Xerox e la sicurezza delle informazioni

I vostri dati, la vostra attività:
Collaborare per proteggere
ciò che è più importante

Sommario

Panoramica

Le informazioni sono la risorsa chiave di ogni azienda, e la sicurezza è fondamentale in ufficio: sicurezza dei documenti e di tutti i dispositivi, stampanti e multifunzione compresi, connessi alla rete. E nel ventunesimo secolo, la rete rappresenta il crocevia di ogni attività aziendale.

Pressoché ogni azienda, e tutto il personale che la compone, è connessa a Internet. La vostra azienda – e ogni organizzazione con la quale collaborate – fa parte di un sistema globale di reti informatiche e server interconnessi utilizzati contemporaneamente da un numero infinito di utenti che svolgono attività, ricevono e trasmettono informazioni, acquistano e vendono prodotti e servizi e comunicano via email, SMS, Skype™, Twitter e molti altri servizi.

La minaccia alla sicurezza è estremamente reale ed i rischi stanno aumentando a velocità esponenziale. Una violazione della riservatezza dei documenti di un'azienda può tramutarsi nell'acquisizione o nell'utilizzo non autorizzato di informazioni confidenziali o proprietarie. Può comportare la divulgazione, il furto o la compromissione di proprietà intellettuale e segreti commerciali. E per molte organizzazioni, tali violazioni della sicurezza possono sfociare in penali e contenziosi legali estremamente costosi, a volte anche nell'ordine di centinaia di migliaia o addirittura milioni di euro.

Le crescenti minacce alla sicurezza assumono varie forme e diversi livelli di gravità. L'esplosiva proliferazione dei dispositivi di rete si traduce in un numero sempre crescente di punti di ingresso potenzialmente vulnerabili ad attacchi fraudolenti. E la minaccia degli "hacker" è costante, con programmi attivi 24 ore al giorno 7 giorni su 7, alla costante ricerca di possibili falle nei sistemi di sicurezza della rete.

Le minacce alla sicurezza vanno dai relativamente innocui messaggi di spam a minacce sofisticate che possono mettere fuori gioco intere reti.

Alla luce di un'attività sul web oramai ininterrotta, è fondamentale assicurarsi che le informazioni riservate della propria azienda siano al sicuro. Ma le esigenze cambiano, e cambiano di giorno in giorno.

Le stampanti e i multifunzione di rete in grado di stampare, copiare, scansire su destinazioni di rete, inviare allegati email e gestire trasmissioni fax in entrata e in uscita sono particolarmente vulnerabili.

Chi si occupa di sicurezza informatica sa bene quanto sia fondamentale per la sicurezza di una rete aziendale mettere al riparo dalle violazioni della sicurezza stampanti e multifunzione connessi alla rete, come anche i dispositivi indipendenti. Dopo tutto, gli attacchi possono verificarsi nei modi più imprevedibili:

- La linea telefonica collegata a un multifunzione potrebbe essere utilizzata per accedere alla rete.
- Il server web utilizzato per gestire multifunzione e stampanti potrebbe essere vulnerabili agli attacchi.
- Dati elettronici non protetti archiviati sul disco rigido o in trasferimento sul/dal dispositivo potrebbero essere violati.
- Email fraudolente possono essere inviate a un multifunzione privo di registro di controllo.

Stampanti e multifunzione sono sofisticate piattaforme IT dotate di molteplici sottosistemi, e pertanto per essere efficaci le misure di sicurezza devono abbracciare ogni singolo elemento della piattaforma.

Stampanti e multifunzione del giorno d'oggi sono ben diversi dai PC e i server di un tempo:

- Sono dispositivi condivisi tra svariati utenti e più amministratori.
- Stampanti e multifunzione sono dispositivi integrati:
  - Potrebbero essere dotati di un vero e proprio sistema operativo.
  - Il sistema operativo potrebbe avere un'interfaccia esterna diretta.
  - Il sistema operativo potrebbe essere proprietario.
  - Il sistema operativo potrebbe essere Microsoft® Windows®.

Panoramica

- Stampanti e multifunzione presentano le seguenti caratteristiche, che di norma sono tutte associate a nodi informatici più avanzati:
  - Stack di protocolli di rete
  - Funzionalità di autenticazione e autorizzazione
  - Crittografia
  - Gestione del dispositivo
  - Server web

L'eterogeneità delle implementazioni di stampanti e multifunzione pone dei problemi.

- Molto più diversificate rispetto ai PC tradizionali
- Alto livello di diversità per quanto riguarda i sistemi operativi di produttori diversi e finanche tra linee di prodotti diversi dello stesso produttore

I controlli di PC e server tradizionali non sono ottimizzati per le stampanti e i multifunzione.

- Approccio agli anti-virus
  - Potrebbero non essere disponibili per il tipo di sistema operativo installato sulla stampante o sul multifunzione
  - In generale, la guerra contro i malware è comunque persa in partenza
  - Complessità di gestione degli aggiornamenti di file di dati in un ambiente distribuito
- Gestione problematica di stampanti e multifunzione
  - Il controllo della versione software di stampanti e multifunzione non è uniforme
  - La gestione della configurazione genera costi di esercizio
- Security Information and Event Management (SIEM)
  - Avvisi e notifiche di stampanti e multifunzione non sono uniformi
  - L'attività di rettifica di stampanti e multifunzione non è standardizzata

La situazione è completamente diversa rispetto alle stampanti e copiatrici di ieri.

Chiunque può lanciare attacchi contro una rete e le risorse informatiche di un'azienda se l'accesso fisico ed elettronico a una stampante o un multifunzione non viene adeguatamente controllato e protetto. Tali attacchi possono essere semplici, come l'appropriarsi di documenti lasciati nel vassoio di uscita della stampante/multifunzione, oppure sofisticati come worm che cancellano documenti sensibili dalla rete.

L'intero sistema di una stampante/multifunzione, nonché tutto il software di gestione dei dispositivi operante in rete, deve essere verificato e certificato di modo che il reparto Sicurezza informatica e tutti i dipendenti di un'azienda siano certi che i loro documenti e la loro rete sono sicuri e protetti sia dai pirati informatici che da violazioni della sicurezza interne.

Sotto tale aspetto, non tutte le stampanti e i multifunzione sono uguali. Pertanto, un approccio globale, basato su un sistema di sicurezza solido, funzionale, avanzato e utilizzabile, è essenziale per la salvaguardia delle risorse informatiche delle aziende di oggi.

Per fortuna, nel campo della sicurezza Xerox ha le competenze necessarie per aiutarvi. Da 20 anni Xerox è l'azienda leader nella fornitura di soluzioni documentali sicure ad aziende di svariati settori in tutto il mondo. Ogni prodotto e servizio Xerox® offerto è progettato per garantire la massima sicurezza e integrarsi facilmente nei sistemi di sicurezza esistenti. Inoltre, la sicurezza viene gestita lungo tutto il ciclo di vita del prodotto: dall'analisi delle esigenze alla progettazione, sviluppo, produzione, distribuzione e smaltimento. Il tutto per offrire a voi e ai vostri clienti massima protezione e la più totale tranquillità.

Xerox vi aiuta a proteggere i vostri dati in ogni potenziale punto di vulnerabilità, liberandovi dall'onere di doverci pensare voi. Focalizzandoci su ciò che sappiamo fare meglio, consentiamo a voi di focalizzarvi su ciò che sapete fare meglio.

Obiettivi di sicurezza di Xerox

Nel nostro sforzo di fornire soluzioni sicure a tutti i nostri clienti, abbiamo individuato cinque obiettivi di sicurezza principali:

RISERVATEZZA

- Nessuna divulgazione non autorizzata di dati in fase di elaborazione, trasmissione o archiviazione

INTEGRITÀ

- Nessuna alterazione non autorizzata dei dati
- Il sistema funziona esattamente come previsto, al sicuro da manipolazioni non autorizzate

DISPONIBILITÀ

- Il sistema funziona perfettamente
- Nessun rifiuto di servizio agli utenti autorizzati
- Protezione contro l'utilizzo non autorizzato del sistema

RESPONSABILITÀ

- L'uso delle apparecchiature è monitorato ed è possibile verificare l'attività di ogni utente

NON-RIPUDIO

- Garanzia reciproca circa il mantenimento di autenticità e integrità delle comunicazioni di rete.

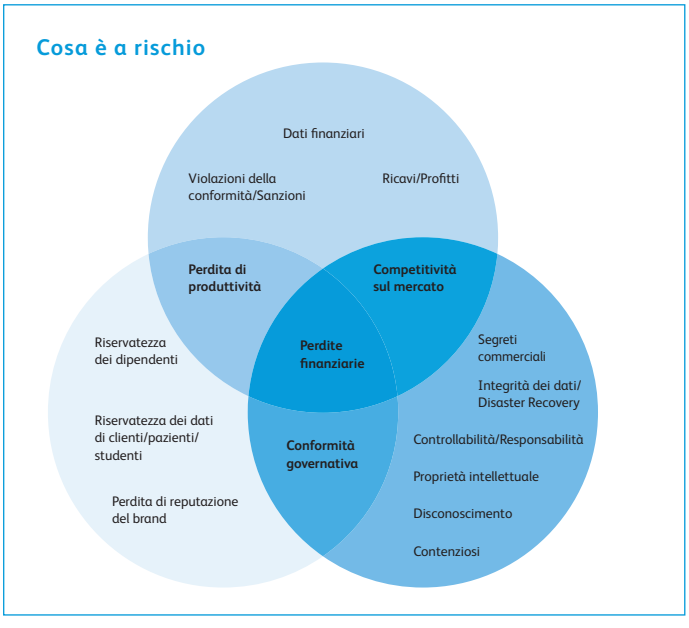
Le vulnerabilità della sicurezza: rischi e costi per il settore

Tutte le aziende, di ogni tipo e dimensione, hanno informazioni sensibili che fanno gola ai pirati informatici e che devono essere protette. Il panorama delle minacce cambia costantemente. Con la sempre maggiore diffusione del BYOD (Bring Your Own Devices), di dispositivi indossabili per il rilevamento di dati sanitari, sistemi di pagamento mobili, archivi cloud e l'Internet delle cose, la minaccia è reale e sempre maggiore.

