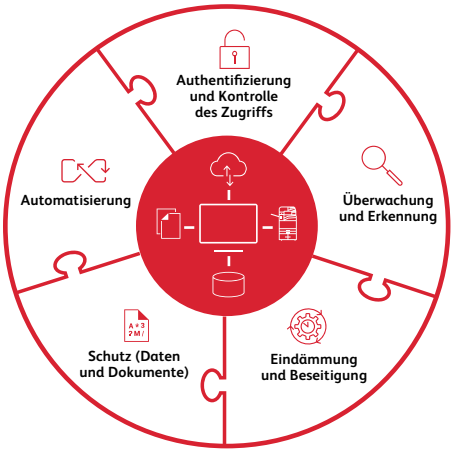
Zero Trust

Cyberkriminalität hat weltweit nie da gewesene Ausmaße erreicht und wird voraussichtlich weiter zunehmen. Unternehmen brauchen neue Strategien und bewährte Verfahren, um sich gegen diese Bedrohungen zu wehren.

Mobile Mitarbeiter von heute müssen jederzeit und von überall aus auf ihre IT-Infrastruktur zugreifen können. Immer mehr Initiativen zur digitalen Transformation erleichtern den Zugriff auf Geschäftsdaten. Eine Vielzahl von IoT-Geräten ist nun mit kritischen Geschäftssystemen verbunden, die das Grundgerüst jedes Unternehmens bilden. Diese Trends setzen Sicherheitsexperten immer mehr unter Druck, den modernen Arbeitsplatz zu schaffen und gleichzeitig die Angriffsfläche für Sicherheit im Unternehmen zu verringern.

Zero Trust hat sich als leistungsstarke Methode erwiesen, um sicheren Zugriff auf autorisierte Benutzer und Geräte zu ermöglichen und gleichzeitig den Sicherheitsstatus des Unternehmens zu verbessern.

Umfassende Sicherheit ist ein Schwerpunktthema von Xerox. Deshalb stellen wir unsere Kunden Produkte und Dienstleistungen zur Unterstützung von Zero Trust-Initiativen zur Verfügung. Konzepte wie „never trust, always verify“, „least privilege access“, proaktive Erkennung und Beseitigung von Bedrohungen, Verschlüsselung und Sicherheitszertifizierungen sind nicht neu. Werden sie jedoch im Rahmen einer kohärenten Sicherheitsstrategie eingesetzt, stellen sie entscheidende Merkmale eines erfolgreichen Zero-Trust-Sicherheitsprogramms dar.



Implementierung von Zero Trust

Wir unterstützen Ihre Zero Trust-Initiativen mit den folgenden bewährten Verfahren und Empfehlungen:

AUTHENTIFIZIERUNG UND KONTROLLE DES ZUGRIFFS

Mit der Richtlinie „Kein implizites Vertrauen“ beginnen und sicherstellen, dass der gesamte Benutzerzugriff überprüft wird

Xerox® Drucker werden ab Werk mit sicheren und eindeutigen Kennwörtern für das Admin-Konto geliefert. Rollenbasierte Zugriffskontrollen können durch sichere Authentifizierung mit lokalen Benutzernamen, PIN-Code-Zugriff, kartenbasierter Authentifizierung und CAC/PIV-Authentifizierung implementiert werden. „Least privilege access“ und kontinuierliche Neuvalidierung können mit Inaktivitäts-Timern/Logouts erzwungen werden. Multifaktor-Authentifizierung wird über Cloud Identity Providers (IDPs) wie Ping Identity, Okta, Microsoft Azure Identity Services sowie Xerox® Workplace Cloud / Xerox® Workplace Suite-Lösungen unterstützt.

Xerox® Workplace Cloud Print Management Solution und Xerox® Workplace Suite Print Management Solution erweitern den Funktionsumfang von Xerox® Druckern auf eine ganze Geräteflotte, um einen einheitlichen Ansatz zu gewährleisten. Sie setzen eine „Never Trust“-Sicherheitsstrategie um, indem sie von Benutzern die Freigabe von Druckern mit Karten/Auseisen, Mobilgeräten oder PIN-Codes vor dem Zugriff auf die verfügbaren Druckerdienste verlangen.

Xerox® Managed Print Services implementieren auf Benutzer- und Systemebene bei jeder neuen Verbindung eine obligatorische Authentifizierung. Sie richten einen definierten rollenbasierten Benutzerzugriff ein und bieten eine Kennwortverwaltung mit nach NIST 800-171R2 genehmigten Methoden. CA/Certificate Management sorgt dafür, dass autorisierte Drucker sicher über das Netzwerk kommunizieren.

