SHARP

Whitepaper

Perchè il tema della sicurezza ha bisogno di un approccio “human-centred”

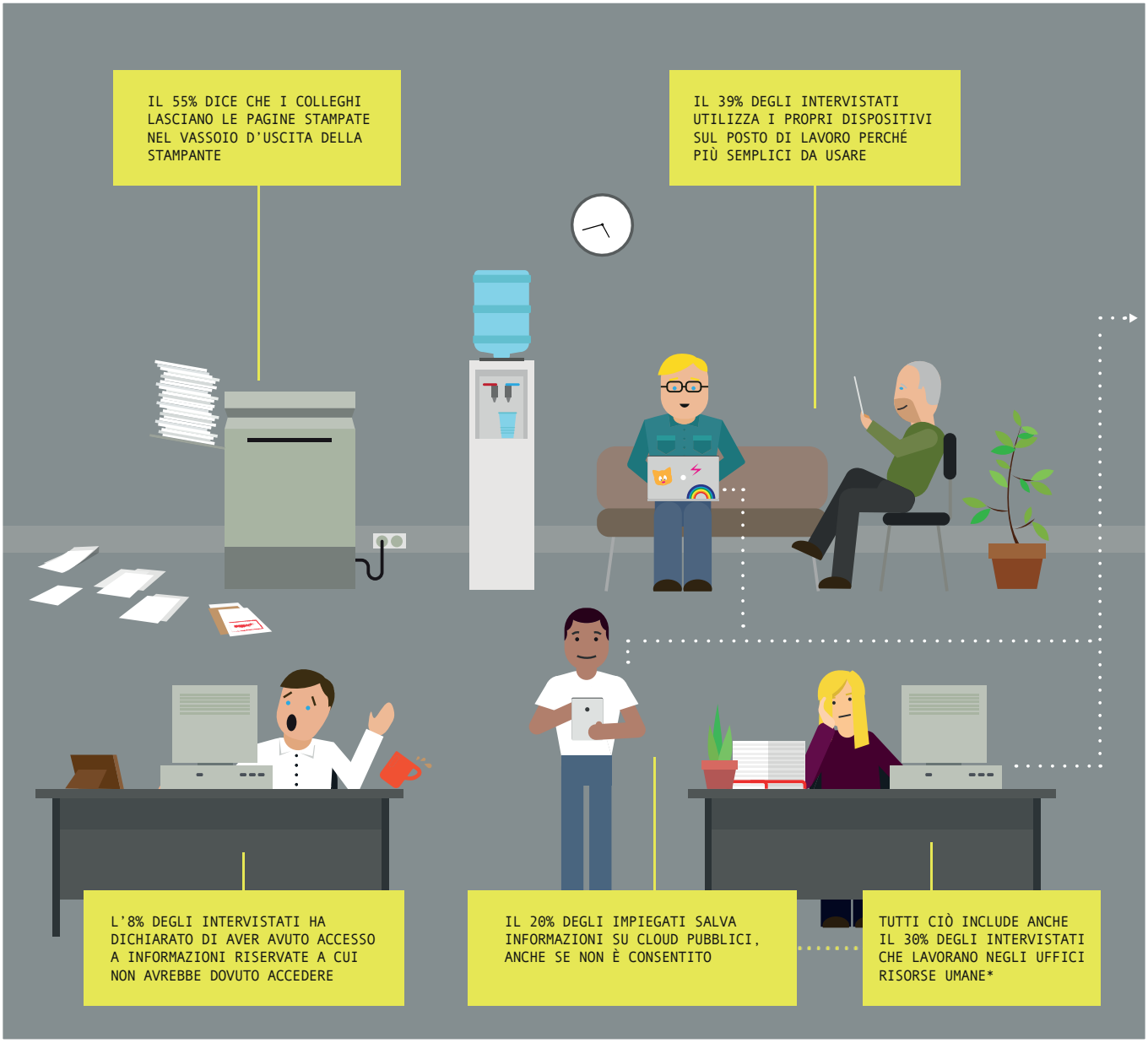
PIU’ DEL 21% DEGLI IMPIEGATI EUROPEI CONDIVIDE DATI SENSIBILI ATTRAVERSO PIATTAFORME PUBBLICHE E NON AFFIDABILI*

Nel nostro recente sondaggio su oltre 6.000 impiegati europei, abbiamo rilevato che il tema della sicurezza dei dati non è affrontato seriamente. Le imprese rischiano violazioni di sicurezza, del tutto evitabili, ma che invece causano sanzioni, perdita di proprietà intellettuale e stress per i dipendenti.

