YSOFT SAFEQ®

PROTEZIONE DELL'AMBIENTE DEI FLUSSI DI LAVORO AZIENDALI

INTRODUZIONE

Siamo circondati dai dati e ogni giorno ne creiamo più di 2,5 quintilioni di byte[1]. Gli strumenti per la protezione dei dati si stanno sviluppando rapidamente ma anche i pirati informatici stanno aumentando di pari passo le loro conoscenze. La rete di dispositivi connessi e dispositivi IoT (Internet of Things) in rapida espansione, unita ai Big Data ha creato un'esplosione di dati che si avviano a diventare la nuova moneta.

Le notizie sulla violazione dei dati occupano spesso le prime pagine dei giornali, ma è necessario tenere in considerazione anche la sicurezza delle informazioni private nell'infrastruttura dei flussi di lavoro aziendali. Nell'Unione Europea, il regolamento generale sulla protezione dei dati (General Data Protection Regulation) è un documento legislativo completo che disciplina l'utilizzo e la protezione dei dati individuali. Per determinate violazioni prevede una sanzione pecuniaria elevata fino a 20 milioni di euro o il 4% del fatturato totale annuo mondiale dell'azienda, a seconda di quale sia l'importo più elevato dei due. Il regolamento si applica anche alle violazioni che si verificano all'interno dell'infrastruttura dei flussi di lavoro aziendali di una società

Questo documento illustra i fattori più importanti da tenere presenti quando si tratta di proteggere i dati nell'ambiente dei flussi di lavoro di stampa, copia e scansione. Esamina inoltre più da vicino il prodotto YSoft SafeQ 6, che è stato appositamente progettato per supportare le misure di sicurezza e aumentare la protezione dei dati all'interno di una soluzione completa e sicura per i flussi di lavoro aziendali.

[1] IBM, Ten Key Marketing Trends

Per ulteriori informazioni su YSoft SafeQ e il GDPR, consultare la Guida alla conformità al GDPR per YSOFT SAFEQ 6

SOLUZIONI PER I FLUSSI DI LAVORO AZIENDALI

SICUREZZA DEI FLUSSI DI LAVORO AZIENDALI - RUOLO CHIAVE DEI DISPOSITIVI MULTIFUNZIONE

Secondo Quocirca, nel 2013 il 63% delle organizzazioni ha subito almeno una violazione della sicurezza tramite la stampa. Ciononostante, uno studio del 2015 del Ponemon Institute[2] dimostra che le strategie di protezione del 56% delle organizzazioni non tengono conto delle stampanti e dei dispositivi multifunzione rendendoli l'anello debole dell'infrastruttura IT. I dispositivi multifunzione sono diventati parte integrante delle attrezzature da ufficio contribuendo a migliorare la produttività e aumentare le comodità di un grande numero di organizzazioni. Poiché tuttavia quasi i tutti i dispositivi multifunzione si trovano in una rete con protocollo IP (Internet Protocol) che offre funzionalità di connessione e accessibilità avanzate, il rischio potenziale per la sicurezza aumenta. Un esempio di questo aspetto può essere un dispositivo multifunzione che supporta i protocolli di rilevamento automatico come Web Services Dynamic Discovery (WS-Discovery) o Universal Plug and Play (UPnP) e segnala l'esistenza del dispositivo multifunzione come un punto di ingresso aperto per la rete. Senza la protezione adeguata, il dispositivo multifunzione può consentire l'accesso non autorizzato alla rete mettendo a rischio i dati aziendali e quelli dei clienti. L'implementazione di un'infrastruttura dei flussi di lavoro aziendali protetta è un aspetto critico per tutte le organizzazioni che intendono chiudere le falle nel sistema di sicurezza.

[2] Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", marzo 2015

SOLUZIONI PER I FLUSSI DI LAVORO AZIENDALI E DISPOSITIVI MULTIFUNZIONE - UN LEGAME IMPRESCINDIBILE

Poiché le soluzioni per i flussi di lavoro aziendali, incluso YSoft SafeQ, sono in genere incorporate nei dispositivi multifunzione e comunicano con sistemi di terze parti, è necessario tenere in considerazione la sicurezza dell'intero sistema. È quindi importante una stretta collaborazione tra il provider della soluzione aziendale, il provider di servizi del dispositivo multifunzione e il reparto IT dell'organizzazione.

