SPECTRUM Hinweise

Einsatz von Managed-Printer-Service- bzw. Fleet-Management-Software für Drucker und Kopierer in Kunden-Netzwerken

In vielen Kanzlei- und Unternehmens-Netzwerken gibt es oft ein Sammelsurium an Druckern, Kopierern, Scannern und Fax-Geräten. Oft stammen die von verschiedenen Herstellern bzw. Lieferanten und brauchen ständig unterschiedliche, inkompatible, herstellerabhägige Verbrauchsmaterialien wie Toner, Kartuschen, Feinstaubfilter, Entwickler, Trommeln usw.. Diese Verbrauchsmaterialien müssen vorgehalten und vor allem immer rechtzeitig nachbestellt und nachgeliefert werden. Dies ist alles aufwändig und wenn man dies durch modernere Techniken verbessern kann, sieht das auf den ersten Blick sinnvoll aus ….

Im Rahmen des Remote-Service, der Fernwartung bieten hier heute die meisten Anbieter von Kopierern und Druckern sogenannte **Managed-Printer-Service- bzw. Fleet-Management-Software** an, die im lokalen Netzwerk installieret werden muss. Im Zeitalter des „Internet-of-Things – IoT“ überwachen diese Programme die Geräte und melden rechtzeitig, wenn sie z.B. Verbrauchsmaterialien bzw. Wartungen benötigen. Eigentlich eine schicke Lösung - der Anwender bekommt, ohne dass er sich darum kümmern muss, rechtzeitig Verbrauchsmaterialien nachgeliefert und der Kopierer- bzw. Druckerlieferant bekommt automatisch laufend z.B. die Zählerstände für seine monatliche Abrechnung (z.B. für die Berechnung des „Zählerklick“-Preises) übermittelt und das Gerät meldet ggfs. rechtzeitig selbständig bedarfsgerecht im Voraus, wann es Verbrauchsmaterialien braucht, wann Wartungszyklen durchgeführt werden müssen, meldet Störungen und Ausfälle um ggfs. nach statistischen Auswertungen schon vorbeugend Teile auszutauschen und ermöglicht dem Wartungspersonal oft auch aus der Ferne die Behebung von Störungen via Remote-Service. Alles toll …. so stellt man sich modernen Service vor ….

ABER: jeder technische Fortschritt hat leider auch Nachteile: Man muss einen Zugang zum Kopierer oder Drucker Gerät einrichten (z.B. Ports in der Firewall freischalten) und diese „Löcher“ können auch von Cyber-Kriminellen bösartig ausgenutzt werden.

Hinweis: Bedenken Sie, dass fast alle Drucker und Kopierer heute Druckaufträge lokal im Gerät speichern und so könnten dann vertrauliche Dokumente ggfs. über unkontrollierte Zugriffe von außen in falsche Hände gelangen. Die Folgen dieser Managed-Printer-Service- bzw. Fleet-Management-Software, die man heute mit zu den Produkten des IoT, des Internet-of-Things zählt, sind neben allen Annehmlichkeiten für Nutzer auch immer mehr offene Türen für Angreifer, über die man Geräte im großen Maßstab infizieren und für schädliche Zwecke missbrauchen kann. Dabei haben es Hacker heute oft sehr leicht, denn leider herrscht bei vielen Herstellern von Managed-Printer-Service- bzw. Fleet-Management-Software oft ein mangelndes Sicherheitsverständnis für die Risiken und eine fehlende Qualitätssicherung. Man hat oft nur den eigenen Vorteil im Blick, ohne die Sicherheitsaspekte voll zu berücksichtigen. Angriffe von außen werden hier oft zum Kinderspiel: IT-Sicherheitsexperten haben weltweit analysiert, dass die heutigen Angriffswellen von Spams, Viren, Trojanern häufig von „gekaperten“ IoT-Geräten erfolgen, d.h. von fremdbestimmten Kopierern, „smarten“ Heizungssteuerungen, IoT-Kühlschränken, IP-Rolladensteuerungen, Regler in Industrieanlagen usw.. Diese gekaperten Geräte sorgen oft für die Verbreitung der heutigen Schadcodes. IoT macht z.B. DDoS-Attacken möglich (Distributed Denial of Service Angriffe), d.h. wo sich zig gekaperte Geräte auf ein bestimmtes Ziel fokussieren und zeitgleich eine große Anzahl von Anfragen starten. Unter der Last der Anfragen bricht dann das Ziel zusammen oder kann reguläre Dienste nicht mehr in gewohnter Weise bearbeiten oder der gesamte Dienst fällt dann aus. Oft ist mangelnde Qualitätssicherung bei der IoT-Software die Ursache, die ja alle auch eine Nachlademöglichkeit für Software-Verbesserungen beinhalten und die dann für das Laden von Schadcode missbraucht werden kann.

Wir möchten Ihrem Kopierer- und Druckerlieferanten nichts Böses unterstellen, aber auch der nutzt zumeist nur Fremdsoftware, die er oft von seinen Geräteherstellern zur Verfügung gestellt bekommt und deren Qualitätssicherung er nicht kennt bzw. selbst nicht überprüfen kann.

Beschreibung der SPECTRUM COMPUTER-SYSTEMHAUS GMBH
Max-Planck-Str. 17, 40699 Erkrath, Telefon: +49 (0)211/695602-0, Telefax: +49 (0)211/695602-99, E-Mail: info@spectrum-news.de

SPECTRUM fühlt sich für das Netzwerk- und IP-Management bei seinen Kunden indirekt (mit-) verantwortlich und warnt daher Kunden vor dem Einsatz solcher Managed-Printer-Service- bzw. Fleet-Management-Software für Druck- und Kopiersysteme, die einen direkten Außenkontakt zum Internet aufbauen können.

