SHARP

Be Original.

Come stampare in sicurezza nelle PMI

Linee guida

Indice

Introduzione

Stampanti e multifunzione (MFP) sono molto diffuse negli uffici.

Peter Plested,
Direttore Information Systems di Sharp Electronics Europe

Nonostante l'aspetto esteriore delle MFP porti a pensare che negli ultimi dieci o addirittura venti anni questi dispositivi non siano stati oggetto di modifiche sostanziali, in realtà – come sanno bene gli IT manager – al loro interno è stata apportata una tale evoluzione che oggi possono essere considerati allo stesso livello di sofisticati sistemi informatici, connessi alla rete aziendale e a Internet.

Anche se in Europa nove impiegati su dieci non ritengono che le stampanti o le MFP possano costituire un rischio per la sicurezza, questi dispositivi sono considerati un obiettivo dagli hacker così come un laptop o un PC e devono essere protetti con la tecnologia, ma anche con un attento utilizzo da parte degli utenti.

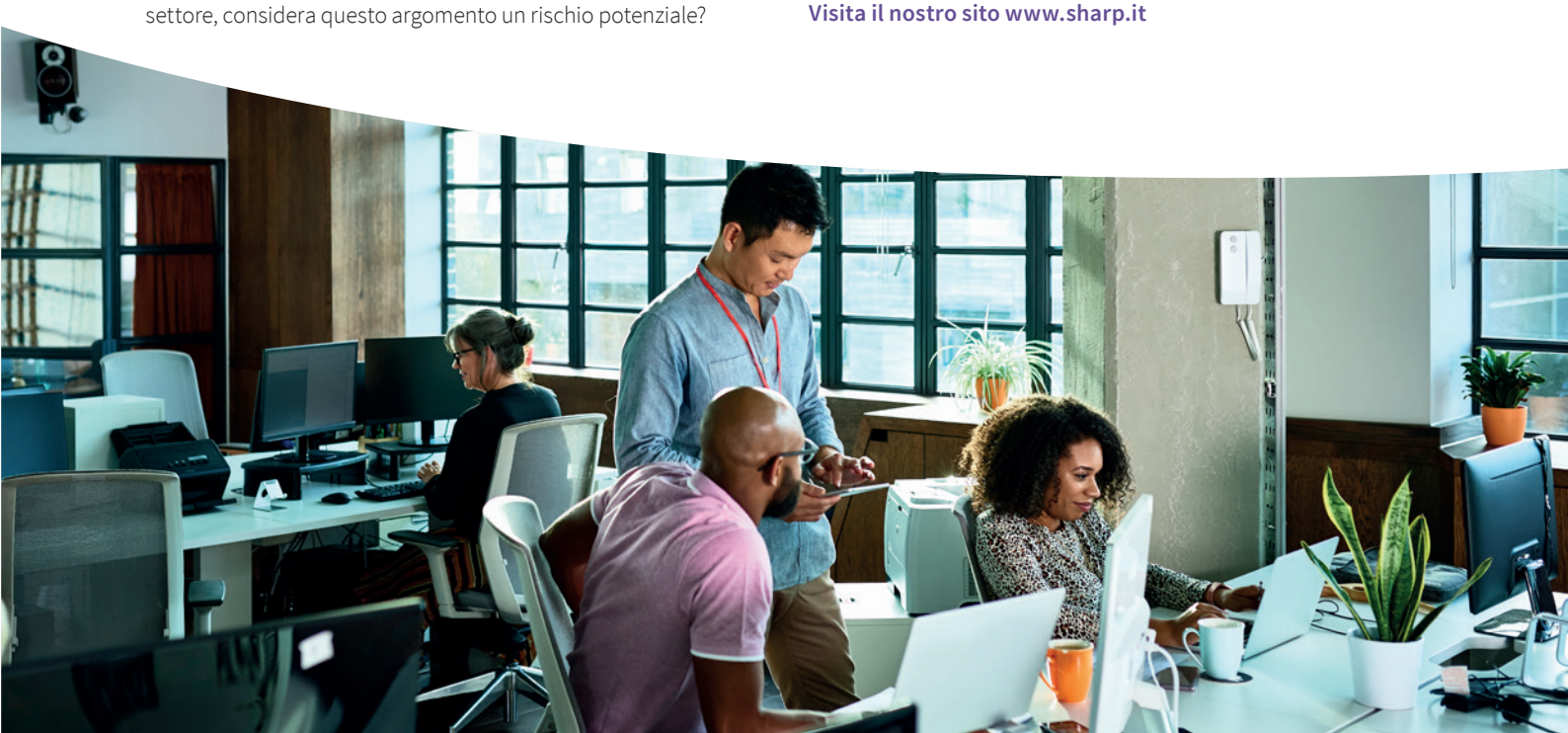
Per Sharp la sicurezza ha un ruolo centrale nelle attività di sviluppo. Con i nostri prodotti vogliamo rendere la vita lavorativa più semplice e produttiva, mantenendo allo stesso tempo la sicurezza dei dati.
Abbiamo voluto conoscere qual è l'atteggiamento delle persone nei confronti della sicurezza delle stampanti. Chi non è del nostro settore, considera questo argomento un rischio potenziale?

