TOSHIBA

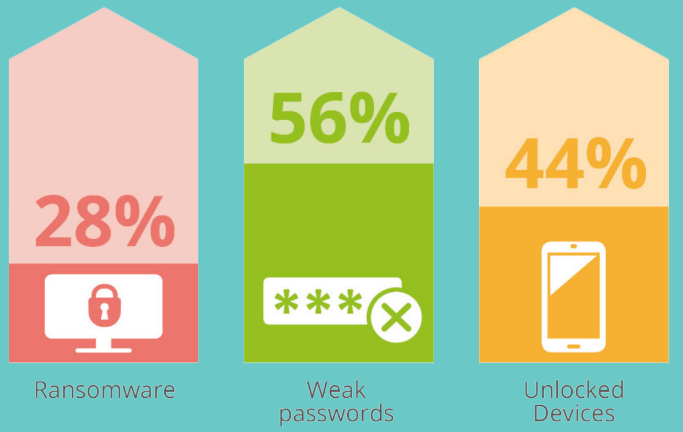
WHITEPAPER

Toshiba

La sicurezza dei dati nei processi di stampa

1 PANORAMICA

La sicurezza delle informazioni è essenziale per qualunque tipologia di organizzazione.
Tuttavia, Tuttavia, le piccole e medie imprese (PMI) sono particolarmente vulnerabili ad attacchi esterni, a causa della mancanza di processi e tecnologie a tutela dei dati.
"Delle PMI intervistate oltre l'80% ha dichiarato che i problemi di sicurezza informatica avrebbe un grave impatto negativo sulla loro attività all'interno una settimana dei problemi che si verificano, su 57% afferma che lo farebbe molto probabilmente fallisce o fallisce".
(Fonte: Agenzia dell'Unione europea per la sicurezza informatica (ENISA), Sicurezza informatica per le PMI, giugno 2021, p. 3)



Fonte: Figura 13: Cybersecurity Threat Landscape, ENISA, Cybersecurity for SMEs, June 2021, p.17

“Non disponendo di una specifica policy di backup up, una soluzione antimalware per endpoint implementata su tutti i tipi di dispositivi e mantenuta aggiornata, utilizzando software obsoleti o semplicemente privi di patch che non si aggiornano automaticamente, potrebbe compromettere seriamente le informazioni critiche e sensibili dell'azienda, rendendo la PMI un facile bersaglio per attacchi informatici come ransomware o altro.” (Fonte: Agenzia dell'Unione europea per la sicurezza informatica (ENISA), Cybersecurity for SMEs, giugno 2021, pag. 16)

Infatti, citando i rapporti di Threat Landscape dell'ENISA del 2021, "Il ransomware era la seconda minaccia più comune ed era correlato a un terzo (28%) degli incidenti di sicurezza. Inoltre, secondo l'ENISA Threat Landscape Report 2018, le password deboli o riutilizzate (56%) e i dispositivi sbloccati (44%) sono due dei maggiori punti deboli all'interno delle organizzazioni". (Fonte: Agenzia dell'Unione europea per la sicurezza informatica (ENISA), Cybersecurity for SMEs, giugno 2021, p. 17)

Ogni giorno si producono e si distribuiscono milioni di documenti riservati. I sistemi multifunzione e le stampanti fanno parte integrante delle reti aziendali, proprio per la loro capacità di memorizzare elevate quantità di dati sul loro disco fisso, e rappresentano dunque dei punti critici di vulnerabilità. Inoltre, la maggior parte dei sistemi di stampa è accessibile anche tramite dispositivi mobili e piattaforme cloud, il che li rende ancora più vulnerabili agli attacchi esterni.
Senza l’implementazione di adeguate misure di sicurezza, i dati sensibili e le informazioni aziendali critiche possono essere facilmente accessibili anche a persone non autorizzate.

Toshiba offre numerose opzioni mirate alla sicurezza dei dati e alla protezione dei documenti per aiutare gli utenti a rispondere alle crescenti esigenze di sicurezza del mondo di oggi.

