Documentazione tecnica

Soddisfate i requisiti di conformità in materia di sicurezza della rete e dei dati

Suggerimenti per applicare i controlli di sicurezza al parco stampanti

Sommario

Cliccate qui per verificare la versione più aggiornata di questo documento

Le violazioni alla conformità normativa possono danneggiare la vostra azienda

Oltre a sanzioni e cause legali, una violazione della sicurezza può causare perdita di profitti e danni alla reputazione. Nella creazione del vostro piano di sicurezza, ricordate che la sicurezza della vostra rete equivale a quella del suo punto più debole. I dispositivi di stampa e imaging presentano molte vulnerabilità analoghe a quelle dei PC. È fondamentale implementare dispositivi e soluzioni che vi aiutino a soddisfare i requisiti di conformità e a proteggere i dati della vostra azienda dalle minacce alla sicurezza.

Qual è il rischio

I problemi di conformità alle normative e alla legge impongono alle aziende globali di farsi carico di costi elevati, tra cui sanzioni, perdita di affari, danni alla reputazione e azioni legali collettive.

Gli endpoint non protetti o non sufficientemente protetti creano opportunità per il crimine informatico. Le organizzazioni intervistate da Ponemon in un recente studio hanno subito in media due attacchi a settimana nel 2016, con un aumento del 23% rispetto all'anno precedente e una perdita media di 9,5 milioni di dollari l'anno per la lotta alla criminalità informatica[1]. Solo lo scorso anno, nel mondo sono stati compromessi più di 4 miliardi di record di dati, con un aumento del 400% rispetto ai due anni precedenti[2].

Sebbene le misure relative alla sicurezza sui computer e sulla rete vengano applicate in maniera rigorosa da parte di molti reparti IT, le minacce relative ai dispositivi di stampa e imaging vengono spesso sottovalutate. Le stampanti, peraltro, possono costituire un punto di ingresso alla rete, ed è per questo altrettanto importante metterle in sicurezza. Di tutte le violazioni gravi segnalate dai manager IT, il 26% ha riguardato le stampanti.[3]

Per contribuire a contrastare la minaccia crescente, gli enti governativi di tutto il mondo stanno implementando norme di sicurezza nuove e maggiormente rigorose che impongono alle aziende di proteggere meglio le informazioni dei clienti. A titolo di esempio, il nuovo Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea è un mandato fondamentale che entrerà in vigore nel 2018. Il regolamento GDPR aumenta i requisiti imposti alle aziende per la tutela dei dati. Ecco perché è consigliabile assicurarsi che ogni dispositivo sulla rete, dai PC alle stampanti e persino ai dispositivi mobili, sia protetto. Il nuovo mandato non interessa solamente i paesi UE: anche le aziende globali dovranno rispettarlo se raccolgono e utilizzano i dati dei residenti nell'Unione Europea. Le aziende dovranno monitorare e valutare ogni dispositivo per rilevare e segnalare le violazioni della protezione entro 72 ore dalla scoperta. Se i controlli di conformità rilevassero violazioni non monitorate o non segnalate, le aziende potrebbero dover pagare sanzioni fino a 20 milioni di euro o al 4% del fatturato annuo dell'azienda.

Utilizzate i comuni controlli di sicurezza per migliorare la conformità

Non è facile mantenersi al passo con la conformità e le normative del settore. Fortunatamente, il CIS (Center for Internet Security) ha creato un set di controlli comuni di sicurezza per semplificare i suggerimenti finalizzati alla sicurezza informatica. I controlli critici di sicurezza indicati dal CIS sono rappresentati da 20 azioni specifiche che possono contribuire a fermare gli attacchi informatici. (Per maggiori informazioni, consultare https:www.cisecurity.org/critical-controls.cfm.) I controlli sono in linea con numerose altre normative del settore quali PCI-DSS, ISO 27001, raccomandazioni US CERT, HIPAA, FFIEC e NIST. I controlli non intendono sostituire tali altri quadri normativi, ma sono frequentemente usati dalle imprese per facilitarne l'applicazione.