Abbiamo intervistato oltre 5.500 impiegati di piccole e medie imprese (PMI) europee, riscontrando che quasi la metà degli intervistati non era assolutamente consapevole che una stampante potesse essere hackerata.

La nostra ricerca ha inoltre messo in evidenza una mancanza di formazione e consulenza sulla sicurezza delle stampanti. Ci siamo quindi posti l'obiettivo di colmare questa lacuna, rendendo disponibili sul nostro sito internet alcuni consigli tecnici e questa guida realizzata in collaborazione con l'hacker etico Jens Müller.

La guida offre un'istantanea sulle abitudini di utilizzo delle stampanti da ufficio in Europa e propone alcuni semplici suggerimenti per i responsabili della tecnologia nelle PMI. Ci auguriamo che questo vademecum possa esserti di aiuto e saremo lieti di raccogliere le tue considerazioni o le principali difficoltà che incontri quando vuoi proteggere i tuoi dati.

Scrivi a @SharpBusinessIT su Twitter
Visita il nostro sito www.sharp.it



La tua rete è sicura?

Sai che le piccole imprese difficilmente dispongono di funzioni di sicurezza per la stampante?

Il 62% delle persone che lavorano in imprese con meno di 49 dipendenti dichiara che chiunque può utilizzare la stampante o la MFP. Questa percentuale scende al 43% per le imprese con 151-250 dipendenti.

I rischi dell'accesso non controllato alla stampante sono molteplici e possono andare dal malware caricato più o meno intenzionalmente nella rete attraverso la stampante, alla perdita di dati sensibili che avviene quando non si ritirano le stampe dal vassoio.

I numeri della ricerca

10%

Solo il 10% degli impiegati ha identificato nelle stampanti o MFP un rischio per la sicurezza sul posto di lavoro.

21%

Il 21% degli impiegati ha dichiarato che nel proprio ufficio non è stato installato nessun sistema di sicurezza per le stampanti o MFP.

25%

Il 25% degli impiegati ha dichiarato di aver trovato informazioni confidenziali o personali lasciate sul vassoio della stampante. Si tratta di una violazione della protezione dei dati.

28%

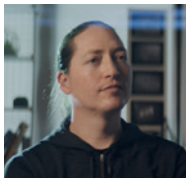
Il 28% degli impiegati ha utilizzato la stampante in ufficio per stampare un documento personale, creato a casa, al di fuori dell'ambiente protetto dell'azienda.

14%

Il 14% ha utilizzato la stampante d'ufficio per stampare un documento scaricato dal web, nonostante riportasse un avviso sulla mancata sicurezza del file, esponendo così la rete aziendale a una potenziale minaccia.