Quelle seguenti sono le sei aree chiave per la sicurezza della connessione tra l'infrastruttura dei flussi di lavoro aziendali e il dispositivo multifunzione.

1. ACCESSO AL DISPOSITIVO E ALLA RETE

L'accesso non autorizzato o aperto a un dispositivo multifunzione crea una potenziale violazione della sicurezza all'interno di un'organizzazione. Il modulo Autenticazione di YSoft SafeQ consente di rimuovere il rischio dell'accesso non autorizzato perché il dispositivo multifunzione rimane bloccato finché l'identità del dipendente non viene verificata correttamente. L'autenticazione dell'utente può essere eseguita tramite smart card di identificazione, codice PIN, password di accesso oppure una combinazione di diversi metodi di autenticazione verificati in base a quelli di una directory aziendale esterna al sistema YSoft SafeQ.

Questo metodo di autenticazione consente di eliminare i documenti stampati lasciati nel vassoio di stampa perché i processi di stampa non vengono elaborati finché l'utente non esegue correttamente l'autenticazione al dispositivo multifunzione. È importante tenere presente che quando viene utilizzata l'autenticazione tramite password, la password viene crittografata prima di essere inviata per la verifica nel server e viene archiviato solo l'hash della password oppure l'autenticazione viene delegata a un server Active Directory. Nessuna password viene archiviata nel dispositivo multifunzione e le credenziali del dominio di Active Directory non vengono mai memorizzate né nel dispositivo multifunzione né in YSoft SafeQ.

Gli amministratori possono inoltre diminuire il rischio potenziale determinato nelle proprie reti dai dispositivi multifunzione monitorando e analizzando il traffico in entrata. Le attività di stampa per il dispositivo multifunzione devono provenire solo da YSoft SafeQ. Tutto l'altro traffico può essere bloccato limitando così gli attacchi al dispositivo multifunzione da altre reti.

L'applicazione mobile di YSoft SafeQ (Mobile Terminal) offre un altro metodo per eseguire l'autenticazione in un dispositivo multifunzione. Gli utenti possono identificare una stampante di rete eseguendo la scansione del codice QR, del tag NFC o del beacon. L'applicazione mobile utilizza un collegamento di attivazione monouso, che viene inviato all'indirizzo e-mail dell'utente quando si connette a YSoft SafeQ per la prima volta.

Dopo l'attivazione, viene generato un token di Mobile Terminal specifico dell'utente che viene quindi usato per eseguirne l'autenticazione. Questa procedura consente di proteggere le credenziali del dominio dagli utenti malintenzionati sostituendo il codice QR, il tag NFC e il beacon che non devono essere immessi nell'applicazione. Le comunicazioni tra Mobile Terminal e il server YSoft SafeQ sono crittografate.

2. STAMPA PULL PROTETTA

La possibilità di inviare un processo di stampa e stamparlo da un dispositivo multifunzione qualsiasi dell'organizzazione (all'interno dello stesso edificio o dall'altra parte del mondo) migliora la comunicazione e la produttività. Ciò contribuisce ovviamente ad aumentare il volume dei dati trasferiti nella rete. È quindi vitale che la soluzione per i flussi di lavoro aziendali protegga i dati consentendo inoltre ai dipendenti di eseguire le proprie attività in modo migliore. Grazie alla stampa pull, è inoltre possibile diminuire l'eventualità che documenti riservati vengano lasciati nel vassoio di stampa. La funzionalità di stampa pull di YSoft SafeQ, denominata Print Roaming®, consente di eseguire una stampa da qualsiasi dispositivo multifunzione o stampante in rete all'interno dell'infrastruttura di stampa, ma solo dopo che il destinatario autorizzato ha effettuato l'autenticazione al dispositivo multifunzione.

