Proteggete i dati nel vostro ufficio

Briefing esecutivo

Guida alla sicurezza delle informazioni aziendali destinata ai dirigenti e ai professionisti della sicurezza informatica

Canon

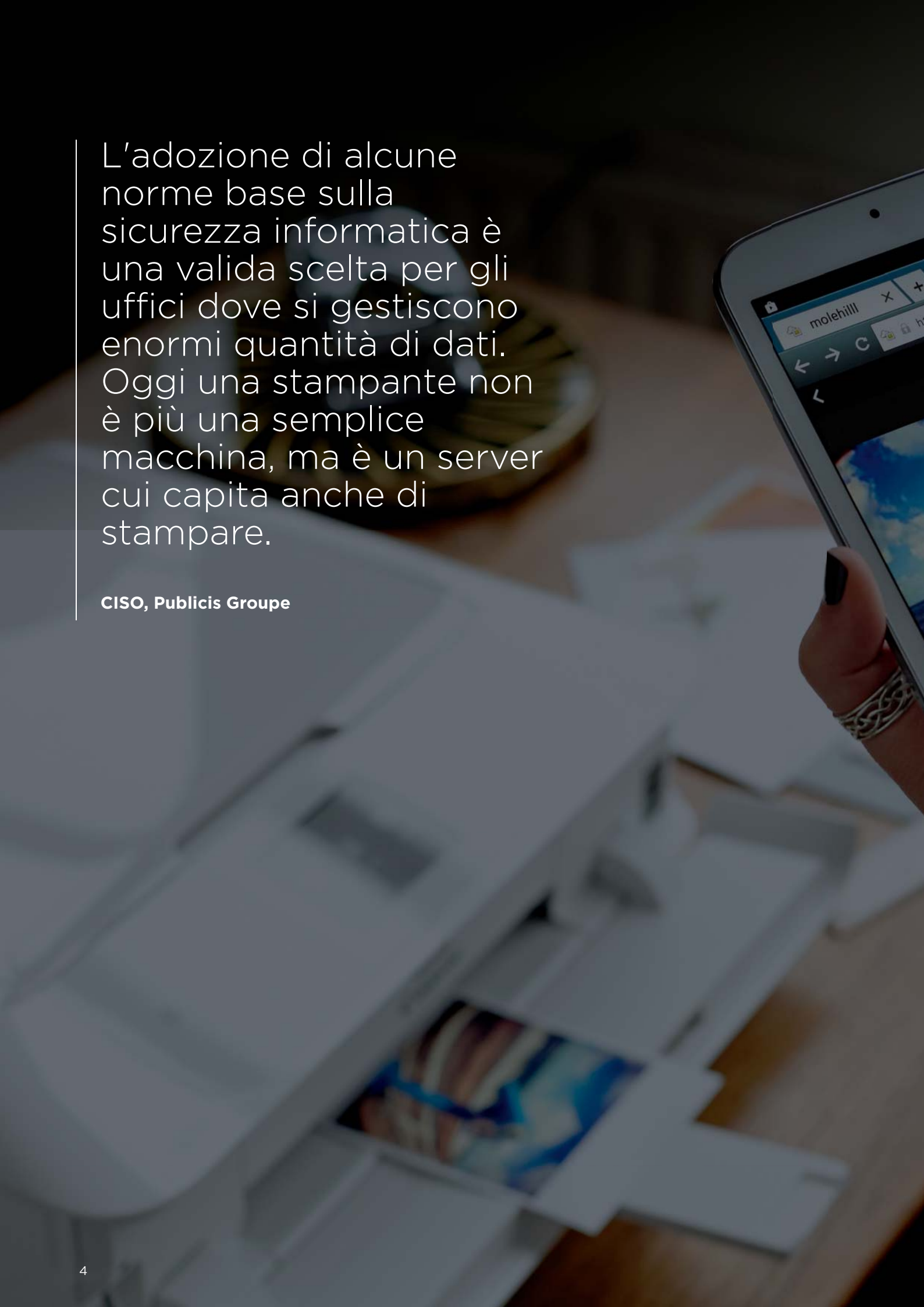
Estratto

La protezione delle informazioni aziendali è diventata una problematica che investe i vertici aziendali.