La ricerca è stata condotta da Censuswide per conto di Sharp. Sono stati intervistati 5.514 impiegati di aziende con 10-250 dipendenti, provenienti da sette paesi europei: Regno Unito, Germania, Francia, Italia, Paesi Bassi, Svezia e Polonia.

Il parere dell’esperto



Jens Müller
Hacker etico

Jens Müller, hacker etico, analizza i risultati della ricerca di Sharp e spiega i potenziali rischi sulla sicurezza dei dati per le PMI in materia di stampanti e MFP.

La ricerca di Sharp ha rilevato che in Europa nove impiegati su dieci non ritengono cha la stampante o la multifunzione possa costituire un potenziale rischio per la sicurezza della loro impresa. Dopo tutto, perché qualcuno dovrebbe avere interesse ad hackerare la stampante o la MFP di un’azienda? Quale profitto ne potrebbe ricavare?

In primo luogo, le stampanti si trovano ovunque. Ogni azienda ne possiede almeno una. Sono dispositivi connessi alla rete e, se sprovvisti di sistemi di protezione adeguati, possono essere facilmente presi di mira dagli hacker.

In secondo luogo, stampanti e MFP possono contenere informazioni preziose e dunque sono potenziali bersagli per attacchi hacker. Le aziende dovrebbero domandarsi quanto siano preziose le informazioni che stanno stampando e scannerizzando. Nell’era del GDPR, il Regolamento sulla Protezione dei Dati Personali che impone alle aziende la protezione dei dati sensibili, bisogna riconoscere che le stampanti o MFP costituiscono un pericoloso punto debole.

Generalmente, ci sono due tipi di hacker: giovani che vogliono divertirsi e testare per pura curiosità le loro abilità e individui più loschi, il cui unico obiettivo è lo spionaggio industriale. Non è facile comprendere quanto il problema della violazione della sicurezza dei sistemi di stampa sia diffuso, ma se proviamo a pensare alle decine di migliaia di stampanti suscettibili di attacchi hacker possiamo avere un’idea di quanto il problema sia potenzialmente enorme.

Sarebbe sbagliato pensare che questo problema riguardi solo le grandi aziende. Le PMI, infatti, sono altrettanto vulnerabili specialmente se – come nel caso di imprese che lavorano per la pubblica amministrazione – il loro business suscita un certo interesse in quei criminali che possono avere dei vantaggi dal rubare i loro dati o dall’interruzione della loro attività. Questo diventa davvero un problema in quanto, come si evince dalla ricerca di Sharp, le piccole imprese hanno risorse e competenze inferiori per gestire la questione della sicurezza informatica rispetto alle grandi organizzazioni.

Preparare il personale aziendale è dunque di fondamentale importanza. Come avviene già per il phishing, i dipendenti delle piccole e medie imprese devono essere formati anche per comprendere i rischi che passano attraverso stampanti e MFP e come superarli. In Europa il 40% degli impiegati non ha mai fatto formazione per stampare in modo sicuro.

Ma in cosa consistono questi rischi? Oltre a consentire l’accesso a dati sensibili contenuti in documenti stampati, scansionati e inviati via fax, stampanti e MFP possono essere utilizzate per immettersi nella rete di una società o per compiere attacchi DDoS (Distributed Denial of Service). Come accaduto nel 2016 con la botnet Mirai, che ha causato ingenti danni a dispositivi di tutto il mondo, incluse le stampanti, compiendo il più grande attacco DDoS della storia. Gli hacker cercheranno sempre di colpire l’anello più debole che potrebbe essere costituito proprio dalla stampante.

