IDC
Analyze the Future

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

Die Schwachstelle der DSGVO (Datenschutz-Grundverordnung): Warum Drucker ein Problem für die Compliance darstellen

Juli 2017

Von Duncan Brown

Gesponsert von HP

Dieses IDC Market Spotlight verdeutlicht die Angreifbarkeit von Druckern in Unternehmensnetzwerken, besonders die Auswirkungen auf ein Compliance-Programm, das sich auf die DSGVO und andere kommende Gesetze stützt. Dieser Report zeigt, wie die Risiken durch ungeschützte Drucker im Unternehmen verringert werden können.

Einführung

Auf die Sicherheit für das Internet of Things (IoT) wird deutlich mehr Wert gelegt, seitdem es zu einer Reihe von ausgeklügelten DDoS-Angriffen (Distributed Denial-of-Service) mit einer großen Menge an bösartigem Datenverkehr kam, die von Tausenden kompromittierten Überwachungskameras, digitalen Videorecordern und anderen angeschlossenen Geräten ausgingen und beliebte Websites ausschalten sollten. Welche Geräte werden als nächstes angegriffen?

Wenn man andere IoT-Geräte betrachtet, die Ähnlichkeiten mit den zuletzt angegriffenen Geräten haben, fallen Drucker von Privatnutzern, kleinen Unternehmen und Großunternehmen ins Auge. Software-Updates und Zugangskontrollen, die bei traditionellen IT-Produkten eine hohe Priorität haben, werden bei Druckern oft übersehen. Drucker könnten das nächste Opfer eines großen IoT-Angriffs werden. Sie könnten aber auch ein neues Risiko für Geschäftsprozesse darstellen, da sie sich im Unternehmensnetzwerk befinden und so Datendiebstahl und DDoS im Inneren des Netzwerks ermöglichen. Durch die DSGVO und weitere kommende Regelungen wird den Auswirkungen von Datenschutzverletzungen auf Unternehmen mehr Aufmerksamkeit geschenkt. Netzwerkdrucker werden noch als Endpunkte vergessen, sollten aber dringend Beachtung finden.

Ihr Drucker ist ein Endpunkt

Denken Sie z. B. an folgendes Szenario: Ein unbekanntes Gerät wird im Unternehmensnetzwerk innerhalb der Perimetersicherheit (z. B. Firewalls, Systeme zur Angriffsabwehr und andere IT-Infrastrukturen) platziert und das Gerät hat uneingeschränkten Zugriff auf alle Netzwerkressourcen im Unternehmen. Ein Webserver wird in das Gerät integriert, um die Funktionalität zu maximieren. Alle Ports sind standardmäßig offen und verfügen über Ethernet-Verbindungen mit bis zu einem Gigabit, um den Zugriff auf das Gerät zu ermöglichen. Das Gerät verfügt über ein leistungsfähiges Betriebssystem wie Linux, um das Funktionsspektrum zu erhöhen. Es wird nicht regelmäßig mit dem Schwachstellenscanner des Unternehmens geprüft, da der integrierte Webserver vermutlich Falschmeldungen an die SIEM-Tools (Security Information and Event Management) ausgibt. Der Schwachstellenscanner wird so konfiguriert, dass das Gerät ignoriert wird. Die Folge ist, dass das Gerät je nach Marke in den 5 bis 10 Jahren Nutzungsdauer nicht aktualisiert, gewartet oder gepatcht wird. Der Geräteschutz besteht aus einem Standardkennwort und nicht geprüfte Drittanbieter warten das Gerät. Das Gerät ist für die Produktivität im Unternehmen wichtig. Auf jeweils 10 Mitarbeiter

kommt ein Gerät. Diese Mitarbeiter nutzen das Gerät nicht nur, sie senden auch vertrauliche persönliche Daten an das Gerät und speichern diese dort. Schlimmer noch, die Daten können ohne Authentifizierung oder Zugangskontrolle an unbeteiligte Beobachter ausgegeben werden.

Für manche ist es ein Albtraum, für andere ein Drucker.