2 PERCHE' STAMPARE IN MODO SICURO?

Ogni azienda dispone di informazioni sensibili che sono essenziali per la sua sopravvivenza. Garantire la privacy dei dati dei clienti e la protezione dei dati personali dei dipendenti è fondamentale quanto la protezione della proprietà intellettuale e dei documenti finanziari dell'azienda. Inoltre, il rispetto di regolamenti e standard governativi sempre più severi (ed estremamente punitivi) rendono ancora più complicata la gestione delle informazioni. In genere, le organizzazioni si concentrano sui dati sensibili archiviati nel database, tuttavia la maggior parte delle organizzazioni non presta sufficiente attenzione al processo di acquisizione documenti e al suo intero ciclo di vita all'interno e all'esterno dell'azienda, aprendo così i propri dati a potenziali furti e violazioni.

Quando si tratta di sicurezza per la stampa, avere un solo dispositivo sicuro non è sufficiente. Qualsiasi implementazione per l'ambiente di stampa deve garantire che la sicurezza sia integrata in hardware, software e applicazioni. Inoltre, è cruciale una gestione efficace delle impostazioni e dei criteri di sicurezza sull'intero parco installato.

In un'azienda il tema "sicurezza" va suddiviso in quattri livelli: dispositivo, accesso, documento e parco dispositivi.

La sicurezza del dispositivo si concentra sulle funzionalità integrate nell'hardware, nel controller e nel software della periferica, garantendo la protezione end-to-end dell'apparecchiatura dall'installazione alla fine del ciclo di vita.

La sicurezza sulle modalità di accesso garantisce che le persone giuste abbiano accesso alle funzioni e ai dati corretti sul dispositivo di stampa. Qualsiasi intrusione deve essere monitorata e gestita in modo proattivo.

Infine, la sicurezza del parco installato aiuta a gestire le impostazioni e le politiche su tutte le periferiche presenti in rete.

Il nostro approcio alla sicurezza di stampa

3 SICUREZZA PERIFERICA

Protezione a ogni livello

I livelli di sicurezza implementati sul dispositivo proteggono l'hardware, il software del controller e le applicazioni dalle minacce esterne durante l'intero ciclo di vita della multifunzione. Alcune delle caratteristiche chiave del dispositivo includono:

Protezione BIOS

Il BIOS del dispositivo è un insieme di istruzioni nell'hardware, che controlla le operazioni di input e output sulla periferica. Solo il BIOS autorizzato dal produttore dovrebbe poter essere caricato sul dispositivo. Inoltre, si consiglia di crittografare il BIOS di sistema in modo che qualsiasi BIOS non autorizzato possa essere severamente vietato.

Criptatura Hard Disk

I dischi fissi possono essere bersaglio di attacchi alla sicurezza, perché i dispositivi di stampa possono archiviare temporaneamente copie di documenti acquisiti, copiati e stampati sugli HDD integrati. Se il disco rigido del sistema multifunzione viene compromesso, tutti i documenti sensibili memorizzati sull'unità sono a rischio. Pertanto, i dati sull'HDD devono essere crittografati, in modo che anche se il supporto di archiviazione, contenente documenti sensibili, viene perso o rubato, il documento non potrà essere assolutamente recuperato. Come ulteriore protezione, il supporto di memorizzazione dovrebbe essere reso automaticamente inutilizzabile quando viene rimosso dal dispositivo di stampa.

Sistema operativo / Firmware / Applicazioni whitelisting (lista applicazioni attendibili)

Recentemente, i difetti di sicurezza in diversi sistemi, incorporati e utilizzati nelle periferiche di stampa, hanno creato punti di ingresso per ransomware e spyware, creando problemi sulle reti aziendali. Le aziende devono garantire che le funzionalità integrati sui propri sistemi di stampa siano stati sottoposti a test approfonditi sulla vulnerabilità della sicurezza e siano aggiornati frequentemente con patch di sicurezza. Inoltre, il dispositivo deve anche proteggersi da qualsiasi tentativo di installazione di software non autorizzato.
Tutti i firmware e le applicazioni software in esecuzione devono essere firmati digitalmente dal produttore e tutti gli altri devono essere rifiutati in modo che non sia possibile installare aggiornamenti dannosi sulla periferica.