Il problema può verificarsi nel caso in cui la stampante o la MFP entri in funzione anche in mancanza di password. Sappiamo che in Europa oltre la metà (52%) degli impiegati non inserisce nessun codice di autenticazione per utilizzare la propria stampante o MFP. I dispositivi meno recenti, proprio perché dotati di sistemi di scurezza non aggiornati, possono essere attaccati più facilmente, come accade ai vecchi dispositivi Windows, che spesso sono la via di accesso per virus o attacchi informatici. Le vulnerabilità dei software obsoleti sono state evidenziate drammaticamente in occasione dell'epidemia di WannaCry nel maggio 2017 e le stampanti possono correre questi stessi rischi.

In che modo, dunque, una PMI può garantire la propria sicurezza messa a rischio da dispositivi di stampa vulnerabili? Bisogna ricordare che la miglior difesa è l'attacco; se gli hacker devono soltanto trovare un modo per entrare, il responsabile IT (o chiunque si occupi dell'IT in un'azienda) deve pensare a ogni potenziale punto debole. La sicurezza rientra tra le spese ordinarie che un'azienda deve gestire e grava sui suoi profitti; questo probabilmente spiega perché questa voce di bilancio è sempre in fondo all'elenco delle priorità. È effettivamente difficile decidere di investire in qualcosa che comunque funziona bene, come una stampante.

Tutto ciò, non riguarda solo la stampa. Anche lo scanner può costituire un punto debole, i documenti scannerizzati possono essere facilmente acquisiti da un hacker. Le PMI devono prendere in considerazione la crittografia dei documenti PDF e controllare che le scansioni di posta elettronica inviate dalla MFP siano sicure.

Naturalmente le aziende che prestano molta attenzione ai dati, non devono mai sottovalutare la minaccia "analogica" per le informazioni conservate sulla carta. In passato, gli hacker hanno trovato dati sensibili nella spazzatura. Può essere molto facile avere accesso alla stampante e alle eventuali copie cartacee lasciate nel vassoio della carta, dal momento che questi dispositivi il più delle volte sono collocati in aree dell'ufficio aperte e condivise.

Anche se il rischio può sembrare incontrollabile, mantenere la sicurezza della stampante è più facile di quanto si possa pensare. Per contrastare questi pericoli esistono modi semplici che non comportano alcun investimento aggiuntivo. Basta poterci dedicare soltanto un po' di tempo.
Ecco alcuni consigli per gli amministratori IT o i responsabili della tecnologia per ufficio.

Consigli per la sicurezza della stampante

I consigli che seguono sono validi per qualsiasi stampante o multifunzione collegata alla rete aziendale. Alcuni riguardano la gestione delle impostazioni che possono essere modificate in autonomia dall'amministratore, altri potrebbero richiedere l'intervento del fornitore della stampante o del servizio assistenza.

Cambiare le password predefinite

Non consentire agli hacker di prendere il controllo della tua stampante. Imposta una password complessa per la pagina web del pannello di controllo immediatamente dopo aver configurato il dispositivo. Le stampanti vengono solitamente distribuite con una password predefinita che è pubblica e quindi nota agli hacker. Pertanto, è fondamentale che gli amministratori IT impostino prontamente una password per ciascuna stampante nel proprio ufficio.

Autenticazione Utente

Assicurati che la tua MFP elabori le stampe provenienti solo da personale autorizzato. Configurala in modo che gli utenti debbano autenticarsi prima di poter stampare qualsiasi documento. L'autenticazione dell'utente può essere abilitata nel pannello di controllo della stampante. Per una efficace strategia della sicurezza è fondamentale limitare l'accesso agli utenti autorizzati allo scopo di tenere lontano gli aggressori e quindi impedire stampe indesiderate e attacchi sofisticati.

Nessun accesso alternativo non tracciato

Assicurati che non esista altra possibilità di stampare e quindi di aggirare i controlli di accesso ed eseguire la stampa non autenticata. Non consentire ai visitatori nemmeno l'accesso temporaneo ai tuoi dispositivi, ma crea una rete riservata agli ospiti: se gli ospiti hanno bisogno di stampare utilizzeranno un dispositivo separato non connesso alla rete aziendale.