*Ricerca commissionata da Sharp e condotta da Censuswide nel mese di aprile 2016.

Un appoccio “human-centred” alla sicurezza

La ricerca condotta da Sharp in Europa ha rilevato che molti impiegati non prestano attenzione alle politiche di sicurezza aziendale. Se le imprese non affrontano questo problema rischiano violazioni di sicurezza che possono causare sanzioni, perdita di proprietà intellettuale e stress per i dipendenti.



Ricerca condotta su 6.045 impiegati di nove paesi europei (Francia, Germania, Regno Unito, Italia, Svezia, Polonia, Olanda, Repubblica Ceca e Ungheria).

*457 intervistati hanno dichiarato di lavorare in uffici di Risorse Umane.

Un appoccio “human-centred” alla sicurezza

- L’8% degli intervistati ha dichiarato di aver avuto accesso a informazioni riservate a cui non avrebbe dovuto accedere.
- Il 21% degli utenti ha affermato di aver utilizzato siti pubblici per la condivisione di file, senza l’approvazione aziendale.

- Quasi un terzo degli intervistati (29%) ha ammesso di ignorare il protocollo dell’ufficio e di portare i documenti a casa per completare il lavoro.
- Il mancato rispetto della politica aziendale è un comportamento comune: un quinto dei lavoratori intervistati (20%) ha ammesso di salvare informazioni di lavoro su cloud pubblici anche se non è consentito.
- Tra questi, il 26% lavora negli uffici Risorse Umane, mettendo potenzialmente a rischio la privacy dei dati personali*.

*457 intervistati hanno dichiarato di lavorare in uffici di Risorse Umane.

Abbiamo chiesto ad un’esperta di privacy e sicurezza, la Dott.ssa Karen Renaud come mai gli impiegati non sono attenti al tema della sicurezza dei dati. In queste pagine, Karen spiega come le aziende possono cambiare questo atteggiamento e come possono proteggersi adeguatamente da minacce esterne e interne.

Analisi e consigli della Dott.ssa Renaud

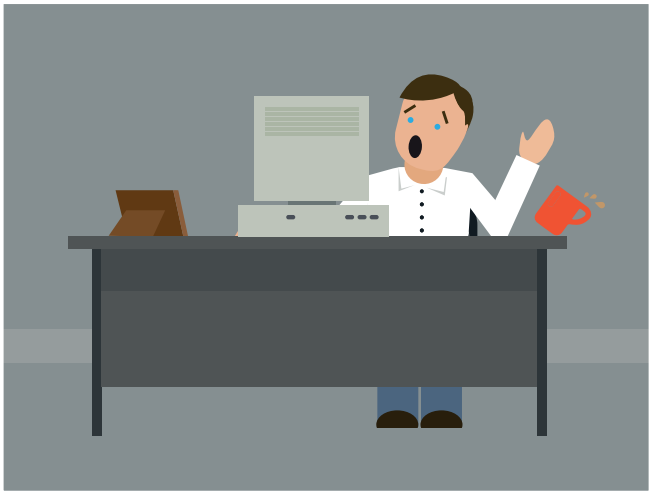
Non sono affatto sorpresa dai risultati della ricerca Sharp, che risultano essere in linea con le ricerche condotte dal Pew Research Center negli Stati Uniti, riguardanti il rapporto tra comportamenti sicuri e dati personali.

Sebbene i dipendenti abbiano la responsabilità di rispettare le norme di sicurezza, non credo che i datori di lavoro facciano correttamente la loro parte.

Molte piccole imprese trattano questo tema semplicemente facendo firmare ai dipendenti il documento contenente la politica di sicurezza. Ma non è realistico pensare di poter dare alle persone semplicemente una lista di istruzioni da seguire.

Si deve avere invece, un approccio “human-centred”, che vuol dire riconoscere che siamo umani, che possiamo sbagliare in alcune aree e che una gran quantità di istruzioni non contribuirà da sola a garantire comportamenti sicuri.

È necessaria una soluzione che sappia coniugare tecnologia ed esperienza.



L’8% DEGLI INTERVISTATI HA DICHIARATO DI AVER AVUTO ACCESSO A INFORMAZIONI RISERVATE A CUI NON AVREBBE DOVUTO ACCEDERE

Perchè non prendiamo sul serio il tema

Molte società pensano di poter risolvere il problema della sicurezza semplicemente mettendo per iscritto le politiche adottate. Tuttavia, occorre essere un pò più realistici, poiché il controllo del comportamento umano è una delle cose più difficili da gestire.