La sicurezza dell'autenticazione garantisce che le persone giuste abbiano accesso ai dati e alle funzioni corrette sul dispositivo di stampa.

4 SICUREZZA DELLE MODALITA' DI ACCESSO

La sicurezza degli accessi garantisce che le persone giuste abbiano accesso, fisico e digitale, ai dati e alle funzioni corrette sulla periferica di stampa, compreso l'accesso alla rete, dai dispositivi mobile e dai servizi cloud. Gli amministratori devono essere in grado di limitare l'accesso, gestire e applicare policy di sicurezza e monitorare in tempo reale qualsiasi log-in non autorizzato.

Autenticazione e accesso alla directory

Le organizzazioni devono disporre di un processo standard per assicurarsi che solo gli utenti autenticati possano accedere ai dispositivi di stampa. Questi metodi di autenticazione possono includere qualsiasi combinazione di credenziali utente, lettori badge, codici PIN o anche autenticazione biometrica. Inoltre, i ruoli utente e i privilegi di accesso devono essere gestiti tramite una directory aziendale centrale per evitare accessi illegali/non autorizzati. Le PMI, in particolare nei settori della conformità normativa, devono anche prendere in considerazione l'autenticazione a due fattori per aggiungere un altro livello di sicurezza al processo di autenticazione.

Gestione delle password e dei criteri di accesso

L'applicazione di una rigorosa politica delle password è una delle misure più semplici che le aziende possono adottare. Una buona politica delle password deve imporne la lunghezza minima, la scadenza e il blocco dell'account. Il criterio dovrebbe anche non consentire stringhe di password usate di frequente o password predefinite.

Blocco delle porte fisiche e di rete

I dispositivi di stampa devono anche disporre di protezioni integrate dall'accesso fisico non autorizzato e attraverso la rete tramite USB disabilitazione delle porte, blocco delle porte di rete e filtro IP/MAC. Questi garantiscono che solo il personale e i dispositivi autorizzati possano comunicare con i dispositivi di stampa, bloccando così qualsiasi accesso non autorizzato.

Monitoraggio e rilevamento delle intrusioni

Registri di controllo a livello di sistema per tutti gli accessi e le attività sui dispositivi di stampa sono altamente consigliati per fornire visibilità agli amministratori in merito a quando e come è stato effettuato l'accesso al dispositivo o al documento. Alcuni settori normativi e rigorosi richiedono questa funzionalità anche sui dispositivi di imaging. Inoltre, le aziende dovrebbero anche monitorare i registri di sistema e di sicurezza delle periferiche tramite antivirus esterno o software SIEM (Security Information & Event Management) per rilevare qualsiasi intrusione in tempo reale. Pertanto, i dispositivi di stampa dovrebbero comunicare perfettamente con quei sistemi di terze parti.

5 SICUREZZA DEL DOCUMENTO

Quando si tratta di sicurezza dei documenti, le aziende devono garantire che le informazioni all'interno, come numeri di previdenza sociale, dettagli della carta di credito e altri dati di identificazione personale (PII), siano protetti durante l'intero ciclo di vita del documento, dal suo inizio a disposizione. I documenti in genere passano attraverso i seguenti tre processi chiave in un ambiente di stampa: acquisizione, archiviazione e consegna.

5.1 CATTURA

In genere, durante un processo di acquisizione, un documento fisico viene convertito in un formato digitale ricercabile tramite un processo di riconoscimento ottico dei caratteri (OCR). Scansione su e-mail, scansione su condivisione di rete e scansione su cloud storage sono alcuni dei metodi utilizzati in quasi tutte le organizzazioni per acquisire documenti fisici e convertirli in formato digitale.