Disabilitare i servizi di stampa non necessari

Configura solo ciò di cui hai veramente bisogno. Disabilita tutti gli altri servizi di rete e di stampa locale per ridurre al minimo le occasioni di attacco. Una volta che hai individuato quali protocolli sono realmente utilizzati nella tua configurazione, disabilita tutti gli altri servizi non richiesti. Ad esempio, se si stampa tramite IPP non è necessario lasciare attivo il servizio di stampa port 9100. Se si stampa solo tramite LAN, non è necessario che la stampante funga da hotspot WiFi / Airprint.

Sicurezza della rete

Internet può essere pericoloso. Assicurati che le tue stampanti non siano direttamente esposte alla rete Internet pubblica per evitare stampe non richieste e limitare le possibilità di attacchi più sofisticati. Anche se questo può sembrare ovvio, attualmente ci sono decine di migliaia di stampanti che hanno accesso ad indirizzi IP indirizzati pubblicamente. È possibile migliorare ulteriormente la sicurezza della rete interna, utilizzando il filtraggio degli indirizzi IP o MAC.

Sicurezza fisica

Per gli utenti non autorizzati può essere più facile accedere fisicamente alle stampanti e ai dispositivi multifunzione piuttosto che accedere a server o workstation, e l'avvio di un lavoro di stampa dannoso da un'unità USB può richiedere solo pochi secondi. Come contromisura, si consiglia di controllare tramite autenticazione oppure disabilitare tutte le porte fisiche come la stampa non autorizzata via USB (lato frontale), cavo parallelo o USB (retro), NFC e Bluetooth.

Non posizionare le stampanti in luoghi comuni. Assicurati che la manutenzione della stampante venga eseguita solo da personale autorizzato e istruisci i tuoi dipendenti nel caso si presentino individui sospetti o sconosciuti.

Non lasciare documenti riservati sul vassoio della stampante. Abilita Secure Print Release (a volte chiamato anche "Pull Printing", "Follow Me Secure Print" o "Pick up protection") che consente il rilascio del documento solo a seguito di autenticazione tramite PIN o badge RFID.

Aggiornamenti del firmware

Negli ultimi dieci anni le stampanti si sono evolute da dispositivi automatici dotati di microchip a sistemi informatici in piena regola. Pertanto, è doveroso trattarle come gli altri componenti del sistema IT. Assicurati sempre di tenere il passo con le ultime patch di sicurezza e gli aggiornamenti del firmware.

La versione più recente è la più sicura. Garantisce l'esecuzione delle ultime funzionalità di sicurezza e dei meccanismi di protezione. Pianifica un appuntamento fisso e periodico per installare gli aggiornamenti del firmware oppure contatta il tuo rivenditore autorizzato quando l'aggiornamento viene rilasciato.

Abilitare il monitoraggio

Cosa accade se hai subito una violazione o hai rilevato attività sospette all'interno della rete della tua organizzazione? I file di log possono rivelare informazioni su cosa è successo esattamente in quanto registrano le prove digitali di eventuali tentativi di intrusione come lavori di stampa malevoli (ricordati di abilitare l'autenticazione dell'utente).

Gli amministratori IT possono abilitare le notifiche via e-mail per essere sempre al corrente di eventuali criticità e delle violazioni della sicurezza.

Smaltimento sicuro

Non limitarti a disfartene. In passato le violazioni della sicurezza si sono verificate perché gli hacker sono entrati in possesso di stampanti dismesse e hanno avuto accesso ai loro dischi rigidi o alla memoria non volatile (NVRAM). Se il dispositivo è stato integrato nella rete dell'organizzazione, potrebbe contenere dati sensibili. Al momento della disattivazione, assicurati che la memoria o l'HDD siano stati cancellati. Se il dispositivo deve essere restituito alla società dalla quale è stato acquistato, utilizza le funzionalità di fine locazione per essere sicuro che tutti i dati riservati vengano sovrascritti prima che il dispositivo lasci la struttura.