La funzionalità Print Roaming di YSoft SafeQ può essere strutturata come Near Roaming, Far Roaming o entrambi in base all'infrastruttura dell'organizzazione:

Near Roaming: quando un processo di stampa viene inviato a YSoft SafeQ in un server locale, i dati passano dalla workstation dell'utente direttamente a YSoft SafeQ tramite una comunicazione crittografata.

Far Roaming: quando un processo di stampa viene inviato dalla workstation dell'utente a YSoft SafeQ in un server locale ma viene stampato da un dispositivo multifunzione in una posizione remota, la comunicazione può passare attraverso un server nella posizione remota. In questo caso, i dati del processo di stampa passano tra il server locale e quello remoto tramite una comunicazione crittografata.

3. STAMPA MOBILE PROTETTA

I dipendenti sono sempre più mobili e gli strumenti e i dispositivi utilizzati cambiano rapidamente e non sempre sono sicuri. La necessità di poter stampare da qualsiasi dispositivo e di utilizzare la funzionalità Bring Your Own Device (BYOD) ha contribuito ad aumentare la flessibilità a discapito della sicurezza. Ora i dipendenti possono connettere facilmente i propri smartphone, tablet e laptop alla rete di stampa approfittando di funzionalità utili ed efficienti per le organizzazioni, che però creano nuovi punti di ingresso per le potenziali minacce.

Il modulo Stampa mobile protetta di YSoft SafeQ consente a dipendenti e ospiti di stampare da qualsiasi dispositivo mobile in modo sicuro supportando la flessibilità del BYOD senza la necessità di un supporto complicato e un'implementazione IT. Unito al modulo Autenticazione, il modulo Stampa mobile consente alle organizzazioni di supportare interamente le esigenze di stampa dei dipendenti che usano dispositivi mobili garantendo la sicurezza dei documenti, l'accesso limitato e il risparmio sui costi.

Il modulo Stampa mobile offre due opzioni per l'invio dei dati di stampa al server YSoft SafeQ. Un utente può connettersi a un'interfaccia Web e, dopo la verifica dell'identità, caricare il documento o utilizzare l'integrazione e-mail, per cui il server e-mail effettua il pull di un allegato e-mail tramite il protocollo POP3 o IMAP. Per entrambe le opzioni è possibile utilizzare la crittografia SSL/TLS.

Un altro modo per inviare i dati del processo al server YSoft SafeQ è tramite il componente Mobile Integration Gateway di Y Soft, che consente di inviare processi dai dispositivi iOS e Android tramite il protocollo IPPSSL.

4. REPORT E MONITORAGGIO DELL'UTILIZZO

In tutte le organizzazioni i dipendenti hanno inevitabilmente accesso alle informazioni riservate. Per evitare potenziali rischi di sicurezza, le organizzazioni devono poter identificare e monitorare chi utilizza il dispositivo multifunzione, ciò di cui viene eseguita la copia, la scansione o la stampa, quando e dove. La raccolta di tali informazioni dai metadati in un report consente di individuare potenziali utilizzi impropri del dispositivo multifunzione, ad esempio la stampa o la scansione di documenti riservati che esulano dall'ambito di competenza dei dipendenti. Il modulo Creazione report di YSoft SafeQ offre agli amministratori la possibilità di creare report sugli accessi ai terminali contenenti informazioni sulle operazioni eseguite nei dispositivi multifunzione per fare in modo che l'ambiente sia protetto e gli utenti rispettino i criteri di utilizzo interni.