Sicurezza nell'acquisizione dei dati

Garantendo che i dispositivi di stampa utilizzino i protocolli di stampa protetta (Secure IPP) e i canali di trasmissione crittografati per la scansione dei documenti, gli amministratori possono essere certi che i dati dei documenti non possano essere intercettati. In effetti, come minimo, i dispositivi di comunicazione dovrebbero essere configurati con TLS 1.2, HTTPS e WPA2 per la sicurezza wireless. La comunicazione wireless non protetta o non utilizzata (Wi-Fi, NFC, Bluetooth) deve essere disabilitata sui dispositivi di stampa. Inoltre, le aziende che utilizzano comunicazioni fax dovrebbero prendere in considerazione la protezione tramite password dei fax in arrivo e la conservazione o la pianificazione dei lavori da stampare durante un'ora specifica del giorno, per evitare l'accesso non autorizzato a tali fax.

Destinazioni scansione whitelist

Inserendo nella whitelist le destinazioni di scansione, le organizzazioni possono garantire che i documenti sensibili possano essere scansionati solo su destinazioni specifiche. Vietando agli utenti di inviare documenti al di fuori delle destinazioni autorizzate, potete essere certi che i documenti possono essere consegnati solo al legittimo proprietario/destinazione e non finiranno nelle mani sbagliate, nemmeno per errore.

5.2 ARCHIVIAZIONE

Dopo che i documenti vengono acquisiti, sono generalmente archiviati all'interno di un file system, un sistema di archiviazione cloud, un sistema di gestione dei documenti o persino su un supporto di archiviazione all'interno del dispositivo di stampa. Devono essere adottate misure di sicurezza per garantire che i luoghi di archiviazione siano monitorati, controllati e protetti dagli hacker. Di seguito sono riportati alcuni consigli per garantire che i documenti aziendali sensibili siano archiviati in modo sicuro.

Crittografia dei documenti

A volte, il disco rigido del dispositivo di stampa viene utilizzato per l'archiviazione elettronica. Come minimo, le aziende devono garantire che i loro documenti aziendali siano crittografati e protetti da password quando vengono archiviati o condivisi, quindi nel caso in cui cadano nelle mani sbagliate, non saranno in grado di aprire i documenti.

Timbri di sicurezza

L'aggiunta di timbri di sicurezza ai documenti archiviati una volta stampati, copiati, archiviati elettronicamente o persino inviati via fax, aiuta le organizzazioni a determinare l'origine dei documenti, evitando così qualsiasi manomissione. Questi timbri possono includere un nome utente e il nome del dipartimento. Questa funzione scoraggia anche gli utenti interni ed esterni dal manomettere documenti e posizioni di archiviazione.

5.3 CONSEGNA

Ogni azienda ha processi di flusso di lavoro documentale (ad esempio, elaborazione degli ordini, reclutamento delle risorse umane, contabilità fornitori, ecc.) che richiedono che i documenti archiviati vengano consegnati a una destinazione esterna o a un dispositivo di output. Pertanto, le organizzazioni devono garantire che il loro processo di consegna dei documenti (esterno o interno) sia completamente sicuro per evitare intercettazioni e attacchi man-in-the-middle. Ecco alcuni passaggi che le aziende possono seguire per proteggere il processo di consegna dei documenti negli ambienti di stampa:

Stampa protetta / privata / trattenuta

Oltre all'autenticazione sul dispositivo, le organizzazioni devono implementare soluzioni di rilascio sicuro delle stampe per il proprio parco stampanti. Il rilascio sicuro della stampa garantisce che i documenti riservati vengano conservati in una coda di stampa protetta, fino a quando il proprietario del lavoro non si autentica e lo rilascia alla stampante. Se il destinatario è una persona diversa dalla persona che invia il documento, la stampa privata consente agli utenti di proteggere con password i propri lavori al fine di garantire che i documenti non vengano rilasciati fino a quando non viene inserita la password corretta sul pannello della MFP. Queste difese garantiscono che i documenti riservati non vengano lasciati incustoditi davanti alla stampante.

