Service

IT-Sicherheit für Druckereien.

HEIDELBERG

Vorwort

Das vorliegende Dokument beschäftigt sich mit den speziellen IT-Fragestellungen und -Lösungen für Druckereibetriebe. Druckereien werden zunehmend anfälliger für Sicherheitsbedrohungen, die sich aus der Implementierung immer komplexerer IT-Infrastrukturen und Datenprozesse und den daraus resultierenden Sicherheitslücken ergeben.

Die Zahl der Cyber-Angriffe verdoppelt sich Jahr für Jahr, und täglich kommen neue Bedrohungen hinzu. Die Sicherung und der Schutz von Daten haben für Druckereien nicht immer höchste Priorität. Das ändert sich jedoch sehr schnell, wenn Auftragsdaten verloren gehen, das versehentliche Löschen von Daten zu längeren Produktionsausfällen führt, Hardware versagt, Wechseldatenträger verloren gehen oder gestohlen werden oder sich Naturkatastrophen ereignen. Dann brauchen sie die Gewissheit, dass so etwas nie wieder passiert und – falls doch – keine Daten verloren gehen und die Produktion möglichst schnell wieder anläuft.

Dasselbe gilt in Sachen Sicherheit. Sie steht nicht selten weit unten auf der Prioritätenliste. Ähnlich wie beim Verlust von Daten treten die Aspekte Schutz und Vorbeugung rasch in den Vordergrund, sobald Druckereien einen Virenbefall verzeichnen oder ihr Produktionsnetzwerk gehackt wurde. Zwischen Datenschutz/-sicherung und Datensicherheit gibt es einen gravierenden Unterschied. Was den Schutz und die Sicherung von Daten betrifft, ist Inhabern von Druckereien häufig nicht vollständig klar, welche speziellen Risiken und Kosten mit einem Daten-/Produktionsverlust einhergehen. Was die Datensicherheit anbelangt, halten sich Druckereien nicht für potenzielle Angriffsziele, da sie nicht als Einrichtungen gelten, die wichtige Privat- und Finanzdaten speichern (im Gegensatz zu Banken, Behörden, Krankenhäusern oder Einzelhandelsketten). Doch in Wirklichkeit ist kein Mensch und kein Unternehmen gegen potenzielle Bedrohungen gefeit.

Ein Grund für ungenügende Datensicherung und -sicherheit ist die Tatsache, dass Druckereien meist kein eigenes IT-Personal beschäftigen, das für die Werkssicherheit zuständig ist, Personal-/Kundendaten schützt und dafür sorgt, dass die Produktion trotz aller Bedrohungen reibungslos läuft.

Wie sorgt man also dafür, dass das Thema Sicherheit die nötige Aufmerksamkeit erhält? Zunächst einmal sollte man Sicherheit nicht als unnötigen Kostenfaktor, sondern vielmehr als Wettbewerbsvorteil betrachten. Wenn die Konkurrenz keine branchenüblichen und von Anbietern empfohlenen Best Practices zur Sicherung ihrer Produktionsanlagen nutzt, „erben“ ihre Kunden unnötige und unbekannte Risiken, die sich aus diesem Fehlen ergeben.

Eugene F. O’Brien, Senior Technical Support Analyst, Prinect® & CtP Services, Heidelberg® USA, Inc.

Eugene F. O’Brien

Eugene F. O’Brien ist Senior Technical Support Analyst bei der Heidelberg USA Inc. Sein Spezialgebiet ist die Internet-Infrastruktur für Druckereien. O’Brien ist seit mehr als 35 Jahren in der Druckbranche tätig und fing 1975 in New York City eine Lehre als Bleisatz-Schriftsetzer an. In seiner Zeit bei Heidelberg hat er sich als Cisco Certified Network Associate, Microsoft Certified Professional für Netzwerktechnik und IBM Certified Specialist für PC-Hardware qualifiziert. Ferner ist er für das UNIX-Betriebssystem von Data General zertifiziert.

eugene.obrien@heidelberg.com
oder Tel. +1 770 794-6205

Inhalt


HEIDELBERG

Kenntnis der wechselhaften Bedrohungslandschaft.

Wie alle Betriebe müssen auch Druckereien auf dem Laufenden bleiben, was die technische Entwicklung in der „Schönen neuen Welt“ des B2B (business-to-business) und B2C (business-to-consumer) eCommerce betrifft. Die Begriffsklärungen dienen dem besseren Verständnis der wechselhaften Bedrohungslandschaft.

PDF-Exploits

Laut McAfee[1] und Symantec[2] gehen fast 50 % aller Browser-basierten Angriffe auf das Konto von PDF-Sicherheitslücken. Dies dürfte vor allem Druckereien interessieren, die regelmäßig PDF-Dateien verarbeiten. Bei Adobe glaubt man, dass die neue und „geräuschlose“ Aktualisierungsfunktion und der „geschützte“ Modus von Adobe Acrobat das Problem aus der Welt schaffen werden. Im geschützten Modus, der standardmäßig aktiviert ist, werden alle Operationen, die zum Darstellen der PDF-Datei benötigt werden, in der so genannten Sandbox, also einem „Sandkasten“, ausgeführt. Bei Operationen, die in der „Sandbox“ unzulässig sind (zum Beispiel das Starten des Anhangs einer PDF-Datei mit einem Fremdprogramm wie Microsoft Word), müssen die diesbezüglichen Aufrufe einen so genannten Vermittler („Broker“) passieren. Dieser Prozess, der nach strengen Regeln über die Zulässigkeit von Aktionen entscheidet, verhindert den Zugriff auf potenziell gefährliche Daten. Adobe beabsichtigt, die „Sandbox“ auch in den Adobe Flash-Player einzubauen, der ebenfalls ein beliebtes Angriffsziel ist. Prinect Portal von Heidelberg ermöglicht eine Alternative für die Handhabung von Acrobat/PDF-Daten bei der Freigabe per Fernzugriff.

Clickjacking

Clickjacking, auch UI-Redressing genannt, ist eine Angriffsform, die dem Benutzer auf einer transparenten Webseite eine Webseitenattrappe vorgaukelt. Klickt der Benutzer auf eine Schaltfläche, weil er glaubt, auf der Webseitenattrappe zu sein, klickt er in Wirklichkeit auf eine Schaltfläche der darunter befindlichen Webseite. Dabei handelt es sich um eine weit verbreitete Methode, mit der Benutzer zur Preisgabe vertraulicher Daten gebracht werden.

SQL-Injection

Unter SQL Injection versteht man das Einschleusen von Schadcode in Variablen zur Speicherung von Benutzereingaben für SQL-Datenbanken. Diese Datenbanken bilden oft die Grundlage von Websites, und hinter dem Angriff steckt die Absicht, Informationen wie etwa Kreditkartennummern zu stehlen. Grundsätzlich sind solche Vorfälle das Ergebnis mangelhafter SQL-Programmierung und können vermieden werden. Sehr häufig ist ein Angriff erfolgreich, weil wichtige Sicherheits-Updates nicht durchgeführt wurden: Es ist ausgesprochen wichtig, dass sowohl die Sicherheits-Patches für das Betriebssystem als auch die Hotfixes für das Anwendungsservicepaket auf dem neuesten Stand sind.

XSS (Cross-Site Scripting)

Das Cross-Site Scripting ist eine typische Schwachstelle von Online-Anwendungen. Es birgt potenzielle Gefahren für Druckereien, die Websites hosten oder deren Mitarbeiter Websites aufrufen. XSS ermöglicht dem Angreifer, Clientseitige Scripts in Webseiten zu injizieren, die von anderen Benutzern aufgerufen werden. Diese Scripts können dann von Angreifern dazu benutzt werden, die in die betroffene Website eingebauten Zugriffskontrollen zu umgehen. Diese Schwachstelle impliziert, dass die Infrastruktur der Verbesserung bedarf.

[1] https://www.mcafee.com/tw/resources/solution-briefs/sb-browser-network-attack-methods.pdf
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

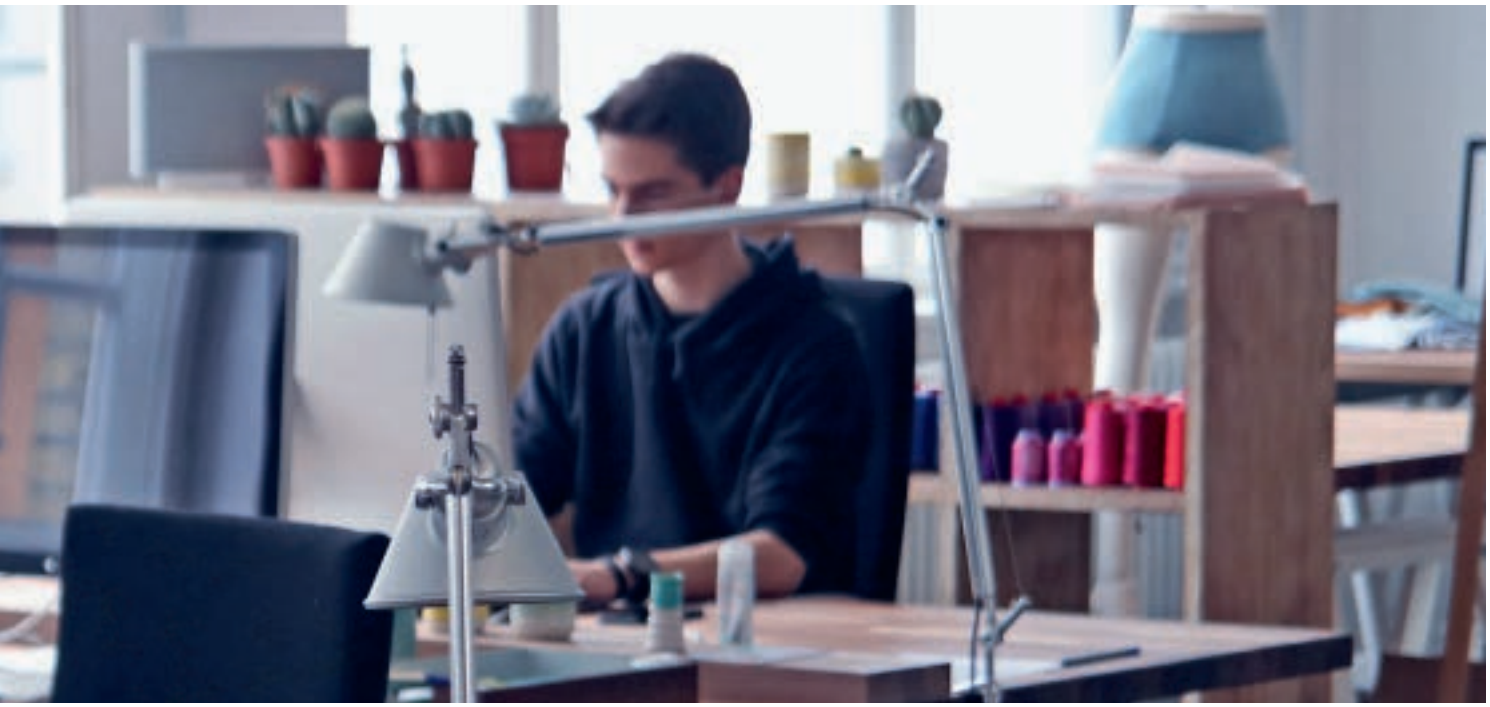
Malware

Malware ist ein Kurzwort für „malicious“ (schädlich) und „Software“ und der Sammelbegriff für Würmer, Viren, Trojaner, Rootkits, Botnets, Adware, Ransomware und andere Schädlinge, die unerwünschte Software auf dem eigenen Rechner installieren. Die möglichen Auswirkungen sind mannigfaltig und reichen von Leistungseinbußen über Rechnerfehlfunktionen und die erzwungene Umleitung auf fremde Websites bis hin zum Identitätsdiebstahl. Für das organisierte Verbrechen im Internet ist Malware das Mittel der Wahl. Stuxnet, eine Malware-Variante, die sich zunehmender Beliebtheit erfreut, zielt auf Branchensoftware ab und hat vor allem Versorgungsunternehmen und Kraftwerke im Visier. Die vergleichsweise neue „Memory Scraping Malware“ erbeutet Daten aus flüchtigen Systemspeichern, um Verschlüsselungsmaßnahmen zu umgehen. Sie erfasst die Daten im Speicher, wo sie dechiffriert werden müssen, um gelesen und verarbeitet werden zu können. Ebenfalls sehr beliebt ist die Verwendung gefälschter Virenschutz-Warnmeldungen, Software-Updates oder Online-Umfragen.

Phishing

Phishing dient dem Abgreifen vertraulicher Daten. Die Angriffe kommen als scheinbar harmlose E-Mails daher oder sind als Internetauftritte vertrauenswürdiger Unternehmen (Finanzinstitute etc.) getarnt. Eine als Spearphishing bekannte Variante zählt laut FBI[3] zu den am schnellsten wachsenden Cyber-Bedrohungen. Im Gegensatz zum Phishing, dessen Opfer nach dem Zufallsprinzip ausgesucht werden, richtet sich das Spearphishing auf bestimmte Zielgruppen, die meist anhand von Daten erkannt werden, die bei Facebook und MySpace oder in Blogs oder Foren einsehbar sind.

[3] http://www.fbi.gov/news/stories/2009/april/spearphishing_040109



Spam

Spam, auch „Junk-Mail“ genannt, bezeichnet den unaufgeforderten Versand großer E-Mail-Mengen. Da diese Vorgehensweise wenig kostet und sich kaum aufhalten lässt, ist Spam nach wie vor weit verbreitet. Das Schlimmste an Spam ist, dass es wertvolle Bandbreite und kostbaren Speicherplatz okkupiert. Normalerweise bedient man sich verschiedener Hard- und Softwarelösungen, um E-Mails aus vertrauenswürdigen Quellen von solchen unseriöser Herkunft zu unterscheiden und das eigene Postfach für letztere zu sperren.

SEO Poisoning

SEO Poisoning bezeichnet das „Vergiften“ der Suchmaschinenoptimierung (SEO, Search Engine Optimization) und wird auch Black Hat SEO genannt. Darum handelt es sich, wenn die Ergebnisse von Suchmaschinen wie Google oder Bing dahingehend manipuliert werden, dass Verkehr auf eine betrügerische Website umgelenkt wird. Auch ehrliche Firmen nutzen die Suchmaschinenoptimierung zur Verbesserung ihrer Position in den Ergebnislisten, da bekannt ist, dass Benutzer meist nicht weiter als bis zur ersten oder zweiten Seite blättern. Hacker kapern diese Ergebnisse, um Benutzer auf kriminelle Websites zu locken, wo sie ihnen vertrauliche Daten stehlen oder Malware unterjubeln. Die Zahl der infizierten Suchergebnisse steigt von Jahr zu Jahr.

Geotracking

Ein typisches Sicherheitsproblem der heutigen Zeit ergibt sich daraus, dass vielen Menschen nicht klar ist, wie viele Informationen sie eigentlich preisgeben, wenn sie Bilder im Internet veröffentlichen. Die meisten Smartphones und einige Digitalkameras können einem Foto die Koordinaten des Orts hinzufügen, an dem die Aufnahme entstand. Das Foto kann also eventuell die exakten Koordinaten enthalten, die man benötigt, um den Ort zu finden. Damit gibt man Einbrechern und Stalkern neue Werkzeuge für ihre kriminellen Machenschaften an die Hand. Wer seine Privatsphäre schützen möchte, sollte darauf achten, dass die Geotracking-Funktion seiner Kamera ausgeschaltet ist.

Whistleblower-Websites

Im Zuge von WikiLeaks wird mit dem Auftauchen weiterer Websites gerechnet, die nicht nur staatliche Stellen, sondern nun auch Gewerbebetriebe und ganze Branchen im Visier haben und Firmengeheimnisse an die Öffentlichkeit zerren werden.

Gängige IT-Mythen und Sicherheitslücken.

Mythen	Fakten
„Apple Computer sind gegen Viren- und Hackerangriffe immun.“	Auch wenn Apple[4] Betriebssysteme weniger Angriffe verzeichnen als Betriebssysteme von Microsoft, gilt die Tatsache, dass kein Computer immun ist. Viren wie OSX/Pinhead-B oder der Trojaner Boonana greifen Mac Rechner an, indem sie die Browser-Aktivität überwachen, um Facebook Benutzer zum Installieren von Malware zu bewegen.
„Wir sind bloß eine kleine Druckerei und für Hacker völlig uninteressant.“	Im Wall Street Journal[5] war zu lesen, dass die Zahl der Hackerangriffe auf Kleinunternehmen dramatisch zugenommen hat. Vielen Kleinbetrieben fehlen schlicht die Mittel, um sich vor Angriffen zu schützen oder die verursachten Schäden zu beheben. Aktuelle Zahlen besagen, dass 20 % der Druckereien keine Virenschutzsoftware verwenden. 60 % benutzen keine Mobilfunk-Verschlüsselung, und 66 % besitzen keine Sicherheitsplanung. Da die Mehrheit der Druckereien keine Vorkehrungen gegen Angriffe trifft, wäre es kaum verwunderlich, wenn Hacker sie für leichte Beute hielten.
„Ich besitze nichts, was ein Hacker haben will.“	Hacker können zum Beispiel Kundenlisten (einschließlich Kontaktdaten oder Kreditkarteninformationen) oder Personaldatenbanken (einschließlich Sozialversicherungsnummern) abgreifen und die vertraulichen Daten gegebenenfalls veröffentlichen. Abgesehen von Hackern könnten auch andere Personen (zum Beispiel unzufriedene Ex-Mitarbeiter) ein Motiv sowie Zugang zu wichtigen Informationen haben.
„Wir sind durch eine Firewall geschützt.“	Eine Firewall schützt nicht vor Bedrohungen von innen. Dazu zählen auch Bedrohungen, die von Wechseldatenträgern (USB-Sticks, CDs/DVDs) oder gefährlichen Links oder E-Mail-Anhängen ausgehen. Hier empfehlen sich zusätzliche Maßnahmen, wie zum Beispiel Upgrades auf DPI-fähige (Deep Packet Inspection) UTM-Geräte (Unified Threat Management) der nächsten Generation , IPS-Systeme (Intrusion Protection System) mit Inhaltsfilterung sowie Gateway-Virenschutzprogramme.

