IDC
Analyze the Future

I D C M A R K E T S P O T L I G H T

Der Schutz der Druckinfrastruktur ist für die digitale Transformation entscheidend

Dezember 2016

Von Robert Palmer, IDC Research Director, Imaging, Printing, and Document Solutions

Im Auftrag von HP Inc.

Der IT-Sicherheitsplan eines Unternehmens hat eindeutig oberste Priorität, wenn es darum geht, einen angemessenen Schutz vor potentiellen Bedrohungen und Sicherheitsverletzungen sicherzustellen. Dabei ist unbedingt auch die Drucksicherheit zu berücksichtigen, besonders im Zeitalter des 3rd-Platform-Computing (Mobilität, Cloud, Big Data und soziale Medien). Jeder umfassende Plan für die Sicherheit der Druckumgebung eines Unternehmens muss daher auch Lösungen und Services enthalten, die die Sicherheit von Geräten und Daten sicherstellen. Im vorliegenden Dokument wird untersucht, wie wichtig der Schutz der Druck- und Dokumenteninfrastruktur ist und welche Rolle Managed Print Services bei der Umsetzung dieses Ziels übernehmen können.

Einführung

Probleme, die mit Sicherheit und Datenschutz in Zusammenhang stehen, haben bei CIOs und IT-Managern schon seit mehr als 10 Jahren höchste Priorität. Eigene Untersuchungen von IDC haben gezeigt, dass der Sicherheit bei den meisten Unternehmen eine der höchsten Prioritäten zugewiesen wird und sie nur knapp hinter einer anderen wichtigen Unternehmensinitiative rangiert – der digitalen Transformation. Beide Aspekte werden als wichtige Alleinstellungsmerkmale angesehen. Daher ist es wichtig zu wissen, wie stark digitale Transformation und Sicherheit miteinander verzahnt sind.

Unternehmen sehen sich beim Schutz ihrer IT-Infrastruktur zahlreichen Bedrohungen ausgesetzt. Die meisten der technisch versierten Unternehmen behandeln die Sicherheit mit hoher Priorität. Der Schwerpunkt liegt dabei auf dem Schutz des Netzwerks vor Angriffen von außen, dem Schutz von Netzwerkgeräten, der Verwaltung des Zugriffs auf Geräte, die mit dem Netzwerk verbunden sind, und dem Schutz vor Offenlegung vertraulicher Daten.

Es ist offensichtlich, dass all diese Aspekte mit der Notwendigkeit in Zusammenhang stehen, die wertvollsten Assets des Unternehmens zu schützen: geschäftliche Informationen und Kundendaten. Unternehmen geben Milliardenbeträge für Document Management- und Enterprise Content Management-(ECM-)Software aus. Dabei fließen große Summen in Systeme, die die Kontrolle über geschäftskritische Inhalte ermöglichen. Verschärft wird die Herausforderung durch die immer stärker werdende Mobilität und durch Cloud Computing. Knowledge Worker benötigen rund um die Uhr Zugriff auf Informationen. Inhalte müssen daher problemlos innerhalb und außerhalb der Unternehmens-Firewall zugänglich sein.

Interessanterweise befindet sich die Druck- und Dokumenteninfrastruktur eines Unternehmens genau an der Schnittstelle zwischen digitaler Transformation und IT-Sicherheit. Dennoch erkennen die meisten Unternehmen die Sicherheitslücken nicht, die mit ihrer vorhandenen Druck- und Dokumentumgebung einhergehen. Eine zentrale Rolle übernimmt dabei der intelligente Multifunktionsdrucker (MFP), der sich zu einem intelligenten Hub für die Verarbeitung der

Geschäftsabläufe entwickelt hat. Dieser Hub dient als Zugriffspunkt für geschäftliche Informationen. Dabei ist es unerheblich, ob die Informationen auf dem Gerät, im Firmennetzwerk, auf Papier oder in der Cloud gespeichert sind.

Eine unsichtbare und nicht verwaltete Bedrohung

Der verbundene MFP stellt wie ein nicht verwaltetes verbundenes Gerät ein potentielles Sicherheitsrisiko dar. Der MFP kann jedoch auch an vorderster Front als Schutz für den Netzwerkzugriff, die Verwaltung der Datensicherheit und für den Schutz des Zugriffs auf Informationen eingesetzt werden.