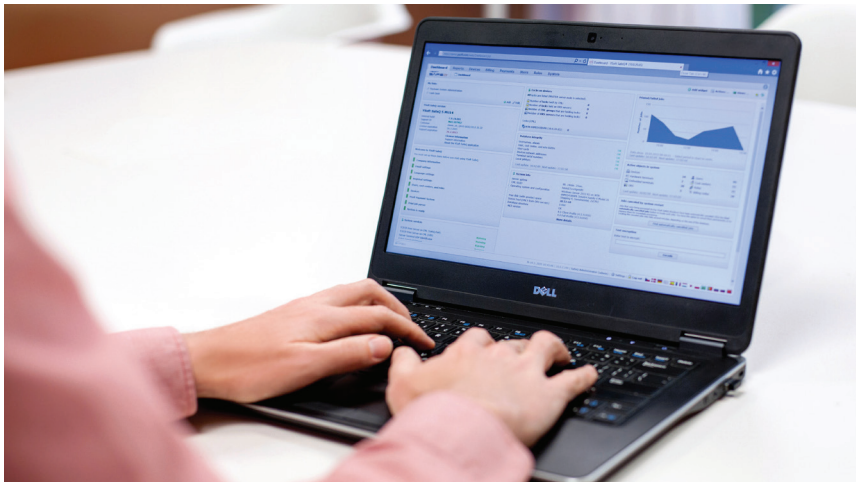
5. SICUREZZA DEL DISCO RIGIDO DEL DISPOSITIVO MULTIFUNZIONE

Tutte le organizzazioni dovrebbero sempre definire, con il provider di servizi dei dispositivi multifunzione, determinati criteri per la protezione dei dischi rigidi dei dispositivi durante le operazioni quotidiane e la manutenzione o quando vengono disattivati. Con YSoft SafeQ, nessun dato relativo a copie o stampe viene archiviato in modo permanente nel disco rigido del dispositivo multifunzione. I flussi di lavoro di scansione, o che prevedono l'invio della scansione a un'e-mail, possono archiviare temporaneamente i dati necessari per creare le scansioni digitali ma tali dati vengono immediatamente cancellati al termine del flusso di lavoro.

6. CRITTOGRAFIA DEI DATI

Qualsiasi dispositivo che invia o riceve dati rappresenta una potenziale minaccia per la sicurezza. Per ovviare a questo problema, i dati devono essere crittografati e firmati digitalmente e le parti che comunicano devono essere sottoposte ad autenticazione per proteggere la riservatezza delle informazioni trasferite e garantire l'integrità della comunicazione. I clienti che dispongono di un'infrastruttura a chiave pubblica (KPI) possono utilizzarla con YSoft SafeQ per garantire l'autenticazione reciproca dei dispositivi multifunzione e dei server SafeQ.

La sezione seguente include dettagli aggiuntivi sulle comunicazioni all'interno di YSoft SafeQ e tra YSoft SafeQ e gli altri sistemi.



YSOFT SAFEQ, SICUREZZA DA PROGETTAZIONE

Come indicato in precedenza, stiamo assistendo a un'esplosione di dati insieme alla diffusione di metodi di accesso non autorizzato sempre più sofisticati. Garantire la sicurezza dei dati nella rete di dispositivi sta diventando un'operazione sempre più complessa, ma fondamentale per soddisfare le esigenze delle organizzazioni che cercano flussi di lavoro e funzionalità per migliorare la produttività. Il passaggio di dati tra dispositivi, server e sistemi e il dispositivo multifunzione determina il trasferimento di grandi quantità di informazioni tramite i percorsi di comunicazione. YSoft SafeQ protegge questi dati mediante comunicazioni crittografate. Per i percorsi di comunicazione vengono utilizzate implementazioni di crittografia standard aperte (non proprietarie). Se tali implementazioni non sono disponibili, vengono comunque utilizzate implementazioni standard aperte degli algoritmi di sicurezza.

In YSoft SafeQ sono disponibili otto percorsi di comunicazione crittografati principali: Figura 1.

