9 MASSNAHMEN ZUR STEIGERUNG DER GERÄTE- UND DATENSICHERHEIT

Reduzieren Sie Risiken in Zusammenhang mit Thermo-Barcodedruckern

VERTRAULICHKEIT

Durchgängige Anwendung des VIV-Modells

INTEGRITÄT | **VERFÜGBARKEIT**

1 VERSCHLÜSSELN ALLER VERBINDUNGEN

Verwenden Sie eine Verschlüsselungs- und Authentifizierungstechnologie, selbst wenn Geräte in einem Ethernet sind oder geschäftskritische Informationen nicht direkt handhaben.

2 WECHSELN VON ANMELDEDATEN

Wechseln Sie Benutzerkennwörter, Schlüssel und Anmeldedaten für Ihre Geräte – diese Aufgabe ist mit einem zentralisierten Geräteverwaltungssystem einfacher.

3 SCHÜTZEN DES ZUGANGS

Benutzerfreundlichkeit sollte nicht zulasten von Sicherheit gehen. Erschweren Sie den Gerätemissbrauch, indem Sie den Zugang schützen und ein einfaches Bedienfeldkennwortsystem aktivieren.

4 ÜBERWACHEN VON KOMMUNIKATIONSMETHODEN

Ziehen Sie in Betracht, ungenutzte Netzwerkdienste, wie z. B. FTP, SNMP und SMTP, zu deaktivieren, die Sie einer Gefahr aussetzen.

5 KONTROLLIEREN VON REMOTE-GERÄTEVERWALTUNGSSYSTEMEN

Remote-Verwaltungssysteme können zwar die IT-Produktivität beträchtlich verbessern, doch der Zugriff und die Berechtigungen sollten sorgfältig kontrolliert werden.

6 REGELMÄSSIGE UPDATES AUF VERTRAULICHE WEISE

Hinweise zum Zeitpunkt und zur Vorgehensweise von Updates sollten nur nach Bedarf gegeben werden.

7 NACHVERVOLGUNG VON GERÄTEN

Nutzen Sie von Anfang an ein Namensschema sowie ein Managementsystem, mit denen Sie Geräte verfolgen können und die ermöglichen zu entdecken, ob sie verlorengegangen sind oder gestohlen wurden, damit Sie die zugehörigen Anmeldedaten ungültig machen können.

8 BERÜCKSICHTIGUNG DES LANGEN LEBENSZYKLUS VON GERÄTEN

Wählen Sie für Geräte, die bis zu 10 Jahre lang halten, ein Betriebssystem, das regelmäßig aktualisiert werden kann, um mit den sich ändernden Standards konform zu sein. Verwenden Sie während der Updates digitale Signaturen, um sicherzustellen, dass die „Integrität“ noch intakt ist.

9 SICHERES AUSMUSTERN VON GERÄTEN

Beim Ausmustern von Geräten sollten Sie Dateien und Einstellungen löschen, Anmeldedaten oder Benutzerkonten entfernen und sicherstellen, dass Ihre Systeme nicht hartcodiert sind, sodass sie kontinuierlich nach den entfernten Geräten suchen, um sie zu nutzen.

Entdecken Sie, wie Link-OS neue Maßstäbe beim Schutz von Barcodedruckern und Daten setzt, und besuchen Sie www.zebra.com/linkos.

ZEBRA

©2016 ZIH Corp. und/oder verbundene Unternehmen. Alle Rechte vorbehalten. ZEBRA und der stilisierte Zebra-Kopf sind Marken von ZIH Corp., die in vielen Ländern weltweit eingetragen sind.