Ein wichtiger Punkt muss geklärt werden. Drucksicherheit ist ein wichtiger Sicherheitsbereich, v. a. wegen des Datenschutzes. Compliance-Standards spielen dabei eine große Rolle. In EMEA betrifft das die DSGVO, aber auch die NIS (Network and Information Systems Security Directive) sowie die aktualisierte Datenschutzrichtlinie für die elektronische Kommunikation und die überarbeitete Payment Services Directive (PSD2). Diese Standards dienen als Grundlage für die *Sicherheit*, ohne genaue technische Angaben zur Compliance zu machen.

Die zentralen Themen der DSGVO

Die DSGVO ist eine lange überfällige Aktualisierung der europäischen Datenschutzgesetze. Sie ersetzt die aktuellen Gesetze aus dem Jahr 1995, also aus der Zeit noch vor dem Internetboom, Twitter, Facebook und der Cloud. Durch die DSGVO wird das Gesetz in Bezug auf diese und zukünftige Entwicklungen aktualisiert, die persönliche Daten erstellen und verwenden.
Ein weiterer Vorteil besteht darin, dass diese Verordnung für alle Mitgliedsstaaten der EU gilt.

Die DSGVO wurde im April 2016 unterzeichnet und tritt am 25. Mai 2018 in Kraft. Unternehmen bleibt somit weniger als ein Jahr Zeit, die Compliance sicherzustellen. Bei Nichteinhaltung kann die Strafe bis zu 4 Prozent des weltweiten Jahresumsatzes oder 20 Mio. € betragen (je nachdem, welche Summe größer ist). Die DSGVO führt auch eine Meldepflicht für Sicherheitsverletzungen ein, die zu Bedenken bei Führungskräften führte, die eine Rufschädigung fürchten.

Der künftige Ausstieg des Vereinigten Königreichs aus der EU (Brexit) hat keine großen Auswirkungen auf die DSGVO:

- Britische Unternehmen, die persönliche Daten von Mitgliedern der EU verarbeiten, müssen sich weiterhin an die DSGVO halten, da sich die DSGVO extraterritorial auf die Daten aller Personen in der EU bezieht.
- Das Vereinigte Königreich wird wahrscheinlich lokale Gesetze wie die DSGVO anwenden, um je nach Zweckmäßigkeit den Datentransfer mit der EU zu vereinfachen.

Die DSGVO ist mehr als ein Sicherheitsthema. Sie umfasst eine Reihe neuer Maßnahmen, inklusive Datenübertragbarkeit, Zustimmung und Widerruf, Altersüberprüfung und das Recht auf Vergessenwerden. Compliance beruht aber zu einem großen Teil auf einem guten Sicherheitskonzept. Was sagt die DSGVO dazu?

Die DSGVO beinhaltet erstaunlicherweise keine genauen Definitionen der Sicherheitsmaßnahmen. Sie umfasst 99 Paragraphen und nur Paragraph 32 bezieht sich auf das Thema Sicherheit. Unternehmen müssen „geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Es ist also jedem Unternehmen überlassen, die Risiken für die persönlichen Daten einzuschätzen und die für nötig erachteten Sicherheitsmaßnahmen zu ergreifen.

Ein Aspekt ist, was GDPR als „Stand der Technik“ bezeichnet. Unternehmen sind nicht verpflichtet, moderne Technologien einzusetzen. Sie sollten sich aber der Bedeutung dessen bewusst sein und sich erklären können. Unternehmen sollten es vermeiden, in die Lage zu kommen, dass Sie erklären müssen, warum sie eine bestimmte Sicherheitskontrolle oder -maßnahme *nicht* angewendet haben, wodurch eine Datenschutzverletzung entstanden ist.

DSGVO-Regulierungsbehörden setzen wahrscheinlich einen Test ein, den IDC „Wie intensiv haben Sie es versucht“ nennt. Die Schwachstellen nicht zu kennen, ist schlecht. Die Schwachstellen zu kennen und nichts zu tun, ist noch schlimmer. Wird eine mögliche Verletzbarkeit der Sicherheit beim Druckerbestand nicht beachtet, so könnte dies zu einem Diebstahl persönlicher Daten führen, der im Falle entsprechender Ernsthaftigkeit die Aufsichtsbehörde hinterfragen lassen könnte, ob angemessene organisatorische und technische Maßnahmen zum Schutz der Daten ergriffen worden waren.

Die DSGVO gilt für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ Mit anderen Worten, Daten müssen nicht im elektronischen Format vorliegen, Ausdrucke von Daten müssen ebenso gesichert werden.

