email vengono predisposte su misura per ogni vittima. L'attaccante può fingersi interessato sostenitore di una causa condivisa dal bersaglio, spacciarsi per qualcuno conosciuto dalla vittima, o utilizzare altre tecniche di social engineering per ottenere la fiducia del malcapitato.

SOCIAL ENGINEERING

Smishing

Lo Smishing (o phishing tramite SMS) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito).

SOCIAL ENGINEERING

Smishing

COME FUNZIONA?

I messaggi di smishing invitano i destinatari a compiere azioni (cliccare link, ecc.) o fornire informazioni con urgenza, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni.

I tuffatori ("smisher") inviano ad esempio messaggi per chiedere ad esempio alle vittime di:

- cliccare un link che conduce ad un form online in cui inserire dati personali, dati bancari o della carta di credito, ecc;
- scaricare un allegato che può contenere programmi malevoli capaci di prendere il controllo dello smartphone o accedere ai dati in esso contenuti;
- rispondere ai messaggi ricevuti inviando dati personali (il codice fiscale, il PIN del Bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza della carta, i dati dell'OTP cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.);
- chiamare un numero di telefono, dove poi un finto operatore o un sistema automatizzato chiedono di fornire informazioni di vario tipo, compresi dati bancari e/o della carta di credito.

SOCIAL ENGINEERING

Smishing

Alcuni esempi di messaggi da valutare con particolare attenzione e cautela:

- una banca o un gestore di carte di credito o una società di recupero crediti che segnalano un account compromesso, generici problemi tecnici o anomalie sul conto bancario o sulla carta di credito, da verificare urgentemente, ecc.;
- offerte di sconti straordinari su beni e servizi, o anche proposte di ricariche telefoniche da effettuare subito a costi incredibilmente vantaggiosi;
- fornitori di beni o servizi che segnalano bollette o rate non pagate da saldare con urgenza; pacchi, lettere o raccomandate da ritirare o che si ha difficoltà a consegnare, ecc.;
- amministrazioni pubbliche che segnalano la necessità di fornire dati, sanzioni da pagare (multe, cartelle esattoriali), anomalie da verificare, ecc.;
- piattaforme che offrono servizi di social media o di messagistica che segnalano una violazione dell'account personale e chiedono di fornire dati e/o compiere determinate azioni (cliccare link, compilare form, chiamare numeri o inviare messaggi, ecc.).

SOCIAL ENGINEERING

Vishing

Il vishing (o phishing vocale) è una forma di truffa, sempre più diffusa, che utilizza il telefono come strumento per appropriarsi di dati personali - specie di natura bancaria o legati alle carte di credito - e sottrarre poi somme di denaro più o meno ingenti.

Di solito le vittime vengono contattate telefonicamente da finti operatori (di banche o di società che gestiscono bancomat o carte di credito) i quali, con la scusa di presunte "anomalie", chiedono alle persone, nel loro stesso interesse, di collaborare a mettere in campo necessarie (e false) "procedure di sicurezza".

I visher fanno leva sul timore legato ad un rischio incombente per convincere le vittime ad abbassare il livello di prudenza e a reagire d'impulso. Una particolare forma di ingegneria sociale che dimostra una elevata efficacia.

SOCIAL ENGINEERING

Whaling

Il Whaling è un particolare attacco di spear-phishing rivolto a dirigenti e vertici aziendali quali CEO, CFO, CIO e in generale tutti quei profili che all'interno di un'azienda sono in possesso sia di informazioni strettamente riservate che di elevati poteri decisionali e di spesa.

L'obiettivo è quello di manipolare la vittima inducendola con l'inganno a divulgare informazioni in suo possesso o a fargli compiere specifiche azioni dannose per l'azienda ma remunerative per l'attaccante, come ad esempio autorizzare un bonifico a beneficio di quest'ultimo

SOCIAL ENGINEERING

Business e-mail compromise (BEC)

Business E-mail Compromise (BEC) è una sofisticata truffa rivolta ad aziende e organizzazioni, in cui i criminali utilizzano tecniche di ingegneria sociale per ottenere l'accesso all'account di posta elettronica di un dipendente o dirigente per avviare bonifici bancari in condizioni fraudolente.

ULTERIORI MINACCE

RILEVANTI

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SPAM

Lo spam consiste nell'invio di messaggi non richiesti in massa. Costituisce una minaccia per la cybersicurezza quando viene utilizzato come vettore di attacco per distribuire o attivare altre minacce.

Lo spam può talvolta essere confuso o erroneamente classificato come campagna di phishing.