I pirati informatici stanno incentrando sempre più la loro attenzione sulle piccole e medie imprese (PMI), perché sono obiettivi più facili rispetto alle grande aziende, e perché solitamente non hanno le risorse necessarie per proteggersi dagli attacchi. Le violazioni di dati nelle grandi aziende fanno notizia, ma purtroppo nessuno parla mai dei cyber-attacchi ai danni delle PMI.

La posta in gioco per le PMI è ancora più alta rispetto alle grandi aziende. Le informazioni dei clienti gestite dalle PMI stanno diventando una merce preziosa, ed i costi di tali violazioni possono essere devastanti per una PMI. Secondo uno studio condotto nel 2015 dall'IBM and Ponemon Institute, il costo totale medio di una violazione di dati per le aziende intervistate è aumentato del 23% in due anni e ha raggiunto la cifra di 3,79 milioni di dollari.[1] Il costo medio pagato per ogni record perduto o rubato contenente informazioni sensibili e riservate è passato da 145 dollari nel 2014 a 154 dollari nel 2015.[1]

E queste cifre non tengono conto di possibili penali, perdita di reputazione e interruzioni dell'attività. La sicurezza può non essere sempre una priorità aziendale chiave, ma la protezione delle informazioni è essenziale per il buon stato di salute di un'organizzazione.



Settore sanitario

I progressi compiuti in ambito IT – compreso l'utilizzo di computer palmari – ha fatto nascere l'esigenza di condividere elettronicamente importanti dati clinici e informazioni sui pazienti, ed è esattamente a questo punto che la sicurezza diventa un grande problema.

Nel 1996 il Governo federale degli Stati Uniti ha approvato lo Health Insurance Portability and Accountability Act (HIPAA) per obbligare tutte le organizzazioni sanitarie ad applicare procedure uniformi di gestione dei dati al fine di proteggere in ogni momento le informazioni e la privacy dei pazienti. Ai sensi dell'HIPAA, è richiesto un registro di controllo per monitorare chi visualizza i dati, quando li visualizza e se chi li visualizza è stato debitamente autorizzato a farlo.

Lo Health Information Technology for Economic and Clinical Health (HITECH) Act ha significativamente ampliato gli sforzi del governo statunitense volti a creare un sistema nazionale di gestione dei record per il settore sanitario. L'HITECH è stato approvato nell'ambito dell'American Recovery and Reinvestment Act del 2009 volto a promuovere l'adozione e un diffuso utilizzo della tecnologia applicata alle informazioni sanitarie.

La mancata conformità all'HIPAA può dar luogo all'applicazione di sanzioni civili e penali, anche in assenza di violazioni.

Settore pubblico

Oggi giorno, i governi locali, statali e federali pongono grossa enfasi sulla necessità di semplificare i processi e migliorare la collaborazione tra le varie agenzie al fine di offrire risultati migliori ai cittadini che servono. A tal fine, stanno adottando varie iniziative volte da un lato a sfruttare al meglio le tecnologie più avanzate, e dall'altro a promulgare normative severe volte a garantire la sicurezza delle informazioni che vengono trasmesse. Un esempio di ciò è la legge sulla violazione dei dati promulgata dallo stato del Massachusetts, una delle leggi più aggressive dell'intera nazione. I sistemi, software e servizi Xerox® sono conformi a tali rigorose linee guida, nonché ad altre.

Nel 2014, il Dipartimento della difesa statunitense ha adottato gli standard del National Institute of Standards and Technology (NIST) 800-53, una pubblicazione che raccomanda controlli sulla sicurezza per sistemi informatici e organizzazioni del governo federale, e controlli sulla sicurezza dei documenti per tutti i sistemi informatici federali, tranne quelli progettati per finalità di sicurezza nazionale.

1. Studio sul costo delle violazioni di dati 2015: Global Analysis, IBM and Ponemon Institute, Maggio 2015.

Le vulnerabilità della sicurezza: rischi e costi per il settore

Inoltre, il Dipartimento della difesa statunitense ha adottato ulteriori misure di sicurezza mediante l'utilizzo del sistema di card CAC (Common Access Cards) e della sua controparte del governo civile, il sistema di card PIV (Personal Identity Verification). Tali card richiedono un'infrastruttura PKI per garantire un ambiente di autenticazione e comunicazione sicuro. Inoltre, la gran parte delle agenzie del governo federale ha adottato lo standard FIPS 140-2 per certificare i moduli di crittografia utilizzati nelle stampanti e nei multifunzione. Infine, molti clienti del governo federale richiedono che i prodotti abbiano la certificazione Common Criteria.

Servizi finanziari

Deposito diretto, home banking, carte di debito e altri progressi nella tecnologia informatica stanno rivoluzionando il settore dei servizi finanziari. Sebbene più pratico per i clienti che per le aziende, questo massiccio utilizzo della tecnologia comporta alcuni rischi per la sicurezza.

Uno scambio sicuro di dati relativi alle carte di credito è fondamentale, e la conformità allo standard per la sicurezza dei dati PCI DSS (Payment Card Industry Data Security Standard) contribuisce a mitigare le vulnerabilità e a proteggere i dati dei titolari delle carte. PCI DSS è uno standard di sicurezza delle informazioni proprietarie per organizzazioni che gestiscono carte di credito, come Visa®, Mastercard®, American Express®, Discover® e JCB.

Il Gramm-Leach-Bliley Financial Services Modernisation Act (GLBA) del 1999 è stato promulgato al fine di assicurare che gli istituti finanziari che raccolgono o ricevono dati di clienti privati dispongano di un piano per la sicurezza in grado di proteggere tali clienti. Per ottenere la conformità, le organizzazioni devono completare un'analisi del rischio inerente ai loro processi in vigore e installare firewall, limitare l'accesso degli utenti, monitorare la stampa e adottare altre misure.

Il Dodd-Frank Wall Street Reform and Consumer Protection Act del 2010 pone ulteriori obblighi relativi a un'accurata raccolta e reportistica dei dati finanziari. Tramite l'Office of Financial Research e le agenzie che ne fanno parte, i dati verranno raccolti e analizzati al fine di identificare e monitorare i nuovi rischi all'economia e rendere tali informazioni pubbliche mediante report periodici e testimonianze annuali al Congresso degli Stati Uniti.

Istruzione

Con il sistema pedagogico attualmente esistente – a livello di istruzione primaria, secondaria e e universitaria – verbali, domande di contributi finanziari e finanche registri scolastici sono tutti disponibili online. Poiché alcuni istituti pedagogici hanno un proprio centro medico, sono tenuti ad archiviare e condividere le informazioni cliniche elettronicamente. Tale ambiente interattivo migliora l'esperienza degli studenti e la produttività del personale, ma espone anche gli istituti scolastici a minacce alla sicurezza.

Poiché tali istituti gestiscono un'ampia varietà di informazioni, negli Stati Uniti sono in vigore numerose normative statali e federali, quali il Computer Fraud and Abuse Act, lo USA Patriot Act, HIPAA e GLBA. Tuttavia, la normativa maggiormente applicabile al settore dell'istruzione statunitense è il Family Education Rights and Privacy Act (FERPA). Questa legge vieta la divulgazione di dati di identificazione personale senza l'autorizzazione scritta dello studente o del suo tutore legale.

Alla luce di un numero così ampio di misure normative e di conformità da rispettare, Xerox ha adottato i requisiti del governo federale, tra gli altri, come linea guida di condotta. Sviluppando soluzioni che si sforzano di rispettare i più rigorosi standard di sicurezza, siamo in grado di offrire soluzioni altamente sicure a tutti i nostri clienti, indipendentemente dal loro settore di attività.

Panoramica sulla sicurezza

La filosofia “Protezione = Sicurezza” ispira lo sviluppo di prodotti, servizi e tecnologie, uno sviluppo improntato sul concetto di sicurezza a ogni livello.

La sicurezza è l'elemento cardine della progettazione dei nostri “sistemi multifunzione intelligenti”. In qualità di azienda leader nello sviluppo della tecnologia digitale, Xerox ha dimostrato il proprio impegno alla sicurezza delle informazioni digitali identificando potenziali vulnerabilità ed eliminandole proattivamente al fine di limitare il rischio. I clienti hanno risposto affidandosi a Xerox quale loro fornitore di fiducia di soluzioni sicure che offrono una ricca gamma di avanzatissime funzioni di sicurezza di serie e opzionali.

La nostra strategia per la sicurezza

Lo sviluppo dei prodotti Xerox® è guidato da un Processo del ciclo di vita dello sviluppo della sicurezza, che tiene conto dell'Open Web Application Security Project (OWASP), del Software Assurance Maturity Model (SAMM) e delle linee guida del SANS Institute. Ciò implica la definizione di requisiti di sicurezza, valutazione dei rischi, analisi delle vulnerabilità e test di penetrazione, oltre alle informazioni ottenute dall'OWASP e dal SANS Institute. Tale strategia è basata su tre pilastri:

Funzionalità di sicurezza di assoluta avanguardia

Stampanti e multifunzione sono sofisticate piattaforme di rete con molteplici sottosistemi, e Xerox offre la più ampia gamma di funzionalità di sicurezza esistenti sul mercato, quali crittografia, autenticazione, autorizzazione per utente e verifica.