Die NIS (Network and Information Systems Security Directive)

Die EU hat verstanden, dass in Anbetracht der wachsenden Zahl an Cyberangriffen wichtige Services geschützt werden müssen. Dies betrifft vor allem die, die für Wirtschaft und Gesellschaft wichtig sind. Die EU hat die NIS-Richtlinie verabschiedet, um die Konsistenz beim Schutz vor Cyberangriffen in allen Mitgliedsstaaten sicherzustellen.

Überraschenderweise umfasst die NIS nicht sehr viele Details in Bezug auf die Sicherheitsanforderungen. Der Schutz der Infrastruktur ist sehr wichtig (inklusive der physischen Assets). Ein Schwerpunkt liegt auf der Ausfallsicherheit (Störungsmanagement, Business Continuity-Management usw.). Sie umfasst eine Meldepflicht für Sicherheitsverletzungen (siehe Paragraph 16), es gibt jedoch keine vorgegebenen Strafen bei Nichteinhaltung.

Da die NIS eine Richtlinie ist, muss sie in einem Mitgliedsstaat rechtlich umgesetzt und vom Gesetzgeber ratifiziert werden. Die NIS trat im August 2016 in Kraft. Die Mitgliedsstaaten haben Zeit bis zum 10. Mai 2018, um die Richtlinie in den nationalen Gesetzen umzusetzen. Sechs Monate später müssen Mitarbeiter für zentrale Services angegeben werden.

Die Vorteile von Druckersicherheit

Die Druckersicherheit konzentriert sich im Gegensatz zur Drucksicherheit nur auf die physischen Geräte, die zum Drucken benötigt werden, und ist Teil der Netzwerksicherheit. Bei der Druckersicherheit werden Drucker als Endpunkte betrachtet und mit der gleichen Sorgfalt wie Notebooks, Server und mobile Geräte behandelt. Auch wenn sie Gemeinsamkeiten haben und sich einige Problembereiche überschneiden, sind Drucksicherheit und Druckersicherheit eigenständige Disziplinen.

Wie angreifbar sind Netzwerkdrucker wirklich?

Drucker empfangen große Mengen an Daten, darunter auch persönliche Daten.
Nur wenige Benutzer, Compliance-Experten oder IT-Administratoren machen sich Gedanken über die Sicherheit von Daten, die an Drucker übermittelt und dort gespeichert werden. Artikel 5.f der DSGVO sieht vor dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet wird, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Doch nur wenige Unternehmen machen sich Gedanken über die Sicherheit der Daten auf Druckern.

Es kommt häufig vor, dass gedruckte Dokumente im Drucker liegen bleiben. Gemäß DSGVO könnten Pull-Printing-Lösungen ein Bestandteil beim Schutz vor zufälligem Verlust persönlicher Daten werden, insbesondere bei Organisationen, bei denen Ausdrucken Teil der primären Verarbeitung von persönlichen Daten darstellt.

Drucker sind ein beliebtes Ziel für Cyberangreifer, da sie nicht als Teil der IT gesehen werden und daher von der Sicherheitsabteilung nicht so viel Aufmerksamkeit erfahren. Die Druckerverwaltung wird oft als Teil der Büroorganisation gesehen. Seit Drucker Teil des Netzwerks sind, galten sie, solange sie sich innerhalb der Firewall befinden, als Geräte mit „geringem Risiko“. Die Angreifbarkeit von Druckerendpunkten wurde selten erkannt.

Kombigeräte mit Druck-, Scan- und Faxfunktionen werden immer komplexer und verfügen über einen allgemeinen integrierten Computer für diese Funktionen. Viele moderne Drucker verfügen über Windows- und Linux-Systeme. Da diese Computer selten abgesichert und gepatcht werden, sind sie oft verwundbar. Viele Funktionen setzen Verbindungen voraus, daher werden viele Drucker für mehr Benutzerfreundlichkeit mit einer Vielzahl offener Ports geliefert.

Eine hohe Rechenleistung und eine Reihe von Verbindungsoptionen in Kombination mit mangelnder Aufmerksamkeit ermöglichen Angreifern den Zugriff auf Drucker auf mehreren Wegen, z. B. über einen modernen Wireless Access Point oder einen mit Spyware infizierten Desktop. Wenn der Zugriff erfolgt ist, erreichen Angreifer andere Rechner im internen Netzwerk und können DDoS-Angriffe (Distributed Denial-of-Service) ausführen. Die meisten Drucker verfügen über einen uneingeschränkten Zugriff auf das interne Netzwerk. Ein Angreifer, der einen Drucker kompromittiert, kann sich überall nach verwertbaren Systemen umsehen.