I controlli critici CIS per la sicurezza pongono la priorità su un numero più ristretto di azioni in grado di determinare risultati particolarmente significativi. Si rivolgono ai modelli di attacco più comuni tratti dai principali report relativi alle minacce informatiche. Sono stati redatti con il contributo di un nutrito gruppo di esperti del settore, tra cui le principali organizzazioni forensi e strutture di intervento in caso di incidente. I controlli, inoltre, sono costantemente aggiornati in base all'evolversi di minacce e attacchi.

Utilizzate i controlli critici CIS per la sicurezza per contribuire a razionalizzare il vostro piano d'azione per la sicurezza e a ottemperare alle normative relative alla conformità. Il presente documento illustra le azioni consigliate per ciascuno dei 20 controlli, al fine di proteggere i vostri dispositivi di stampa, i dati e i documenti nell'ambito del vostro più ampio programma di sicurezza. I controlli 4, 6, 8, 12, 13 e 15 riguardano nello specifico le attività di monitoraggio e protezione dei dati relativamente ai nuovi requisiti di GDPR.

Controlli critici per la sicurezza CIS e azioni suggerite

CCS 1: inventario dei dispositivi autorizzati e non autorizzati

Controllo. Gestire attivamente (inventario, monitoraggio e correzione) tutti i dispositivi hardware in rete, in modo tale che solo i dispositivi autorizzati dispongano dell'accesso. I dispositivi non autorizzati e non gestiti verranno identificati e verrà impedito loro l'accesso.

Suggerimento. Assicuratevi che tutti i dispositivi di stampa in rete siano documentabili e gestiti attivamente nel rispetto della vostra policy di sicurezza. Uno strumento efficace di gestione della sicurezza di stampa può scoprire e dare visibilità a tutta la rete e ai dispositivi connessi ai PC.

CCS 2: inventario dei software autorizzati e non autorizzati

Controllo. Gestire attivamente (inventario, monitoraggio e correzione) tutto il software in rete in modo tale che sia installato ed eseguibile solo software autorizzato. Il software non autorizzato e non gestito verrà identificato e ne verrà impedita l'installazione o l'esecuzione.

Suggerimento. Accertatevi che tutti i firmware e le soluzioni caricate nei dispositivi di stampa e imaging siano aggiornate, firmate e convalidate come autentiche. Scegliete dispositivi di stampa dotati di protezione integrata di BIOS e firmware, per assicurarvi che venga caricato solo codice autentico. Gli aggiornamenti proattivi del firmware possono essere imposti all'intero parco dispositivi mediante apposite soluzioni di gestione del parco stampanti. Il software (basato su server o su client) deve essere sottoscritto e convalidato come autentico.

CCS 3: configurazioni di sicurezza per hardware e software su dispositivi mobile, notebook, workstation e server

Controllo. Fissare, implementare e gestire attivamente (monitoraggio, reporting e correzione) la configurazione della sicurezza di notebook, server e workstation mediante una gestione rigorosa delle configurazioni; modificare la procedura di controllo al fine di impedire ai violatori di sfruttare i servizi e le impostazioni più vulnerabili.

Suggerimento. Come altri endpoint di rete, anche le stampanti devono essere configurate in modo sicuro. Il vostro compito è quello di creare e implementare una policy di sicurezza valida per tutti i dispositivi di stampa e di correggere attivamente ogni deviazione da tale policy. Gli elenchi di controllo per la sicurezza (come il NIST) o i servizi di consulenza sulla sicurezza possono aiutarvi a progettare e implementare una policy di stampa completa. Uno strumento efficace per la gestione della sicurezza di stampa può automatizzare la creazione, l'implementazione, la valutazione della policy e la correzione delle impostazioni dei dispositivi in tutto il parco stampanti. Le stampanti multifunzione di livello enterprise dispongono di oltre 250 impostazioni di sicurezza, quindi l'automatizzazione della procedura di esecuzione può assicurare un significativo risparmio di tempo.