Abilitare la crittografia

I tuoi dati sono preziosi. Tutti i documenti stampati su una stampante di rete, se non vengono crittografati, verranno trasmessi in chiaro sul cavo, consentendo a tutti "nel mezzo" di accedere ai lavori di stampa. Per abilitare la crittografia in transito, gli amministratori IT possono scegliere fondamentalmente tra due opzioni: sicurezza del livello di trasporto (TLS / SSL) e IPSec, che crittografa l'intero traffico di rete.

Se devi inviare file riservati come documenti scansionati su canali non sicuri, utilizza S/MIME la crittografia end-to-end dei messaggi di posta elettronica basata su certificati o utilizza la crittografia PDF con una password complessa. Per garantire l'archiviazione sicura dei documenti sulla stampante o sulla stampante MFP, abilita la funzione di crittografia del disco fisso della stampante.

Glossario

Autenticazione
Identificazione univoca ottenuta generalmente attraverso due informazioni come nome utente e password.

Porte
Le porte vengono utilizzate dai dispositivi di rete (PC, server, stampanti ecc.) per comunicare tra loro (ad es. una workstation per connettersi a una stampante). Porte e servizi aperti non custoditi possono essere utilizzati come vettore di attacco, ad esempio per la propagazione di malware.

Protocolli
Per protocollo si intende un insieme di regole e formati che consentono ai sistemi di informazione di scambiare dati. Nell'ambito di una rete informatica, ad esempio, IP e TLS / SSL sono dei protocolli.

Transport Layer Security (TLS / SSL)
Tipo di tecnologia che serve a crittografare i dati trasportati o trasferiti da un dispositivo a un altro allo scopo di impedirne l'intercettazione. TLS / SSL è ampiamente utilizzato per i siti web ma può essere usato anche per proteggere servizi di altro genere.

Internet Printing Protocol (IPP)
Protocollo Internet di stampa in grado di eseguire l'autenticazione e gestire la coda dei lavori di stampa. IPP è supportato e abilitato di default sulla maggior parte delle stampanti e MFP moderne.

Indirizzi IP
Ogni dispositivo connesso a Internet deve avere un numero univoco (indirizzo IP) per connettersi ad altri dispositivi. Esistono attualmente due versioni di indirizzamento IP: IPv4 e la versione successiva aggiornata denominata IPv6.

IPsec (Internet Protocol Security)
Suite di protocolli per garantire la sicurezza delle comunicazioni IP (Internet Protocol) a livello di rete. IPsec include anche protocolli per la creazione di chiavi crittografiche.

S/MIME (Secure/Multipurpose Internet Mail Extensions)
Serie di specifiche che servono a proteggere i messaggi di posta elettronica. Utilizzano MIME, formato ampiamente diffuso, e seguono un protocollo che garantisce la sicurezza attraverso firme digitali e crittografia.

MAC addresses
L'indirizzo MAC (Media Access Control), detto anche indirizzo fisico, permette di identificare in modo univoco ogni scheda di rete (NIC, network interface card) di un particolare dispositivo.
Ciò significa che un dispositivo connesso alla rete può essere identificato in modo univoco grazie al suo indirizzo MAC.

Filtro degli indirizzi IP o MAC
Il filtro garantisce che gli indirizzi IP e MAC siano controllati rispetto a una “whithelist” prima che i dispositivi possano connettersi alla rete.

Servizi di rete
I servizi di rete facilitano il funzionamento della rete stessa. In genere vengono forniti da un server (che può mettere a disposizione uno o più servizi), basato su protocolli di rete. Alcuni esempi sono il DNS (Domain Name System), il protocollo di configurazione host dinamico (DHCP), il protocollo VoIP (Voice over Internet Protocol).