Certificazione

ISO 15408 (Common Criteria) per la valutazione della sicurezza IT è l'unico standard di certificazione della sicurezza riconosciuto a livello internazionale. Xerox è stato il primo produttore a richiedere e ottenere le certificazioni per i dispositivi multifunzione “completi”. Poiché ciascun elemento della piattaforma multifunzione è un potenziale punto di ingresso, una certificazione sulla sicurezza degna di questo nome deve comprendere tutti gli elementi, quali sistema operativo, interfaccia di rete, dischi rigidi, server web, interpreti PDL, interfaccia utente, porte hardware locali e sistema fax.

Manutenzione

In Xerox, garantire la sicurezza delle nostre stampanti e multifunzione lungo tutto il loro ciclo di vita richiede un'attenzione costante ad assicurare una protezione continua contro l'insorgere di sempre nuove minacce. Ciò viene ottenuto:

- Assicurando aggiornamenti software su base regolare
- Notificando nuovi bollettini sulla sicurezza con feed RSS
- Rispondendo alle vulnerabilità identificate
- Fornendo linee guida per un'installazione e gestione sicura dei dispositivi
- Fornendo informazioni sulla certificazione Common Criteria
- Rendendo patch disponibili su www.xerox.com/security

TIl Modello di sicurezza Xerox, congiuntamente al Ciclo di vita dello sviluppo della sicurezza, è la nostra garanzia che tutte le caratteristiche e funzionalità del sistema, non solo una o due di esse, sono sicure

Un approccio globale alla sicurezza di stampanti e multifunzione

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 globale abbraccia quattro aspetti chiave.**

1. Prevenzione delle intrusioni

Il primo e più ovvio punto di vulnerabilità è l'interfaccia utente: le persone che hanno accesso fisico alla stampante e alle sue funzionalità. Autenticazione utente è l'elemento base per garantire l'accesso a stampanti e multifunzione Xerox® per utenti in locale e di rete autorizzati. Una volta eseguita l'autenticazione, l'utente può interagire con il dispositivo o accedere ai dati dei clienti, che sono tuttavia soggetti a limitazione in base al ruolo dell'utente. Stampanti e multifunzione Xerox® impiegano una varietà di tecnologie per assicurare l'accesso autorizzato alle funzionalità del dispositivo da parte di utenti e altri dispositivi di rete. A questo punto ci occupiamo dei punti di vulnerabilità meno ovvi: tutto ciò che viene inviato alla stampante e il modo in cui la tecnologia Xerox® ConnectKey® intercetta gli attacchi di file danneggiati e software dannoso. Il nostro software di sistema, DLM e weblet inclusi, è dotato di firma digitale: 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.

AUTENTICAZIONE DI RETE

Autenticazione di rete fa sì che per poter utilizzare il dispositivo l'utente debba prima autenticarsi inserendo nome utente e password. Autorizzazione di rete consente a un utente di accedere a uno o a una qualsiasi combinazione dei seguenti servizi: Stampa, Copia, Fax, Server Fax, Ristampa lavori salvati, Email, Internet Fax e Server di scansione del flusso di lavoro. Inoltre, l'utente può essere autorizzato ad accedere a uno o ad una qualsiasi combinazione dei seguenti percorsi macchina: Servizi, Stato del lavoro o Stato della macchina.

1. Prevenzione delle intrusioni

Impedire l'accesso generale a dispositivi protetti con accesso utente e firewall interno.

2. Rilevamento dispositivo

Invio di un avviso all'avvio o su richiesta in caso di rilevamento di modifiche dannose alla stampante.

3. Protezione di dati e documenti

Massima protezione delle informazioni personali e riservate grazie alla crittografia del disco rigido (AES 256 a bit, convalida FIPS per molti prodotti) e sovrascrittura immagini.

4. Partnership esterne

Proteggete i vostri dati e il vostro dispositivo da intrusioni fraudolente con la tecnologia Whitelisting di McAfee, l'integrazione con Cisco® Identity Services Engine (ISE), enti di certificazione e organizzazioni di test di conformità.

MICROSOFT® ACTIVE DIRECTORY® SERVICES

La funzione Microsoft Active Directory Services (ADS) consente al dispositivo di autenticare gli account utente a fronte di un database di account utente centralizzato, anziché utilizzare esclusivamente il database di account utente gestito localmente sul dispositivo.

AUTENTICAZIONE LDAP

Autenticazione LDAP (BIND) è supportata per eseguire l'autenticazione con i server LDAP per la ricerca e l'utilizzo di informazioni. Quando un client LDAP si collega al server, lo stato di autenticazione predefinito della sessione è impostato su anonimo. La funzione BIND stabilisce lo stato di autenticazione per una sessione.

AUTENTICAZIONE SMPT

Questa funzione convalida l'account email dell'utente e impedisce agli utenti non autorizzati di inviare email dal dispositivo. Gli amministratori di sistema possono abilitare TLS per tutte le operazioni di invio e ricezione SMTP.

Panoramica sulla sicurezza

AUTENTICAZIONE POP3 PRIMA DI SMTP

Come ulteriore livello di sicurezza, i multifunzione Xerox® consentono agli amministratori di sistema di abilitare o disabilitare l'autenticazione POP3 prima della funzione SMTP. L'autenticazione POP3 prima di SMTP fa sì che per poter inviare email via SMPT l'utente debba prima accedere correttamente a un server POP3.

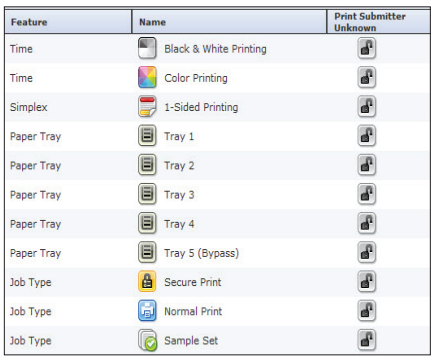
CONTROLLO DELL' ACCESSO IN BASE AL RUOLO (RBAC)

La funzione RBAC assicura che gli utenti autenticati vengano assegnati a un ruolo: Utente non collegato/Utente collegato, Amministratore di sistema o Amministratore di contabilità Ad ogni ruolo sono associati privilegi con appropriati livelli di accesso a funzioni, lavori e attributi della coda di stampa. Ciò consente agli amministratori di scegliere con precisione quali funzioni sono permesse per un determinato ruolo. Una volta che l'utente esegue il login al dispositivo inserendo nome utente e password, il dispositivo può stabilire quali ruoli sono assegnati a quel particolare utente. Vengono applicate limitazioni sulla base dei ruoli assegnati. Se l'utilizzo di un'intera funzione è limitato, la funzione può apparire bloccata all'utente dopo che questi ha eseguito l'autenticazione, oppure potrebbe non apparire affatto.

Utente non collegato/ Utente collegato	Amministratore di sistema	Amministratore di contabilità

AUTORIZZAZIONI UTENTE PER LA STAMPA

Le autorizzazioni utente Xerox consentono di limitare l'accesso alle funzioni di stampa per utente, gruppo, ora del giorno e applicazione. È possibile configurare utenti e gruppi con diversi livelli di accesso alle funzioni di stampa. Ad esempio, è possibile impostare limiti che consentono di stampare lavori a colori solo in certe ore del giorno; impostare la stampa delle presentazioni Microsoft® PowerPoint® automaticamente in modalità fronte/retro, o la stampa delle email Microsoft Outlook® sempre in bianco e nero.



Impostate le autorizzazioni utente per il colore e altre limitazioni di stampa grazie a interfacce utente intuitive.

AUTENTICAZIONE CON SMART CARD

Nota anche come Autenticazione con scheda magnetica o Autenticazione con Smart Card di prossimità, la funzione Autenticazione con Smart Card protegge stampanti e multifunzione dall'accesso in locale non autorizzato. I dispositivi Xerox® supportano svariati lettori card (CAC/PIV, .NET, Rijkspas e altre smart card o schede di prossimità), circa 30 diversi tipi di lettori card e 65 diverse schede di prossimità. Con Autenticazione Smart Card, l'utente può essere identificato mediante un sistema di identificazione a due fattori – possesso della card e di un numero di identificazione personale inserito nell'interfaccia utente del dispositivo – per acquisire l'accesso alle funzioni walkup del dispositivo e sulla rete.

Common Access Card/Personal Identity Verification (CAC/PIV) è una smart card emessa dal Dipartimento della difesa statunitense come sistema di identificazione standard per il personale militare in servizio attivo e di riserva, impiegati civili, altri dipendenti non di enti governativi e il personale qualificato di enti appaltatori. La card CAC/PIV può essere utilizzata per finalità di identificazione generale, per l'accesso controllato a edifici e per l'autenticazione di PC, nonché per stampanti/multifunzione e per le reti che connettono tali dispositivi.

Panoramica sulla sicurezza

144k CAC/PIV è una versione della smart card. L'utente può essere autenticato mediante identificazione a due fattori per acquisire l'accesso a servizi walk-up presso il dispositivo.

144k CAC/PIV offre i seguenti vantaggi:

- Crittografia S/MIME per Scansione su email a sé stessi o a qualsiasi destinatario presente nella rubrica locale del multifunzione o nella rubrica globale LDAP
- Firma digitale mediante il Certificato di firma email della card dell'utente
- Compilazione automatica del campo "A:" quando si utilizza la funzione Scansione su email del multifunzione
- Chiave di certificazione fino a 2048 bit
- Limitazione delle trasmissioni in uscita ai destinatari dotati di certificati validi
- Ricezione di report di conferma delle email e gestione di registri di controllo
- Accesso unico a Scansione su home e LDAP

Schema di configurazione per Sistema CAC (Common Access Card/Sistema PIV (Personal Identity Verification)

1. Si inserisce una card nel lettore, e all'utente viene chiesto di inserire un PIN nel multifunzione.
2. Il multifunzione verifica il server OCSP per confermare che il certificato della card non sia scaduto, e quindi ritrasmette la "Chain of Trust" a un ente di certificazione conosciuto.
3. Il multifunzione avvia un dialogo crittografato di tipo problema/risposta tra il controller di dominio e il Sistema CAC. In caso di esito positivo, il controller di dominio emette un "Ticket di assegnazione ticket" e l'autorizzazione è completa.
4. L'autorizzazione sblocca le funzioni walk-up del multifunzione:
   - Scansione su email:
   - Copia
   - Fax
   - Servizi personalizzati
   - Scansione del flusso di lavoro

Panoramica sulla sicurezza

XEROX® PRINTSAFE SOFTWARE

Xerox® PrintSafe Software fornisce l'autenticazione di stampa protetta per i dati stampati su gran parte delle stampanti e dei multifunzione, su dispositivi sia Xerox che di altre marche. Questo software e aperto e può funzionare con una varietà di lettori e card sicuri standard del settore.