L'ufficio è un ambiente a noi familiare, in cui ci sentiamo protetti. Eppure proprio i sistemi e le soluzioni che utilizziamo con maggiore frequenza possono mettere a repentaglio la sicurezza dei nostri dati.

Il presente documento è destinato ai dirigenti di alto livello ed evidenzia le minacce per la sicurezza più diffuse nell'ambiente ufficio e che possono incidere sulla protezione delle informazioni sensibili gestite all'interno dell'azienda. In queste pagine non cerchiamo di fornire soluzioni tecniche ma semplicemente analizziamo le problematiche e indichiamo la via da seguire per affrontarle.

Indice



L'adozione di alcune norme base sulla sicurezza informatica è una valida scelta per gli uffici dove si gestiscono enormi quantità di dati. Oggi una stampante non è più una semplice macchina, ma è un server cui capita anche di stampare.

CISO, Publicis Groupe

Introduzione

In base a un'analisi condotta da IDC, le minacce alla sicurezza costano a un'azienda media 1,3 milioni di dollari all'anno, escludendo le violazioni più gravi. L'80% delle organizzazioni intervistate si aspetta di subire almeno un attacco che richiederà un importante intervento di ripristino.

Per mettere a repentaglio la sicurezza informatica basta un clic

Violazione dei dati: qualcuno ha avuto accesso ai dati di un vostro cliente. Non sapete di quali informazioni sia entrato in possesso.

Sappiamo che la sicurezza dei dati è importante per voi. Ecco perché è ragionevole pensare alle misure che potete adottare per proteggervi PRIMA che si verifichi una violazione. Dopo, sarà più difficile tentare di ricostruire la reputazione della vostra azienda.

Recenti indagini di settore suggeriscono che per un'azienda è pressoché inevitabile subire una violazione dei dati. L'implementazione di un valido piano di contenimento dei rischi garantisce pertanto indubbi vantaggi.

Ogni azienda è diversa. Ma tutte condividono la necessità di proteggere i propri dati. La protezione delle informazioni aziendali da attacchi interni o esterni richiede che i dirigenti conoscano l'impatto che le tecnologie, come i sistemi di stampa e di copiatura, possono esercitare a livello di sicurezza.

È forse compito di qualcun altro? La recente introduzione del Regolamento generale sulla protezione dei dati (GDPR) nell'Unione Europea impone a tutti i dipendenti l'obbligo di salvaguardare i dati aziendali. Per proteggere la propria azienda, è necessario conoscere esattamente quali sono le principali aree a rischio.

In Canon ci rendiamo conto che ogni azienda presenta un diverso livello di propensione al rischio: un ingente investimento in strumenti di protezione dei dati può essere adeguato per un'organizzazione ma considerato del tutto inopportuno per un'altra di pari dimensioni, che opera nello stesso settore. La vostra propensione al rischio determinerà l'importanza che attribuite alla sicurezza e agli strumenti ad essa collegati.

È la vostra storia. Noi ci limitiamo a fornirvi una consulenza proattiva sui nostri prodotti e servizi. In questo documento presentiamo tre argomenti importanti:

1. **Cosa dovete sapere sulle apparecchiature per ufficio e i rischi che comportano?**
2. **Quali misure potete adottare per ottimizzare la gestione dei rischi legati alla sicurezza dei dati?**
3. **Quale aiuto può offrire Canon?**

La sicurezza delle informazioni e l'ufficio

Cosa dovete sapere sulle apparecchiature per ufficio e i rischi che comportano?