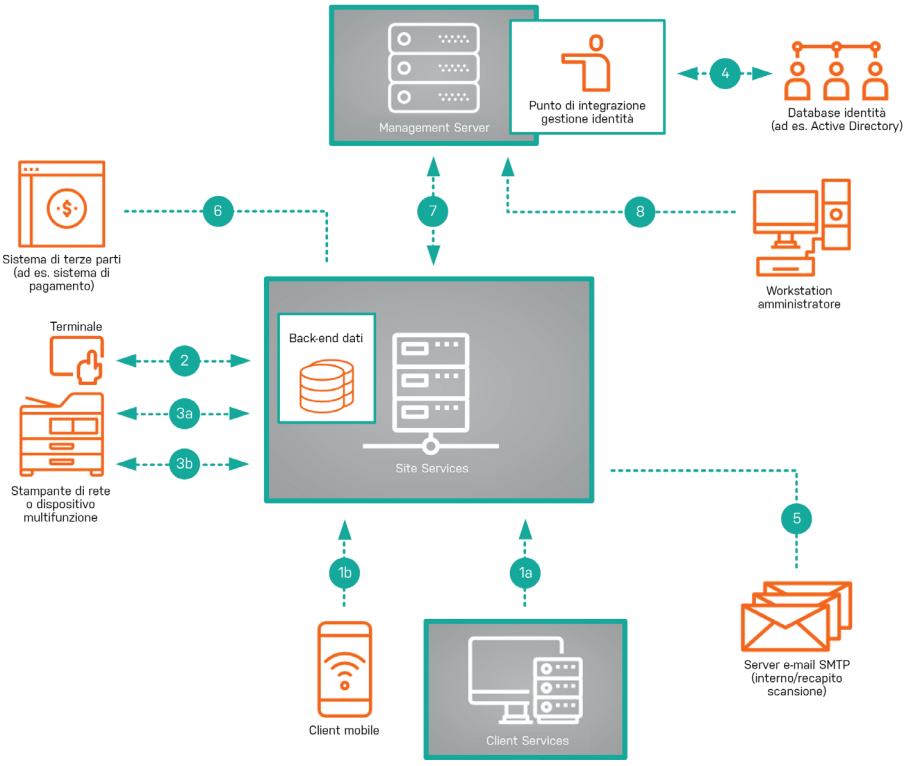


Figura 1.
Percorsi di comunicazione di YSoft SafeQ

1. Stampa - Comunicazione da YSoft SafeQ quando:
   a. Un processo di stampa viene inviato da una workstation client
   b. Un processo viene inviato da un client mobile

2. Autenticazione del dispositivo multifunzione - Comunicazione dal terminale/lettore del dispositivo multifunzione a YSoft SafeQ per la verifica delle credenziali di accesso di un utente

3. Comunicazione da YSoft SafeQ al dispositivo multifunzione in rete:
   a. Processo di stampa gestito con la stampa pull
   b. Verifica dell'autenticazione, autorizzazione e contabilizzazione

4. Integrazione con il database di gestione delle identità o il provider di identità/autenticazione

5. Connessione da YSoft SafeQ a un server e-mail SMTP o una cartella di rete condivisa per il recapito dei dati delle scansioni digitali

6. Integrazione con applicazioni o sistemi di terze parti, ad esempio per il recapito delle scansioni digitali a un repository di documenti basato sul cloud

7. Comunicazione tra server. In base ai requisiti dell'organizzazione in termini di failover e ridondanza, è possibile che più livelli di Site Services o di Management Server si trovino in più posizioni remote. In questo caso, le comunicazioni tra i livelli nelle varie posizioni sono necessarie per l'elaborazione dei processi di stampa e il trasferimento dei metadati sui processi di stampa per la creazione di report.

8. Accesso dell'amministratore all'interfaccia di gestione di YSoft SafeQ

PROTEZIONE DEI DATI CON QUALSIASI STATO

I dati di stampa, copia e scansione possono avere tre stati, ovvero in uso, in transito e inattivi.

- **Dati in uso:** dati attivi che sono al momento utilizzati dall'applicazione e vengono archiviati solo nella memoria non persistente. Un documento da stampare sottoposto all'analisi di un dispositivo multifunzione è un esempio di dati in uso.

- **Dati in transito o in movimento:** dati in corso di trasferimento o spostamento all'esterno di un server da una posizione a un'altra. Un'e-mail in fase di invio da un flusso di lavoro di scansione automatico o dalla funzionalità di scansione a e-mail sono entrambi esempi di dati in movimento.