Hinweis: Nach Art. 28 der EU-DSGVO sind wir außerdem explizit als Ihr IT-Dienstleister verpflichtet, Sie auf mögliche Datenschutzprobleme hinzuweisen. Hier der Text dieser Verpflichtung: „Ist der Auftragnehmer (also SPECTRUM) der Ansicht, dass eine Weisung des Auftraggebers (also z.B. Aufträge von unseren Kunden zur Firewall Port-Freischaltung für solche Managed-Printer-Service- bzw. Fleet-Management-Software) gegen dieses Gesetz (EU-DSGVO, d.h. von Datenschutzvorschriften für personenbezogene Daten) oder andere Vorschriften über den Datenschutz (z.B. § 203 StGB, Berufsrecht, sonst. Vorschriften) verstößt, hat er (SPECTRUM) den Auftraggeber (also Sie) unverzüglich darauf hinzuweisen“.

Dieser Hinweispflicht sind wir hiermit nachgekommen und können Ihnen resultierend nur empfehlen solche Managed-Printer-Service- bzw. Fleet-Management-Software für Druck- und Kopiersysteme nicht zu installieren!

Unsere Steuerberaterkunden haben außerdem noch die Spezialproblematik, dass nach § 203 Strafgesetzbuch StGB ein „absolutes Offenbarungsverbot bzw. Verschwiegenheitsgebot“ bezüglich der den Steuerberatern anvertrauten Mandantendaten besteht (siehe auch die Berufs-Gesetzgebung wie §§ 57 ff und §§ 62 ff des Steuerberatergesetzes [StBerG], §§ 43 ff und §§ 50 ff des Gesetzes über die Berufsordnung der Wirtschaftsprüfer [WPO], §§ 43 der Bundesrechtsanwaltsordnung [BRAO] und §§ 2 der Berufsordnung für Rechtsanwälte [BORA] usw.). D.h. Steuerberater müssen z.B. alles nach dem Stand der Technik zu unternehmen, um die Mandantendaten voll umfänglich zu schützen und vor fremden Zugriffsmöglichkeiten zu bewahren!

Auch nach dem „Gesetz zum Schutz von Geschäftsgeheimnissen“ (GeschGehG) ist jeder Geschäftsführer oder Vorstand einer Kapitalgesellschaft heute verpflichtet, alles nach dem Stand der Technik zu unternehmen, um die Unternehmensdaten zu schützen und jeden ungewollten Fremdzugriff zu verhindern. Die Abgabenordnung (AO), das Handelsgesetzbuch (HGB), das Haftungsrecht bzw. Vorschriften im GmbH- und Aktienrecht und die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) verlangen, dass alles nach dem Stand der Technik getan werden muss, um den Fremdzugriff auf Unternehmensdaten zu verhindern.

Wir möchten außerdem darauf hinweisen, dass Sie (Kanzlei, Unternehmen) nach Art. 28 EU-DSGVO im Vorfeld verpflichtet sind mit Ihrem Kopierer- oder Druckerlieferanten eine sog. „**Vereinbarung zur Auftragsvereinbarung nach Art. 28 EU-DSGVO“** abzuschließen. Hierbei muss Ihr Kopierer- oder Druckerlieferant Ihnen gegenüber auch seine **„technischen und organisatorischen Maßnahmen – TOM’s“** und sein **„Datenschutz-Management“** nach EU-DSGVO schriftlich nachweisen.

Alternative: Fragen Sie Ihren Kopierer- oder Druckerlieferanten, ob er Ihnen alternativ nicht eine Managed-Printer-Service- bzw. Fleet-Management-Software anbieten kann, die keine Öffnung von Firewall-Ports verlangt und die stattdessen die Möglichkeit bietet die sinnvollen und gewünschten Statusmeldungen (Kopienverbrauch, Serviceanforderung, Verbrauchsmaterialmeldungen usw.) via E-Mail zu verschicken.

Bitte betrachten Sie diese SPECTRUM-Hinweise nicht als Schikane, wir möchten Sie nur vor Schaden bewahren und sind unsererseits sogar gesetzlich verpflichtet, Sie hierauf hinzuweisen.

Zur Information: Die meisten der SPECTRUM-Kunden aus der Rechts- und Steuerberaterbranche haben - nach Abwägung aller Vor- und Nachteile - bisher darauf verzichtet, eine solche Managed-Printer-Service- bzw. Fleet-Management-Software für Kopiersysteme zu installieren, die in der Lage ist, selbständig Verbindungen zum Internet aufbauen können.

ABER: Der Kunde ist bei SPECTRUM König und Ihr Wunsch ist uns ein Befehl!

Wenn Sie trotz dieser Warnungen von SPECTRUM eine Firewall-Port-Freischaltung oder die Installation einer Managed-Printer-Service- bzw. Fleet-Management-Software wünschen – wobei wir das grundsätzlich immer nur auf den lokalen PCs und nie auf den Servern installieren werden - dann teilen Sie uns bitte (von einem Weisungsberechtigten) folgendes schriftlich mit: *„Wir haben die SPECTRUM-Hinweise ‚Einsatz von Managed-Printer-Service- bzw. Fleet-Management-Software für Drucker und Kopierer in Kunden-Netzwerken‘ gelesen und möchten hiermit trotzdem SPECTRUM beauftragen entsprechend den Spezifikationen des Drucker- bzw- Kopierer-Lieferanten Ports in der Firewall freizuschalten und die beigestellte Managed-Printer-Service- bzw. Fleet-Management-Software auf dem lokalen Netzwerk zu installieren“* (E-Mail reicht).