La differenza principale tra i due è il fatto che il **phishing** è un'azione mirata, che ha come **obiettivo il furto dei dati degli utenti**. Lo **spam** è invece una tattica per **inviare e-mail non richieste** in massa a un elenco di destinatari.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

VIOLAZIONE DEI DATI

Una violazione dei dati è un tipo di **incidente di cybersicurezza caratterizzato dall'accesso a informazioni senza la giusta autorizzazione**, in genere con intento doloso, che ha come conseguenza la potenziale perdita o il potenziale uso improprio di tali informazioni.

Secondo le ricerche dell'ENISA, **occorrono circa 206 giorni per identificare una violazione dei dati** in un'organizzazione. Pertanto, il tempo necessario per contenere, riparare e recuperare i dati significa tempi più lunghi per il ritorno alla normalità.

PRINCIPIO DI MINIMIZZAZIONE COME MISURA DI SICUREZZA

COME DIFENDERSI

La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

1. Le persone

Le persone svolgono un ruolo essenziale nell'ecosistema della sicurezza informatica. Il rapporto richiama l'attenzione sull'importanza della responsabilità e della consapevolezza dei dipendenti, della formazione e delle politiche di sicurezza informatica, nonché della gestione di terze parti in relazione a informazioni riservate e/o sensibili.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

2. Processi

Il monitoraggio dei processi aziendali interni include l'esecuzione di audit, pianificazione e risposta agli incidenti, password, patch software e protezione dei dati.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

3. Tecnico

A livello tecnico, dovrebbero essere considerati una serie di aspetti in relazione alla sicurezza della rete, antivirus, crittografia, monitoraggio della sicurezza, sicurezza fisica e protezione dei backup.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

RUOLO

DELL'AMMINISTRATORE DI SISTEMA

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

DISCIPLINA

La disciplina del ruolo dell'ADS è prevista nel Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e pubblicato in G.U. n. 300 del 24 dicembre 2008:

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

DEFINIZIONE

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

DESIGNAZIONE

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

OUTSOURCING

Responsabile del trattamento

Art. 28 GDPR

INTERNO

Incaricato al trattamento

Art. 29 GDPR

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

ELENCO DEGLI AMMINISTRATORI DI SISTEMA

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l´elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Nel caso di servizi di amministrazione di sistema affidati in **outsourcing** il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

VERIFICA DELLE ATTIVITÀ

L´operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Pertanto, risulta opportuno predisporre annualmente delle relazioni riepilogative circa le attività di amministrazione dei sistemi nonché le modifiche all'infrastruttura IT ed eventuali incidenti di sicurezza occorsi.

REGISTRAZIONE DEGLI ACCESSI

Le Organizzazioni devono adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di **completezza**, **inalterabilità** e possibilità di verifica della loro **integrità** adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell´evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

ATTIVITÀ DI PERTINENZA DELL'ADS

AGGIORNAMENTO DEI SISTEMI INFORMATICI

VALUTARE LE MISURE DI SICUREZZA IMPLEMENTATE

AGGIORNAMENTO DEI SISTEMI INFORMATICI

FONTE DI AGGIORNAMENTO: CSIRT

Nell'esecuzione delle attività aziendali, l'ADS deve garantire l'aggiornamento dei sistemi operativi, delle applicazioni, dei software, firmware, dei singoli componenti di ciascuna applicazione o strumento all'ultima versione anche con l'utilizzo di fonti di informazione istituzionali quale l'ACN - Agenzia per la Cybersicurezza Nazionale: https://www.csirt.gov.it/

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

MISURE DI SICUREZZA

Tra le funzioni tipiche dell'ADS rientra la valutazione delle misure di sicurezza ex art. 32 del GDPR.

Articolo 32
Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

MISURE DI SICUREZZA

In alcuni casi, le misure di sicurezza possono essere individuate e richieste già dalla normativa di settore:

- Sanità = Pseudonimizzazione e Cifratura
- Whistleblowing = Crittografia
- Enti pubblici = Misure AGID

Dove le misure non siano già disciplinate dal Legislatore, queste devono essere valutate e implementate dal Titolare del trattamento, con il supporto con dell'ADS:

- Misure di sicurezza ENISA.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Guida alla cibersicurezza per le piccole e medie imprese

12 AZIONI

PER RENDERE SICURA LA PROPRIA IMPRESA

La crisi COVID-19 ha messo in evidenza l'importanza di internet e dei computer in generale per le piccole e medie imprese (PMI). Per proseguire l'attività durante la pandemia, numerose PMI hanno dovuto adottare misure di continuità operativa, quali il ricorso a servizi cloud, il miglioramento dei propri servizi internet, il potenziamento dei siti web e il lavoro a distanza per i dipendenti.

Il presente opuscolo propone alle PMI 12 azioni pratiche di alto livello per proteggere meglio i rispettivi sistemi e attività. La pubblicazione accompagna la più dettagliata relazione dell'ENISA **«Cibersicurezza per le PMI: sfide e raccomandazioni»**.