Flussi di lavoro sicuri, pratici e flessibili

L'utente invia il documento.

Semplicemente premendo "Stampa", il documento viene trattenuto

L'utente può recarsi presso qualsiasi stampante o multifunzione in rete abilitato ad accettare un lavoro PrintSafe, e si autentica semplicemente strisciando la card o inserendo un PIN.

Una volta autenticatosi, l'utente può scegliere di rilasciare un solo lavoro o tutti i lavori protetti presso la stampante o il multifunzione.

Xerox® PrintSafe Software non è limitato ai dispositivi Xerox®. Qualsiasi stampante o multifunzione* registrato a Xerox® PrintSafe Software può stampare

I flussi di lavoro flessibili consentono all'utente di caricare software sul proprio client PC per la stampa diretta o su un server di stampa esistente, che può essere facilmente configurato per Xerox® PrintSafe Software.

*I dispositivi non Xerox® richiedono un accessorio di rete; consultare il proprio rappresentante Xerox per informazioni sulle marche/i modelli supportati.

ACCESSO ALL'INTERFACCIA UTENTE DEL DISPOSITIVO E ALL'INTERFACCIA UTENTE REMOTA

Gli amministratori di sistema possono bloccare l'accesso alle schermate di impostazione del dispositivo per gli utenti non autorizzati dal pannello comandi e dall'utilità Interfaccia utente remota al fine di proteggerne le informazioni sulla configurazione.

2. Rilevamento dispositivo

Nel caso improbabile che le difese dei dati e della rete vengano superate, la tecnologia Xerox® ConnectKey® eseguirà un test di verifica del firmware completo, all'avvio* o su attivazione da parte di utenti autorizzati e provvederà quindi a inviare avvisi qualora vengano rilevate modifiche dannose alla stampante o al multifunzione. Se vengono rilevate anomalie, sul dispositivo viene visualizzato un messaggio nel quale si consiglia all'utente di ricaricare il firmware. Le nostre avanzatissime soluzioni integrate utilizzano la tecnologia Whitelisting** di McAfee®, che esegue un monitoraggio costante e impedisce automaticamente l'esecuzione di malware dannoso.

In collaborazione con Cisco, Xerox ha implementato il sistema di profilazione dei nostri dispositivi in Cisco® Identity Services Engine (ISE). 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.

Per ulteriori informazioni, consultare i seguenti white paper:

White Paper sulla tecnologia Whitelisting di McAfee (solo in inglese):
http://www.office.xerox.com/latest/SECWP-03.PDF

White Paper su Cisco ISE (solo in inglese):
http://www.office.xerox.com/latest/SECWP-04.PDF

*Stampanti e sistemi multifunzione Xerox® VersaLink®
**Stampanti e sistemi multifunzione Xerox® AltaLink® e i-Series

3. Protezione di dati e documenti

Protezione dei documenti

Una volta attivate tutte le misure di sicurezza della rete necessarie per proteggere efficacemente i dati sensibili che vengono trasferiti tra i computer degli utenti e i dispositivi di stampa dell'ufficio, le tecnologie di sicurezza devono anche assicurare che i vostri documenti cartacei sensibili siano ricevuti e letti solo dai destinatari a cui sono indirizzati. Xerox impiega le più recenti tecnologie per proteggere i documenti, si tratti di stampare copie cartacee o di distribuire documenti elettronici.

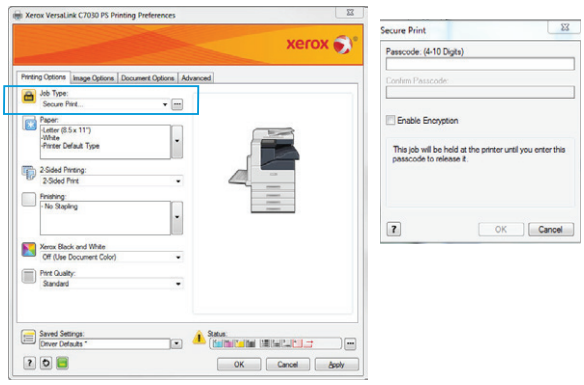
CRITTOGRAFIA DEI DATI DI SCANSIONE

Gli utenti dei nostri multifunzione intelligenti i-Series, VersaLink® e AltaLink® abilitati alla tecnologia Xerox® ConnectKey® hanno anche la possibilità di crittografare i file PDF con una password quando si utilizza la funzione Scansione su email.

- Protezione all'esterno del firewall
  - Protezione dei dati in un ambiente non sicuro
  - Utilizzo di protocolli standard del settore, quali ad esempio TSL e Secure PDF

CRITTOGRAFIA DEL FLUSSO DI STAMPA

Xerox® Global Print Driver® e i driver di alcuni prodotti supportano la crittografia dei documenti quando gli utenti inoltrano lavori di stampa protetta a dispositivi abilitati alla tecnologia ConnectKey. I sistemi multifunzione Xerox® AltaLink e i-Series supportano inoltre la crittografia dei documenti per i normali lavori di stampa. Per la crittografia del driver di stampa non è necessario hardware aggiuntivo.



STAMPA PROTETTA

I lavori di stampa riservati vengono trattenuti nella stampante o nel multifunzione finché il proprietario del documento non li rilascia inserendo il PIN univoco tramite l'interfaccia utente del dispositivo. In tal modo, il destinatario del documento deve essere fisicamente presente durante la stampa di informazioni sensibili e può immediatamente rimuovere il documento dalla stampante o dal multifunzione prima che altri utenti possano vederlo.

La stampa protetta basata sulle tecnologie CAC (Common Access Card)/ PIV (Personal Identity Verification) consente di associare il lavoro di stampa al certificato di identità dell'utente che lo invia. Presso il dispositivo, prima di poter rilasciare il lavoro di stampa l'utente deve autenticarsi con la propria card CAC/PIV.

PDF CRITTOGRAFATO/PDF PROTETTO DA PASSWORD

Quando si esegue la scansione di un documento cartaceo per la distribuzione in formato elettronico tramite la funzionalità Scansione su email, con i multifunzione Xerox® è possibile creare PDF protetti da password o con crittografia AES a 128 o 256 bit, che vengono quindi trasmessi in rete in modo sicuro e che possono essere aperti, stampati o modificati solo dagli utenti in possesso della password corretta.

INOLTRO FAX SU EMAIL E RETE

I multifunzione Xerox® con funzionalità di inoltro fax possono indirizzare i fax in arrivo alle caselle di posta elettronica di specifici destinatari e/o a un archivio di rete protetto, dove potranno essere visualizzati solo dagli utenti autorizzati.

CONFERMA DESTINAZIONE FAX

Il mittente del fax riceve automaticamente la conferma che il fax è stato ricevuto correttamente dal destinatario corretto.

Panoramica sulla sicurezza

FIRME DIGITALI

Una firma digitale è uno schema matematico per dimostrare l'autenticità di un messaggio o documento digitale. La firma digitale viene utilizzata per proteggere il firmware del dispositivo da modifiche non rilevate e per fornire l'autenticazione dell'origine dei dati. Grazie alle smart card, è possibile firmare digitalmente le email con il certificato del mittente. Una firma digitale valida dà al destinatario la tranquillità di sapere che il messaggio è stato creato da un mittente noto e che non è stato modificato durante il trasferimento.

FILIGRANA PROTETTA

Alcune stampanti e sistemi multifunzione Xerox® dispongono di una funzione Filigrana protetta che impedisce la copia di originali con informazioni riservate. Se si effettua la copia di un documento con filigrana protetta, l'immagine della filigrana diventa visibile, rendendo evidente che il documento contiene informazioni riservate duplicate illegalmente.

TIMBRO UTENTE/ORA/DATA

Attraverso i driver Xerox®, è possibile applicare un timbro utente/ora/data su qualsiasi documento stampato da qualsiasi dispositivo in rete. In questo modo, un percorso di verifica consentirà di sapere chi ha stampato cosa e quando.

FILTRO INDIRIZZI IP

Il filtro Internet Protocol (IP) consente agli amministratori di sistema di creare delle regole allo scopo di accettare o rifiutare le informazioni dirette al multifunzione in base a specifici indirizzi o intervalli di indirizzi IP. Ciò consente all'amministratore del sistema di controllare e regolare l'accesso al dispositivo.

Indirizzi IP registrati:
Disponibili

Indirizzi IP non registrati:
Non disponibili

SECURE SOCKETS LAYER (SSL)/TRANSPORT LAYER SECURITY (TLS)

Molte organizzazioni sono tenute a rispettare norme di sicurezza che impongono di rendere sicure tutte le transazioni tra il client e la stampante o il multifunzione mediante transazioni web protette, trasferimenti file protetti e messaggi email protetti. I dati trasmessi in rete senza crittografia possono essere letti da chiunque utilizzi la rete. Per limitare questo problema Xerox utilizza i protocolli SSL (Secure Sockets Layer)/TLS (Transport Layer Security) per le trasmissioni di dati su determinati protocolli come HTTPs e IPP.