CCS 4: valutazione costante e correzione delle vulnerabilità

Controllo. Acquisire, valutare e agire costantemente sulle nuove informazioni per identificare le vulnerabilità, correggere e ridurre al minimo le finestre di opportunità per i violatori.

Suggerimento. Le soluzioni SIEM (Security Information and Event Management) quali ArcSight, Splunk e SIEMonster possono monitorare l'attività nella vostra rete in tempo reale e informare gli amministratori in caso di incidente. Monitorare i dispositivi di stampa è importante quanto monitorare i PC: assicuratevi che le vostre stampanti siano in grado di inviare messaggi syslog relativi agli eventi al vostro strumento SIEM.

Scegliete dispositivi di stampa dotati di funzionalità che consentano di rilevare in tempo reale gli attacchi, ripristinare automaticamente e ottimizzare i tempi di esercizio riducendo al minimo gli interventi dell'IT.

Per ridurre le vulnerabilità, utilizzate uno strumento di gestione della sicurezza dei dispositivi in grado di identificare le nuove stampanti e applicare automaticamente le impostazioni relative alle vostre policy di sicurezza aziendali non appena i dispositivi vengono connessi alla rete. Programmate una serie di intervalli di valutazione/correzione per mantenere l'intero parco stampanti sempre conforme alla policy.

CCS 5: uso controllato dei privilegi di amministratore

Controllo. Monitoraggio, controllo, prevenzione e correzione dell'uso, delle assegnazioni e della configurazione dei privilegi di amministratore su computer, reti e applicazioni.

Suggerimento. Scegliete dispositivi di stampa in grado di autenticare gli utenti e controllare in base al ruolo della persona gli accessi alle funzioni, in modo tale che solo il personale IT o altri addetti autorizzati possano impostare e configurare i dispositivi. Utilizzate un software di gestione della sicurezza del parco stampanti per implementare le password di amministratore in tutto il parco dispositivi.

CCS 6: manutenzione, monitoraggio e analisi dei registri di controllo

Controllo. Raccolta, gestione e analisi dei registri di controllo relativi a eventi che possono aiutare a rilevare, comprendere o ripristinare dopo un attacco.

Suggerimento. I dispositivi di stampa devono poter generare messaggi syslog relativi a incidenti, consentendo al vostro team addetto alla sicurezza di verificare regolarmente i registri di controllo e di scoprire e risolvere i problemi. Per lo svolgimento di una corretta revisione e rispondere agli altri requisiti di conformità, scegliete dispositivi in grado di inviare tali messaggi alle soluzioni di gestione della sicurezza del parco stampanti e agli strumenti SIEM, consentendo sia il monitoraggio in tempo reale sia la generazione di report.

CCS 7: protezione di e-mail e browser Web

Controllo. Ridurre al minimo i margini di attacco e le opportunità per i violatori di manipolare i comportamenti umani mediante l'interazione con browser Web e sistemi di posta elettronica.

Suggerimento. Le stampanti multifunzione sono spesso connesse a Internet, ad esempio, per inviare scansioni tramite e-mail. Assicuratevi che le scansioni inviate per e-mail siano crittografate per proteggere i dati sensibili. Implementate dispositivi e soluzioni in grado di autenticare gli utenti e controllare l'accesso alle risorse interne al dispositivo (ad esempio server Web o funzionalità e-mail) in base al ruolo della persona. Create un elenco di "siti fidati" per le vostre stampanti multifunzione e gestitelo adeguatamente per assicurarvi che dal dispositivo si acceda solo a tali siti fidati. Integrate diversi metodi di autenticazione (come PIN/PIC, LDAP e autenticazione Kerberos) con Active Directory per facilitare la gestione e accrescere la sicurezza. I dispositivi di stampa connessi alla rete devono disporre di protezione integrata da malware e virus; il firmware delle stampanti deve essere regolarmente aggiornato affinché siano attive le protezioni più avanzate.

CCS 8: difese da malware

Controllo. Controllare l'installazione, la diffusione e l'esecuzione di codice dannoso presso molteplici punti nell'azienda, ottimizzando nel contempo l'utilizzo dell'automazione per consentire un rapido aggiornamento della difesa, della raccolta dati e delle azioni correttive.