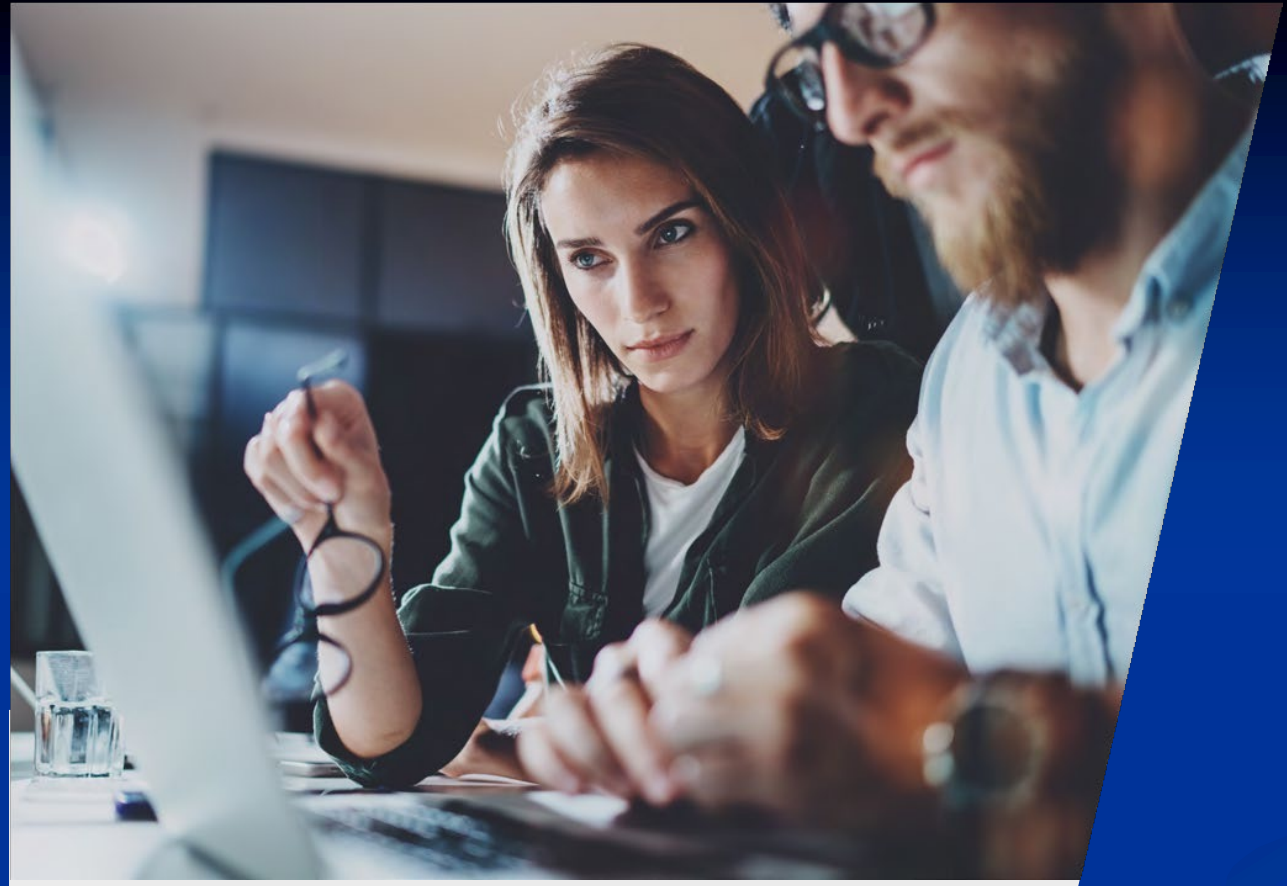
1 SVILUPPARE UNA SOLIDA CULTURA DELLA CIBERSICUREZZA

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 cibersicurezza 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.

COINVOLGERE IL PERSONALE

Coinvolgere i dipendenti mediante un'efficace comunicazione sulla cibersicurezza da parte della dirigenza, sostenendo apertamente le iniziative per la cibersicurezza, offrendo formazioni appropriate ai dipendenti e definendo regole chiare e specifiche al riguardo nelle politiche in materia di cibersicurezza.



PUBBLICARE POLITICHE IN MATERIA DI CIBERSICUREZZA

Dovrebbero essere definite regole chiare e specifiche nelle politiche in materia di cibersicurezza per i dipendenti sul comportamento da seguire quando usano l'ambiente, le attrezzature e i servizi informatici dell'impresa. Tali politiche dovrebbero altresì evidenziare le conseguenze cui potrebbe andare incontro un dipendente qualora non si conformasse alle politiche. Le politiche devono essere riviste e aggiornate regolarmente.