CRITTOGRAFIA IPSEC

Il protocollo IPsec (Internet Protocol Security) protegge tutte le comunicazioni a livello IP e viene utilizzato principalmente per crittografare i lavori di stampa inviati al dispositivo. Consente di crittografare tutto il traffico dal punto A al punto B in modo tale che solo gli utenti attendibili possano inviare e ricevere le informazioni, i dati non vengano modificati durante la trasmissione e solo gli utenti autorizzati possano ricevere e leggere le informazioni.

IPsec è progettato per fornire i seguenti servizi di protezione:

- Crittografia del traffico (per impedire alle parti non autorizzate di leggere le comunicazioni private)
- Convalida di integrità (per impedire la modifica dei dati lungo il percorso)
- Autenticazione peer (per accertarsi che il traffico provenga da una fonte attendibile)
- Anti-replay (per impedire la ripetizione di una sessione protetta)

ABILITAZIONE/DISABILITAZIONE PORTE DI RETE

Con l'abilitazione/disabilitazione delle porte di rete, è possibile disattivare le porte e i servizi non necessari per impedire l'accesso non autorizzato o fraudolento. Sui dispositivi desktop più piccoli, è possibile regolare queste opzioni tramite il relativo pannello comandi o il software di configurazione basato su PC. Su sistemi multifunzione più grandi, vengono forniti strumenti per impostare i livelli di sicurezza e disabilitare porte e servizi specifici.

Panoramica sulla sicurezza

CERTIFICATI DIGITALI

I certificati digitali sono documenti elettronici che utilizzano una firma digitale per associare una chiave pubblica a un'identità: informazioni quali il nome di una persona o di un'organizzazione, il loro indirizzo, e così via. Il certificato può essere utilizzato per verificare che una chiave pubblica appartiene a una persona.

I multifunzione possono aggiungere firme digitali che verificano l'origine e l'autenticità di un documento PDF. Quando i destinatari aprono un file PDF che è stato salvato con una firma digitale, possono vedere le proprietà del documento per esaminare il contenuto della firma, come l'ente di certificazione, il nome del prodotto di sistema, il numero di serie e la data/ora di creazione. Se la firma è una firma di dispositivo, conterrà anche il nome del dispositivo che ha creato il documento, mentre una firma di utente verifica l'identità dell'utente autenticato che ha inviato o salvato il documento.

Sui multifunzione Xerox® è possibile caricare un certificato firmato da un ente di certificazione come VeriSign, oppure il vostro amministratore di sistema può creare un certificato autofirmato sul dispositivo stesso. Impostando un certificato sul vostro dispositivo, potete abilitare la crittografia per specifici tipi di flussi di lavoro.

SNMPV3

Simple Network Management Protocol (SNMP) è un protocollo Internet standard per la gestione di dispositivi su reti IP, che fornisce maggiore accuratezza proteggendo i dati da tentativi di manomissione, assicurando che l'accesso venga limitato agli utenti autorizzati mediante autenticazione e crittografando i dati inviati in rete.

I dispositivi che solitamente supportano SNMP sono router, switch, server, workstation, stampanti, rack di modem e altri ancora. Viene utilizzato soprattutto nei sistemi di gestione rete per monitorare i dispositivi connessi alla rete per condizioni che richiedono attenzione da parte dell'amministratore. SNMP è un componente della Internet Protocol Suite così come definita dalla Internet Engineering Task Force (IETF). Il protocollo SNMPv3 fornisce funzionalità di sicurezza significativamente più avanzate, quali crittografia dei messaggi e autenticazione.

STRINGHE DI NOME COMUNITÀ SNMP

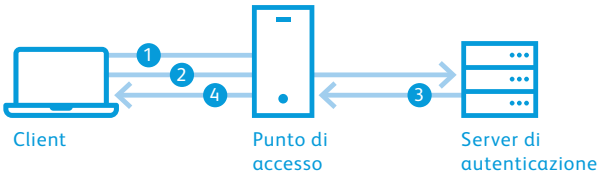
Di norma i dati MIB (Management Information Base) di sola lettura utilizzano la stringa "pubblica" e le stringhe di comunità in lettura-scrittura impostate su "privata". Utilizzando le stringhe di nomi di comunità in lettura-scrittura sui dispositivi, un'applicazione può modificare l'impostazione di configurazione del dispositivo utilizzando variabili MIB. Le stringhe di nomi di comunità in lettura-scrittura su dispositivi Xerox® possono essere modificate dall'amministratore di sistema per accrescere la sicurezza quando si gestiscono multifunzione utilizzando SNMP.

AUTENTICAZIONE 802.1X

IEEE 802.1X è uno Standard IEEE per PNAC (port-based Network Access Control). Fa parte del gruppo di protocolli di rete IEEE 802.1. Fornisce un meccanismo di autenticazione ai dispositivi che intendono connettersi a una LAN (local area network) o a una WLAN (wireless local area network). La funzionalità IEEE 802.1X è supportata da numerosi switch Ethernet e può impedire a sistemi guest, fraudolenti o non gestiti, non in grado di autenticarsi correttamente, di connettersi alla vostra rete.

Come funziona: Autenticazione 802.1X

L'autenticazione 802.1X per LAN wireless fornisce l'autenticazione centralizzata basata su server degli utenti finali.



1. Un client invia un messaggio di "avvio" a un punto di accesso, il quale richiede l'identità del client.
2. Il client replica con un pacchetto di risposta contenente un'identità, e il punto di accesso trasmette il pacchetto a un server di autenticazione.
3. Il server di autenticazione invia un pacchetto di "accettazione" al punto di accesso.
4. Il punto di accesso mette la porta del client in stato autorizzato, e il traffico ha l'autorizzazione a procedere.

Panoramica sulla sicurezza

Il protocollo 802.1X è diventato predominante a seguito della maggiore diffusione delle reti wireless. Molte organizzazioni bloccano l'accesso porte alle loro reti interne utilizzando questo protocollo. Ciò impedisce il passaggio di ulteriori informazioni sulla rete fino a quando il dispositivo non viene autenticato. Dal punto di vista della gestione dei rischi, ciò consente sia ai dispositivi wireless che a quelli cablati di dimostrare chi sono prima che una qualsiasi informazione venga trasmessa mediante la rete. Se viene tentato un accesso non autorizzato, la porta viene bloccata fino a quando non viene sbloccata dall'amministratore di sistema.

EAP (Extensible Authentication Protocol) è una struttura di autenticazione che svolge le proprie funzioni come parte dell'autenticazione 802.1X. I tipi di protocollo EAP attualmente supportati dai multifunzione Xerox® sono:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (prodotti AltaLink® e i-Series)

FIREWALL

Un firewall è un componente di un computer o di una rete progettato per proteggere il dispositivo da minacce esterne e accessi non autorizzati e consentire al contempo le comunicazioni autorizzate. Il dispositivo può essere configurato in modo da consentire o rifiutare le trasmissioni di rete in base a una serie di regole e altri criteri. Gli amministratori di rete possono limitare l'accesso a segmenti di rete, servizi e porte di dispositivi al fine di proteggere i dispositivi.

SEPARAZIONE DI FAX E RETE

La separazione dell'interfaccia fax dal controller di rete elimina il rischio di intrusione in una rete di ufficio tramite la linea fax.

Il multifunzione non fornisce una funzione per accedere alla rete tramite la linea telefonica del fax. Il protocollo Fax Class 1 utilizzato sul multifunzione risponde solo ai comandi fax che consentono lo scambio di dati fax. I dati trasmessi dal PC client possono essere soltanto dati immagine compressi con informazioni di destinazione. Tutti i dati che non siano dati immagine (come virus, codice di sicurezza o un codice di controllo che accede direttamente alla rete) vengono abbandonati in questa fase, e il multifunzione termina immediatamente la chiamata. Pertanto, non esiste alcun meccanismo mediante il quale poter accedere al sottosistema di rete tramite la linea fax.

Protezione dei dati

La tecnologia ha trasformato il modo di lavorare dei dipendenti. Oggi i documenti non hanno più soltanto la tradizionale forma di documenti cartacei, come note scritte a mano o bozze di comunicazioni, ma appaiono anche in forma di documenti elettronici come file e email. Poiché i dipendenti creano, archiviano, condividono e distribuiscono tali documenti elettronici in modo diverso rispetto ai tradizionali documenti cartacei, tali informazioni possono essere vulnerabili a nuovi tipi di rischi. Per restare competitiva, un'azienda deve fare fronte a tali minacce proteggendo i documenti e i sistemi di gestione dei documenti che contengono la risorsa più preziosa di un'azienda: la conoscenza.

Informazioni e sistemi di gestione dei documenti sono esposti a un'ampia gamma di minacce alla sicurezza. Alcuni esempi di tali minacce sono atti deliberati di spionaggio come hackeraggio, furto, frode e sabotaggio informatico, nonché atti non intenzionali quali errore umano e disastri naturali. La sicurezza delle informazioni va al di là della loro protezione.
Riguarda il garantire accesso e disponibilità immediati al contenuto dei documenti al fine di migliorare i processi aziendali e le prestazioni. Riguarda anche la gestione dei contenuti originali e la conformità alle leggi.

Sin dall'introduzione dei primi dispositivi digitali, Xerox è consapevole dei rischio legato al recupero non autorizzato dei dati memorizzati in unità di archiviazione non volatili, e ha integrato nei propri dispositivi funzionalità e contromisure per aiutare i clienti a salvaguardare i loro dati.