- **Dati inattivi:** dati inattivi archiviati in modo permanente. I metadati di un processo di stampa utilizzati per la creazione di report e archiviati in un database sono un esempio di dati inattivi. Un altro esempio è un ambiente multi-tenant in cui i dati dei vari tenant vengono archiviati in isolamento in un database di produzione e gli utenti che hanno accesso ai dati per la creazione di report non hanno accesso al database di produzione (e viceversa).

Garantire che protocolli di crittografia aggiornati vengano distribuiti correttamente è un aspetto fondamentale della protezione dei dati. È importante sottolineare che le minacce alla sicurezza rappresentano un problema costante per l'intera comunità IT. Il team che si occupa della sicurezza dei prodotti Y Soft tiene continuamente monitorati protocolli e algoritmi di crittografia e li aggiorna per fare in modo che YSoft SafeQ soddisfi sempre gli standard di sicurezza del settore. I membri del team continuano inoltre a seguire percorsi di formazione per riconoscere potenziali vulnerabilità e individuare procedure ottimali per la codifica sicura.

Il team esegue anche analisi dei modelli di minaccia e del codice statico conformemente alla metodologia Microsoft Security Development Lifecycle. Vengono identificate le minacce a livello di programmazione e implementazione e vengono applicate contromisure logiche per ridurre i rischi. La conoscenza specifica delle minacce consente di adottare un approccio strutturato nell'ambito della sicurezza. Misure di sicurezza concrete consentono di identificare i dati a rischio e proteggerli in modo appropriato in base alla loro importanza.

CRITTOGRAFIA INCORPORATA

La crittografia riveste un ruolo di primo piano per la sicurezza dei dati e va di pari passo con un firewall potente. Lo scopo della crittografia è quello di proteggere tutti i dati che hanno uno qualsiasi dei tre stati all'interno dell'intero sistema e in tutti i percorsi di comunicazione. Anche se la crittografia di per sé non può impedire la violazione della sicurezza, garantisce sicuramente un determinato livello di protezione. Se i dati dovessero finire nelle mani sbagliate sarebbero comunque inutilizzabili dato che sono crittografati. Se i dati in chiaro o il testo normale vengono crittografati con un algoritmo sicuro, solo gli utenti che dispongono della chiave di decrittografia possono leggere i dati. La crittografia non richiede alcun input da parte dell'utente perché viene eseguita in modo trasparente in background.
Sono disponibili due tipi principali di crittografia, simmetrica e asimmetrica, che nella pratica vengono spesso combinate sotto il nome di crittografia ibrida. La crittografia simmetrica prevede l'utilizzo della stessa chiave segreta sia per la crittografia sia per la decrittografia dei dati. La crittografia asimmetrica utilizza invece due chiavi diverse, ovvero una chiave privata, che viene tenuta segreta e usata per la firma e la decrittografia, e una chiave pubblica che viene condivisa liberamente e usata per la crittografia e la verifica della firma.

La lunghezza delle chiavi e i pacchetti di crittografia vengono scelti e aggiornati regolarmente in base alle vulnerabilità e agli attacchi noti. La velocità dei cambiamenti in questo ambito fa sì che gli algoritmi o le loro implementazioni possano diventare rapidamente obsoleti lasciando i dati senza protezione se il problema non viene gestito correttamente. È possibile stare al passo con gli sviluppi recenti seguendo i consigli di alcune organizzazioni importanti del settore come NIST, Mitre o Apache Foundation.

Ciascuno dei tre stati dei dati illustrati in precedenza rappresenta una sfida specifica in termini di sicurezza perché tutti i dati non protetti, indipendentemente dallo stato, offrono il fianco a possibili attacchi.

- **Dati in uso:** la crittografia non è una soluzione appropriata per proteggere i dati in uso perché devono essere disponibili per l'elaborazione. Ci sono tuttavia altri metodi per proteggere questo tipo di dati. In YSoft SafeQ è ad esempio possibile limitare l'accesso degli utenti, non archiviare inutilmente i dati riservati e utilizzare funzionalità come Autenticazione e Creazione report per supportare la sicurezza dei dati in uso.

