# BUONE PRATICHE D'USO

ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

## Aggiornamento dei dispositivi

È utile prendere in considerazione l'aggiornamento del proprio parco stampanti. Molte nuove stampanti dispongono di funzionalità di sicurezza integrate che semplificano la protezione della rete e la protezione da un attacco informatico.

## Mantenere aggiornato il software dei dispositivi

Le stampanti hanno spesso un firmware che le aiuta a funzionare, potrebbero anche avere un software antivirus o anti-malware integrato. È bene consultare il manuale del proprio dispositivo per conoscere le diverse caratteristiche e la sua manutenzione. È inoltre importante installare eventuali patch di sicurezza o aggiornamenti, poiché il software obsoleto è spesso una delle cause principali che porta alla violazione dei dati.

## Creare policy aziendali per proteggere i dati contenuti negli hard disk e sui documenti lasciati nei vassoi delle stampanti

Creare una serie di regole pratiche e norme di condotta sono la base per ottenere una linea di difesa verso gli attacchi. Una serie di policy adeguate può aiutare a proteggere sistemi e utenti, anche coloro che lavorano in remoto.

## Mettere in atto un processo di autenticazione

Una buona pratica è quella di verificare che le stampanti dispongano di misure di sicurezza come pass code univoci per trattenere le stampe fino a quando un utente non è fisicamente presente per ritirarli. Questo processo permette di verificare i dati inviati, per questo le stampanti potrebbero subire altre vulnerabilità che potrebbero rivelarsi sfruttabili, anche da remoto I sistemi di stampa e digitalizzazione sono dotati di funzionalità che garantiscono la protezione delle informazioni, come l'autenticazione e l'autorizzazione per verificare l'identità degli utenti prima che venga rilasciata qualsiasi stampa. I metodi di convalida possono essere diversi: lettori badge, codici PIN o sistemi di autenticazione biometrica.

## Utilizzare i software di monitoraggio

Il software di monitoraggio dei dispositivi di stampa permette di avere sotto controllo tutte le attività di stampa della propria organizzazione. Questi cruscotti sono inoltre in grado di individuare attività sospette e consentire una reazione tempestiva agli attacchi.
Gli utenti dei servizi di stampa gestiti (MPS) possono anche ottenere regolari report di conformità, che dovrebbero includere il monitoraggio e la segnalazione delle violazioni dei dati.

## Posizionare i dispositivi di stampa e digitalizzazione su una rete separata e dedicata all'interno dello spazio di lavoro

Posizionare le stampanti su una rete separata non eliminerà la minaccia di malintenzionati che accedono alla rete aziendale da questi dispositivi, ma impedirà loro di utilizzarli come potenziali punto di ingresso nella rete aziendale.

## Formare e rendere consapevoli gli utenti su minacce e attacchi

Questa pratica consente di rendere informati gli utenti sui rischi legati ai dispositivi di stampa. Sensibilizzare gli utenti dotandoli di regole di comportamento è il primo passo verso una maggiore sicurezza. Una survey contenuta nel Rapporto Clusit 2023 sulla Sicurezza ICT in Italia, ha evidenziato che le policy e le procedure di sicurezza pubblicate sono conosciute da dipendenti e collaboratori solo in un terzo (33%) delle aziende.

## Sanificazione dei dati al momento della sostituzione dei dispositivi

È importante accertarsi che il dispositivo sia sottoposto ad un procedimento di sanificazione certificata dei dati che include la distruzione degli hard disk, o la loro formattazione in modalità sicura a basso livello, e la cancellazione di tutti i dati presenti nelle rubriche interne al dispositivo, come per esempio rubrica e-mail, rubrica telefonica-fax, al momento della sua sostituzione. Questa pratica consente di distruggere in modo definitivo tutti i dati contenuti in questi dispositivi e la certificazione, dichiarazione emessa dal fornitore che effettua il servizio, tutela l'azienda o il privato che ha utilizzato il dispositivo fino a quel momento.

## Servizi professionali di Print Security Risk Assessment

Come già detto, spesso il perimetro dei dispositivi di stampa non viene tenuto nella giusta considerazione da parte del personale IT, che tende a valutare come sicuro un ambiente nel quale invece i potenziali bug di sicurezza sono presenti. È raccomandato valutare col proprio fornitore di dispositivi di stampa la possibilità di usufruire di un servizio professionale di Security Risk Assessment per i dispositivi di stampa grazie al quale verranno analizzate in profondità tutte le potenziali aree di rischio: hardware, firmware, network, processi e procedure, asset management, configurazioni iniziali e manutenzione delle stesse, patching, governance.

## Buone pratiche a casa

Avere una stampante non protetta collegata alla rete domestica o aziendale è come lasciare una porta aperta nella propria stanza o in ufficio. Quindi, è bene assicurarsi di rivedere e disabilitare tutto ciò che comporta la stampa su Internet. Ciò include la configurazione delle impostazioni di rete in modo che la stampante risponda solo ai comandi provenienti dal router di rete. Inoltre, non dimenticare di scollegare la stampante quando non è in uso: se non c'è connessione, i malintenzionati non possono compromettere la rete.