Wie die anderen Endpunktgeräte, die geschützt werden müssen, sind Drucker nicht nur das Einfallstor, sondern auch das Ziel von Cyberangreifern. Auf Druckern werden oft vertrauliche Daten gespeichert. Häufig ist ein Scanner integriert und die Dokumente im Scannerarchiv werden länger gespeichert, als die meisten Menschen vermuten.

Weitere Anmerkungen

Wenn die Druckersicherheit bisher in Ihrem Unternehmen kein Thema war, gibt IDC Ihnen einige Empfehlungen für den Einstieg.

Das Wichtigste ist die Transparenz

Fangen Sie mit den grundlegenden Dingen an. Dies gilt für den Schutz aller Endpunkte. Schritt eins ist immer die Transparenz. Erstellen Sie eine Liste aller Drucker, inklusive Marke, Modell, Funktionen und Konfigurationen. Die Erstellung einer solchen Liste kann problematisch sein, da die einzelnen Abteilungen oft Drucker an unbekannten Orten aufstellen (Schatten-IT). In Laboren, Büros von Führungskräften oder im Außendienst werden Drucker einfach ohne Beachtung der Auswirkungen auf die Sicherheit mit dem Netzwerk verbunden oder direkt an einen PC angeschlossen.

Eine Auflistung der Endpunkte inklusive Drucker kann idealerweise über einen NAC (Network Access Controller) oder ein Asset-Management-Tool, deren wichtigste Funktion die Geräteerkennung ist, erstellt werden. Ohne NAC ist eine vollständige Transparenz bei Druckern nur schwer zu erreichen. Einige Druckermodelle verfügen möglicherweise über Funktionen zur automatischen Erkennung, wenn sie mit dem Netzwerk verbunden werden. Wenn in Ihrer Netzwerkumgebung keine derartigen Drucker installiert sind, bietet sich NAC an.

Absicherung der Druckerendpunkte

Drucker im Unternehmen müssen wie alle anderen verbundenen Endpunkte behandelt werden. Deaktivieren Sie alle nicht benötigten Services des Druckers, z. B. FTP. Die meisten Unternehmen benötigen keinen FTP-Zugriff auf ihrem Drucker und meist sind mehr Nachteile als Vorteile damit verbunden. Einige Drucker ermöglichen es Angreifern beispielsweise, FTP-Anfragen zu stellen und Druckaufträge anonym vom Drucker zu nehmen. Viele FTP-Services auf modernen Druckern sind Opfer von FTP-Bounce-Angriffen. Mit einem Tool wie Nmap (Network Mapper) kann ein Angreifer die

Quelle eines Portscans verschleiern und dafür sorgen, dass ein kompatibler FTP-Server Proxy-FTP-Verbindungen zulässt. Obwohl FTP-Bounce-Scans alte Methoden sind, ist eine erstaunliche Anzahl neuer Druckserver anfällig für derartige Angriffe.

Das Wichtigste bei der Absicherung eines Druckers ist jedoch die Kennwortverwaltung. Der größte Fehler besteht darin, dass Unternehmen die Standardkennwörter nicht ändern. Nach dem in 2016 erschienenen Report von Verizon *Data Breach Investigations* war die Ursache für 63 % der bestätigten Datenschutzverletzungen ein schwaches, gestohlenes oder Standardkennwort. Wenn die Drucker von den Einrichtungen oder von Drittanbietern verwaltet werden, hat Bequemlichkeit höchste Priorität (für sie). Ein Kennwort zu finden, kann zum Problem werden. Wenn auf 10 Mitarbeiter ein Drucker kommt, muss ein Unternehmen mit 10.000 Mitarbeitern 1.000 Kennwörter verwalten. Dabei wird die Sicherheit der Bequemlichkeit geopfert. Probleme bei der Kennwortverwaltung liegen nicht nur bei den Mitarbeitern, die nicht im technischen Bereich arbeiten. Der nächste große Fehler ist es, Benutzername und Kennwort frei zugänglich und unverschlüsselt für jeden mit einer http://-Verbindung verfügbar zu machen.