ESEGUIRE AUDIT PER LA CIBERSICUREZZA

Sarebbe opportuno svolgere periodicamente audit 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 alle PMI, non coinvolti nelle operazioni informatiche quotidiane.

TENERE A MENTE LA PROTEZIONE DEI DATI

A norma del regolamento generale dell'UE sulla protezione dei dati ([1]), 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.

([1]) Regolamento generale sulla protezione dei dati https://ec.europa.eu/info/law/law-topic/data-protection_it

2

FORNIRE UNA FORMAZIONE APPROPRIATA

Fornire a tutti i dipendenti formazioni periodiche di sensibilizzazione alla cibersicurezza in modo che possano riconoscere e affrontare le varie minacce alla cibersicurezza. I corsi di formazione dovrebbero essere personalizzati per le PMI e concentrarsi su situazioni di vita reale.

Fornire ai responsabili della gestione della cibersicurezza in seno all'impresa formazioni specifiche sulla cibersicurezza in modo che abbiano le capacità e le competenze necessarie per svolgere il loro lavoro.

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.

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.

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:

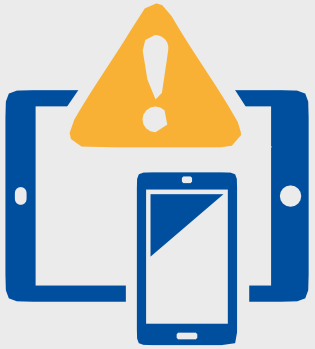
- deve essere lunga e avere caratteri minuscoli e maiuscoli, possibilmente anche numeri e caratteri speciali;
- evitare ovvietà, ad esempio «password», sequenze di lettere come «abc» o di numeri come «123»;
- evitare di usare informazioni personali reperibili online.

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.

6

RENDERE SICURI I DISPOSITIVI



Mantenere sicuri i dispositivi in uso al personale – che si tratti di PC, laptop, tablet o smartphone – è un punto cruciale in un programma di cibersicurezza.

MANTENERE IL SOFTWARE CORRETTO E 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.

ANTI–VIRUS

Si consiglia di attuare una soluzione anti-virus gestita a livello centrale su tutti i tipi di dispositivi e aggiornarla per assicurarne l'efficacia continua e di evitare di installare un software pirata perché potrebbe contenere malware.

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.

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.

7 RENDERE SICURA LA PROPRIA RETE

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.

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 impiegarti firewall per proteggere tutti i sistemi critici, in particolare dovrebbe essere utilizzato un firewall per proteggere la rete della PMI da internet.

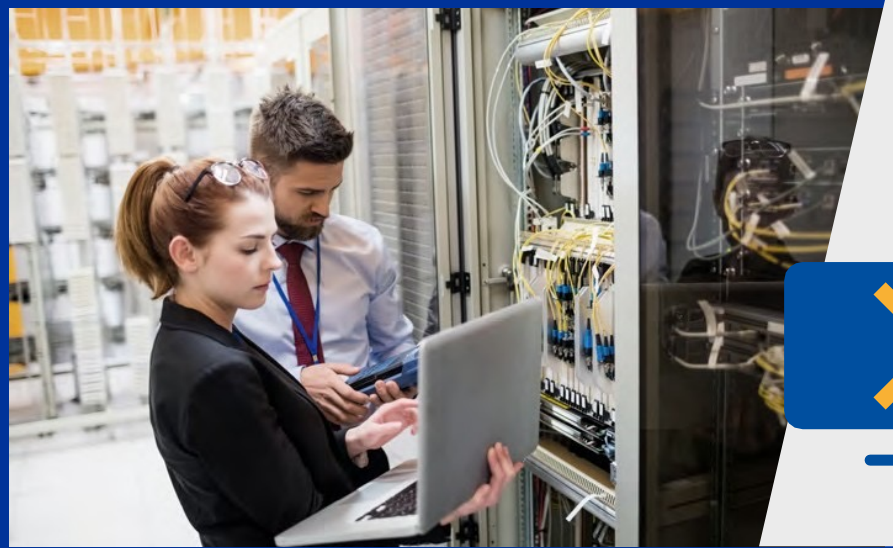
ANALIZZARE LE SOLUZIONI DI ACCESSO REMOTO

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.

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. Idocumenti sensibili stampati non dovrebbero essere lasciati incustoditi e quando non sono utilizzati andrebbero archiviati in modo sicuro.



9 RENDERE SICURI I BACKUP

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.

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» ([2]) 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.

([2]) https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

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.

12 CERCARE E CONDIVIDERE LE 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 cibersicurezza e di come sono state superate piuttosto che se ne vengono a conoscenza attraverso relazioni del settore o indagini sulla cibersicurezza.

Grazie per l'attenzione

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS