pepress World of Print
www.worldofprint.de • www.worldofprint.com

Interview mit Stephen Miller, Direktor für Produktmanagement bei der Kodak Software Division

Herausforderung Cybersicherheit

Jahr für Jahr nehmen die Auswirkungen von Cyberangriffen auf Unternehmen jeder Größe zu. Nach Schätzungen wird der durch Internetkriminalität jährlich verursachte Schaden bis zum Jahr 2021 einen Wert von 6 Billionen US-Dollar erreichen. Angreifer im Internet unterscheiden nicht nach Branchen, weshalb es für Druckdienstleister unabdingbar ist, diese Bedrohung ernst zu nehmen, wenn sie Investitionen in neue Druck- und Produktionstechnik tätigen. Wir unterhielten uns mit Stephen Miller, Direktor für Produktmanagement bei der Kodak Software Division, Eastman Kodak Company, über die größten Herausforderungen in puncto Cybersicherheit und Lösungen, wie Drucker ihre Betriebe am besten schützen können.

Stephen Miller, Direktor für Produktmanagement bei der Kodak Software Division, Eastman Kodak Company

Was sind heutzutage die größten Herausforderungen beim Kampf gegen Bedrohungen der Cybersicherheit, über die Drucker Bescheid wissen sollten?
Für Druckunternehmer, gerade auch jene, die kleine und mittlere Unternehmen führen, ist es wichtig, die Gefahr eines Angriffs nicht zu ignorieren. Wir neigen zu der Annahme, dass nur große und bedeutende Unternehmen gefährdet sind, weil sie im Licht der Öffentlichkeit stehen, doch das bedeutet nicht, dass dies nicht auch einem unbekannten Unternehmen widerfahren kann. Hacker unterscheiden nicht nach Größe oder Renommee. Tatsächlich geht aus neuen Statistiken zur Cybersicherheit hervor, dass die meisten Datenverstöße (58 %) bei Kleinunternehmen festgestellt wurden.

Hacker haben herausgefunden, dass der verletzlichste Teil eines Computernetzwerks der Mensch ist. Sie haben erkannt, dass sie nicht mehr den schwierigen Weg mit komplexen Tools gehen müssen, um Sicherheitsprobleme von Computernetzwerken auszunutzen, sondern dass sie einfach auf einen Menschen zurückgreifen können, um die Pforten zu öffnen. Und die Tür, durch die sie hereinmarschieren, ist in vielen Fällen das E-Mail-Konto eines Mitarbeiters.

Diese schädlichen E-Mails veranlassen Nutzer durch Täuschung dazu, Dateianhänge zu öffnen oder auf einen Link zu einer infizierten Internetseite zu klicken. Sobald sie Zugang zu den Ressourcen eines Unternehmens erlangt haben, können sie Informationen stehlen oder betriebliche Abläufe lahmlegen.

Welche Auswirkungen haben diese Cyberangriffe auf Druckereien?
Die Art dieser Angriffe kann unterschiedlich sein. Zum Beispiel sind Phishing-E-Mail-Kampagnen typischerweise dafür konzipiert, Schadsoftware (Malware) zu installieren, die einem Unternehmen verschiedene Probleme bereiten kann. Sie kann den Zugang zu wichtigen Netzwerkkomponenten so lange blockieren, bis das Unternehmen dem Hacker ein „Lösegeld" bezahlt, oder sie kann einzelne Teile so stören, dass der Betrieb des gesamten Systems nicht mehr möglich ist. Außerdem gibt es Spyware, die sich verdeckt Informationen verschafft, indem Daten von Festplatten im Unternehmen übertragen werden. In jedem Fall bedeutet dies für das im Visier der Hacker stehende Unternehmen massive Probleme und eine Beeinträchtigung seiner Abläufe, während an der Behebung der Angriffsfolgen gearbeitet wird. Wie lange dies dauert und wie kostenaufwendig es sein wird, hängt von Schwere und Ausmaß des feindlichen Einfalls ab. In einem kürzlich von der Versicherungsgesellschaft Chubb veröffentlichten Bericht werden die durchschnittlichen Kosten, die einem Unternehmen für die Behebung der durch einen Cyberangriff verursachten Schäden entstehen, mit 400.000 US-Dollar angegeben, was für kleine und mittlere Unternehmen existenzbedrohend sein kann.

Neben den nachteiligen Folgen für den Unternehmensertrag kann dies den Ruf eines Unternehmens beschädigen und das Vertrauen der Kunden in Mitleidenschaft ziehen. Jeder Druckunternehmer kann sich selbst vorstellen, was passieren würde, wenn seine internen Systeme geschädigt würden. Zum Beispiel kann Folgendes passieren: Ein Mitarbeiter öffnet versehentlich einen Link in einer harmlos aussehenden E-Mail, der dann eine schädliche Datei freisetzt, welche die Server des Unternehmens sperrt, auf denen sich wichtige Druckdateien von Kunden befinden. Hat man Glück, verursacht die Problembehebung geringere Unannehmlichkeiten. Es kann jedoch auch Tage oder Wochen dauern, bis der Schaden behoben ist, was Zeit- und Geldverluste sowie unzufriedene Kunden mit sich bringt.

Welche praktischen Maßnahmen können Drucker heute ergreifen, um die Gefahr einer Cyberattacke zu mindern?

Es ist wichtig zu verstehen, dass die Kosten für zusätzlichen Schutz zur Stärkung der Netzwerksicherheit weit niedriger sein können als die Kosten der Behebung eines Sicherheitsvorfalls nach einem Angriff. Dies sollte wirklich in gleicher Weise betrachtet werden wie der Abschluss einer Kfz-Versicherung für den Unternehmensfuhrpark oder einer Feuerversicherung für die Produktionsgebäude. Der einzige Unterschied bei der Verbesserung der Netzwerksicherheit besteht darin, dass das Risiko eines Angriffs aktiv entschärft wird. Wir empfehlen, die folgenden drei Schritte möglichst kurzfristig umzusetzen:

Geschäftskritische Daten isolieren: Es reicht nicht aus, Daten nur per Sicherungskopie zu sichern. Es muss bekannt sein, welche Daten für die Geschäftsprozesse und betrieblichen Abläufe eines Unternehmens unerlässlich sind. Dann müssen diese Daten mittels Software isoliert werden, die fähig ist, den Prozess der Speicherung geschäftskritischer Daten an einem Ort außerhalb des Unternehmens zu automatisieren. Wenn ein Hacker die Daten nicht sehen kann, kann er auch nicht auf sie zugreifen.

Das Personal entsprechend schulen: Eine angemessene Schulung der Mitarbeitenden ist von zentraler Bedeutung. Heute kommen 90 % der Angriffe sozusagen direkt durch die Eingangstür in Form von Phishing-E-Mails. Im Internet sind hervorragende Ratschläge zur Schadensabwehr zu finden, man kann aber auch externe Beratungsfirmen mit Schulungen bezüglich der Abwehr dieses Problems beauftragen.

Möglichkeiten zur Verlagerung wichtiger Daten und Systeme an einen externen Ort untersuchen: Zusätzlich zur Isolierung und Sicherung geschäftskritischer Daten kann die Verlagerung dieser Daten weg vom lokalen Netzwerk eines Unternehmens in eine wesentlich sicherere Umgebung, wie zum Beispiel das Hosten der Software und Daten in einer sicheren Cloud-Umgebung, in Betracht gezogen werden.

Wie hilft Kodak Druckereien, ihre Netzwerke vor äußeren Bedrohungen zu schützen?

Computernetzwerke, wie jenes, das Druckereien jeden Tag für ihre Verwaltung und Produktion nutzen, sind von Natur aus für den Austausch von Informationen konzipiert. Wenn in einem Computernetzwerk ein Informationsaustausch stattfindet, werden Computer über „Netzwerkfreigaben" miteinander verbunden und leiten die Informationen von Gerät zu Gerät weiter. So sorgt das Netzwerk für die unglaubliche Geschäftseffizienz, die wir alle heute als selbstverständlich ansehen. Natürlich kann dasselbe Netzwerk auch dafür verwendet werden, schnell einen bösartigen Virus zu übertragen, dessen Absicht es ist, die Geschäftstätigkeit von Unternehmen zum Stillstand zu bringen.

Bei Kodak gehen wir dieses Problem vonseiten der Softwareentwicklung mittels der sogenannten Netzwerksegmentierung an. Ein Bestandteil dieser Herangehensweise ist die Isolierung von Daten, denn wenn ein Hacker die Daten nicht sehen kann, kann er auch nicht auf sie zugreifen. Bei den SaaS-Angeboten (Software as a Service) von Prinergy haben wir einen auf dem Prinergy Server installierten Prinergy Cloud Agent, der als verschlüsselter Kanal zum sicheren Cloud-Speicherkonto einer Druckerei fungiert. Nutzt eine Druckerei Prinergy VME mit Managed Services, werden ihre Dateien von ihrem lokalen Netzwerk entfernt und über das Internet zu ihrem Cloud-Speicherkonto gesendet, wo automatisch mehrere Kopien der Dateien erstellt und in zwei verschiedenen Microsoft Azure Rechenzentren sicher gespeichert werden.

Außerdem bieten unsere Kodak Prinergy Managed Services, die zur IaaS-Kategorie (Infrastructure as a Service) gehören, Druckereien den Zugang zu erstklassigen Sicherheitstools, um ihr Netzwerk zu stärken und ihre betriebliche Effizienz, Redundanz sowie Produktionsverfügbarkeit zu verbessern.

Die über Prinergy verfügbaren Services haben den Vorteil, auf der Microsoft Azure Plattform gehostet zu werden, bei der Microsoft jährlich 1 Milliarde US-Dollar in Sicherheitsforschung investiert. Das übertrifft bei weitem, was ein Unternehmen durch die Anstellung eines Sicherheitsspezialisten tun könnte. Kodak belässt es jedoch nicht bei den von Microsoft bereitgestellten Sicherheitsfunktionen, sondern arbeitet zusätzlich mit dem IT-Sicherheitsdienstleister Wipro zusammen. Dabei werden für alle Microsoft Rechenzentren, in denen Kodak Prinergy Software gehostet wird, vierteljährliche Risiko- und Sicherheitsbeurteilungen sowie Penetrationstests durchgeführt.

Letztlich dreht sich bei der Frage der Sicherheit alles darum, zusätzliche Schutzebenen einzuziehen. Da Unternehmen hinsichtlich der sich ständig weiterentwickelnden Sicherheitsbedrohungen auf dem Laufenden bleiben müssen, besteht für Druckereien der Vorteil der Verlagerung in die Cloud unter Sicherheitsaspekten darin, dass ihnen immer die neuesten Werkzeuge und Prozesse zur Verfügung stehen, um ihre Daten und Geschäftsabläufe im sicheren Bereich zu halten.

Herr Miller, wir danken Ihnen vielmals für das interessante Gespräch!

Das Problem der Cybersicherheit ist in einer Industrie, die hauptsächlich aus kleinen und mittelgroßen Unternehmen besteht, besonders akut, wenn man sich vor Augen hält, dass es sich 2017 bei mehr als 60 % der Opfer von Datenangriffen um Unternehmen mit weniger als 1.000 Mitarbeitenden handelte.