AGENZIA DELL'UNIONE EUROPEA
PER LA CIBERSICUREZZA

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.

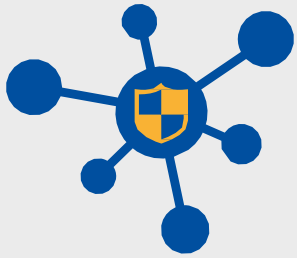
UTILIZZARE STRUMENTI DI PROTEZIONE PER I MESSAGGI DI POSTA ELETTRONICA E IL WEB

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. I documenti 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.

AGENZIA DELL'UNIONE EUROPEA
PER LA CIBERSICUREZZA

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in materia di sicurezza informatica, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche del futuro. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Per maggiori informazioni, visitare il sito www.enisa.europa.eu.

ENISA
Agenzia dell'Unione europea per la cibersicurezza

Sede di Atene
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Grecia

Sede di Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grecia

enisa.europa.eu