È veramente molto complicato controllare gli esseri umani e assicurarsi che facciano le cose in un certo modo, specialmente quando si tratta di attività abituali.

Come umani, siamo capaci di imparare nuove abilità e ogni volta che ripetiamo un comportamento appreso, tendiamo a meccanizzarlo. Tutte le azioni che compiamo regolarmente per la nostra mente diventano automatiche. Per questo motivo la richiesta di controllare attentamente le email per evitare il phishing non è realistica, semplicemente perché la mente umana funziona diversamente. Se di solito non ci sono problemi, supponiamo che le cose vadano sempre bene, facendoci sfuggire quell’unica email di phishing.

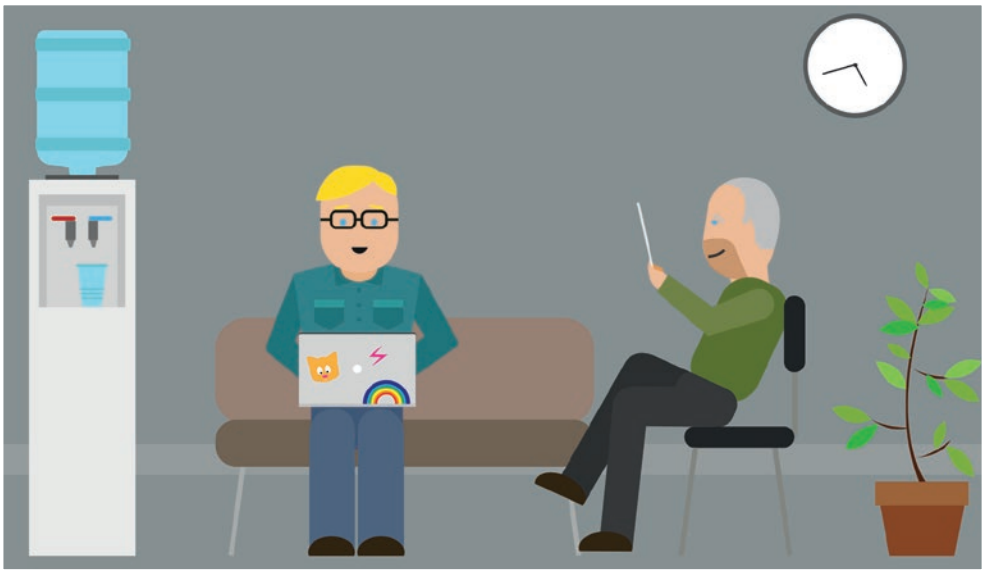
Un altro problema è che mentre insegniamo ai dipendenti ad agire e a rispondere in determinati modi, le organizzazioni spesso li bombardano con messaggi confusi.

Prendiamo ad esempio le email. Se un’azienda invia molte email contenenti link da cui recuperare informazioni, non può poi chiedere ai suoi dipendenti di essere prudenti, perché questi sono abituati ad accedere alle informazioni tramite proprio i link forniti via email.

Spesso le persone non pensano che una violazione di sicurezza possa accadere, perché la tecnologia si è evoluta più velocemente del cervello umano. Siamo pronti a reagire a cose che ci danneggiano immediatamente, pertanto, è difficile vedere le conseguenze di una scarsa sicurezza, quando queste non sono immediate.

Ad esempio, quando scegliamo una password semplice non accade nulla nell’immediato, cosi che continuiamo a creare password facili. Ci lasciamo ingannare dal fatto che in quel preciso momento non ci sono conseguenze dirette e non pensiamo che una violazione potrà avvenire in futuro, sorprendendoci negativamente.

IL 39% DEGLI INTERVISTATI UTILIZZA I PROPRI DISPOSITIVI SUL POSTO DI LAVORO PERCHÉ PIÙ SEMPLICI DA USARE



Costruire una cultura della sicurezza

Le persone imparano guardando come si comportano gli altri all’interno di un’organizzazione, per questo bisogna concentrarsi a costruire una cultura della sicurezza all’interno delle aziende.

Si può iniziare semplicemente con la formazione giusta, assicurandosi non solo che sia attinente, ma anche interessante e variegata. Non si può chiedere alle persone di seguire solo una riunione webinar per fare la differenza.