Scambio sicuro di documenti

Con l'uso diffuso del cloud e della tecnologia mobile, le organizzazioni devono anche garantire che i documenti condivisi su rete, Internet e infrastruttura Wi-Fi/mobile siano completamente sicuri. Quando i documenti vengono scambiati con un pubblico esterno, è necessario assicurarsi che solo il destinatario previsto possa accedere al file. Il monitoraggio e la traccia dell'accesso sono fondamentali per la sicurezza del documento, quando è condiviso con un pubblico esterno.

Protezione e monitoraggio copia dei documenti

Alcuni tipi di documenti, come buste paga o documenti classificati, non dovrebbero mai essere copiati o scansionati. Pertanto, i dispositivi di stampa devono fornire un meccanismo per proteggere tali documenti da copia, stampa o scansione. Le funzioni di sicurezza della copia cartacea all'interno dei dispositivi multifunzione proteggono i documenti classificati dalle copie illegali. Inoltre, qualsiasi azione illegale di questo tipo dovrebbe essere registrata e segnalata agli amministratori.

6 SICUREZZA PARCO INSTALLATO

Ultimo ma non meno importante, che la vostra sia una azienda con due dispositivi o con centinaia di periferiche, è fondamentale essere in grado di impostare, applicare e gestire le policy di sicurezza con facilità in tutta la vostra organizzazione. Inoltre, avere uno strumento che permetta di monitorare i vostri dispositivi da remoto, senza dover accedere fisicamente al dispositivo, sarebbe ancora più conveniente. Pertanto, una soluzione di sicurezza per la stampa deve includere uno strumento di gestione del parco dispositivi che supporti il monitoraggio e la gestione centralizzata delle politiche di sicurezza in tutti i dispositivi di stampa. Questo strumento dovrebbe consentire agli amministratori di creare criteri di sicurezza e distribuirli su un parco di qualsiasi dimensione. Eventuali violazioni a queste politiche dovrebbero essere notificate ed eventualmente corrette automaticamente. È preferibile che questo strumento di gestione sia basato su cloud per maggiore praticità e gestione.

e-BRIDGE CloudConnect

Impostare e gestire le policy di sicurezza con facilità in tutta la vostra organizzazione.

7 PERCHE' TOSHIBA

Con la tecnologia e-BRIDGE Next, Toshiba offre i migliori dispositivi multifunzione della categoria per la sicurezza della stampa end-to-end e offre ai suoi clienti caratteristiche uniche e distintive.
Toshiba è un fornitore leader nel settore IT e da sempre diamo la massima priorità alla protezione dei dati.
I prodotti Toshiba e-BRIDGE Next sono conformi ai Common Criteria della Evaluated Assurance con livello 3 (EAL 3), conformi a ISO/ IEC15408 e soddisfano gli standard IEEE 2600.1. Ma questo cosa significa? I nostri sistemi sono stati progettati per integrarsi facilmente in infrastrutture IT sicure e contribuire alla protezione dei dati durante i flussi di lavoro.
Già nel 2012 Toshiba ha iniziato a dotare tutti i nuovi sistemi e-BRIDGE con un Secure Hard Disk Drive. Questo HDD non solo funziona con sistemi di crittografia all'avanguardia, ma è dotato anche di un sofisticato sistema di autenticazione, che assicura la protezione dei dati anche nel caso in cui l'HDD dovesse finire nelle mani sbagliate.
Per la massima sicurezza la funzione opzionale Sovrascrittura Dati sovrascrive automaticamente tutti i dati fino a cinque volte, cancellandoli completamente dopo aver stampato, scannerizzato, copiato o inviato via fax un documento. In questo modo nulla viene salvato in modo permanente sull'HDD e non rimangono dati che potrebbero venire compromessi.