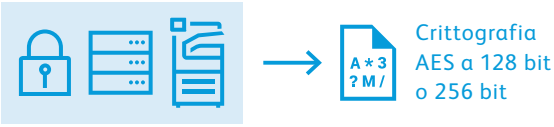
CRITTOGRAFIA DEI DATI IMMAGINE

Utilizzando la crittografia AES a 128 bit o 256 bit, molti dispositivi Xerox® sono dotati della funzione di crittografia dati a livello di lavoro, immagine e dati cliente, che protegge i dati archiviati nel vostro multifunzione Xerox® dall'accesso non autorizzato. Con la crittografia dati, il disco viene partizionato e viene crittografata solo la partizione con i dati utente. Le partizioni dei dati relative al sistema operativo non sono e non possono essere crittografate.

- Crittografia AES a 128 bit o 256, convalida Federal Information Processing Standard (FIPS) 140-2
- Tutti i dati immagine dell'utente presenti sul disco rigido vengono crittografati

Panoramica sulla sicurezza

AES è uno standard di crittografia agile, rapido e difficile da violare ed è adatto per un'ampia gamma di dispositivi o applicazioni. Rappresenta la più avanzata combinazione di sicurezza, prestazioni, efficienza, facilità di implementazione e flessibilità. Molti dispositivi Xerox® possono essere impostati in modalità FIPS 140-2, il che significa che utilizzeranno solo algoritmi di crittografia certificati FIPS 140-2.



SOVRASCRITTURA IMMAGINI

La funzione Sovrascrittura immagini cancella i dati immagine dal disco rigido del vostro dispositivo Xerox® una volta che i dati non sono più necessari. Questa operazione può essere eseguita automaticamente una volta completata l'elaborazione di ciascun lavoro, pianificata periodicamente, oppure eseguita su richiesta dell'amministratore di sistema. I dispositivi Xerox® sono dotati sia di Sovrascrittura immagini immediata che di Sovrascrittura immagini su richiesta.

MEMORIA VOLATILE E NON VOLATILE

All'interno di ogni multifunzione Xerox®, il contoller è dotato di memoria volatile (RAM) e memoria non volatile (disco rigido). Con la memoria volatile, tutti i dati immagine vanno perduti allo spegnimento o al riavvio del sistema. Con la memoria non volatile, i dati immagine vengono solitamente memorizzati in un'unità flash o sul disco rigido del multifunzione, e conservati fino a quando non vengono cancellati.

Col crescere dei timori relativi alla sicurezza dei dati, i clienti vogliono sapere dove e in che modo i dati possono essere manomessi. Le Dichiarazioni di volatilità sono documenti creati per aiutare a identificare dove vengono archiviati i dati immagine dei clienti all'interno dei dispositivi Xerox®. Una Dichiarazione di volatilità descrive la posizione, la capacità e il contenuto dei dispositivi di memoria volatile e non volatile all'interno di un dato dispositivo Xerox®.

Sono state create Dichiarazioni di volatilità per numerosi dispositivi Xerox® per aiutare i clienti particolarmente sensibili al tema della sicurezza. È possibile ottenere tali documenti contattando il team di assistenza Xerox locale (per i clienti esistenti),un rivenditore Xerox (per i nuovi clienti) oppure sul sito www.xerox.com/security.

FAX PROTETTO

I fax riservati in entrata vengono trattenuti fino al loro rilascio da parte dell'amministratore di sistema.

PROTEZIONE PASSWORD PER SCANSIONE SU MAILBOX

Quando si utilizza la funzione Scansione su mailbox di un multifunzione, la mailbox designata può essere protetta da password per garantire che solo gli utenti autorizzati possano accedere ai documenti scansiti archiviati al suo interno. La sicurezza offerta dalla funzione Scansione su mailbox è ulteriormente accresciuta dalla crittografia della partizione dei dati immagine del disco rigido.

S/MIME PER SCANSIONE SU EMAIL

Secure/Multipurpose Internet Mail Extensions (S/MIME) fornisce i seguenti servizi di protezione crittografica per la funzione Scansione su email: autenticazione, integrità dei messaggi e non ripudio dell'origine (con utilizzo della firma digitale) e protezione della privacy e dei dati (mediante utilizzo della crittografia).

Nella comunicazione S/MIME, quando si inviano dati alla rete, viene aggiunta una firma a ciascun messaggio di email in base alle informazioni del certificato conservate nel dispositivo. La crittografia viene eseguita quando si inviano dati sulla base del certificato che corrisponde all'indirizzo designato di ciascun messaggio di posta. Il certificato viene verificato quando vengono inserite le informazioni sulla trasmissione dati, nonché al momento di inviare i file. La comunicazione S/MIME viene eseguita solo dopo che la validità del certificato è stata confermata.

CRITTOGRAFIA DI SCANSIONE SU EMAIL

La crittografia delle email mediante Autenticazione con Smart Card consente all'utente di inviare fino a 100 email crittografate a più destinatari nella directory LDAP di un'organizzazione utilizzando le chiavi pubbliche dei destinatari. La gran parte dei multifunzione Xerox® che utilizzano Autenticazione con Smart Card offrono anche la capacità di apporre firme digitali alle email. L'utente può visualizzare i certificati di potenziali destinatari prima di inviare le email. Il multifunzione non consente l'invio agli utenti senza un certificato di crittografia. Inoltre, il multifunzione registra tutti i record delle email inviate con la possibilità per l'amministratore di ricevere report di conferma.

NASCONDI REGISTRO LAVORI

La funzione Nascondi registro lavori standard assicura che i lavori elaborati dal dispositivo non siano visibili a un utente walkup o tramite l'Interfaccia utente remota. Le informazioni sul registro lavori, benché nascoste, restano comunque accessibili da parte dell'amministratore di sistema, il quale può stampare il registro lavori per mostrare l'utilizzo dei lavori di copia, fax, stampa e scansione eseguiti sul dispositivo.

OFFERTA DI CONSERVAZIONE DISCO RIGIDO

Xerox Fornisce un'Offerta di conservazione disco rigido per i dispositivi Xerox® ai clienti i quali nutrono il timore che i dati immagine sul loro disco rigido siano particolarmente sensibili o addirittura classificati. Questo servizio a pagamento consente a un cliente di conservare i propri dischi rigidi e sanitizzarli o distruggerli in un modo che ritiene garantisca la sicurezza dei dati immagine.

CONVALIDA DATI TRAMITE REMOTE SERVICES

Numerosi dispositivi Xerox® ottengono l'assenso del cliente prima di trasmettere dati di identificazione personale (PII - Personal Identifiable Information) e dati di identificazione cliente (CII - Customer Identifiable Information) tramite Remote Services a Xerox.

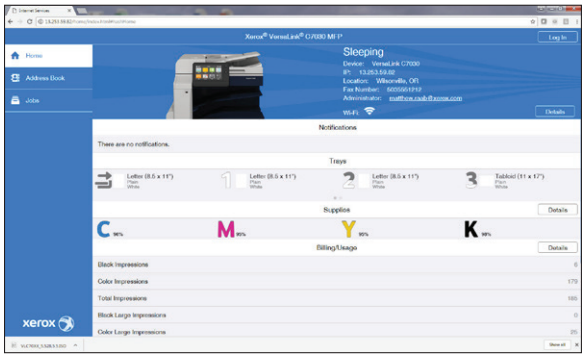
PASSWORD POSTSCRIPT

Un'altra area di rischio correlata alla stampa si verifica quando si stampa con il linguaggio PDL Adobe® PostScript®. PostScript comprende comandi che consentono ai lavori di stampa di modificare le impostazioni predefinite del dispositivo, il che potrebbe esporre il dispositivo a pericoli. Poiché il linguaggio PostScript comprende utilità molto potenti che potrebbero essere utilizzate per compromettere la sicurezza di un dispositivo, gli amministratori possono configurare il dispositivo in modo che per i lavori PostScript sia necessario inserire una password per modificare le impostazioni predefinite del dispositivo. I privilegi di base dell'interprete PostScript all'interno del controller sono volutamente limitati, ma gli amministratori possono in certa misura gestire il funzionamento del sottosistema PostScript.

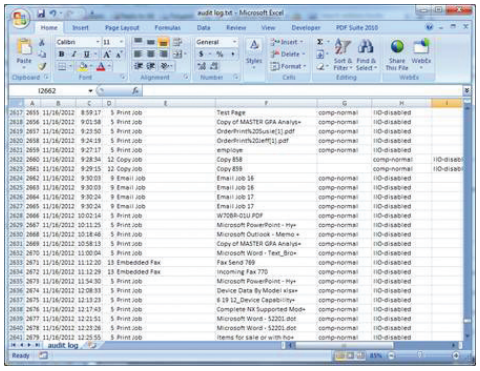
REGISTRO DI CONTROLLO

I multifunzione Xerox® e molte delle nostre stampanti possono gestire registri di controllo per monitorare l'attività a livello di documento, utente e funzione. Il registro di controllo è abilitato per impostazione predefinita sui dispositivi più recenti e può essere abilitato o disabilitato dall'amministratore di sistema. Può monitorare l'accesso e i tentativi di accesso al dispositivo e trasmettere i registri di controllo a un sistema SIEM o al server dei registri di controllo. Un esempio di voce del registro di controllo è: "L'utente xx ha eseguito l'accesso al multifunzione Xerox® AltaLink® alle 12:48 e ha inviato via fax 10 pagine al numero 888.123.1234."

Per i sistemi multifunzione abilitati alla tecnologia Xerox® ConnectKey®, il registro di controllo può essere inviato automaticamente e in modo sicuro al sistema SIEM per garantire il costante monitoraggio del multifunzione.



È possibile accedere all'interfaccia Registro di controllo dalla workstation di un amministratore di sistema utilizzando un qualsiasi browser Web.



Il registro può poi essere esportato in un file .txt e aperto in Microsoft® Excel®.

4. Partnership esterne

Xerox collabora con organizzazioni di verifica della conformità e aziende leader nel campo della sicurezza quali McAfee per abbinare il loro know-how e i loro standard di eccellenza alle proprie soluzioni per la sicurezza. Le seguenti funzioni di protezione da malware sono disponibili sui multifunzione abilitati alla tecnologia Xerox® ConnectKey® (sistemi multifunzione Xerox® AltaLink® e i-Series).