Suggerimento. Scegliete dispositivi di stampa che carichino solo codice verificato e firmato e che dispongano di funzionalità anti-malware integrate per monitorare attivamente la memoria del dispositivo e riavviarlo in caso di attacco. Uno strumento efficace per la gestione della sicurezza di stampa può valutare e correggere automaticamente le impostazioni dei dispositivi di tutto il parco stampanti. Si deve inoltre verificare che tutte le soluzioni software di stampa siano firmate e convalidate come autentiche.

CCS 9: limitazione e controllo di porte di rete, protocolli e servizi

Controllo. Gestione (monitoraggio, controllo e correzione) dell'utilizzo operativo corrente di porte, protocolli e servizi sui dispositivi in rete, per ridurre al minimo le finestre di vulnerabilità disponibili ai violatori.

Suggerimento. Qualora non già disabilitate per impostazione predefinita, disabilitate le porte non usate e i protocolli non sicuri (ad esempio FTP e Telnet), che gli autori degli attacchi possono usare per accedere al dispositivo. Fate risparmiare tempo all'IT e riducete i rischi implementando uno strumento di gestione della sicurezza di stampa che consenta di mantenere automaticamente le impostazioni dei dispositivi conformi in tutto il parco dispositivi. Utilizzate password di amministratore, autenticazioni e controlli di accesso basati sul ruolo per limitare l'accesso a funzioni e impostazioni dei dispositivi.

CCS 10: funzionalità di ripristino dei dati

Controllo. Effettuare un adeguato backup dei dati critici con una metodologia collaudata, per un tempestivo ripristino.

Suggerimento. Questo controllo non si applica attualmente alle stampanti.

CCS 11: protezione delle configurazioni per dispositivi di rete come firewall, router e switch

Controllo. Fissare, implementare e gestire attivamente (monitoraggio, reporting e correzione) la configurazione di sicurezza dei dispositivi dell'infrastruttura di rete, utilizzando una gestione rigorosa delle configurazioni, e modificare la procedura di controllo al fine di impedire ai violatori di sfruttare i servizi e le impostazioni più vulnerabili.

Suggerimento. Le stampanti sono in rete e, come altri endpoint, devono essere configurate in modo sicuro. Uno strumento efficace per la gestione della sicurezza di stampa può automatizzare l'implementazione, la valutazione e la correzione delle impostazioni dei dispositivi di tutto il parco per contribuire al mantenimento della sicurezza della rete, facendo risparmiare tempo all'IT.

CCS 12: difesa dei dati esterni e in transito

Controllo. Rilevamento, prevenzione e correzione del flusso di dati mediante trasferimento di reti dotate di diversi livelli di affidabilità con attenzione ai dati potenzialmente dannosi per la sicurezza.

Suggerimento. Utilizzate la crittografia dei dati per proteggere i dati in transito (processi di stampa o scansione che transitano verso o dalla stampante) e presenti nel disco rigido dei dispositivi. Scegliete dispositivi e soluzioni di stampa in grado di autenticare gli utenti e controllare gli accessi alle funzioni in base al ruolo della persona: ad esempio, solo gli utenti autorizzati potranno inviare per e-mail le scansioni o inviare file su destinazioni cloud. Impostate i siti Web fidati nell'elenco "siti fidati" del dispositivo per impedire l'accesso a siti dannosi. Le soluzioni per la sicurezza della stampa da mobile possono facilitare la stampa da dispositivi mobile e nel contempo proteggere la rete.

CCS 13: protezione dei dati

Controllo. Prevenire le esfiltrazioni di dati, ridurre gli effetti di eventuali esfiltrazioni di dati, assicurare la privacy e l'integrità dei dati sensibili.

Suggerimento. Utilizzate la crittografia dei dati per proteggere i dati in transito (processi di stampa o scansione che transitano verso o dalla stampante) e presenti nel disco rigido dei dispositivi. Implementate soluzioni di stampa pull per evitare di lasciare documenti sensibili in vassoi di raccolta non vigilati. Accertatevi che i dati memorizzati nei dischi rigidi dei dispositivi vengano cancellati in modo sicuro prima di restituire i dispositivi noleggiati o in leasing o prima di riciclarli a fine vita.

CCS 14: accesso controllato basato sul principio del "need to know"

Controllo. Monitoraggio, controllo, prevenzione, correzione e protezione dell'accesso a risorse critiche (ad es. dati, risorse e sistemi) a seconda di una risoluzione formale relativa a chi, quali computer e applicazioni necessitino e siano autorizzati ad accedere a tali risorse critiche in base a una pre-classificazione approvata.

Suggerimento. Scegliete dispositivi e soluzioni di stampa in grado di autenticare gli utenti e controllare gli accessi alle funzionalità in base al ruolo della persona. Integrate diversi metodi di autenticazione (come PIN/PIC, LDAP e autenticazione Kerberos) con Active Directory per facilitare la gestione e accrescere la sicurezza. Le soluzioni di stampa pull possono proteggere i documenti sensibili dal finire nelle mani sbagliate.

CCS 15: controllo accesso wireless

Controllo. Monitoraggio, controllo, prevenzione e correzione dell'utilizzo di reti LAN wireless, access point e sistemi client wireless.

Suggerimento. Uno strumento efficace di gestione della sicurezza di stampa può automatizzare l'implementazione, la valutazione e la correzione delle impostazioni dei dispositivi, incluse quelle wireless di tutto il parco dispositivi. Usate le soluzioni di controllo degli accessi per limitare l'accesso alle funzionalità del dispositivo, come la scansione verso e-mail, in base al ruolo dell'utente. Le soluzioni per la sicurezza di stampa da mobile possono facilitare la stampa da dispositivi mobile e nel contempo proteggere la rete. Ad esempio, i dispositivi che supportano la stampa wireless peer-to-peer consentono agli utenti mobile di stampare direttamente mediante un segnale wireless riservato alla stampante, senza accedere alla rete o al servizio wireless aziendale.

CCS 16: monitoraggio e controllo degli account

Controllo. Gestione attiva del ciclo di vita degli account di sistemi e applicazioni: creazione, uso, quiescenza, cancellazione, al fine di ridurre al minimo le opportunità di utilizzo da parte dei violatori.

Suggerimento. Scegliete dispositivi e soluzioni di stampa in grado di autenticare gli utenti e controllare gli accessi alle funzionalità in base al ruolo dell'utente. Integrate l'autenticazione con Active Directory per una gestione centralizzata e una maggiore protezione. Verificate regolarmente gli account utente e disabilitate quelli non necessari, utilizzate soluzioni di monitoraggio per controllarne l'uso. Crittografate i nomi utente relativi agli account e le credenziali di autenticazione, sia in transito sia archiviate del dispositivo. I consulenti per la sicurezza possono aiutarvi a redigere un piano completo di sicurezza di stampa per ridurre al minimo i rischi e, in alcuni casi, anche a gestire la sicurezza, inclusi il monitoraggio e il controllo degli account.

CCS 17: valutazione delle capacità in ambito sicurezza e formazione adeguata per risolvere le criticità

Controllo. Identificare le competenze specifiche, le capacità e i talenti necessari per sostenere la difesa dell'azienda; sviluppare ed eseguire un piano integrato per la valutazione, l'identificazione e la correzione dei problemi, mediante policy, pianificazione organizzativa, formazione e programmi di informazione per tutti i ruoli funzionali dell'azienda.

Suggerimento. I consulenti di sicurezza per la stampa dispongono delle competenze specifiche per aiutarvi a valutare i vostri rischi alla sicurezza, sviluppare una policy e un piano di sicurezza completi, e implementare i suggerimenti relativi a processi e tecnologie. Alcuni servizi per la sicurezza possono persino gestire per voi sicurezza di stampa e conformità.

CCS 18: sicurezza dei software applicativi

Controllo. Gestire il ciclo di vita di sicurezza di tutti i software sia sviluppati internamente sia acquistati al fine di prevenire, rilevare e correggere i punti di debolezza nella sicurezza.

Suggerimento. Aderite alle best practice relative allo sviluppo in sicurezza per tutte le soluzioni di stampa sviluppate. Scegliete soluzioni software firmate e convalidate come autentiche.

CCS 19: intervento e gestione di incidenti

Controllo. Proteggere i dati e la reputazione aziendale, sviluppando e implementando un'infrastruttura di intervento in caso di incidente (ad es. piani, ruoli definiti, formazione, comunicazioni e supervisione gestionale).

Suggerimento. Confermate che il vostro ambiente di stampa sia incluso nel vostro piano di intervento in caso di incidente.

CCS 20: test di penetrazione ed esercitazioni del red team

Controllo. Mettere alla prova la robustezza complessiva delle difese di un'azienda (tecnologie, processi e persone) simulando gli obiettivi e le azioni dell'autore di un attacco.

Suggerimento. Includete l'ambiente di stampa nel corso dei test di penetrazione. Valutate periodicamente il vostro ambiente di stampa in relazione alle vulnerabilità e aggiornate il piano di sicurezza al fine di affrontare eventuali punti di debolezza.

Fate il prossimo passo

L'implementazione dei suggerimenti contenuti in questo documento può aiutarvi a potenziare la sicurezza di stampa e a rispettare le normative in materia di conformità. Serve aiuto? I servizi di gestione della sicurezza di stampa e di consulenza possono aiutarvi a sviluppare un piano e a implementare procedure e tecnologie in grado di accrescere la sicurezza dei vostri dispositivi di stampa, dati e documenti.

Appendice A: funzionalità, soluzioni e servizi HP per la sicurezza di stampa

Le funzionalità di sicurezza integrate nei dispositivi HP, unite a soluzioni e servizi software leader di settore, vi aiutano a soddisfare i requisiti di conformità e a proteggere i dati della vostra azienda dalle minacce alla sicurezza.

Le funzionalità per la sicurezza integrate nelle stampanti e nelle multifunzione HP Enterprise difendono dai malware e sono in grado di rilevare automaticamente un attacco ed effettuare il ripristino. Solo la sicurezza di stampa HP offre il rilevamento in tempo reale, il monitoraggio automatizzato e il software di convalida integrato in grado di bloccare le minacce quando si presentano.[4] (Contribuisce al rispetto dei CCS 2, 4, 6, e 8.) hp.com/go/PrintersThatProtect

Le soluzioni HP Access Control forniscono numerosi controlli di accesso basati su autenticazione e ruolo, per aiutare a ridurre le potenziali violazioni alla sicurezza, oltre al monitoraggio dei lavori e alla rendicontazione. (Contribuisce al rispetto dei CCS 5, 7, 10, 12, 13, 14, 15 e 16.) hp.com/go/hpac

La crittografia e le soluzioni per il flusso di lavoro HP JetAdvantage proteggono i dati sia archiviati sui dispositivi HP Enterprise sia in transito verso e da dispositivi di stampa o cloud. (Contribuisce al rispetto dei CCS 12 e 13.) hp.com/go/upd, hp.com/go/documentmanagement

Le soluzioni HP di stampa pull proteggono i documenti riservati mediante l'archiviazione dei documenti di stampa su server protetto, su cloud o nel vostro PC. Gli utenti si autenticano presso il punto scelto in cui richiamano il documento ed effettuano la stampa. (Contribuisce al rispetto dei CCS 10, 13 e 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect offre agli utenti mobile facile accesso alla stampa da smartphone e tablet, mantenendo il livello di sicurezza e il controllo di amministratore di cui avete bisogno. (Contribuisce al rispetto dei CCS 12 e 15.) hp.com/go/JetAdvantageConnect

I dati delle stampanti HP sono inviabili a strumenti SIEM quali ArcSight, Splunk e SIEMonster. Il team della sicurezza può in tal modo proteggere gli endpoint di stampa HP FutureSmart nell'ambito di un più ampio ecosistema IT, eseguendo azioni correttive. (Contribuisce al rispetto dei CCS 4 e 6.)