Le organizzazioni non devono concepire la formazione come una sorta di “vaccino” e pensare che tutto sia in ordine dopo aver “vaccinato” i dipendenti. Infatti, sappiamo tutti che una volta formati i collaboratori, inizialmente si comporteranno in modo sicuro, ma nel tempo quegli effetti cominceranno ad esaurirsi e i comportamenti sicuri risulteranno noiosi e pesanti.

È essenziale far capire ai dipendenti quanto sia importante il tema della sicurezza e che possono garantirla, svolgendo allo stesso tempo, bene il loro lavoro.

Per le organizzazioni il confine tra l’essere eccessivamente sicure ed essere insicure è delineato da una sottile linea di demarcazione. Garantire la sicurezza, rendendola un ostacolo da evitare, non vuol dire impedire alle persone di svolgere in modo efficace i loro compiti. Con una cultura aperta le aziende possono conoscere cosa sta accadendo e garantire la giusta sicurezza, mantenendo il corretto l’equilibrio tra lavoro e protezione dei dati.

IL 21% DEGLI UTENTI HA AFFERMATO DI AVER UTILIZZATO SITI PUBBLICI PER LA CONDIVISIONE DI FILE, SENZA L’APPROVAZIONE AZIENDALE

Progettare la sicurezza nei sistemi

Quando si parla di creare una politica di sicurezza aziendale, le organizzazioni devono progettare un sistema che impedisca il sorgere dell’insicurezza. In questo modo è solo l’utente ad avere l’onere di attenersi alla politica di sicurezza.

Le stampanti sono un ottimo esempio, infatti possono essere facilmente configurate per assicurare che i dati restino privati. Di solito in un piccolo ufficio, dopo averli inviati alla stampante le persone non raccolgono subito i documenti. Cosi informazioni che potrebbero essere riservate, rischiano di diventare pubbliche.

Tuttavia, molte stampanti prevendono l’aggiunta di un ulteriore livello di sicurezza, come un codice o un lettore di scheda d’identificazione, da utilizzare prima che il processo di stampa venga elaborato. In questo modo, solo una volta che l’utente è davanti alla stampante può recuperare il proprio lavoro. Così si garantisce un comportamento sicuro, senza richiedere uno sforzo supplementare all’utente finale, che avrebbe comunque raggiunto la stampante per ritirare le copie stampate.

Esistono molti sistemi di sicurezza come questo, da utilizzare nell’ambiente di lavoro. Tuttavia è necessario avere le giuste competenze, per questo sarebbe meglio per le piccole imprese affidarsi a fornitori esperti in outsourcing. Non ci si può aspettare che delle persone seppur specializzate, ma in altre aree, debbano essere esperti di sicurezza informatica.

IL 55% DICE CHE I COLLEGHI LASCIANO LE PAGINE STAMPATE NEL VASSOIO D’USCITA DELLA STAMPANTE

Sistema pubblico contro sistema privato

La condivisione di documenti in sistemi pubblici sta diventando sempre più comune nelle imprese, mettendo potenzialmente a rischio le informazioni aziendali.

Come società, anziché cercare di vietarne l’uso, dovresti analizzare il motivo per cui le persone usano questo servizio e quale tipo di informazione archiviano. La maggior parte delle persone utilizzano gli strumenti per la condivisione di documenti poiché rappresentano il modo di più semplice per condividere i dati con i colleghi fuori ufficio.

Se ritieni che questi motivi siano validi, devi essere in grado di fornire un’alternativa più sicura. Se non lo fai, i tuoi collaboratori continueranno a usare di nascosto siti pubblici per la condivisione dei file, pur sapendo che è vietato. Sharp ha scoperto che il 20% delle persone archivia informazioni di lavoro nel cloud pubblico, anche senza autorizzazione; non mi sorprenderebbe se questo dato fosse anche più alto.

Alcune regole potrebbero aiutare a rendere le cose più semplici e chiare, come ad esempio stabilire che i dati sensibili sono archiviati tutti in un unico file e che non possono essere rimossi o trasferiti, mentre i dati non sensibili possono essere archiviati ovunque e possono essere facilmente condivisi.

Conclusioni

Le persone non sono computer e non possono essere programmate. È essenziale che l’approccio alla sicurezza sia “human-centred”: pensato per gli umani e non per i robot.

Le organizzazioni dovrebbero usare sempre la tecnologia, affinché l’opzione più sicura diventi quella automatica. Tuttavia, le imprese devono garantire il giusto livello di controllo senza impedire alle persone di svolgere il proprio lavoro in modo efficiente. Se ciò accade a causa delle politiche di sicurezza adottate, è necessario valutare nuovamente le tecnologie in uso.