Whitelist
Una whitelist è un elenco esclusivo di persone, entità, applicazioni o processi a cui sono concessi permessi speciali o diritti di accesso. Nel caso di un’azienda, la lista potrebbe comprendere, ad esempio, i dipendenti della società e i loro diritti di accesso all’edificio, alla rete e ai computer. In termini di rete o computer, una whitelist può determinare quali applicazioni e procedure hanno il permesso di entrare nelle aree sicure dell’archiviazione dati.

DoS/DDoS
Un Denial of Service (DoS) è una tipologia di attacco puramente distruttivo che punta a interrompere o annullare il normale funzionamento o servizio fornito da una rete o dispositivo. Un DDoS (Distributed Denial of Service) è una particolare tipologia di attacco DoS che utilizza contemporaneamente più sistemi di attacco per amplificare la quantità del traffico di rete, inondando i sistemi o le reti bersaglio.

Attacco di phishing
Il phishing è una particolare tipologia di truffa effettuata attraverso l’invio di e-mail apparentemente provenienti da aziende conosciute con l’obiettivo di indurre i destinatari a rivelare informazioni personali quali password e numeri di carte di credito.

Attacco Spoofing
Lo spoofing è un tipo di attacco informatico che si verifica quando un malintenzionato falsifica l’identità di un altro dispositivo o utente su una rete per lanciare attacchi contro host di rete, rubare dati, diffondere malware o bypassare i controlli di accesso.

Attacco man-in-the-middle
Man-in-the-middle (MITM) è una tipologia di attacco informatico nel quale l’aggressore si trova segretamente tra due parti che credono di comunicare direttamente tra loro e tramite una connessione privata. In realtà, l’aggressore non solo intercetta lo scambio di messaggi ma può anche alterare la comunicazione.

Attacco di malware
Un malware può essere definito come un software dannoso e indesiderato che viene installato nel sistema operativo senza il tuo consenso. Può collegarsi al codice legittimo e propagarsi, oppure può nascondersi in applicazioni utili o diffondersi su Internet.

Funzionalità di sicurezza Sharp

Sharp fornisce una suite di funzionalità (applicazioni e software) per aiutare le imprese a proteggere informazioni e documenti da molteplici minacce.

L'ultima gamma di multifunzioni Sharp MFP A3* e A4** sono le più sicure fino ad oggi, offrendo un approccio alla sicurezza unico e a 360 gradi, e fornendo alle PMI gli strumenti per controllare e gestire la politica aziendale di stampa. Inoltre, Sharp aiuta a proteggere le informazioni riservate, sia che vengano stampate, copiate, scansionate, inviate via fax, archiviate o condivise sulla loro rete.

Sharp ha la soluzione giusta che fa per te: da Network Security, che copre tutte le reti aziendali e tutte le periferiche connesse, alla Output Security, che controlla e traccia l'accesso, fino a Document Security, che protegge sia i documenti digitali che quelli analogici.

Per ulteriori informazioni, visita il nostro sito web e consulta il Libro Bianco o la sezione dedicata alla Sicurezza: https://www.sharp.it/cps/rde/xchg/it/hs.xsl/-/html/information-security.htm

- Sicurezza della rete
- Sicurezza dell'output
- Sicurezza dei documenti
- Conformità GDPR

Questo approccio globale alla sicurezza garantisce inoltre che la tua azienda raggiunga il massimo livello di adeguamento alle più recenti norme, comprese quelle contenute nel Regolamento generale sulla protezione dei dati (GDPR).

Per maggiori informazioni riguardanti gli standard di sicurezza per la tua azienda non esitare a contattarci.

Prenditi cura della tua impresa, alla sua sicurezza ci pensa Sharp.

* Modelli A3: MX-6071, MX-6051, MX-5071, MX-5051, MX-4071, MX-4061, MX-4051, MX-3571, MX-3561, MX-3551, MX-3071, MX- 3061, MX-3051, MX-2651.
** Modelli A4: MX-C304W, mX-C303W

www.sharp.eu

SHARP

Be Original.