HP JetAdvantage Security Manager è l'unico strumento di conformità per la sicurezza della stampa del settore basato su policy.[5] Aiuta a fissare una policy di sicurezza valida per l'intero parco dispositivi, automatizzare le correzioni alle impostazioni dei dispositivi, installare e rinnovare i certificati univoci ottenendo nel contempo i report necessari per dimostrare la conformità. La funzionalità Instant-on inclusa nella soluzione configura automaticamente i nuovi dispositivi al momento della loro aggiunta alla rete o dopo un riavvio. (Contribuisce al rispetto dei CCS 1, 2, 3, 4, 5, 6, 8, 9, 11 e 15.) hp.com/go/securitymanager

HP Secure Managed Print Services offre le protezioni per la sicurezza di stampa più solide e complete del settore.[6] La sicurezza della stampa può rivelarsi complessa. Lasciate che HP gestisca la vostra sicurezza di stampa, dal rafforzamento dei dispositivi alle soluzioni di sicurezza avanzate rivolte a persone, processi e requisiti di conformità. (Contribuisce al rispetto dei CCS 2, 3, 12, 16, 17, 18 e 19.) hp.com/go/SecureMPS

I servizi HP Print Security Professional offrono l'ausilio di esperti di sicurezza per aiutarvi a valutare il vostro ambiente di stampa, fissare proattivamente le policy di sicurezza e mantenere aggiornato il vostro piano di sicurezza. Possiamo anche gestire per voi l'intera conformità della sicurezza di stampa. (Contribuisce al rispetto dei CCS 2, 3, 12, 16, 17 e 19.) hp.com/go/SecureMPS

Note

[1] Studio Ponemon sponsorizzato da HPE, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation", 2016.

[2] Report 2016 Year End Data Breach QuickView di RiskBased Security, gennaio 2017.

[3] Il 26,2% dei partecipanti al sondaggio ha riscontrato gravi violazioni della sicurezza IT, che hanno richiesto un intervento; oltre il 26,1% di tali incidenti ha coinvolto i dispositivi di stampa. IDC, "IT and Print Security Survey 2015" IDC #US40612015, settembre 2015.

[4] Si applica ai dispositivi HP di classe Enterprise introdotti dall'inizio del 2015 e sulla base di verifiche HP pubblicate nel 2016 sulle funzionalità di sicurezza integrate nelle stampanti della stessa categoria dei produttori concorrenti. Solo HP offre una combinazione di funzionalità di sicurezza per la verifica dell'integrità del BIOS con capacità di auto-riparazione. Per attivare le funzionalità di sicurezza potrebbe essere necessario un aggiornamento dei service pack FutureSmart. Per un elenco dei prodotti compatibili, consultare hp.com/go/PrintersThatProtect. Per maggiori informazioni, consultare hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager deve essere acquistato separatamente. Per maggiori informazioni, consultare hp.com/go/securitymanager. Dichiarazione sulla concorrenza basata su una ricerca interna HP sui prodotti concorrenti (Device Security Comparison, gennaio 2015) e Solutions Report su HP JetAdvantage Security Manager 2.1 di Buyers Laboratory LLC, febbraio 2015.

[6] I nostri fornitori di servizi, leader nel settore, vi offriranno funzionalità di sicurezza per dispositivi, dati e documenti. In base a verifiche HP sulle informazioni pubblicate nel 2015 e nel 2016 su servizi per la sicurezza, funzionalità di sicurezza integrate in dispositivi e software di gestione della stessa categoria di produttori concorrenti. Per maggiori informazioni, consultare hp.com/go/MPSsecurityclaims or hp.com/go/mps.

Iscrivetevi per ricevere gli aggiornamenti
hp.com/go/getupdated

Condividi il documento con i colleghi

4AA6-8821ITE, Giugno 2017, Rev. 1