- **Dati inattivi:** queste informazioni vengono inizialmente protette impostando correttamente i diritti di accesso, nonché utilizzando firewall e programmi antivirus, ma la crittografia del disco rigido può migliorare ulteriormente la sicurezza. Le aziende possono utilizzare Microsoft Encryption File System (EFS) per crittografare i dati inattivi prima dell'archiviazione oppure crittografare l'unità di archiviazione stessa. La crittografia a livello del sistema operativo può fornire un enclave sicuro per l'archiviazione delle chiavi di crittografia. EFS consente di crittografare in modo trasparente i file quando vengono archiviati utilizzando l'algoritmo AES (lo standard corrente per la crittografia simmetrica).

- **Dati in transito o in movimento:** i collegamenti di comunicazione con dati riservati vengono protetti mediante il protocollo TLS (Transport Layer Security) standard e più pacchetti di crittografia configurabili, ordinati in base al livello di sicurezza per ottenere la massima protezione e la possibilità di supportare allo stesso tempo i dispositivi legacy. TLS non solo assicura la riservatezza e l'integrità ma impedisce anche di ripetere il traffico acquisito in precedenza. Consente inoltre al reparto IT di aumentare facilmente la protezione modificando i valori della configurazione del pacchetto di crittografia nel caso di aggiornamenti alle procedure di sicurezza o quando i criteri di protezione dell'organizzazione cambiano, ad esempio se l'utilizzo di SHA-1 (Secure Hash Algorithm 1) non è più consigliato.

ESPERIENZA UTENTE SEMPLIFICATA

La protezione della propria organizzazione non è un'attività meramente burocratica. Integrare la protezione dei dati nella mentalità dell'azienda contribuisce ad avvalorarne l'importanza. È necessario affrontare la sfida posta dalla protezione dei dati e dalla prevenzione delle violazioni della sicurezza soprattutto considerando i continui cambiamenti introdotti dall'IoT, dal BYOD, dall'esplosione dei dati dai malware e dai dispositivi esterni.

Le estreme conseguenze che la violazione della sicurezza può comportare, contribuiscono ad inserire la protezione dei dati tra le sfide aziendali più importanti. La soluzione YSoft SafeQ consente di ridurre i rischi di sicurezza unendo la protezione dei documenti e della stampa al controllo degli accessi ai dispositivi. Gli utenti non devono eseguire altre operazioni oltre all'autenticazione nel dispositivo multifunzione. Il processo back-end non influisce in alcun modo sull'esperienza utente che rimane inalterata in termini di velocità delle operazioni, come quella dei servizi bancari online.

DOMANDE FREQUENTI

Dove vengono tenuti i dati durante l'elaborazione di processi di stampa, scansione e copia?

- **Processi di stampa:** quando si utilizza Print Roaming, i dati vengono tenuti a livello di Client Services e Management Server di YSoft SafeQ. Se si usa Client Based Print Roaming, il processo di stampa viene tenuto nella workstation client e solo i metadati del processo di stampa vengono comunicati a Client Services tramite il livello Management Server di YSoft SafeQ.

- **Invio della scansione a e-mail o al file system e flussi di lavoro di scansione automatici:** i dati vengono temporaneamente tenuti nel disco rigido del dispositivo multifunzione e vengono cancellati quando il processo viene completato. Se si utilizza la scansione a e-mail, l'e-mail inviata dal dispositivo multifunzione alla workstation può essere recapitata tramite la comunicazione crittografata. Per migliorare ulteriormente la sicurezza con la crittografia end-to-end, sono supportati anche i file PDF crittografati. Con i flussi di lavoro di scansione automatici, la scansione digitale viene recapitata a una posizione predefinita tramite la comunicazione crittografata.

- **Copia:** i dati vengono tenuti temporaneamente nel disco rigido del dispositivo multifunzione e vengono cancellati quando il processo viene completato.

YSoft SafeQ può fornire una prova dell'eliminazione dei dati nel disco rigido del dispositivo multifunzione?