Solo con una corretta combinazione di tecnologia, formazione continua e un approccio alla sicurezza “human-centred” può rendere un’impresa sicura.

Occorre ricordare però che non esiste un antidoto perfetto, si tratta solo di fare esperienza.

IL 20% DEGLI IMPIEGATI SALVA INFORMAZIONI SU CLOUD PUBBLICI ANCHE SE NON È CONSENTITO

Sharp offre una vasta gamma di soluzioni di sicurezza per le aziende. Dalle funzioni di sicurezza di serie nell'hardware delle multifunzione (MFP) Sharp, per stampare in modo sicuro, a un servizio basato su Cloud per l'archiviazione e la condivisione dei file, nonchè un servizio IT per la protezione dei PC e assistenza sui back-up. Qualunque siano le dimensioni della tua azienda, Sharp può aiutarti a proteggere le tue informazioni, senza dover caricare i tuoi collaboratori con ulteriori compiti.

La sicurezza è di serie nelle MFP Sharp

Le MFP e stampanti di nuova generazione, utilizzate oggi dalle grandi aziende, hanno molte delle stesse funzionalità di archiviazione dati e informazioni che hanno i PC, pertanto occorre porre molta attenzione per rendere sicure le tue MFP alla stessa stregua dei computer. Le Multifunzione Sharp hanno molte caratteristiche di serie per proteggerti dalle minacce:

- **Autenticazione**
  Autenticazione dell'utente e mantenimento in memoria delle stampe vuol dire che i documenti stampati non restano nel vassoio d'uscita della MFP, con il rischio di essere visti da chiunque in ufficio.

- **Accesso**
  Gli hacker possono cercare di accedere a informazioni sensibili e agli indirizzi elencati nell'hard disk della MFP. Le MFP Sharp per evitare questo rischio sono organizzate con password amministrative, filtri di indirizzi IP e MAC, controllo porta e diversi sistemi di autenticazione utente. Il Data Security Kit di Sharp è un kit di protezione dati, con tecnologie di crittografia, che rende praticamente impossibile intercettare o recuperare eventuali dati residuali da una MFP Sharp.

- **Scansioni sicure**
  Alcune delle MFP Sharp prevedono l'utilizzo della funzione scan-to-home che assicura la corretta archiviazione delle immagini acquisite. Ciò garantisce che le informazioni sensibili non siano scansionate accidentalmente e salvate nella cartella di rete sbagliata. La protezione per i documenti sensibili può essere assicurata anche tramite Sharp-encrypted Adobe® PDF per la scansione e la stampa.

- **Accesso da dispositivi mobili**
  Molte persone oggi stampano da tablet e smatphone. Sharp fornisce una soluzione sicura per collegarsi alla rete aziendale tramite la MFP utilizzando l'autenticazione utente, un protocollo sicuro basato su internet che tiene in stand-by il documento da stampare finchè l'utente non si trovi vicino alla stampante.

- **Attività di controllo**
  Per essere protetto dai rischi devi essere in grado di rilevare qualsiasi attività sospetta. Grazie all'attività di controllo minuziosa e ai registri lavori, Sharp è in grado di fornire un ampio controllo su tutte le attività di utenti e dispositivi.

- **Smaltimento sicuro**
  La maggior parte delle MFP Sharp offre il sistema standard di fine noleggio che assicura la cancellazione o sovrascrittura di tutti i dati riservati in essa contenuti.

Servizi Sharp Optimised IT

I servizi Sharp Optimised IT sono tutto ciò di cui hai bisogno per costruire e mantenere un'infrastruttura IT affidabile e duratura, pronta per il futuro.

Quando affidi a Sharp la gestione dei tuoi servizi IT, svolgiamo subito una valutazione della rete per capire quanto il tuo sistema informatico sia esposto ai cyber-attack. In seguito lavoriamo con te per verificare le effettive vulnerabilità e assicurarci che siano presenti gli elementi fondamentali per rendere la tua rete sicura.

Un importante passo per rendere sicura la tua rete è occuparsi dei semplici processi IT, sottovalutati dalle Pmi, ad esempio:

- **Accesso**
  Assicuratevi che gli account utenti di chi ha lasciato l'organizzazione vengano cancellati in modo che l'accesso non sia lasciato aperto a chiunque abbia quelle credenziali. Controllate che le password siano cambiate regolarmente e che non siano semplici da indovinare.