Wartung und Patches

Die meisten Sicherheitsverletzungen sind das Ergebnis mangelnder Sorgfalt. Nach dem in 2016 erschienenen Report von Verizon *Data Breach Investigations* machten in 2015 die 10 größten ausgenutzten Schwachstellen 85 % der erfolgreichen Angriffe aus. Die am häufigsten ausgenutzten Schwachstellen sind bekannt und veröffentlicht. Cyberangreifer folgen bewährten Pfaden und maximieren die Investitionen in ihre Malware-Tools.

Durch Wartung und Patches können Sie Ihre Drucker absichern und Cyberangreifer müssen sich an Unternehmen halten, die ihre Systeme nicht schützen.

In Bezug auf Patches sind nicht alle Drucker gleich. Einige Hersteller bieten Verwaltungstools, mit denen Sie manche Fabrikate und Modelle der Drucker überwachen, verwalten und patchen können. Diese Tools sind von großem Wert, da der Schwachstellenscanner des Unternehmens vermutlich aufgrund des integrierten Webservers Probleme mit Druckern haben wird. Drucker mit leistungsfähigen Verwaltungstools sind von Vorteil. Alternativ müssen Sie jeden Drucker manuell patchen, da die Zusammenstellung einer automatisierten Lösung schwierig sein kann.

Unternehmen konfigurieren ihre Schwachstellenscanner oft so, dass Drucker ignoriert werden, um übermäßige Meldungen in SIEM-Tools zu vermeiden. Das Problem sind sowohl die SIEM-Tools und Schwachstellenscanner als auch die Drucker. Die Konfiguration dieser Tools kann kompliziert sein, wenn sie nur bestimmte Meldungen von Druckern empfangen sollen. Auf kurze Sicht dient dieser Aufwand aber dem Schutz des Netzwerks vor Infektionen durch Drucker.

Sichere Verbindung

Nutzen Sie verstärkt die Verwaltungsprotokolle, die für Drucker genutzt werden. Die meisten modernen Drucker unterstützen die Verwaltung über HTTP und/oder HTTPS, einige sogar Telnet oder Secure Shell (SSH). Wählen Sie sorgfältig ein Verwaltungsprotokoll aus, das Verschlüsselung wie HTTPS oder SSH bietet und deaktivieren Sie schwache oder defekte Verschlüsselungsalgorithmen wie SSLv3.

Stellen Sie zuletzt sicher, dass Ihr Drucker keinen offenen Zugriff auf das interne Netzwerk ermöglicht. Die Segmentierung von Unternehmensnetzwerken ist eine Best Practice bei der Netzwerksicherheit auf Drucker ausgeweitet werden sollte. Zertifikate ermöglichen den logischen Zugriff auf Netzwerkressourcen und die Verschlüsselung des Datenverkehrs. Diese zusätzlichen Sicherheitsmaßnahmen können jedoch Auswirkungen auf die Funktionalität des Druckers haben und beispielsweise den Zugriff auf Verzeichnisdienste (z. B. Active Directory) und die cloudbasierte

Verwaltung und Überwachung einschränken. Um das richtige Gleichgewicht von umfassender Druckersicherheit und dem Erhalt der Geschäftsfunktionalität zu erreichen, müssen Sie die Geschäftsrisiken einschätzen und beurteilen.

Zusammenfassung

Drucker haben bisher nicht die gleiche Aufmerksamkeit erhalten, wie andere, von Cyberangriffen bedrohte Geräte. Die Bedrohungen und die entsprechenden Risiken sind sehr real. Unternehmen jeder Größe müssen Maßnahmen ergreifen – und zwar schnell. Cyberangreifer sind gierige Nachahmungstäter. Wenn eine Schwachstelle von einem Angreifer identifiziert wurde, folgen bald weitere Angreifer.

Die finanziellen und rufschädigenden Konsequenzen einer vernachlässigten Druckersicherheit werden durch die DSGVO bis zur Geschäftsleitungsebene eskaliert. Es wäre bedauerlich, wenn ansonsten konform arbeitende Organisationen, die intensiv an ihren Sicherheitsverfahren und -technologien im Informationswesen gearbeitet haben, durch einen Schwachpunkt bei Druckern gefährdet werden.
