RICOH
imagine. change.

Soluzioni per la sicurezza Ricoh

Soluzioni per la sicurezza informatica delle aziende

La sicurezza informatica costituisce la principale minaccia per la sopravvivenza e il successo delle aziende. Queste, infatti, sono in costante pericolo di cadere vittime di attacchi pericolosi, quali phishing, DDoS o ransomware. Il costo reale di questi attacchi può ammontare a milioni di euro. Secondo uno studio condotto nel 2017 dal Ponemon Institute, il costo totale medio di un data breach è di 3,62 milioni di dollari. Tale costo è destinato ad aumentare nei prossimi anni a causa delle normative governative, come il GDPR (Regolamento generale sulla protezione dei dati), che hanno lo scopo di punire con pesanti multe le aziende che non riescono a proteggere in modo appropriato i propri sistemi e i propri dati. Per evitare tali misure punitive, è necessario che la capacità di un'azienda di proteggere i dati sia verificabile. Ciò richiede la visibilità completa di tutte le vulnerabilità all'interno dell'azienda.

A complicare ulteriormente la sfida rappresentata dalla sicurezza informatica è l'espansione e la digitalizzazione dello spazio di lavoro moderno, oltre alla crescita esponenziale del volume dei dati. I flussi di lavoro spesso sono condivisi attraverso dispositivi, reti e paesi differenti. Poiché le informazioni corrono i rischi maggiori quando vengono trasmesse all'interno dell'azienda, è necessario proteggerle durante ciascuna fase di questo processo. Considerati i rischi per la sicurezza, le aziende moderne non possono più operare senza rendere sicuri i propri sistemi di gestione di documenti e dati. Allo stesso tempo, le funzionalità delle stampanti e dei dispositivi multifunzione da ufficio sono aumentate in modo esponenziale negli ultimi anni. Ora tali dispositivi sono responsabili di una grande parte dei dati ricevuti, trasmessi, trasferiti e archiviati. Per questo motivo sono attualmente tra i più pericolosi vettori di minacce per gli uffici, e tuttavia spesso vengono sottovalutati.

Sebbene molte altre aziende sostengano di offrire soluzioni in tal senso, Ricoh sviluppa soluzioni e servizi per la sicurezza dell'ambiente di lavoro da decenni. Le nostre stampanti, ad esempio, dispongono della funzionalità di sovrascrittura del disco fisso da 20 anni.

La sicurezza è parte integrante dell'intero portfolio dei nostri prodotti per il digital workplace. Attualmente offriamo più di 4 milioni di prodotti per l'ufficio. Ciascuno di questi prodotti e ogni servizio offerto prevede funzionalità di sicurezza integrate. Inoltre, molti dei nostri prodotti utilizzano il sistema operativo Ricoh. Questa è una delle nostre difese di sicurezza principali, poiché offre controllo e isolamento dalle minacce specifiche che colpiscono i sistemi operativi più utilizzati.

Ricoh offre ai clienti un servizio di assistenza e supporto continuo a livello mondiale che assicura che informazioni e soluzioni riguardo alle minacce vengano condivise e implementate in modo efficiente. Oltre ad avere ottenuto la certificazione IEEE 2600 su tutti i dispositivi di stampa, Ricoh è uno dei membri più importanti e il principale fondatore della IEEE Standards Association. Ricoh ha ottenuto inoltre la certificazione ISO 27001, e continua ad impegnarsi per rispettare questo sistema di gestione della sicurezza delle informazioni. Quando progettiamo i prodotti, la nostra priorità è rispondere alle esigenze aziendali e ai problemi relativi alla sicurezza dei nostri clienti. Per farlo, utilizziamo una serie di programmi innovativi orientati al cliente a livello globale.

Per soddisfare anche i requisiti più esigenti in materia di sicurezza informatica, in ogni prodotto e servizio del portfolio di Ricoh sono incluse per impostazione predefinita funzionalità di sicurezza. Crediamo fermamente che una visibilità completa delle vulnerabilità sia fondamentale per la sopravvivenza delle aziende attuali.

ESIGENZE DI SICUREZZA DEL CLIENTE

TENDENZE: Con l'aumento del volume di dati, aumentano anche le vulnerabilità, gli attacchi e le sanzioni.

Protezione e ottimizzazione degli uffici digitali

Ricoh vuole ottimizzare e proteggere i documenti digitalizzati, indipendentemente dalla località in cui operano i dipendenti. Nella moderna economia digitale ciò significa prendere in considerazione anche le attività che si svolgono al di fuori degli uffici tradizionali. Gli uffici e i dipendenti remoti consentono alle aziende di aumentare notevolmente la flessibilità e la produttività nelle attività giornaliere. Inoltre, aiutano le aziende a soddisfare meglio le aspettative e i requisiti di assistenza dei clienti.

Tuttavia l'utilizzo della rete, ad esempio, pone dei rischi per la sicurezza aziendale. I dati generati dai dipendenti e dai dispositivi remoti devono essere protetti in modo adeguato. I dipendenti spesso utilizzano reti diverse e si trovano in aree geografiche differenti, complicando ulteriormente il compito. Inoltre, le normative governative quali il GDPR obbligano le aziende a proteggere i dati in modo verificabile per tutto il loro ciclo di vita per evitare pesanti sanzioni. Con l'evoluzione degli uffici e l'utilizzo dei flussi di lavoro digitali, il ciclo di vita dei dati aziendali diventa gradualmente più complicato. Esaminiamo come, passo per passo.

Il primo elemento da considerare sono i dispositivi di acquisizione e immissione dei dati, una parte essenziale del sistema di sicurezza Ricoh. Quindi, i dati devono essere trasferiti su reti diverse e archiviati in modo sicuro. In questa fase è fondamentale garantire l'integrità dei dati. I sistemi Ricoh limitano l'accesso alle funzionalità di reti e dispositivi da parte degli utenti per assicurare che non sia possibile alterare i dati quando vengono trasferiti. Tali servizi includono controllo degli accesi, crittografia e protezione da copia. Chiamiamo questa fase Controllo.

Una volta archiviati, tuttavia, i documenti devono essere resi disponibili perché possano essere utilizzati da tutti i dipendenti che ne hanno bisogno. La capacità di ottenere le informazioni quando sono richieste e di visualizzarle in modo efficace dipende da tale disponibilità. L'analisi dei dati è un elemento fondamentale degli uffici digitali efficienti, poiché offre informazioni importanti per ogni reparto dell'azienda, dall'ufficio vendite all'HR. L'infrastruttura di autorizzazione offre rapidamente l'accesso sicuro, indipendentemente dalla posizione dell'utente o dal dispositivo utilizzato. È importante assicurare che i protocolli di sicurezza non influiscano negativamente sull'innovazione o sulle funzionalità o che non vengano rifiutati dai dipendenti. Chiamiamo questa fase Conservazione.

Infine, i dati devono essere eliminati in modo sicuro e verificabile. Questo passaggio è essenziale per garantire il rispetto dei requisiti normativi e minimizza la possibilità di furto o perdita dei dati. Questo processo in realtà viene applicato durante tutta la vita di un documento, e non solo durante la sua eliminazione finale. Quando si stampa un file, un'immagine latente del documento rimane sul disco rigido dei multifunzione. Questa deve essere sovrascritta per impedire accessi non autorizzati ai dati. I servizi Ricoh per la rimozione dei dati includono pulizia del disco rigido, svuotamento della memoria, eliminazione dei file non stampati e cancellazione alla disconnessione per impedire ai pirati informatici di ottenere informazioni sensibili. Chiamiamo questa fase Distruzione.

Per proteggere in modo efficace i dati durante l'intero ciclo di vita, Ricoh utilizza i principi di privacy e sicurezza adottati dalla "CIA": confidenzialità, disponibilità e integrità. Questi sono i principi che seguiamo nella progettazione dei nostri prodotti e soluzioni per sodisfare tutti gli standard e le normative richieste. Tale approccio consente di innovare e ottimizzare l'ufficio mantenendo allo stesso tempo processi efficienti e sicuri.

L'APPROCCIO DI RICOH ALLA SICUREZZA

Seguiamo i principi di privacy e sicurezza adottati dalla "CIA": confidenzialità, integrità e disponibilità

La sicurezza è nel nostro DNA. Ogni prodotto e servizio realizzato e offerto da Ricoh dispone di capacità e funzioni di sicurezza integrate

Ricoh offre una suite completa di prodotti e servizi di sicurezza che consentono di proteggere la creazione di documenti durante tutto il processo.

Ora passeremo a descrivere ogni fase critica: controllo, conservazione, distruzione e supporto.

QUATTRO FASI PER LA SICUREZZA DEGLI UFFICI DIGITALI

1 CONTROLLO

Eseguire controlli efficienti dei dati è fondamentale per garantire la confidenzialità e integrità dei dati stessi. Le informazioni aziendali sono una risorsa importantissima e devono essere protette. I dispositivi hardware sono terminali informativi che possono costituire dei gateway vulnerabili per le informazioni aziendali. A tale scopo, Ricoh utilizza una serie di strumenti per l'autenticazione utente e la gestione dei dispositivi che consentono di controllare e proteggere i dati aziendali. Tali strumenti includono le impostazioni sui dispositivi fisici che permettono o impediscono l'accesso a determinati dati e funzionalità. La limitazione dell'accesso dei dipendenti alle informazioni trasmesse a un multifunzione è una best practice fondamentale per garantire la sicurezza dei documenti. La fase di controllo include anche la protezione da attacchi malware utilizzando l'approccio su tre livelli Ricoh per il firmware dei dispositivi.

Controllo delle copie non autorizzate

Per impedire la copia non autorizzata e garantire la sicurezza dei documenti cartacei, Ricoh offre un'eccellente soluzione. La funzione di protezione da copia consente di stampare o copiare i documenti con speciali motivi invisibili sullo sfondo. Se il documento stampato o copiato viene fotocopiato e/o scansionato, i motivi vengono riprodotti sulle copie. Il modulo di protezione contro la copia non autorizzata consente al multifunzione di rilevare tali motivi e sostituire l'immagine originale con un'immagine grigia per impedire la fuga di informazioni. Questa funzione è molto utile per la stampa di informazioni confidenziali. La limitazione della copia delle informazioni confidenziali previene la fuga di questo tipo di informazioni.

Stampa protetta

Un documento ricevuto da un PC può essere archiviato nell'unità disco rigido del multifunzione. Quando si utilizza la funzione Stampa riservata di Ricoh, viene specificata una password quando l'utente invia il documento, e tale password deve essere immessa nel multifunzione per stamparlo. Poiché il documento non verrà stampato prima che il proprietario raggiunga il dispositivo, la Stampa riservata garantisce che quest'ultimo abbia il controllo sul documento.

Protezione avanzata per la scansione

Il portfolio di soluzioni avanzate di acquisizione Ricoh offre diversi livelli di crittografia e decrittografia tramite livelli di elaborazione, per tutte le fasi del processo di acquisizione. Gli amministratori possono autorizzare l'accesso utilizzando i dati di accesso di un singolo utente o le credenziali di un gruppo. Ulteriori livelli di sicurezza includono l'utilizzo di Security Assertion Markup Language (SAML) per il framework di Single Sign On (SSO), Personal Identity Verification (PIV) e crittografia con infrastruttura a chiave pubblica (PKI).

Controlli di autenticazione integrati

I protocolli di accesso ai dispositivi e autenticazione dell'identità di tutti i prodotti Ricoh possono essere gestiti in modo centralizzato. I metodi disponibili includono l'utilizzo di un badge, un numero PIN, i dati di accesso alla rete o l'autenticazione a più fattori che prevede una combinazione degli elementi descritti sopra. L'autenticazione a più fattori aumenta la sicurezza ma può rallentare il lavoro degli utenti. Il sistema Single Sign On (SSO) aiuta a risolvere questo problema, perché consente agli utenti di accedere facilmente a diversi dispositivi. Inoltre, il sistema di autenticazione rapida Ricoh, che utilizza un software di autenticazione basato su un lettore di schede magnetiche, è preinstallato su tutti i nostri dispositivi, consentendo agli utenti di accedere facilmente ai documenti. L'utilizzo di un lettore/scrittore NFC semplifica il processo di accesso degli utenti, proteggendo e controllando allo stesso tempo l'accesso ai multifunzione. Questo metodo di accesso può anche essere utilizzato insieme all'impostazione di autenticazione del multifunzione per limitare l'accesso degli utenti alle funzioni del dispositivo secondo le disposizioni del cliente.

Streamline NX (SLNX)

Il modulo di gestione dei dispositivi all'interno della piattaforma Streamline NX è il software Ricoh per la gestione e il monitoraggio dei dispositivi di una rete. Il software consente agli amministratori di visualizzare o configurare le impostazioni di sicurezza dei dispositivi che utilizzano modelli preconfigurati e parametri personalizzati. Le impostazioni di sicurezza includono attivazione/disattivazione dei protocolli, impostazione dell'indirizzo IP, gestione delle password amministratore, invio di avvisi tramite e-mail, impostazioni di crittografia e molto altro. SLNX è in grado di segnalare qualsiasi stampante che non è conforme ai requisiti del cliente.

Protezione dei dispositivi da attacchi malware

Ricoh applica un approccio su tre livelli per proteggere i propri dispositivi dagli attacchi malware. Prima di tutto, i dispositivi Ricoh possono funzionare solo utilizzando un linguaggio macchina o un sistema operativo Ricoh. In secondo luogo, per prevenire la manomissione intenzionale del software dei dispositivi, tutti gli aggiornamenti del firmware devono essere scritti e approvati esclusivamente nel linguaggio macchina di Ricoh. Infine, tutti gli aggiornamenti del devono avere la firma digitale di Ricoh. Grazie a questo metodo in tre fasi, i firmware non autorizzati non possono essere caricati sui dispositivi di Ricoh, consentendo di evitare efficacemente attacchi malware, spyware e virus.

Protezione dei documenti cartacei

Le best practice di sicurezza non sono sempre complicate. Gli uffici sono luoghi affollati e i documenti cartacei rappresentano un'importante minaccia per la sicurezza aziendale, sia per il rischio di furti che a causa della negligenza dei dipendenti. Ricoh offre una serie di opzioni fisiche aggiuntive di sicurezza per impedire l'accesso non autorizzato ai documenti cartacei. Ad esempio, chiudere a chiave i cassetti che contengono i documenti è una soluzione che aiuta a prevenire il furto di documenti sensibili, come le ricette mediche in ambiente sanitario. È consigliabile anche fissare la piastrina di chiusura di tutti i cavi per prevenire la manomissione dei dati da parte di minacce interne. La soluzione per il rilascio sicuro dei documenti (funzione Print-to-me) assicura che i documenti vengano stampati solo in presenza del proprietario, in modo da eliminare il rischio che i documenti stampati vengano lasciati incustoditi.

2 CONSERVAZIONE

Secondo i requisiti normativi passati e presenti, le aziende devono garantire sia la confidenzialità delle informazioni, in modo che queste non possano essere rubate o perse, sia l'integrità, in modo che non possano essere alterate. Per raggiungere questo obiettivo, le aziende devono limitare l'accesso ai documenti sensibili. Questa misura consente di impedire la modifica non autorizzata e la falsificazione dei dati. Inoltre, agisce come protezione da attacchi mirati o opportunistici all'interno dell'azienda.

Il lavoro mobile complica evidentemente il panorama della sicurezza informatica. È necessario implementare misure di sicurezza aggiuntive per supportare la condivisione dei file da diverse posizioni. I file devono essere protetti sia durante il trasferimento sulle reti che durante l'archiviazione. Una tecnologia di crittografia avanzata può proteggere i dati in modo efficace durante il loro ciclo di vita. Naturalmente tale tecnologia può essere applicata ai documenti ma anche agli elementi cruciali della sicurezza, come password archiviate, impostazioni delle macro e rubriche. Grazie alla crittografia, nel caso di un tentativo di violazione, anche nell'eventualità che i pirati informatici riuscissero ad accedere alla rete aziendale, non riuscirebbero ad estrarre alcuna informazione utile conservandone l'integrità.

Per molte aziende è fondamentale mantenere elevati i tempi di attività ed evitare le interruzioni. Eventi imprevisti, quali ad esempio i disastri naturali, possono quindi rappresentare un rischio diretto per l'azienda. Nell'eventualità di eventi di questo tipo, i documenti cartacei devono essere protetti in modo particolare. L'utilizzo di un repository protetto basato sul cloud per i documenti digitalizzati offre sicurezza per far fronte ai disastri naturali o provocati dall'uomo. Tuttavia, è necessario implementare delle misure di scurezza appropriate per proteggere i dati digitali.

Crittografia dei dati

Per proteggere le informazioni quando vengono trasferite da un dispositivo all'altro, è possibile abilitare la crittografia dei dati trasferiti o archiviati sul disco fisso di un multifunzione Ricoh. Le opzioni integrate del software offrono la crittografia end-to-end per i file scansionati e stampati utilizzando un'infrastruttura a chiave pubblica (PKI). Questa offre protezione dagli attacchi "man in the middle" nell'ambiente IT del cliente.

Per aumentare ulteriormente la sicurezza, i dati di stampa vengono continuamente sovrascritti dal sistema di protezione con sovrascrittura dati (DOSS) di Ricoh, che verrà illustrato più dettagliatamente nel capitolo che descrive la fase Distruzione del ciclo di vita dei dati.

Protezione del BIOS e dei sistemi operativi

I multifunzione Ricoh utilizzano il Trusted Platform Module (TPM), un modulo di sicurezza hardware che offre protezione contro qualsiasi manomissione. Il TPM esegue funzioni di crittografia e archivia in modo sicuro i dati crittografati. Ricoh utilizza il TPM per archiviare la chiave radice della crittografia che protegge la chiave di crittografia dei dati del disco fisso e il certificato digitale del multifunzione. Questo consente agli amministratori di eseguire operazioni di avvio sicure e di convalidare l'autenticità del firmware del multifunzione prima di consentirne l'utilizzo.

Convalida del firmware

La chiave radice e le funzioni di crittografia sono sempre mantenute all'interno del TPM e non possono essere alterate al di fuori del firewall, consentendo di prevenire l'utilizzo scorretto o la manomissione intenzionale dei nostri prodotti. Questo processo offre un sistema di convalida di alto livello del firmware del multifunzione, dell'identità del dispositivo e della sicurezza del disco fisso. Si tratta di un altro esempio che dimostra come i prodotti multifunzione Ricoh siano progettati mantenendo come priorità le esigenze di sicurezza dei clienti.

Gestione delle password

Quando si configurano i dispositivi Ricoh, è possibile impostare più utenti amministratore, ognuno con un ruolo differente sui dispositivi e con password diverse. Le password di questi utenti possono essere configurate da remoto tramite gli strumenti web di amministrazione e verificate regolarmente. Ciò consente la "separazione dei compiti", che è un requisito di molte normative aziendali.

Restrizioni di accesso utente

Lo strumento di gestione degli utenti di Ricoh consente agli amministratori di sistema di limitare i privilegi di accesso degli utenti. Ad esempio, l'amministratore può configurare dei privilegi per consentire a degli utenti selezionati di accedere alla rubrica registrata nel multifunzione. Ciò consente di bloccare qualsiasi accesso non autorizzato alle informazioni personali e ai dati archiviati nei dispositivi dell'ufficio.

Funzione di blocco utente

Se durante il processo di accesso viene immessa una password errata più volte consecutivamente, i multifunzione Ricoh sono in grado di stabilire se è in corso un tentativo di ottenere tale password. Ciò attiva la funzione di blocco, che blocca il nome utente in questione. Il nome utente bloccato non potrà essere autenticato anche utilizzando la password corretta. Il blocco può essere rilasciato dopo un determinato intervallo di tempo o da un amministratore, prevenendo in modo efficace qualsiasi tentativo di manomissione da parte di utenti malintenzionati.

3 DISTRUZIONE

La rimozione sicura dei dati è un elemento fondamentale di qualsiasi sistema di sicurezza informatica. È facile cadere nell'errore di pensare che le responsabilità dell'azienda nei confronti dei dati finiscano quando questi abbandonano l'organizzazione. Diverse normative esigono che la distruzione dei dati sia un processo completo, che elimini in maniera definitiva qualsiasi rischio di furto o utilizzo scorretto. Gli obblighi di un'azienda nei confronti dei dati non sono finiti fino a quando questa non può provare di aver completato correttamente tale processo.

I dispositivi dell'ufficio alla fine del ciclo di vita o dismessi rappresentano un rischio per le informazioni aziendali che viene spesso trascurato. Ricoh offre un servizio certificato e verificabile che garantisce la rimozione definitiva di tutti i dati dai dispositivi alla fine del ciclo di vita. Nel servizio sono inclusi dati spesso ignorati, quali impostazioni di rete, dati utente, dati del disco rigido e persino le etichette adesive lasciate sul dispositivo. Ignorando tali dati, le aziende corrono il grave rischio di esporre informazioni aziendali e personali confidenziali. Per garantire la conformità alle normative, è necessario applicare tale processo ai dispositivi durante tutto il loro ciclo di vita. Ciò assicura che le aziende abbiano il controllo assoluto dei dati per i quali sono responsabili.

Sovrascrittura immagine: Sistema di protezione con sovrascrittura dati (DOSS)

I dischi fissi dei dispositivi multifunzione archiviano le immagini latenti dei dati dei documenti nella propria memoria per l'elaborazione dei processi. Il sistema di protezione con sovrascrittura dati Ricoh assicura che queste vengano sovrascritte costantemente prima che venga avviato il processo successivo. In questo modo, se un utente accedesse al disco fisso con cattive intenzioni, non potrebbe ottenere accesso alle "tracce" lasciate dai dati dei processi precedenti. Ricoh è orgogliosa di offrire questa misura di sicurezza da oltre 20 anni.

Servizio di pulizia dei dati per i dispositivi alla fine del ciclo di vita

Ricoh offre il servizio Data Cleansing completo per i dispositivi alla fine del ciclo di vita che consente di cancellare definitivamente i dati dai moduli di memoria e dal disco fisso di multifunzione e stampanti utilizzando soluzioni di sicurezza che vantano certificazioni del settore. Tra i servizi IT offerti da Ricoh è incluso anche un servizio per la dismissione in sicurezza dei dispositivi che comprende diversi processi per la rimozione certificata dei dati.

Sostituzione del disco fisso e dei supporti di archiviazione rimovibili

Ricoh offre inoltre un servizio per lo smaltimento dei dischi fissi che offre ai clienti il controllo assoluto del proprio disco fisso, sostituendolo con un disco nuovo e vuoto al termine del contratto di noleggio. Ciò garantisce che l'azienda abbia il controllo completo e verificabile del proprio ambiente dati.

4 SUPPORTO

Con la crescita di un'azienda è destinato ad aumentare anche il numero di connessioni tra dispositivi e reti. Le aziende hanno bisogno di strategie per evitare che la crescita di tale infrastruttura rappresenti un rischio per la sicurezza. Inoltre, devono conoscere le vulnerabilità esistenti nei propri sistemi per prevenire in modo efficace attacchi mirati e opportunistici.

Spesso per analizzare la struttura aziendale e identificare tali vulnerabilità sono richieste profonde conoscenze in materia di sicurezza IT. Per molte aziende è impossibile mantenere un team IT interno con le conoscenze necessarie per gestire il proprio ambiente di sicurezza informatica. Il costo e l'inefficienza di tale strategia spesso obbligano le aziende a non fare nulla al riguardo, correndo rischi pericolosi.

Il servizio di supporto Ricoh offre servizi di fornitura e di configurazione dei dispositivi IT, monitoraggio remoto e assistenza, oltre alla gestione della transizione, per rafforzare ulteriormente i processi di sicurezza informatica. Per una sicurezza informatica efficace, è necessaria una comprensione generale di tutti i rischi aziendali. Il team di risoluzione degli incidenti di sicurezza Ricoh (SIRT) assicura che informazioni vitali sulle minacce vengano condivise con i clienti di tutto il mondo, consentendo di coordinare le risposte in modo efficace.

Valutazione della sicurezza dell'infrastruttura

Streamline NX (SLNX) di Ricoh per la gestione dei dispositivi è progettato anche per eseguire funzioni di controllo delle politiche di sicurezza. SLNX offre una funzionalità che i manager IT possono utilizzare per configurare i dispositivi in base ai criteri di sicurezza dell'azienda, distribuire tali impostazioni e analizzarle utilizzando il report che può essere visualizzato. SLNX può anche avvisare i manager quando un dispositivo non è conforme ai criteri aziendali.

Ottimizzazione della protezione della stampa

Ricoh offre il servizio Print Security Optimisation (PSO), che, se utilizzato con i servizi di consulenza professionali e di gestione, consente di identificare i problemi di sicurezza relativi ai dispositivi. Si tratta di uno strumento web con una procedura guidata grafica che offre una panoramica dello stato corrente dei dispositivi e consente a Ricoh di offrire consigli allo scopo di ridurre i rischi.

Team di risoluzione degli incidenti di sicurezza

La risposta attiva di Ricoh contro le nuove minacce e per lo sviluppo di contromisure efficaci è gestita tramite il programma Product Security Incident Response Team (PSIRT). Si tratta di un programma utilizzato da Ricoh per assicurare che l'intera suite di prodotti (hardware e software) venga continuamente aggiornata e protetta contro le ultime minacce e vulnerabilità rilevate. Questo ci consente di mantenere un livello costantemente elevato di assistenza a livello globale e di minimizzare l'impatto dei problemi di vulnerabilità sui prodotti Ricoh.

Documentazione di supporto

La preparazione e la documentazione sono elementi cruciali per la configurazione di qualsiasi sistema di sicurezza informatica. È necessario fornire ai clienti formazione oltre a documentazione di supporto, manuali utente e white paper sulla sicurezza. Come per molti elementi nell'ambito della sicurezza informatica, è fondamentale che la conformità sia verificabile e la documentazione ha un ruolo importante in tutto ciò.

COME PUÒ AIUTARTI RICOH?

La posizione unica di Ricoh, che le consente di offrire soluzioni di sicurezza leader del settore per la stampa e l'ambiente IT, si basa su una profonda comprensione dei cambiamenti del mercato e sulla conseguente evoluzione della strategia. Le nostre soluzioni sono progettate per proteggere tutte le informazioni durante l'intero ciclo di vita e si basano sulle quattro fasi per la sicurezza dei dati descritte in questo report.

Disponiamo di esperti dedicati in materia responsabili dell'analisi delle esigenze di mercato, inclusi i requisiti specifici del settore, per rispondere ai quali è possibile creare nuove soluzioni o modificare soluzioni esistenti.

Ci impegniamo anche ad aumentare le nostre capacità interne per progettare e implementare soluzioni di sicurezza. A tale scopo, abbiamo creato dei team dedicati all'interno dell'organizzazione della distribuzione dei nostri servizi, che hanno il compito di sviluppare nuovi servizi di government, gestione dei rischi, conformità e sicurezza informatica.

Autorizzazione e autenticazione utente

- Stampa riservata
- Software per l'autenticazione integrato
- Autenticazione utente/restrizioni di accesso
- Single sign-on
- Ruoli di amministratore multipli
- Protezione tramite password dei documenti PDF (password per documenti scansionati)
- Protezione contro la copia non autorizzata
- Controllo degli accessi in base all'intervallo IP
- Gestione sicura di stampe e dispositivi
- PKI (Infrastruttura a chiave pubblica)/Supporto di SmartCard
- Stampa sicura (print2me/stampa riservata)

Protezione dei dispositivi da attacchi malware

- Server
- Minore predisposizione agli attacchi malware
- SOP – versione protetta di Android
- Sistema operativo Ricoh (linguaggio di controllo della macchina) per gli MFP
- Approccio su 3 livelli: firma digitale, download tramite lo strumento Ricoh, scrittura in un linguaggio di controllo specifico

Smaltimento del disco fisso

- Smaltimento del disco fisso, sovrascrittura immagini
- Servizio di pulizia completa dei dati
- Assistenza prodotti alla fine del ciclo di vita: distruzione dei dati all'interno dei moduli di memoria

Gestione dei dispositivi

- Impostazione quote/limiti account
- DMNX: gestione con interfaccia a finestra unica di controlli di sicurezza, password, monitoraggio, avvisi

Protezione del BIOS e dei sistemi operativi

- Avvio sicuro tramite la piattaforma Trusted Platform Module (TPM)

Sovrascrittura immagini e supporti di archiviazione rimovibili

- Sistema di protezione con sovrascrittura dati (DOSS)
- Disco fisso rimovibile

Crittografia dei dati

- Crittografia del disco fisso tramite TPM
- Chiavi di crittografia tramite TPM
- Crittografia end-to-end dei file di stampa e di scansione tramite chiave PKI
- Disco fisso con certificazione FIPS (Federal Information Processing Standards)
- Crittografia end-to-end per la stampa
- Crittografia end-to-end per la scansione

Aggiornamenti del firmware e gestione della password

- Verifica remota password
- Funzione di blocco utente
- Convalida del firmware tramite TPM

Conformità agli standard del settore

- Certificazione ISO 27001
- Certificazione IEEE 2600.2 per prodotti selezionati
- Certificazione ISO 15408 per prodotti selezionati
- Documentazione sulla sicurezza e formazione

L'APPROCCIO RICOH SU PIÙ LIVELLI PER LA SICUREZZA DEI DISPOSITIVI

Non c'è dubbio che il ruolo dei fornitori di dispositivi multifunzione si è evoluto ben oltre la semplice fornitura di hardware e comprende ora anche la gestione dei dati. Le funzionalità dei dispositivi multifunzione includono l'acquisizione di informazioni da più canali di input, la classificazione dei dati acquisiti e l'integrazione nei flussi di lavoro, fino all'archiviazione e all'analisi in un ambiente protetto. In questo scenario complesso di regole, normative e requisiti di conservazione dei dati, a cui si aggiunge il rischio di perdita, distruzione o manomissione dei dati a causa di minacce interne ed esterne, adottiamo un approccio su più livelli per garantire la sicurezza dei dispositivi ed assicurare la massima protezione per i multifunzione e i sistemi a cui si connettono.

1. Dispositivi

I dispositivi sono alla base di tutto per Ricoh. Quando vengono progettati, prodotti e installati, la sicurezza rappresenta un requisito fondamentale. Il sistema operativo Ricoh non condivide le vulnerabilità presenti in molti sistemi operativi commerciali standard. Inoltre, i nostri dispositivi dispongono dello standard IEEE2600.2 per impostazione predefinita. La crittografia e la sovrascrittura del disco fisso sono misure di sicurezza che assicurano che i dati elaborati rimangano confidenziali.

2. Smart Operation Panel (SOP) per l'interfaccia utente

Come i dispositivi multifunzione, anche il SOP utilizza il sistema operativo Ricoh. Non è necessario installare alcun componente aggiuntivo e non è possibile accedere al root. Ricoh ha lavorato a lungo per garantire che la sicurezza dei dispositivi non venga compromessa dal SOP.