Quando prendiamo in considerazione i dispositivi come le stampanti collegate in rete e le implicazioni che queste possono avere per la sicurezza, pensiamo immediatamente alla stampa non autorizzata di documenti, ma i rischi possono essere ben più gravi. Ecco alcune cose che la maggior parte delle persone non sa riguardo alla sicurezza delle apparecchiature per l'ufficio:

Qualsiasi dispositivo collegato alla rete è una via di accesso ai dati conservati sui computer

Viviamo in un mondo digitale iper-connesso dove, in teoria, qualsiasi dispositivo informatico può collegarsi a un altro dispositivo, a meno che non siano stati implementati adeguati controlli. Nel caso delle LAN, le organizzazioni investono ingenti somme di denaro ogni anno per limitare l'accesso ad altri computer collegati in rete. Qualsiasi dispositivo che si collega a una rete informatica rappresenta una potenziale minaccia per quella rete. Il controllo di questa minaccia richiede la corretta configurazione dei dispositivi e un solido approccio che consenta di identificare i soggetti che intervengono nell'ecosistema della sicurezza: utenti, dispositivi, endpoint e altro ancora. I dispositivi multifunzione possono produrre e distribuire contenuti non strutturati come documenti stampati, e-mail e fax in qualsiasi punto del mondo, immediatamente. Oppure possono acquisire dati cartacei per convertirli in formato digitale e consentirne la successiva trasmissione.

Tutto questo pone dei problemi già di per sé, ma il fatto ancora più preoccupante è che questi dispositivi rappresentano un punto di accesso alla vostra rete. Persone senza scrupoli potrebbero accedere ai vostri dati tramite internet, installare trojan sugli hard drive del dispositivo per spiare il vostro traffico di rete, oppure salvare gli indirizzi e-mail delle persone registrate sul dispositivo.

Domande da porsi:

- ☐ Per l'approvvigionamento dei dispositivi avete adottato degli standard precisi in modo da garantire una configurazione coerente?
- ☐ I vostri fornitori/produttori offrono delle linee guida per la sicurezza e adottano una configurazione uniforme delle impostazioni per ridurre al minimo i rischi?
- ☐ I dispositivi consentono l'accesso incontrollato a Internet o a dispositivi di terzi, come le chiavette USB?

In base al rapporto di una ricerca condotta da un Identity Theft Resource Centre (ITRC), pubblicato nel 2014, il 14% delle violazioni di dati riguarda documenti cartacei.

I moderni dispositivi multifunzione possiedono le stesse capacità di elaborazione di un server di rete.

Nel caso delle apparecchiature per ufficio, l'atteggiamento nei confronti della sicurezza è molto più superficiale rispetto ai livelli di protezione adottati per computer e dispositivi personali, il che è piuttosto strano se si considera che alcuni sistemi multifunzione hanno la stessa capacità di elaborazione e di archiviazione di un server di rete. In base a un'analisi di InfoTrends, ci sono circa 30 milioni di stampanti e multifunzione sparsi negli uffici e nelle case di tutto il mondo e se anche solo la metà di questi dispositivi fosse connessa a Internet o a un dispositivo esterno... Una recente ricerca condotta da Quocirca riferisce che il 63% delle aziende intervistate ammette di avere subito una o più violazioni dei dati legate alla stampa, Basta poco per violare la sicurezza della rete e causare problemi.

Domande da porsi:

- ☐ Le organizzazioni sanno dove vengono utilizzati i dispositivi e da chi?
- ☐ Con quale frequenza i rischi per la sicurezza sono associati con le apparecchiature per l'ufficio?
- ☐ Verificate che i dispositivi siano collegati alla rete corretta?

I dispositivi incorporano hard disk/ memorie che possono contenere dati riservati

In un ambiente ufficio sono presenti diversi dispositivi con la capacità di conservare i dati: smartphone, chiavette USB, stampanti e sistemi multifunzione. Ognuno di questi può potenzialmente contenere un malware o memorizzare enormi quantità di dati sensibili. Per non parlare dei dispositivi più grandi, che possono integrare degli hard drive e porre ulteriori problemi.

Domande da porsi:

- ☐ Quali dispositivi utilizzati in ufficio contengono memorie fisiche indirizzabili all'utente?
- ☐ Le procedure per la distruzione dei dispositivi di memorizzazione al termine della loro vita utile sono state formalizzate?

La sicurezza delle informazioni e l'ufficio

Quando i dispositivi arrivano nel vostro ufficio, potrebbero non essere configurati per ottimizzare la protezione contro le minacce alla sicurezza.

