9 MISURE PER INCREMENTARE LA SICUREZZA DI DATI E DISPOSITIVI

Riducete i rischi associati alle stampanti termiche per codici a barre

RISERVATEZZA

Applicate il modello RID a 360 gradi

INTEGRITÀ

DISPONIBILITÀ

1 CRITTOGRAFARE TUTTE LE CONNESSIONI

Utilizzate una tecnologia di crittografia e autenticazione, anche se i dispositivi si trovano su una rete Ethernet oppure non gestiscono direttamente informazioni di tipo business-critical.

2 RUOTARE LE CREDENZIALI

Cambiate a rotazione password utente, chiavi e credenziali dei dispositivi; è un'operazione semplice se usate un sistema di gestione dispositivi centralizzato.

3 PROTEGGERE L'ACCESSO

Non sacrificate la protezione per una maggiore facilità d'uso. Riducete il rischio di un utilizzo non conforme dei dispositivi proteggendo l'accesso e attivando una semplice procedura di login con password dal pannello frontale.

4 MONITORARE I METODI DI COMUNICAZIONE

Valutate la possibilità di disattivare servizi di rete come FTP, SNMP e SMTP, che possono esporvi a rischi.

5 CONTROLLARE I SISTEMI DI GESTIONE REMOTA DEI DISPOSITIVI

I sistemi di gestione remota possono migliorare la produttività dell'IT, ma è importante controllarne attentamente l'accesso e le autorizzazioni.

6 ESEGUIRE GLI AGGIORNAMENTI PERIODICI IN MODO RISERVATO

Le comunicazioni su tempi e modalità degli aggiornamenti devono essere divulgate solo nei casi in cui è strettamente necessario.

7 MONITORARE I DISPOSITIVI

Utilizzate fin dall'inizio uno schema di denominazione dei dispositivi e un sistema di gestione che consentano di localizzare i dispositivi e di individuare rapidamente quelli che potrebbero essere smarriti o rubati, in modo da ritirare prontamente le relative credenziali.

8 CONSIDERARE I LUNGHI CICLI DI VITA DEI DISPOSITIVI

Per i dispositivi che dureranno fino a 10 anni, selezionate un sistema operativo che possa essere aggiornato regolarmente per stare al passo con i nuovi standard. Durante gli aggiornamenti, utilizzate una qualche forma di firma digitale per assicurare che la sua "integrità" rimanga intatta.

9 RITIRARE I DISPOSITIVI IN SICUREZZA

Quando ritirate i dispositivi, cancellate file e impostazioni, rimuovete le credenziali e gli account utente e verificate che nessuno dei vostri sistemi sia codificato permanentemente in modo da continuare a cercare o tentare di utilizzare i dispositivi ritirati.

Scoprite come Link-OS migliora il livello di protezione delle stampanti per codici a barre e dei dati; visitate www.zebra.com/linkos.

ZEBRA

©2016 ZIH Corp e/o affiliate. Tutti i diritti riservati. ZEBRA e il disegno della testa di Zebra sono marchi commerciali di ZIH Corp, registrati in molte giurisdizioni del mondo.