Toshiba offre anche altre possibilità per proteggere i dati riservati da accessi non autorizzati. Di seguito le principali categorie:
• Sicurezza di accesso
– Limitare l'accesso aiuta a prevenire la perdita di dati. L'accesso basato sui ruoli assicura pieno controllo su quali funzionalità del dispositivo possono essere utilizzate e da quale utente. Inoltre Toshiba offre una serie di soluzioni di autenticazione e di output management avanzate, che semplificano uso e configurazione del controllo di accesso.
• Sicurezza dei documenti
– Per garantire che le informazioni riservate siano protette da accessi non autorizzati, Toshiba offre diverse soluzioni per darti un controllo avanzato sui tuoi documenti. Sia che creiate PDF protetti, archiviate i file in cartelle protette o usiate la funzione di stampa privata, potete essere certi che i vostri dati saranno sempre al sicuro.
• Sicurezza dei dispositivi
– I sistemi Toshiba e-BRIDGE possono essere protetti dagli attacchi informatici proprio come qualsiasi altro dispositivo di una rete IT. Il protocollo SSL utilizza la crittografia per proteggere tutti i dati che viaggiano da e verso gli MFP, mentre il filtro IP funge da firewall per proteggere la rete interna dagli intrusi. Inoltre la funzionalità di firma SMB aggiunge una firma digitale per verificare che i dati vengano ricevuti da fonti autenticate e assicura l'integrità di tutte le comunicazioni.
.

7 PERCHE' TOSHIBA

Invece, per monitorare tutti i dispositivi presenti in azienda, Toshiba ha sviluppato una piattaforma cloud, che consente di gestire da remoto i sistemi e-STUDIO e raccogliere in modo sicuro e affidabile i dati operativi trasmessi dalle MFP utilizzando una connessione HTTPS/SSL.
Questo tool proprietario fornisce un'analisi approfondita delle loro prestazioni: gli avvisi tecnici in tempo reale consentono di risolvere i problemi in modo proattivo; inoltre, l'esecuzione sicura di varie operazioni quali la lettura dei contatori e l'aggiornamento del firmware da remoto, contribuiscono a ridurre al minimo i tempi di fermo macchina.

SUPPORTO FLESSIBILE PER LA SICUREZZA
Gli MFP Toshiba offrono la funzionalità e-BRIDGE e supportano il protocollo HTTPS. e-BRIDGE CloudConnect garantisce la gestione sicura dei dati, quali lo stato operativo del dispositivo. L'applicazione supporta firewall, server proxy e varie configurazioni e autenticazioni, garantendo un supporto flessibile per le policy di sicurezza.

e-BRIDGE CloudConnect gestisce solo le informazioni riguardanti lo stato operativo del dispositivo. Queste includono i dati riferiti ad addebiti e manutenzione, come ad esempio i dati dei contatori (numero di fogli usati, ecc.), le informazioni su guasti e sostituzioni dei consumabili, e le impostazioni e regolazioni del dispositivo.

Poiché e-BRIDGE CloudConnect non gestisce i dati dei documenti, non esiste alcun rischio di divulgazione delle informazioni contenute in copie, fax, stampe e scansioni.
Utilizzando gli stessi principi adottati dai PC client, e-BRIDGE CloudConnect accede ai dati protetti tramite browser con HTTPS (autenticazione e crittografia del server). I dati possono essere inviati solo dagli MFP e l'accesso è limitato ai server e-BRIDGE CloudConnect con certificati di autenticazione validi.
Ciò garantisce un'eccellente sicurezza.

Il futuro è adesso.

Non importa in quale settore lavoriate, vale la stessa regola: digitalizzare e automatizzare processi quando possibile.

Cogliete l'opportunità di iniziare ad aumentare i margini della vostra azienda, ora e in futuro. Iniziate la vostra strategia digitale, non solo per superare i colli di bottiglia nei processi della vostra azienda, ma per snellire l'intero flusso di informazioni.

Contattaci!

Toshiba Tec Italia Imaging Systems S.p.A.

Telefono
+39 039 6241711

Email
info@toshibatec-tiis.com

Sito Web
www.toshibatec.i t