ÜBERWACHUNG UND ERKENNUNG

(Potenzielle) Sicherheitsbedrohungen kontinuierlich überwachen und erkennen

Xerox® Drucker sind mit digital signierter und verschlüsselter Firmware ausgestattet und mit Firmware-Verifizierung darauf ausgelegt, sich selbst vor Manipulationsversuchen mit der Systemsoftware zu schützen. Trellix*[1] Whitelisting/Eintrag zulassen überwacht in Echtzeit auf Malware, blockiert böswillige Aktivitäten und weist Benutzer auf diese hin. Trusted Boot[4] gewährleistet die Integrität des Systemstartprozesses.

Syslog/Audit Log-Datengenerierung und Integration mit SIEM-Tools[2] wie LogRhythm, Splunk und Trellix* Security Manager liefern nützliche Erkenntnisse zur Erkennung und Eindämmung von Sicherheitsbedrohungen. Mithilfe von Cisco Identity Services Engine (ISE) können wir unbefugte Drucker erkennen und verhindern, dass eine Verbindung zu Ihrem Netzwerk aufgebaut wird.

Xerox® Workplace Cloud und Xerox® Workplace Suite lassen sich in Ihr ID-Management-System integrieren, um nahtlosen Zugriff und Authentifizierung zu gewährleisten. Dadurch werden Synchronisierungsprobleme zwischen dem Zugriffskontrollmechanismus und dem ID-Anbieter verhindert. Auf lokaler/Geräteebene verwenden wir Tools wie reCAPTCHA, um erkannte Angriffsversuche zu überwachen und zu blockieren.

Xerox® Managed Print Services bieten eine vom Kunden festgelegte Frequenz der Sicherheitsüberwachung. Wir implementieren eine geräteübergreifende Geräteverwaltung mit Xerox® Printer Security Audit Service. Mit dieser Lösung lässt sich die Konfiguration der gesamten Flotte intuitiv abwickeln, indem Druck- und Sicherheitsrichtlinien per Fernzugriff festgelegt werden. Sie wird auch als Grundlage für interaktive Dashboard-Stile und Echtzeit-Datenberichte verwendet. Sicherheitspatches und Firmware-Updates werden entsprechend den Sicherheitsrichtlinien des Kunden angewendet.

Zero Trust

EINDÄMMUNG UND BESEITIGUNG

Im Falle einer potenziellen Gefährdung die Bedrohung eindämmen und eine rasche Abhilfe bieten, um diese zu beseitigen

Wir bei Xerox haben unsere Drucker mit einem „Security-First"-Ansatz entwickelt, der verhindert, dass sie durch Angriffe infiziert werden. Mehrere Schichten von Sicherheitsmerkmalen schränken mögliche Sicherheitslücken weiter ein. Mit der Druckerfunktion „Configuration Watchdog"[3] können Systemadministratoren beispielsweise bis zu 75 Sicherheitseinstellungen implementieren und diese bei Änderungen proaktiv korrigieren (zurücksetzen).

Auf Flottenebene gewährleisten Xerox® Printer Security Audit Services die Einhaltung von Richtlinien und führen bei allen Geräten, die nicht konform sind, proaktiv Korrekturen durch. Wir führen regelmäßige Überprüfungen von Konfigurationsrichtlinien durch (um sicherzustellen, dass sie aktuelle Sicherheitsanforderungen erfüllen), informieren den Kunden und geben fortlaufend Sicherheitsempfehlungen.

SCHUTZ (DATEN UND DOKUMENTE)

Datenverschlüsselungstechniken und Softwarelösungen nutzen, um Daten und Dokumente vor absichtlicher und unbeabsichtigter Offenlegung zu schützen

Die Speicherlaufwerke auf unseren Druckern sind durch 256-Bit-Verschlüsselung geschützt. Nicht mehr benötigte gespeicherte Daten können mit den vom National Institute of Standards and Technology (NIST) und dem US-Verteidigungsministerium genehmigten Algorithmen zur Datenbereinigung und Datenlöschung gelöscht werden. Die Druckausgabe wird durch die Verwendung eines PIN- oder Kartenfreigabesystems geschützt. Und wir verhindern, dass Unbefugte Scaninformationen erhalten, indem wir digital signierte, verschlüsselte und kennwortgeschützte Dateiformate verwenden.

