Un approccio globale alla sicurezza dei dispositivi di stampa

Stampanti e sistemi multifunzione sono ora il cuore pulsante delle vostre attività aziendali. Con la crescita esponenziale di dispositivi wireless e di servizi e software basati su cloud, la vostra stampante non solo deve interagire con queste tecnologie, ma deve anche essere in grado di proteggersi da esse.

Prevenire

Rilevare

Proteggere

Parnership Esterne

PREVENIRE

Il primo e più ovvio punto di vulnerabilità è l'interfaccia utente e il controllo di chi ha accesso fisico alla vostra stampante e alle sue funzionalità. Le misure di sicurezza Xerox iniziano con la funzionalità di **Autenticazione utente** per garantire che solo il personale autorizzato possa accedere al dispositivo. Una volta eseguito l'accesso, la funzione di **Controllo dell'accesso basato sul ruolo** garantisce che ciascun componente del team veda solo le funzioni a cui è autorizzato. Ogni azione eseguita da ciascun utente viene inoltre registrata, in modo da offrire un Registro di **controllo** completo.

A questo punto ci occupiamo dei punti di vulnerabilità meno ovvi: tutto ciò che viene inviato alla stampante e il modo in cui viene inviato. La tecnologia Xerox® ConnectKey® intercetta gli attacchi provenienti da file infetti e software dannoso.[1] Il nostro software di sistema è dotato di **firma digitale**, il che significa che qualsiasi tentativo di installare versioni infette o non firmate comporterà il blocco automatico del file. I file di stampa vengono inoltre eliminati se una loro qualsiasi parte non viene riconosciuta come legittima.

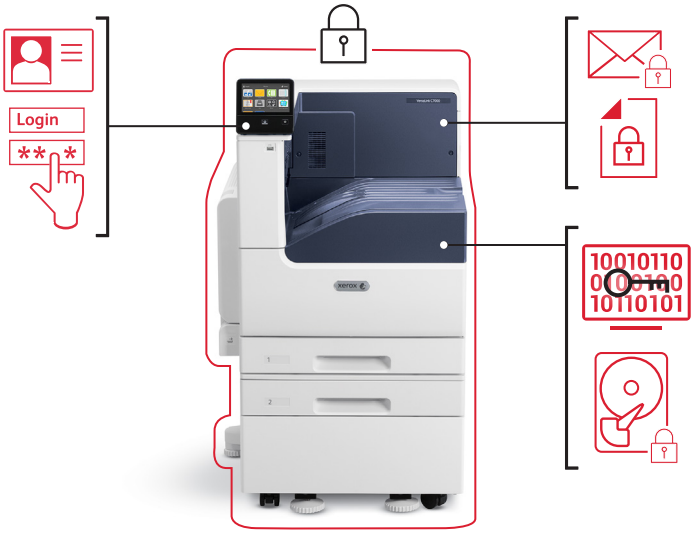
PROTEZIONE OLISTICA PER LA VOSTRA STAMPANTE

Xerox ha da tempo riconosciuto e accettato questo cambiamento nella tecnologia e nelle esigenze in continua evoluzione del mondo del lavoro. Offriamo una serie completa di funzioni di protezione per garantire la sicurezza di dispositivi e dati. Xerox protegge ogni singolo anello della catena di dati: **stampa, copia, scansione, fax, download di file** e **software di sistema**. Il nostro approccio multilivello si basa su quattro aspetti chiave.

xerox™

RILEVARE

Nel caso improbabile che le difese dei dati e della rete vengano superate, la tecnologia Xerox® ConnectKey® eseguirà un test completo di **verifica del firmware**, all'avvio[2] o su attivazione da parte di utenti autorizzati. L'utente riceve un avviso qualora vengano rilevate modifiche dannose alla stampante. Le nostre più avanzate soluzioni integrate utilizzano la tecnologia **Whitelisting di McAfee®**[3] che assicura un continuo monitoraggio e impedisce automaticamente l'esecuzione di qualsiasi malware dannoso. L'integrazione con **Cisco® Identity Services Engine (ISE)** consente di rilevare automaticamente i dispositivi Xerox® sulla rete e di classificarli come stampanti per finalità di implementazione della politica di sicurezza e conformità. Interagendo con le piattaforme leader del mercato McAfee® DXL e Cisco® pxGrid, i sistemi multifunzione Xerox adottano una risposta orchestrata che neutralizza le minacce all'origine nel momento in cui si verificano.



PROTEGGERE

Noi di Xerox curiamo ogni dettaglio. Le nostre soluzioni di sicurezza complete proteggono anche i documenti stampati e scansiti, impedendone la divulgazione o le modifiche non autorizzate. La tecnologia Xerox® ConnectKey contribuisce a bloccare il trasferimento deliberato o accidentale di dati riservati a tutti coloro che non sono autorizzati a riceverli.

Proteggiamo l'output di stampa utilizzando un **CODICE Pin** o un sistema di rilascio tramite **scheda/carta**. Impediamo che i documenti scansiti giungano ai destinatari sbagliati, grazie all'utilizzo di **formati** file con **firma digitale, crittografati e protetti da password**. I dispositivi abilitati alla tecnologia ConnectKey consentono inoltre di **bloccare i campi "A/Cc/Ccn"** delle e-mail, limitando le destinazioni di scansione a **indirizzi interni**.

Xerox protegge inoltre tutte le informazioni archiviate, utilizzando i più sofisticati livelli di **crittografia**. Eliminiamo tutti i dati elaborati o archiviati che non servono più utilizzando gli **algoritmi di cancellazione dati**[4] approvati dal National Institute of Standards and Technology (NIST) e dal Dipartimento della Difesa statunitense.

PARTNERSHIP ESTERNE

Collaboriamo con aziende di test di conformità e leader del settore della sicurezza come ad esempio **McAfee** e **Cisco** per integrare nei propri sistemi i loro standard globali e il loro know-how.

Come prova indipendente di terzi che otteniamo i migliori livelli di conformità, organismi di certificazione come **Common Criteria (ISO/ IEC 15408)** e **FIPS 140-2** misurano le nostre prestazioni sulla base di standard internazionali e certificano il nostro approccio globale alla sicurezza dei dispositivi.

ISO/IEC 15408 COMMON CRITERIA	**CONVALIDA** FIPS 140-2

Le aziende e i governi maggiormente sensibili al tema della sicurezza scelgono Xerox.

- 10/10 delle principali banche internazionali
- 10/10 delle maggiori università
- Tutti e 50 i governi statali degli Stati Uniti

[1] Intercettazione di malware con la tecnologia Whitelisting di McAfee®
[2] Stampanti Xerox® VersaLink®
[3] Multifunzione Xerox® AltaLink®, Multifunzione Xerox® WorkCentre® i-Series e Multifunzione Xerox® WorkCentre EC7836/EC7856
[4] Solo per i dispositivi con disco rigido

Ulteriori informazioni: **www.xerox.com/SecuritySolutions**

9/19 PN03659 BR27139 XOGFS-62IC