Der IDC-Studie *User Perspectives on Print Security, 2015* zufolge wenden mehr als 30 % der Unternehmen keine Sicherheitsrichtlinien bei der Verwaltung des Zugriffs und der Kontrolle der Zugriffsrechte für Drucker und MFPs im Netzwerk an. Gleichzeitig äußerten mehr als die Hälfte der Befragten Bedenken hinsichtlich der unbefugten Verwendung von Kopierern oder MFPs.

Bei der Betrachtung der eigenen aktuellen IT-Sicherheitsmaßnahmen sind ähnliche Diskrepanzen festzustellen. Der IDC-Studie *MaturityScape Benchmark: Print Security in the United States, 2016* zufolge haben mehr als 70 % der Befragten angegeben, dass die Drucksicherheit beim Kauf oder Mieten von Druckern und MFPs eine große Rolle spielt. Überraschenderweise liegt der Anteil der Befragten, die die Drucksicherheit als „sehr wichtig“ ansehen, nur bei 26 % oder unter dem Anteil derjenigen, die Bedenken hinsichtlich der IT-Sicherheit im Allgemeinen äußerten.

Viele Sicherheits- und IT-Manager sind davon ausgegangen, dass die zum Schutz des Netzwerks implementierten Systeme auch die anderen verbundenen Peripheriegeräte mit einschließen. Die Sicherheit im Netzwerk ist jedoch nicht mehr so umfassend. Jedes Gerät, das mit dem Netzwerk verbunden ist, stellt ein Risiko für die Endpunkt-Sicherheit dar – Drucker und MFPs eingeschlossen.

Die Bedrohung ist real: Sicherheitsverletzungen können durch böswillige Angriffe über einen Netzwerkdrucker oder MFP als Einfallstor oder durch die unbeabsichtigt nachlässige Verwendung von Geräten durch Mitarbeiter verursacht werden. Die Druckumgebung ist einzigartig, da sie speziell für die Verwaltung von Daten, Dokumenten und Informationen sowohl in digitaler als auch in Papierform genutzt wird. Geschäftskritische Inhalte sind demnach vielen Risiken ausgesetzt. Wird der Schutz der Druckumgebung in der IT-Gesamtstrategie vernachlässigt, ist das Unternehmen genauso verwundbar als würden gar keine IT-Sicherheitsmaßnahmen ergriffen.

Das Ergebnis einer Sicherheitsverletzung der Druck- und Dokumenteninfrastruktur ist dasselbe wie bei jeder anderen Sicherheitsverletzung: immense Kosten durch Ausfallzeiten, die zur Identifikation und Behebung der Sicherheitsverletzung erforderlich sind, Geldstrafen wegen der Nichteinhaltung von Corporate Governance und rechtlichen Bestimmungen oder sonstige Schäden, die mit einem Imageverlust des Unternehmens einhergehen.

Sichere Druckservices

Die Herausforderungen, die Teil der Druck- und Dokumentsicherheit sind, lassen sich schnell identifizieren. Die Entwicklung einer sicheren Druckstrategie hat sich jedoch für viele Unternehmen als eher schwierig erwiesen. Ein Problem sind die unterschiedlichen Verantwortlichkeiten innerhalb des Unternehmens. Für die Gerätesicherheit ist in der Regel die IT-Funktion zuständig. Dazu gehören normalerweise IT-Abteilung, Security Manager, Helpdesk sowie Endpunkt- und Netzwerksicherheit. Zudem ist häufig auch das Facility-Management in die Diskussionen zur Sicherheit von Druckern und MFPs eingebunden.

Die Sicherheit von Inhalten wird dagegen häufig in Zusammenhang mit Problemen bei der Einhaltung von rechtlichen Bestimmungen betrachtet. Die Verantwortlichen sind daher oft in den Bereichen zu finden, die für Unternehmensrisiken und Corporate Governance verantwortlich sind. Des Weiteren

können Mitarbeiter aus den Bereichen ERP-Anwendungen, Datenbank-Cluster, Content Management sowie Manager aus weiteren Geschäftsbereichen involviert sein. Die Sicherheit für Inhalte und Drucker wird viel zu oft getrennt betrachtet. Auf diese Weise entstehen Integrationslücken und vermehrt Schwachstellen. Gleichzeitig sind Unternehmen die verschiedenen am Markt erhältlichen Lösungen für sicheres Drucken sowie professionelle Services nicht bekannt.