MCAFEE® EMBEDDED CONTROL – SICUREZZA MIGLIORATA

I multifunzione Xerox® basati sulla tecnologia Xerox® ConnectKey® sono dotati del sistema McAfee Embedded Control Powered by Intel® Security, il che fa di essi la prima linea di sistemi multifunzione del settore che si autoproteggomo da potenziali minacce esterne. La tecnologia Whitelisting di McAfee rileva tentativi non autorizzati di lettura, scrittura o modifica di file e directory protetti e ne invia notifica. Inoltre, la perfetta integrazione con Xerox® CentreWare® Web Software, la serie di strumenti MPS Xerox® e McAfee ePolicy Orchestrator® (McAfee ePO™) consentono di eseguire il monitoraggio dalla console preferita.

MCAFEE EMBEDDED CONTROL – CONTROLLO DELL'INTEGRITÀ

Il controllo di integrità sviluppa ulteriormente le funzionalità di sicurezza avanzata e aumenta la capacità di impedire l'esecuzione di nuovi file da una qualsiasi posizione con mezzi non affidabili. È consentita l'esecuzione soltanto di software approvato, prevenendo in tal modo attacchi sia generali che mirati. Utile soprattutto per l'implementazione di sistemi di sicurezza a livello di tutta l'azienda, la tecnologia Whitelisting offerta da Xerox e Intel Security garantisce che la sola funzione che quei dispositivi stanno svolgendo sono i servizi che voi intendere erogare. Questa stessa tecnologia viene impiegata per proteggere server, distributori bancomat, terminali di punti vendita e dispositivi integrati come ad esempio i dispositivi mobili.

EPOLICY ORCHESTRATOR (EPO) DI MCAFEE

ePolicy Orchestrator (ePO) di McAfee è un software di gestione della sicurezza che facilita la gestione dei rischi e della conformità ad organizzazioni di ogni dimensione. Presenta all'utente dashboard drag-and-drop che forniscono informazioni sulla sicurezza di tutti gli endpoint – dati, dispositivi mobili e reti – per fornire immediatamente un quadro generale chiaro e accelerare i tempi di risposta. ePolicy ottimizza le infrastrutture IT esistenti collegando la gestione di soluzioni di sicurezza McAfee e di terzi a LDAP, operazioni IT e strumenti di gestione della configurazione.

Come prova indipendente di terzi del fatto 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 degli standard internazionali Tali organismi riconoscono il nostro approccio globale alla sicurezza delle stampanti.

INTEGRAZIONE CON CISCO® IDENTITY SERVICES ENGINE (ISE)

Gestione e applicazione centralizzate delle politiche di sicurezza delle stampanti. La nostra partnership con Cisco fornisce maggiori funzionalità di rilevamento dei dispositivi Xerox®, per un'applicazione più capillare delle politiche di sicurezza. I dispositivi Xerox® vengono riconosciuti automaticamente e classificati da Cisco ISE, che consente il totale controllo degli accessi alla rete e riduce l'intervento degli operatori in quanto elimina l'immissione manuale degli attributi della stampante. La profilazione delle stampanti con Cisco ISE blocca eventuali tentativi di spoofing da parte di malintenzionati volti a ottenere libero accesso ai sistemi riservati. L'integrazione dei dispositivi di stampa Xerox® con Cisco ISE fornisce un approccio efficace sul piano operativo che permette di raggiungere gli obiettivi delle politiche di sicurezza.

Conformità alle normative e alle politiche

Le stampanti e i multifunzione moderni sono elementi focali per quanto riguarda la conformità in virtù dei dati personali e sensibili che utilizzano, archiviano e trasmettono. La mancata conformità può causare la perdita di affari, la perdita di clienti, o finanche azioni legali. I livelli di conformità richiesti variano in base al paese e al mercato verticale.

Lo Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti e il Data Protection Act nel Regno Unito sono esempi di standard che potrebbe essere necessario soddisfare per poter condurre l'attività in modo legale.

La certificazione Common Criteria è uno standard di sicurezza riconosciuto a livello internazionale che soddisfa le specifiche del Dipartimento della difesa statunitense.

Con funzionalità di sicurezza al vertice del settore e un approccio flessibile alla configurazione e all'implementazione, i dispositivi Xerox® possono conformarsi a qualsiasi standard e sono dotati di controlli in grado di soddisfare ogni esigenza.

Sistemi, software e servizi Xerox® sono conformi a riconosciuti standard del settore a alle più recenti leggi sulla sicurezza. I nostri prodotti offrono funzionalità che consentono ai nostri clienti di soddisfare tali standard. Ecco alcuni esempi di tali standard:

- Payment Card Industry (PCI) Data Security Standards Version 3.0
- Sarbanes-Oxley
- Basel II Framework
- Health Insurance Portability and Accountability Act (HIPAA)
- Direttiva sulla privacy elettronica (2002/58/EC)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- Health Information Technology for Economic and Clinical Health Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408 (Common Criteria) per la valutazione della sicurezza IT
- ISO-27001 per la gestione in sicurezza delle informazioni
- Control Objectives for Information and Related Technology
- Statement on Auditing Standards No. 70
- NIST 800-53, adottato da Governo degli Stati Uniti e DOD nel 2014
- Federal Risk and Authorisation Program (FedRAMP)

Valutazione della sicurezza dei prodotti

Sicurezza dei documenti significa totale tranquillità. Uno degli elementi chiave della linea di prodotti Xerox® è l'attenzione posta alla sicurezza delle informazioni. I nostri sistemi, software e servizi sono conformi a riconosciuti standard del settore a alle più recenti leggi sulla sicurezza.

Certificazione Common Criteria

La certificazione Common Criteria fornisce un attestato obiettivo e indipendente dell'affidabilità e qualità dei prodotti IT. È uno standard su cui gli utenti possono contare come ausilio per prendere decisioni informate sui loro acquisti IT. Common Criteria stabilisce specifici obiettivi di assicurazione in materia di informazioni relativi a integrità, riservatezza e disponibilità di sistemi e dati, responsabilità a livello individuale e garanzia del conseguimento di tutti gli obiettivi. La certificazione Common Criteria è un requisito richiesto sui dispositivi hardware e software utilizzati dal governo statunitense sui sistemi di sicurezza nazionale.

Acquisizione della certificazione Common Criteria

La certificazione Common Criteria è un processo rigoroso che comprende la verifica di prodotti da parte di un laboratorio indipendente accreditato dal National Voluntary Laboratory Accreditation Program (NVLAP) e incaricato di eseguire una valutazione dei prodotti per verificarne i requisiti di sicurezza. I prodotti vengono testati a fronte di rigorosi requisiti funzionali riguardanti la sicurezza sulla base di livelli EAL (Evaluation Assurance Levels) predefiniti o di specifici requisiti di sicurezza.

Ma l'esigenza di sicurezza non è meno importante per i settori sanitario, dei servizi finanziari e altri ancora. La garanzia che reti, dischi rigidi e linee telefoniche siano al sicuro da hacker, virus e altre attività fraudolente e in grado di proteggere la privacy dei clienti o risorse intellettuali e finanziarie è fondamentale. La certificazione Common Criteria, pur non essendo obbligatoria al di fuori del Governo degli Stati Uniti, può fornire una convalida indipendente.

Con circa 150 dispositivi che hanno completato la procedura di certificazione, Xerox vanta uno dei più ampi parchi multifunzione dotati di certificazione Common Criteria. Inoltre, Xerox è stato il primo produttore a certificare l'intero dispositivo, ed è a tutt'oggi l'unico produttore che certifica sempre l'intero dispositivo.

Visitate il sito www.xerox.com/information-security/common-criteria-certified per un elenco dei multifunzione Xerox® dotati di certificazione Common Criteria.

Valutazione e mitigazione del rischio

Sicurezza proattiva per le minacce emergenti

Offrirvi i prodotti più sicuri disponibili sul mercato è solo parte della nostra storia. I nostri ingegneri e tecnici sono dediti a sviluppare la nuova generazione di innovative tecnologie di sicurezza per combattere le minacce di domani e garantire la sicurezza dei vostri documenti: micro-stampa, stampa in fluorescenza e a infrarossi, Xerox® Glossmark® e tecnologia di Marcatura di correlazione, per citare solo alcuni esempi. Per ulteriori informazioni su tali tecnologie, visitare il sito www.xerox.com/security.

Altre cose che Xerox fa:

Monitoraggio di nuovi tipi di rischi

Eseguiamo un monitoraggio costante dei siti di analisi delle vulnerabilità per avere informazioni costantemente, liberandovi dall'incombenza di doverlo fare voi.

Pubblicazione di bollettini sulla sicurezza

Forniamo proattivamente aggiornamenti e patch sulla sicurezza quando necessario, mantenendo così le vostre apparecchiature aggiornate e i vostri dati sicuri.

Distribuzione di feed RSS

Gli aggiornamenti vengono distribuiti automaticamente ai lettori di feed RSS dei clienti.

Fornitura di una ricca gamma di informazioni

Per coloro che desiderano approfondire determinati argomenti, offriamo un'ampia e sempre crescente libreria di articoli, white paper e guide sulla sicurezza.

Visitate il sito www.xerox.com/security per accedere alla nostra ampia gamma di risorse sulla sicurezza.

Oltre alla propria accurata attività di verifica interna, Xerox monitora regolarmente i siti di analisi delle vulnerabilità resi disponibili da enti e risorse quali US-CERT ed il report Critical Patch Updates di Oracle® e i Bollettini sulla sicurezza Microsoft®, per rilevare eventuali vulnerabilità a livello di software o di sistema operativo;nonché bugtraq, SANS.org e secunia.com per le vulnerabilità dei software open source. Applichiamo inoltre un accurato programma interno di verifica della sicurezza che prevede analisi delle vulnerabilità e test di penetrazione per fornire patch accuratamente testate. Visitate il sito www.xerox.com/security per leggere il documento sulla politica di gestione e divulgazione delle vulnerabilità.