Bei unseren Druckern[4] können Sie die E-Mail-Felder „An/Kopie (cc)/Blindkopie (bcc)" sperren, um das Scanziel nur auf bestimmte Domänen (z. B. interne Domänen) zu begrenzen. Mit der Imaging Security-Funktion nutzen Xerox® AltaLink® Drucker Infrarot-Technologie (IR), um sensible Dokumente zu kennzeichnen und zu erkennen. Dies verhindert deren unbeabsichtigte Vervielfältigung und erstellt Warnungen und Überwachungsprotokolle, um Vervielfältigungsversuche nachzuverfolgen.

Nicht genutzte Netzwerk-Dienste können deaktiviert werden, um die Angriffsfläche des Netzwerks zu verringern. IP-Filter können implementiert werden, um den Netzwerkzugriff nur auf zugelassene Clients für Scan-, Druck- und Geräteverwaltung zu beschränken. Sichere Protokolle wie IPsec, HTTPS, LDAPS und SFTP schützen Daten bei der Übertragung. Der FIPS-Modus kann aktiviert werden, um sicherzustellen, dass nur die sichersten Protokolle mit dem Gerät interagieren dürfen.

Xerox® Workplace Cloud-Lösung verschlüsselt Inhalte bei der Übertragung und im Ruhezustand. In der Cloud bei Xerox gespeicherte Inhalte können mit einem kundeneigenen Verschlüsselungsschlüssel verschlüsselt werden. Durch den Einsatz ihres eigenen Verschlüsselungsmanagements profitieren Kunden von allen Vorteilen der Umstellung auf cloudbasiertes Druckmanagement und behalten die Kontrolle darüber, wer den Inhalt ihrer Daten einsehen kann. Die Inhaltssicherheitsfunktion der Xerox® Workplace Cloud und Workplace Suite-Lösungen ermöglicht die Erkennung vordefinierter sensibler Inhalte und die Erstellung von Warnmeldungen und Berichten auf der Grundlage der Verwendung dieser Daten.

Xerox® Printer Security Audit Services stellen sicher, dass Daten- und Dokumentenschutzfunktionen in der Geräteflotte aktiviert sind, beheben Richtlinienverstöße und berichten über die Einhaltung der Vorschriften.

AUTOMATISIERUNG

Sicherheitsrichtlinien optimieren, um optimale Ergebnisse zu erzielen

Automatisierung führt zu Einfachheit und ermöglicht es Sicherheitsteams, sich auf wichtige Probleme zu konzentrieren. Die Fleet Orchestrator-Funktion von Xerox® Druckern automatisiert die Gerätekonfiguration und wendet Firmware-Updates auf ein Netzwerk von Druckern an. Dies gewährleistet Compliance und entlastet die IT-Mitarbeiter. Durch die Integration von Cisco ISE und Trellix* ePolicy Orchestrator kann jeder Drucker bei der Erkennung von Bedrohungen automatisch unter Quarantäne gestellt werden. So wird eine Beschädigung des Druckers verhindert und das Netzwerk und andere Endpunkte werden geschützt.

Xerox® Printer Security Audit Services nutzen einen zentralisierten Richtlinienmechanismus und Gerätegruppen, um die Verwaltung des Gerätebestands mit minimalem Aufwand zu optimieren. Compliance-Durchsetzung und -Validierung erfolgen vollautomatisch. Dashboards präsentieren Informationen zu Gerätebestand, Richtlinien und Gerätekonformität in einem übersichtlichen, grafischen Format.

Ein erfolgreiches Sicherheitsprogramm hängt von einer einfachen und durchsetzbaren Sicherheitsrichtlinie ab, die von Produktfunktionen und -diensten unterstützt wird, durch die die Einhaltung von Vorschriften gewährleistet wird. Zero Trust wird in Unternehmen jeder Größe schnell zum bevorzugten Sicherheitsmodell. Durch die Implementierung der in dieser Übersicht beschriebenen Sicherheitsempfehlungen von Xerox können Unternehmen autorisierten Benutzern sicheren Zugriff gewähren, die Gefährdung im Falle von Datenschutzverletzungen begrenzen und die Reaktion auf potenzielle Sicherheitsbedrohungen automatisieren.

[1] Xerox® AltaLink®, EC-Serie und Xerox® Multifunktionsdrucker der VersaLink® 7100 Serie.
[2] AltaLink® direkte Integration von SIEM, alle anderen Geräte über Xerox® Managed Print Services.
[3] Xerox® Multifunktionsdrucker der AltaLink® 8000 und 8100 Serie.
[4] Xerox® AltaLink® und Xerox® VersaLink®.
*Trellix, früher bekannt als McAfee.

Weitere Informationen über Xerox Security finden Sie unter
www.xerox.de/de-de/uber-uns/sicherheitslosungen.