Sarebbe un errore presumere che i dispositivi siano perfettamente configurati per rispondere alle vostre esigenze di sicurezza dei dati nel momento in cui arrivano nel vostro ufficio e vengono collegati dal tecnico. Perché? Perché ogni organizzazione ha un proprio livello di accettazione del rischio. Per esempio, un'agenzia di comunicazione potrebbe considerare la funzione di stampa diretta da USB perfetta per promuovere la propria produttività mentre uno studio legale considererebbe questa stessa funzionalità come uno dei peggiori pericoli per la sicurezza delle informazioni. In Canon, configuriamo i nostri dispositivi attivando le funzionalità più richieste e *disattivando* quelle che potrebbero creare dei problemi. Inevitabilmente, abbiamo clienti che attivano le funzioni da noi disattivate e viceversa. È disponibile una guida pensata per i manager responsabili della sicurezza dei dispositivi collegati in rete. Questo documento spiega come i dispositivi siano configurati di serie in modo ottimale ed evidenzia alcuni punti cui fare attenzione qualora si desideri modificare tale configurazione, per aiutare ad allineare l'attivazione delle funzioni alle politiche di sicurezza adottate dall'organizzazione.

Domande da porsi:

- ☐ Avete implementato delle politiche riguardo alle configurazioni di sicurezza dei dispositivi di stampa?
- ☐ Tutta l'azienda concorda sul livello di consolidamento della sicurezza ritenuto appropriato per i dispositivi di rete?
- ☐ Il vostro fornitore offre una guida o dei consigli su come configurare i dispositivi in funzione delle vostre esigenze?
- ☐ I dispositivi per ufficio, così come altri dispositivi endpoint, vengono sottoposti a un audit annuale per valutare il rischio che essi rappresentano per la sicurezza?

Le minacce per la sicurezza delle informazioni assumono forme diverse: non si tratta solo di tecnologia

Come avviene per molte questioni legate al mondo aziendale, si potrebbe pensare che una tecnologia idonea potrebbe spazzare via qualsiasi problematica o ostacolo alla sicurezza dei dati e che, con un'adeguata strategia IT, le organizzazioni potrebbero riprendere la loro normale attività. Ma la realtà è ben diversa. Le attitudini e i comportamenti delle persone svolgono un ruolo importante per la sicurezza delle informazioni. Sono le persone, non i computer, che escono dall'azienda con in tasca una chiavetta piena di dati sensibili che poi smarriscono da qualche parte, che trafugano i dati dai vostri sistemi finanziari o che decidono di vendere il vostro database clienti a un'altra società di marketing. La tecnologia rimane un ottimo supporto nell'ecosistema della sicurezza delle informazioni ma nulla più. Dopotutto, se la tecnologia fosse stata in grado di risolvere le molteplici sfide che le aziende devono affrontare in merito alla sicurezza, perché questo problema dovrebbe oggi coinvolgere i vertici aziendali?

Nel suo Briefing esecutivo *Fondamenti della sicurezza per l'azienda digitale* Canon evidenzia cinque questioni importanti che influiscono sui rischi che le organizzazioni devono affrontare in merito alla sicurezza delle informazioni. Consigliamo di leggere anche questo documento per approfondire l'argomento.

Domande da porsi:

- ☐ Le vostre politiche operative e HR minimizzano l'impatto delle persone e dei processi sui livelli di minaccia alla sicurezza?

Trovare il giusto equilibrio

Le persone che leggono questo documento saranno giunte a un determinato stadio lungo il percorso di formalizzazione dei loro standard di sicurezza delle informazioni. Ognuno di loro starà affrontando le proprie sfide, utilizzerà la propria combinazione di tecnologie e stabilirà il proprio livello di propensione al rischio.

Quali misure potete adottare per ottimizzare la gestione dei rischi legati alla sicurezza dei dati?

Non esiste alcuna formula universale che le aziende possano adottare per proteggersi dalla perdita dei dati. Detto questo, nel momento in cui le organizzazioni avviano un programma per formalizzare il loro approccio alla sicurezza delle informazioni, seguiranno un percorso collaudato. Ed è proprio sui segnali che costellano questo percorso che noi appuntiamo la nostra attenzione, concentrandoci soprattutto sulla sicurezza dell'ambiente ufficio, dove abbiamo maturato una valida esperienza. Raccomandiamo vivamente di rivolgersi a consulenti professionali che sappiano integrare e consolidare i suggerimenti forniti in queste pagine.