Bollettini sulla sicurezza e sviluppo di patch

Gli sviluppatori Xerox seguono un ciclo di vita formale sullo sviluppo della sicurezza che gestisce i problemi di sicurezza mediante un processo di identificazione, analisi, prioritizzazione, codifica e verifica. Ci sforziamo di fornire patch il più rapidamente possibile in base alla natura, origine e gravità della vulnerabilità. A seconda del livello di gravità della vulnerabilità, della dimensione della patch e del prodotto, la patch può essere distribuita separatamente o assumere la forma di una nuova release di software per quel prodotto.

A seconda di quale prodotto Xerox® richiede una patch, i clienti possono scaricare le patch di sicurezza su www.xerox.com/security. Per altri prodotti Xerox®, la patch di sicurezza viene resa disponibile come parte di una nuova versione di release del software di sistema. Potete registrarvi per ricevere i bollettini regolarmente. Negli Stati Uniti, i clienti devono registrarsi al feed RSS sulla sicurezza. Per tutti gli altri paesi, contattare il centro di assistenza Xerox locale.

Dal sito web www.xerox.com/security, potete accedere a tempestivi aggiornamenti di informazioni e risorse importanti:

- Bollettini sulla sicurezza
- Feed RSS: accesso ai bollettini sulla sicurezza
- Domande frequenti sulla sicurezza dei prodotti Xerox®
- Varie versioni del documento Information Assurance Disclosure Paper
- Prodotti con certificazione Common Criteria
- Politica di gestione e divulgazione delle vulnerabilità
- Guida alla sicurezza dei prodotti
- Articoli e white paper
- Dichiarazioni di volatilità
- Tabella di ricerca rapida delle release di software
- Guida FTC per copiatrici e multifunzione digitali

www.xerox.com/security è il portale che vi consente di accedere a un'ampia gamma di informazioni e aggiornamenti relativi alla sicurezza, come bollettini, white paper, patch e molto altro ancora.

Prassi di sicurezza adottate da produttori e fornitori

Xerox e i suoi principali partner di produzione sono membri della Electronic Industry Citizenship Coalition (http://www.eicc.info). Sottoscrivendo il Codice di condotta di EICC, Xerox e altre aziende dimostrano di attuare un rigoroso controllo dei loro processi di produzione.

Inoltre, Xerox ha relazioni contrattuali con i propri fornitori primari e secondari che le consentono di condurre verifiche in sede al fine di garantire l'integrità del processo fino al livello dei singoli componenti.

Xerox è inoltre membro della U.S. Customs Agency Trade Partnership Against Terrorism. Tale iniziativa è incentrata sulla sicurezza della catena di fornitura. Esempi di prassi adottate da Xerox ai sensi di questo programma sono quelle implementate per combattere il furto o l'appropriazione fraudolenta. In Nord America, tutti i rimorchi in transito tra la fabbrica e i centri di distribuzione dei prodotti (PDC), e tra i PDC ed i centri logistici dei trasportatori (CLC) vengono sigillati presso il sito di origine. Tutti i camion sono dotati di rilevatore satellitare e vengono costantemente monitorati.

Restituzione e smaltimento di prodotti

Offerta di conservazione dischi rigidi per i prodotti Xerox®

Xerox fornisce una Offerta di conservazione dei dischi rigidi per consentire ai clienti negli Stati Uniti di conservare il disco rigido su prodotti Xerox® noleggiati. L'offerta è a pagamento. Tale servizio potrebbe essere richiesto da clienti che gestiscono dati estremamente riservati o finanche classificati, o con politiche interne o standard normativi che richiedono specifici procedure di trattamento per i dischi rigidi.

Su richiesta per questa offerta di servizio, un tecnico di assistenza Xerox si recherà nella sede del cliente, rimuoverà il disco rigido e lo fornirà 'nello stato in cui si trova' a un rappresentante del cliente. Attualmente, Xerox non fornisce servizi di sanitizzazione, pulizia o distruzione dei dischi rigidi nella sede del cliente. I clienti dovranno prendere accordi per il trattamento finale del disco rigido fisico ricevuto dal tecnico.

Per stabilire se il vostro prodotto Xerox® contiene un disco rigido, o per esaminare le funzioni di sicurezza disponibili per proteggere dati e dischi rigidi, visitare il sito www.xerox.com/harddrive.

Per ulteriori informazioni su questo programma, contattare il rappresentante Xerox o visitare il sito www.xerox.com/security sotto Risorse per la sicurezza nella sezione Articoli e white paper.

Inoltre, praticamente tutte le nuove stampanti e multifunzione Xerox® sono dotati di serie di crittografia disco AES a 256 bit, nonché di sovrascrittura dati immagine a 3 passaggi per garantire che i dati dei nostri clienti siano protetti sin dal primo giorno sulle loro nuove apparecchiature.

Riepilogo

La sicurezza della rete e dei dati è una delle tante problematiche con cui le aziende devono combattere quotidianamente. E poiché le stampanti e i multifunzione di oggi svolgono il ruolo di veri e propri centri operativi dell'attività aziendale che ricevono e inviano dati importanti attraverso una varietà di funzioni, garantire un sistema di sicurezza completo è di fondamentale importanza.

È indispensabile che l'intero sistema di un multifunzione, insieme a tutto il software di gestione del dispositivo in rete, venga valutato e certificato di modo che il reparto di sicurezza informatica e tutti i dipendenti di un'organizzazione siano certi del fatto che i loro documenti e la loro rete sono al sicuro da pirati informatici o finanche da violazioni della sicurezza interne. Sotto tale aspetto, i multifunzione Xerox® sono al vertice del settore. Il nostro approccio globale, basato su un sistema di sicurezza solido, funzionale, avanzato e utilizzabile, è essenziale per la salvaguardia delle risorse informatiche dei nostri clienti.

Essendo consapevole di ciò, Xerox continua a progettare e sviluppare tutti i suoi prodotti in modo da garantire il più alto livello possibile di sicurezza su tutti i potenziali punti di vulnerabilità. Siamo impegnati a salvaguardare i vostri dati di modo che voi possiate concentrarvi sulle attività che consentiranno alla vostra azienda di raggiungere i più grandi successi.

Per ulteriori informazioni sui tanti vantaggi nel campo della sicurezza offerti da Xerox, visitate il sito www.xerox.com/security.

Elenco di controllo sulla sicurezza

I responsabili della sicurezza IT sono già oberati da richieste di gestione della sicurezza. Le piccole aziende devono fare affidamento su sistemi e software per la sicurezza efficienti per poter svolgere al meglio il loro lavoro. L'ultima cosa di cui voi e il vostro personale avete bisogno è un aumento degli interventi manuali necessari per monitorare e mantenere aggiornati tutti i dispositivi e flussi di dati del vostro ambiente di lavoro, comprese le stampanti e i multifunzione.

Un piano di sicurezza della rete globale deve basarsi su tre pilastri, e deve contemplare una strategia per ciascuno di essi affinché possa rivelarsi efficace.

1. I dispositivi ad "autoprotezione automatica" resistenti a nuovi attacchi
2. Conformità ai più aggiornati standard e normative sulla sicurezza
3. Completa visibilità sulla rete

Il nuovo standard di sicurezza per una nuova era

- La sicurezza non può essere relegata in secondo piano.
- Le informazioni sono una proprietà intellettuale sempre più preziosa.
- I firewall non sono sufficienti; le politiche sulla sicurezza devono essere olistiche e onnipresenti.
- La protezione dei dispositivi integrati è oggi parte integrante dell'imperativo di sicurezza del mondo d'oggi.

Xerox offre un sistema di sicurezza multilivello globale facile da implementare e installare, e vi aiuta a mantenere la vostra azienda conforme agli standard governativi e del settore. La tecnologia Xerox® è testata e approvata come in grado di proteggere contro tentativi di accesso non autorizzato, furti di dati e di identità.

Nel confrontare i sistemi multifunzione Xerox® con i prodotti di altre marche, utilizzate il seguente elenco di controllo per stabilire se i dispositivi della concorrenza offrono lo stesso livello di sicurezza end-to-end di quello fornito da Xerox.

		Concorrente		
	Xerox	**1**	**2**	**3**
Filtro indirizzo IP/MAC	✓			
Crittografia IPsec	✓			
IPv6	✓			
Autenticazione 802.1X	✓			
Stampa protetta	✓			
Crittografia di Scansione su email	✓			
PDF crittografato/PDF protetto da password	✓			
Firme digitali	✓			
AES a 256 bit Crittografia del disco fisso	✓			
Sovrascrittura immagini	✓			
Fax protetto	✓			
Blocco delle porte	✓			
Protezione password per Scansione su email	✓			
Offerta di conservazione dischi rigidi	✓			
Limitazioni sulla stampa	✓			
Registro di controllo	✓			
Controllo dell'accesso in base al ruolo	✓			
Autenticazione con Smart Card	✓			
Scheda ad accesso comune (CAC)/Verifica identità personale	✓			
Autorizzazioni dell'utente	✓			
Certificazione Common Criteria per "l'intero sistema"	✓			
Integrazione con gli strumenti di gestione di rete standard	✓			
Aggiornamenti sulla sicurezza tramite feed RSS	✓			
Protezione McAfee integrata basata su Intel® Security	✓			
McAfee® Integrity Control	✓			
Integrazione McAfee® ePolicy Orchestrator®	✓			
Integrazione con Cisco® Identity Services Engine (ISE)	✓			

Per saperne di più, visitate il sito **www.xerox.com**.

05/18 BR21699 SECGD-01IC