So sichern Sie Ihre Endpunktgeräte zur Erfüllung von Complianceanforderungen.

Aufgrund der allgemeinen EU-Datenschutzverordnung müssen Unternehmen technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten ergreifen und gegebenenfalls die betroffenen Einzelpersonen und die Behörden benachrichtigen, wenn personenbezogene Daten von einem Sicherheitsvorfall betroffen sind.

Dies ist für Unternehmen eine Herausforderung in Bezug auf den zeitlichen Aufwand und die Ressourcen, die für die Umsetzung dieser Vorordnung erforderlich sind.

Wenn sie jedoch nicht mehr als eine einfache Firewall einrichten, kann dies zu Verstößen führen, die Bußgelder in Millionenhöhe nach sich ziehen. Es bestehen kaum Zweifel, dass es in jedem Unternehmen irgendwann zu einem Verstoß kommt. Daher ist es wichtig zu erkennen, wann dies genau passiert, und dies so schnell wie möglich mit den richtigen Produkten, Prozessen und Tools zu korrigieren.

Diese Checkliste ist eine praktische Ressource für all jene, die ihre IT-Sicherheit steigern und die kostenintensiven Folgen eines Sicherheitsverstoßes vermeiden möchten. Wenn Sie mit den Grundlagen einsteigen und sich bis zu den maximalen Sicherheitsschichten durcharbeiten, können Sie sich darauf verlassen, dass Ihre Drucker-Endpunkte sicher sind und die Anforderungen der DSGVO erfüllen.

Eine praktische Liste zur Sicherung von Endpunktgeräten in Ihrem Netzwerk.

Basis-Sicherheitsschicht

- Erwerben Sie nur Geräte mit integriertem Malware-Schutz und verschlüsselten Festplatten.
- Aktualisieren Sie die Firmware, insbesondere bei kritischen Sicherheits-Updates – genauso oft, wie Sie es bei Apps auf Ihrem Mobiltelefon tun.
- Konfigurieren Sie Geräteschnittstellen und beenden Sie Protokolle wie FTP und Telnet, die von Ihren Anwendungen nicht benötigt werden.
- Überprüfen Sie neue Geräte und schließen Sie nicht verwendete Ports oder Protokolle, um Eindringlingen den Zugang zu verwehren.
- Verwenden Sie eindeutige Administrator-Passwörter für jedes Gerät.
- Verriegeln Sie das Front Panel, um den Zugang zu Administratorfunktionen auszuschließen.
- Verschlüsseln Sie alle ein- und ausgehenden Daten des Gerätes.
- Setzen Sie Verfahren zum Löschen von Altdaten von Festplatten um – insbesondere an Druckern, die Sie austauschen.

Fahren Sie nach Abschluss mit der nächsten Sicherheitsschicht fort.

Mittlere Sicherheitsschicht

- Integrieren Sie die Protokolldaten von Druckersystemen in Ihr SIEM-Tool, um das Netzwerk hinsichtlich Bedrohungen noch umfassender zu überwachen. Hinsichtlich neuer Compliancerichtlinien ist Sichtbarkeit der Schlüssel, um Reportinganforderungen zu erfüllen.
- Wenden Sie eine Benutzerauthentifizierung am Drucker an, um nachzuverfolgen, wer über dieses Gerät kopiert, scannt und faxt. Diese Daten sind nach einem Verstoß für eine forensische Untersuchung hilfreich.
- Wenden Sie die Pull Printing-Funktion an, um zu vermeiden, dass sensible Informationen vergessen werden. Dies unterstützt auch Ihre Umweltstandards durch die Reduzierung von überflüssigen Drucken.

Fahren Sie nach Abschluss mit der letzten Sicherheitsschicht fort.

Erweiterte Sicherheitsschicht

- Richten Sie die Auftragsnachverfolgung und Kontoberichte ein.
- Ziehen Sie das Erstellen von automatisierten Regeln in Betracht, die bestimmen, wer auf welchen Drucker zugreifen und diesen verwenden kann (mit rollenbasierter Autorisierung).
- Wenden Sie für jeden Drucker eindeutige digitale Zertifikate an, wie Sie dies auch mit anderen Geräten in Ihrem Netzwerk mit Internetzugang tun würden.
- Wenden Sie für die Datenverschlüsselung, den Gerätezugriff im Netzwerk und die Benutzerauthentifizierung und Nachverfolgung eine verwaltete mobile Drucklösung an.

4AA7-1093DEE