1. Iniziare dalle cose più semplici

È un'ottima idea fare un giro per l'ufficio e controllare scrivanie, vassoi di consegna delle stampanti e cestini per scoprire quali tipi di contenuti vengono lasciati incustoditi, quanti dispositivi vengono lasciati accessi ed esposti a possibili violazioni, quanti documenti o e-mail vengono lasciati aperti sugli schermi, quanti badge e chiavette USB vengono lasciati in bella vista sulle scrivanie, quanti cassetti di archivi contenenti documenti sensibili vengono lasciati socchiusi e quante porte di sicurezza non si chiudono correttamente... l'elenco è pressoché infinito. Un semplice giro per il piano vi consentirà di scoprire i potenziali rischi alla sicurezza delle informazioni.

2. Definire e raccogliere il consenso sulla propensione al rischio.

Coloro che gestiscono il portfolio della sicurezza delle informazioni dovrebbero operare in modo da far convergere i gruppi dirigenti su un'opinione condivisa in merito alla propensione al rischio dell'azienda. Potrebbe essere utile affidarsi a un auditor indipendente per coordinare questo processo. Il vostro fornitore dovrebbe essere in grado di fornire delle analisi sui fattori industriali e di produrre delle prospettive esterne sugli approcci migliori. Canon è pronta a impegnarsi per aiutare i responsabili di progetto a comprendere gli aspetti della sicurezza che dovrebbero essere inclusi nel processo di formulazione della policy sulla sicurezza nell'ambiente ufficio.

3. Formalizzare le dichiarazioni emerse riguardo alla policy sulla sicurezza delle informazioni

Prendere degli appunti serve a consolidare e chiarire i concetti e le idee discusse tra colleghi. Ma il tempo e le energie richiesti per trasformare gli "ideali" di sicurezza in politiche formali può rappresentare un pesante fardello per i team dirigenziali già gravati dalle pressanti richieste operative della loro organizzazione. Per questo motivo, Canon ha sviluppato un approccio basato su workshop in cui aiutiamo i dirigenti a formalizzare rapidamente i risultati che desiderano ottenere per la sicurezza dei loro uffici.
A questo scopo, ci concentriamo sull'ufficio e poniamo delle domande al gruppo di dirigenti interessati. Chiediamo ai partecipanti di ponderare le risposte in modo da raggiungere un equilibrio adeguato tra limitazione del rischio e livelli di invasività delle misure di sicurezza.

Trovare il giusto equilibrio

4. Sviluppare un piano di azione con dati di riferimento e iniziative mirate di rapido impatto

In qualsiasi processo di cambiamento, adeguati dati di riferimento (per misurare il successo) e iniziative di rapido impatto (per evidenziare i progressi compiuti e la validità del percorso intrapreso) sono essenziali per una buona riuscita. Il processo di cambiamento richiesto per l'implementazione di adeguate misure di sicurezza delle informazioni non è diverso. Quando valutate da dove partire, o come procedere, considerate in quale misura il rischio sia già limitato da altre soluzioni di sicurezza, *chi* trarrà vantaggio dal cambiamento e perché, *quali* inconvenienti potrebbero verificarsi in seguito al cambiamento e *quanto* invasiva sarà la misura di sicurezza per gli utenti?

5. Articolate e comunicate il vostro piano

È improbabile che i soggetti interessati abbiano il desiderio o l'esperienza necessaria per commentare piani studiati nei minimi dettagli, ma fornire una sintesi esaustiva dei risultati, delle priorità e dei piani di azione è importante per ottenere il consenso e l'impegno dei colleghi che potrebbero inizialmente pensare che la sicurezza delle informazioni è un "problema IT", quando in realtà non lo è affatto.

6. Adottare un approccio alla governance della sicurezza basato sul ciclo di vita

La governance della sicurezza non nasce da un giorno all'altro. Deve essere creata, implementata, gestita e riesaminata, creando un ciclo di vita caratterizzato da un miglioramento continuo e infinito. Esistono numerosi documenti utili in materia di sicurezza delle informazioni che possono aiutare le aziende a muovere i primi passi verso la formalizzazione del loro approccio basato sul ciclo di vita. Invitiamo il lettore a rivolgersi ad organizzazioni professionali per ottenere queste informazioni.