- **Aggiornamenti**
  Tenete aggiornato il patching è essenziale per bloccare i gap nella sicurezza dei sistemi informatici.

- **Protezione da virus**
  Assicurarsi che l'antivirus sia aggiornato. I servizi acquistati e non aggiornati sono la prima causa di violazione dei dati e ransomware.

- **Backup**
  I backup sono l'ultima possibilità in caso di malware o ransomware. Spesso i backup non vengono fatti, o se lo sono raramente vengono provati, così non si ha nessuna rete di sicurezza se accade il peggio.

Optimised Software Solutions: Output Management

Sharp offre soluzioni di gestione della stampa per tutti i tipi di organizzazione, a prescindere dalle dimensioni, consentendo di allocare i costi di stampa. Oltre al codice di serie per la fatturazione delle stampe, le MFP e le stampanti Sharp sono compatibili con varie applicazioni che offrono un controllo degli accessi semplificato e caratteristiche che consentono di contenere i costi. I vantaggi includono:

- **Accesso**
  Semplice autenticazione con username e password o carta d'identità.

- **Permessi**
  Gestione delle funzioni delle MFP e impostazione dell'accesso per utente o per divisione, per una maggiore sicurezza.

- **Controllo**
  Controllo di tutte le attività. Gestione e monitoraggio delle attività di stampa/copia/scansione per controllare i costi e ottimizzare le risorse.

- **Recupero costi**
  È possibile rifatturare i costi ai clienti.

Gestione documentale e Workflow: Cloud Portal Office

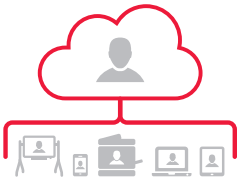
Cloud Portal Office di Sharp è una soluzione software, con diversi riconoscimenti, per la collaborazione e la sicura gestione documentale, per archiviare e condividere documenti elettronici e scansioni. Perfettamente integrato alle MFP Sharp e ai sistemi di monitor interattivi BIG PAD, Cloud Portal Office ti aiuta a lavorare in modo più efficiente ed è un'alternativa sicura per gli impiegati che usano servizi cloud pubblici.

- **Accesso**
  Cloud Portal Office presenta caratteristiche di sicurezza secondo gli standard europei per applicazioni SaaS (Software as a Service). Grazie ai firewall installati sulle periferiche esterne e interne della rete protegge da connessioni e attività non sicure. Il sistema Cloud Portal Office è installato all'interno di un Virtual Private Cloud (VPC) per fornire la massima sicurezza dagli attacchi esterni e da accessi non autorizzati.

- **Controllo**
  Tutti i dati su Cloud Portal Office sono sotto la supervisione del tuo amministratore IT. A ogni account della società viene fornito un login per uno o più amministatori. Questi login sono tipicamente usati dallo staff IT per monitorare e gestire gli utenti nell'ambito degli account della società.

- **Condivisione file**
  Cloud Portal Office ti consente uno stretto controllo su chi può accedere, modificare e condividere i tuoi file. Quando condividi un documento o una cartella con un collega, puoi impostare diversi livelli di permessi, da quello di sola lettura, a quello di scrittura, eliminazione e condivisione. Puoi anche inviare documenti senza usare Cloud Portal Office, tramite un link a scadenza, dando alle persone l'accesso per poter svolgere il loro lavoro, minimizzando così i rischi di sicurezza.

- **Accesso da dispositivi mobili**
  Coniugando sicurezza e accessibilità, Cloud Portal Office fornisce un facile accesso "On-the-go" ai contenuti archiviati. Gli utenti di dispositivi mobili in cui è installato Cloud Portal Office Mobile posso accedere a CPO per recuperare documenti con una connessione SSL sicura. Per garantire la sicurezza, gli utenti devono autenticarsi prima di accedere ai dati, le loro credenziali vengono criptate sul loro dispositivo come tutti i sistemi di accesso. In caso di furto del dispositivo mobile, puoi reimpostare la tua password dal browser.



Benvenuti in Sharp

Noi di Sharp innoviamo costantemente, per consentire alle aziende di potenziarsi al massimo. Le nostre tecnologie integrate hanno rivoluzionato la relazione tra imprese e informazione e siamo pronti a fare lo stesso anche per la tua azienda. Scopri oggi stesso come possiamo potenziare il tuo business.

SHARP

Inspiring ideas from technology

www.sharp.it