Tutti i dati archiviati temporaneamente durante la scansione vengono immediatamente cancellati. Il provider di servizi del dispositivo multifunzione e l'organizzazione devono disporre di processi per la protezione del disco rigido del dispositivo multifunzione durante l'utilizzo e la manutenzione o quando viene disattivato. Tali processi includono l'eliminazione dei dati nel disco rigido. Si tenga tuttavia presente che il disco rigido del dispositivo multifunzione non fa parte dell'area di responsabilità di YSoft SafeQ.

YSoft SafeQ può garantire la conformità con i sistemi gateway di pagamento?

YSoft SafeQ non comunica con alcun sistema gateway di pagamento. Nel caso del modulo Credito e fatturazione di YSoft SafeQ o del dispositivo di pagamento, YSoft SafeQ riceve solo la notifica da parte dell'istituto finanziario che conferma che il pagamento e l'importo sono stati ricevuti.

YSoft SafeQ è in grado di integrare in modo sicuro i dati per la creazione di report nel portale Web del cliente?

I portali Web vengono in genere protetti tramite certificati firmati supportati da YSoft SafeQ. I dati per la creazione di report di YSoft SafeQ possono essere integrati con un portale Web per visualizzare i dati di stampa, copia e scansione.

Come è possibile crittografare i dati durante il loro ciclo di vita?
Se in YSoft SafeQ si utilizza il client di spooling, il protocollo IPP su TLS per la crittografia, l'autenticazione e l'integrità dei dati trasferiti al dispositivo multifunzione, i dati lasciano la workstation solo quando il processo viene rilasciato. La funzionalità Print Roaming basata su server può inoltre inviare i dati dalla workstation al server YSoft SafeQ tramite un canale HTTPS. Lo stesso succede per il trasferimento dei dati di stampa tra i server quando la funzionalità Far Roaming è attivata. Quando i dati sono inattivi nel server, è possibile utilizzare Microsoft EFS standard per proteggere i dati di stampa.

Un'organizzazione può vedere i documenti stampati dai dipendenti?
Se si utilizza Print Roaming, un amministratore che dispone dell'accesso al file system, può vedere i flussi di stampa relativi a tutti i processi che si trovano a livello di YSoft SafeQ Management Server, ovvero i processi che devono essere stampati, quelli già stampati e quelli contrassegnati come preferiti. È tuttavia possibile configurare YSoft SafeQ in modo che elimini automaticamente i processi di stampa dopo la stampa. Se YSoft SafeQ è in esecuzione con un account del servizio nominativo e utilizza Microsoft EFS, l'amministratore deve conoscere la password dell'account del servizio per vedere i processi. Tutte le attività eseguite con l'account del servizio nominativo vengono registrate nei log di controllo di Windows. Microsoft EFS consente inoltre di abilitare la separazione dei compiti, per cui all'interno di una stessa azienda alcuni amministratori gestiscono server e applicazioni ma non possono accedere ai dati dei processi di stampa mentre altri amministratori dispongono delle autorizzazioni di sicurezza per accedere ai dati dei processi di stampa.

Quando si utilizza Client Based Print Roaming, vengono acquisiti solo i metadati del processo di stampa. Per vedere il processo effettivo, è necessario accedere alla workstation.

Gli utenti possono vedere quali documenti sono stati stampati dagli altri?
No.

In che modo YSoft SafeQ consente alle organizzazioni di rispettare le norme del GDPR?
Informazioni dettagliate sono disponibili nella Guida alla conformità al GDPR per YSOFT SAFEQ 6.

In breve, YSoft SafeQ consente agli amministratori di gestire i diritti degli utenti relativi ai loro dati personali in possesso dell'organizzazione (Diritto di accesso), correggere i dati (Diritto alla rettifica), impedire l'elaborazione dei dati (Diritto alla limitazione dell'elaborazione) e cancellare i dati (Diritto all'oblio).

Un utente può richiedere la cancellazione dei dati che lo identificano personalmente dal sistema YSoft SafeQ ma rimanere anonimo per scopi di reporting?
Sì. Una query di eliminazione consente di rimuovere i dati di un utente dal sistema YSoft SafeQ senza rimuovere i dettagli relativi alla stampa che possono quindi essere utilizzati per scopi di reporting. Nel report l'utente verrà semplicemente visualizzato come anonimo.