7. Considerare l'adozione di standard riconosciuti

Standard per la Sicurezza delle informazioni come ISO 27001 possono essere obbligatori per le aziende su cui gravano obblighi contrattuali nei confronti di clienti o fornitori. Per le organizzazioni che invece ritengono inopportuno o inutile investire ingenti risorse nel processo di certificazione, potrebbe comunque essere utile seguire la best practice indicata da questo standard. Alla base della rigorosa disciplina della norma ISO 27001 vi sono delle valide politiche che vi aiuteranno a proteggere la vostra organizzazione da diverse forme di violazione dei dati. Prendete anche in considerazione gli standard del governo britannico, come Cyber Essentials e Cyber Essentials plus (ogni governo UE avrà standard simili a questo) (https://en.wikipedia.org/wiki/Cyber_Essentials)

Quale aiuto può offrire Canon?

Cosa facciamo

Canon è un partner proattivo per le aziende che sono alla ricerca di una soluzione per la protezione dei dati che si integri con una valida politica di sicurezza delle informazioni. I nostri clienti potranno gestire il loro business in tutta tranquillità sapendo che Canon sarà sempre al loro fianco, pronta a evidenziare e ad affrontare in modo proattivo qualsiasi minaccia alla sicurezza dei dati. Sebbene nessun fornitore di tecnologia possa far fronte a tutte le potenziali minacce alla sicurezza con cui la vostra azienda potrebbe doversi confrontare in futuro, in Canon desideriamo contribuire sempre in modo positivo all'infrastruttura tecnologica e alle politiche dei nostri clienti, adottando un'etica di *sicurezza sin dalla progettazione*. Questo significa che integriamo nei nostri prodotti e servizi funzioni intelligenti pensate per ridurre al minimo i rischi che i nostri clienti potrebbero dover affrontare. Offriamo consulenza sull'impatto che la nostra tecnologia e i nostri servizi possono esercitare sulla sicurezza e mettiamo a disposizione *un team specializzato* che si occupa sia della nostra sicurezza IT interna sia di fornire informazioni e consulenza professionale ai clienti.

I nostri prodotti e servizi

Canon è probabilmente nota in tutto il mondo per le sue fotocamere e le sue tecnologie di stampa ma il nostro portfolio è molto più ampio. Disponiamo di un'apprezzabile organizzazione per la gestione delle informazioni che fornisce persone, processi e tecnologie studiate per aiutare le aziende a lavorare in modo più intelligente e a crescere più velocemente. Occupiamo anche un posto di rilievo nel settore dell'outsourcing business to business e la nostre tecnologie interessano i settori più disparati: soluzioni di imaging medicale che salvano vite, videocamere di sorveglianza che proteggono proprietà e persone, giorno e notte, e tecnologie di stampa 3D che stanno rivoluzionando le modalità operative della catena di produzione. Vi invitiamo a visitare il nostro sito web per scoprire la varietà di prodotti e di servizi che possiamo offrirvi.

Workshop sulla sicurezza dei dati: come funzionano

Ci vogliono meno di due ore per aggiornarvi sui rischi che circondano l'uso delle informazioni in ufficio e per spiegarvi il veloce esercizio che abbiamo ideato per aiutare coloro che si occupano di policy a formalizzare la propensione al rischio della loro azienda, trattando i principali aspetti della governance della sicurezza delle informazioni che coinvolge persone, processi e tecnologie dell'odierno posto di lavoro.
Per ulteriori informazioni e per un primo colloquio informativo, vi invitiamo a contattare il vostro rappresentante o partner Canon.

Canon Electronics Inc.
canon.com

Canon Europe
canon-europe.com

Canon UK Ltd.
Woodhatch
Reigate
Surrey
RH2 8BF
United Kingdom

Canon Ireland
3006 Lake Drive
Citywest
Saggart
Co Dublin
Ireland

Edizione italiana