In diesem Bereich könnten Managed Print Services (MPS) bei der Optimierung der Druck- und Dokumentensicherheit eine wichtige Rolle übernehmen. Während viele Unternehmen Verträge mit einem MPS-Anbieter abgeschlossen haben, um die Druckinfrastruktur zu optimieren und so die Effizienz zu steigern und die Ausgabekosten zu senken, wird die Druck- und Inhaltssicherheit in den meisten vertraglichen Vereinbarungen häufig gar nicht berücksichtigt. Heute verfügen einige MPS-Anbieter über die Kapazitäten, Tools und Ressourcen, um Unternehmen bei der Identifizierung und Priorisierung der aktuellen Sicherheitsbedrohungen zu unterstützen. Dieser Prozess könnte eine Vorabbewertung der Sicherheit beinhalten, die für die Identifizierung von Schwachstellen in der aktuellen Geräte- und Dokumenteninfrastruktur entscheidend ist. Die Unternehmen können dann gemeinsam mit dem Service-Anbieter sichere Managed Print Services entwickeln und bereitstellen, die aktuelle Schwachstellen beheben, die Dokumenteninfrastruktur stärken und künftige Sicherheitsrisiken minimieren.

Darüber hinaus arbeitet der MPS-Anbieter mit den verschiedenen Beteiligten zusammen, um vertraglich vereinbarte Druckservices in sämtlichen Abteilungen des Unternehmens bereitzustellen – ein entscheidender Aspekt bei der Bereitstellungen eines holistischen Ansatzes für die Sicherheit von Geräten und Inhalten. Dieser Ansatz fördert auch die Entwicklung eines Sicherheitsplans, der auch die unternehmenseigene Strategie zur digitalen Transformation mit einschließt. Sichere Druckservices können die grundlegende Sicherheit für den Schutz von Geräten und Daten umfassen, oder aber auch erweiterte Maßnahmen beinhalten, die eine komplexere Implementierung erfordern und einen besseren Schutz von Geräten und Inhalten bieten.

Fazit: Von reaktiv zu proaktiv

Die Druck- und Dokumenteninfrastruktur hat bisher noch nicht dieselbe Aufmerksamkeit erhalten wie andere Bedrohungen in den Bereichen Netzwerk- und Cyber-Sicherheit. Sicherheitsverletzungen führen zu Angst und Unsicherheit. Zudem können die negativen Auswirkungen auf Betriebskosten, Arbeitsleistung und das Image des Unternehmens beträchtlich sein.

Unternehmen müssen proaktiv handeln und Maßnahmen ergreifen, um die Sicherheitsbedenken hinsichtlich Druck- und Dokumentenstruktur aus dem Weg zu räumen. Der MPS-Anbieter sollte dabei als wichtiger Partner angesehen werden. Bei der Suche nach geeigneten Druckserviceanbietern sollten Sie die Anbieter in Betracht ziehen, die ihre Kompetenz bei der Bewertung von Bedrohungsstufen und der Beseitigung von Bedrohungen unter Beweis gestellt haben.

Wählen Sie außerdem Partner, deren Hardware und Lösungen auf einem Sicherheits-Ökosystem aufsetzen, das mit den folgenden Schwachstellen in der Dokumenteninfrastruktur umgehen kann:

- Benutzerauthentifizierung und -autorisierung
- Geräteverwaltung
- Schutz von Geräten vor Malware
- Firmware-Updates und Kennwortverwaltung
- Inhaltssicherheit, Daten und Datenintegrität

- Funktionen für die Mitarbeiter, die an Installation, Konfiguration und Verwendung der Geräte beteiligt sind

MPS-Lösungen sollten so konzipiert sein, dass eine Integration in Document Management und ECM-Systeme von Drittanbietern möglich ist. Auf diese Weise können der Schutz und die Einhaltung von Unternehmensrichtlinien und rechtlichen Bestimmungen optimiert werden.

Ein holistischer Ansatz bietet Unternehmen die Möglichkeit, Sicherheitslücken zu beheben und den Schutz in der Druck- und Dokumentenumgebung zu stärken, die vermutlich das schwächste Glied Ihres Unternehmens hinsichtlich der Sicherheit darstellt.

Unternehmenszentrale: 5 Speen Street Framingham, MA 01701 USA Tel.: 508.872.8200 Fax:508.935.4015
www.idc.com