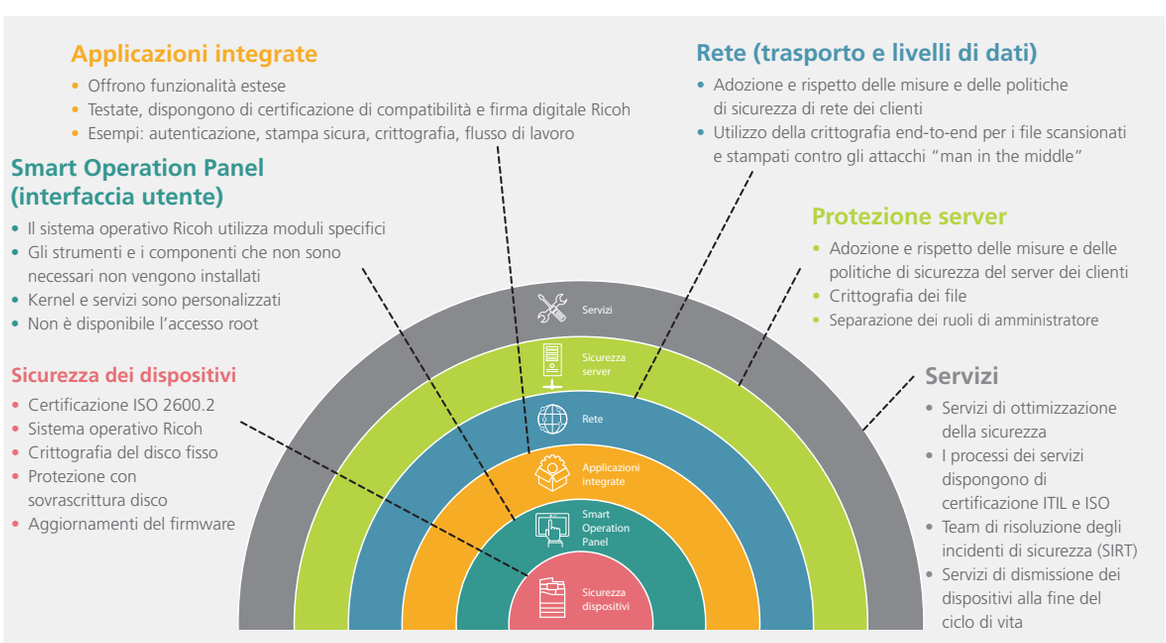
3. Applicazioni smart

Queste possono essere integrate direttamente nel SOP, fornendo ulteriori funzionalità per la gestione dei flussi di lavoro e l'acquisizione dei dati. Alcune applicazioni offrono funzioni di sicurezza fondamentali. Queste includono la funzione di stampa protetta, l'accesso tramite badge e la crittografia. Le applicazioni vengono sviluppate da Ricoh o dai membri del Ricoh Developer Programme. Inoltre, tutte le applicazioni devono passare il test di compatibilità Ricoh e devono ottenere la firma digitale prima di essere eseguite nel SOP.

4. Reti e server

Indipendentemente da chi gestisce l'infrastruttura IT, Ricoh assicura che i propri prodotti e servizi soddisfino le politiche IT e di sicurezza della rete. La crittografia end-to-end dei file stampati e scansionati, la crittografia dei dati sui server e la separazione delle mansioni degli amministratori sono strategie utilizzate per proteggere i dati dagli attacchi "man in the middle" o "inside jobs".

La nostra offerta di prodotti include una gamma completa di servizi di sicurezza. Questi includono la consulenza e servizi gestiti per aiutare i clienti a monitorare, ottimizzare e gestire la sicurezza di documenti e informazioni. Offriamo anche una vasta gamma di servizi per i prodotti alla fine del ciclo di vita che garantiscono la rimozione completa di tutti i dati dalla RAM e dal disco fisso dei dispositivi ritirati dai clienti prima che questi vengano dismessi.



CHE TIPO DI PROTEZIONE OFFRE RICOH AGLI UFFICI DIGITALI

I nostri clienti hanno una serie di preoccupazioni in materia di sicurezza legate alla realtà aziendale, poiché con l'aumento del volume di dati sono aumentate anche le vulnerabilità, gli attacchi e le sanzioni. Assicurare la confidenzialità e la sicurezza dei dati, e proteggerli da qualsiasi tentativo di manomissione, è un compito arduo. Per fare un esempio, Ricoh blocca 8 miliardi di attacchi firewall ogni mese. Esistono decine di migliaia di normative internazionali, nazionali e del settore in materia di sicurezza dei dati, e le aziende devono essere in grado di dimostrare continuamente la propria conformità ad esse. A tale scopo, le aziende cercano un partner affidabile, un partner che le aiuti a mantenere protetti i dati attraverso un portfolio di prodotti che comprendono l'intero ufficio digitale.

Ricoh ha sviluppato una vasta gamma di soluzioni per ridurre i rischi a cui sono esposte le aziende. Poiché il panorama delle minacce di sicurezza muta in maniera incredibilmente veloce, Ricoh mette a disposizione programmi "voce del cliente" per sviluppare ulteriormente i suoi servizi.

I nostri Consigli di amministrazione dei clienti sono una parte strategica dei nostri gruppi di lavoro. Tali comitati ci consentono di ottenere una migliore comprensione delle tendenze, degli obiettivi e delle priorità che sono alla base delle aziende dei nostri clienti. Le nostre Conferenze consultive sulla tecnologia offrono informazioni importanti da parte dei decision maker del settore. I team di progettazione e Ricerca e Sviluppo di Ricoh utilizzano queste conferenze per ottenere feedback importanti da parte dei clienti su idee, concetti e prototipi. Per concludere, Ricoh collabora con i clienti per sviluppare funzioni di sicurezza nuove e avanzate per i clienti dei mercati generale e verticale. Tale approccio orientato al cliente ci consente di rafforzare la strategia alla base dei nostri prodotti e di aiutare i clienti a trarre vantaggio dalla nostra rete globale di servizi e assistenza.

L'ufficio digitale moderno deve essere dinamico quanto le minacce a cui è esposto e flessibile come le modalità lavorative necessarie per il suo funzionamento. Per questa ragione crediamo che la sicurezza informatica debba essere applicata senza soluzione di continuità per tutta la tecnologia utilizzata dai nostri clienti per ottimizzare i propri uffici. Il nostro impegno per garantire la certificazione ISO 27001 in tutta la nostra organizzazione, la certificazione IEEE 2600 per tutti i nostri prodotti e il sistema operativo Ricoh integrato, dimostrano che i sistemi di sicurezza Ricoh funzionano in modo ottimale.

Considerando le minacce alle sicurezza, i requisiti normativi e i complessi standard del settore è chiaro che il potenziale rischio di danno economico e di reputazione a causa degli attacchi informatici non è mai stato maggiore. È arrivato il momento di scegliere un partner fidato che aiuti la tua azienda a proteggere le risorse più vulnerabili e i progetti per il futuro.

RICOH
imagine. change.

www.ricoh.ch