[4] http://support.apple.com/kb/ht1222

[5] http://online.wsj.com/article/SB10001424052748703483604574630690362605018.html?mod=dist_smartbrief
http://blogs.wsj.com/tech-europe/2011/03/21/hacker-threat-to-business-increasing/
http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html

Bei Installations- und Wartungsterminen vor Ort und auch bei der Bearbeitung von Support-Anfragen stellen wir immer wieder fest, dass Kunden ihre IT-Sicherheit vernachlässigen.

Mangelhafte Passwortregeln

Passwörter, die nicht nach festen Zulässigkeitsregeln gebildet werden, bleiben oft anfällig für Angriffe.
Typische Passwortschwächen:

- Für Netzwerkanwendungen wie Firewalls, Switches, Router, Mobilfunkzugangspunkte etc. verwenden Druckereien oft nach wie vor das unveränderte Standardpasswort des Herstellers. Diese Standardpasswörter sind Hackern bestens bekannt und können problemlos in Bedienungsanleitungen nachgeschlagen oder über eine herkömmliche Suchmaschine recherchiert werden. In diesem Fall sind alle vertraulichen Daten gefährdet.
- Benutzerpasswörter für Server und Workstations sind entweder nicht vorhanden oder kinderleicht zu erraten (zum Beispiel „Passwort“ oder „123456“), oder sie stehen auf einem Zettel, der am Gerät klebt.
- Passwörter sind unbekannt. Beim Versuch, sich in die Konfiguration eines Geräts einzuloggen (zum Beispiel zwecks Störungsbehebung), stellt sich heraus, dass niemand im Betrieb das Passwort kennt, weil es zu alt ist oder der Passwortgeber die Firma verlassen hat.

Mangelhafte Internet-Infrastruktur

Die Internetnutzung einer typischen Druckerei hat drei Aspekte:

- Das Surfen im Internet und das Verschicken und Empfangen von E-Mails durch die Mitarbeiter
- Das Ausführen von Fernzugriffsdiensten durch Anbieter wie Heidelberg
- Uploads/Downloads/Softproofing/digitale Freigaben durch die Kunden

Fehlender Virenschutz

Viele Druckereien lassen keine Virenschutzsoftware auf ihren Systemen laufen. Virenbefall droht nicht nur aus dem Internet, sondern auch beim Einführen bzw. Einlegen von USB-Sticks und CDs/DVDs.

Mangelhafte Netzwerkinfrastruktur

Die ideale Netzwerkinfrastruktur sollte nicht nur gut funktionieren und zuverlässig sein, sondern auch den Betrieb schützen.
Hier ein paar typische Fehler:

- Verwendung von Netzwerk-Equipment für den Heimbereich anstelle von Geräten für die gewerbliche Nutzung.
- Verwendung von Equipment, das nicht mehr produziert wird, dessen Garantie abgelaufen ist und für das es keine aktuellen Sicherheits-Updates zum Schutz gegen neue Bedrohungen gibt.
- Schutz des Infrastruktur-Equipments mittels USV (unterbrechungsfreie Stromversorgung) mit Batteriereserve. Schon kleine Über- oder Unterspannungen können das Netzwerk vorübergehend zum Erliegen bringen, sodass die Produktion unterbrochen wird, während die Geräte wieder hochfahren.
- Die Geräte-Firmware wird nicht fortlaufend aktualisiert, sodass kritische Sicherheitslücken, die Hacker ausnutzen können, nicht rechtzeitig geschlossen werden.
- Konfigurationen entsprechen nicht den branchenüblichen und vom Hersteller empfohlenen Standards.
- Mobilfunkinstallationen sind sehr unsicher, Zugriffspunkte für potenzielle Angreifer sind nicht verschlüsselt, nutzen veraltete Firmware und sind mit Standardpasswörtern gesichert, wodurch das WLAN sehr anfällig für die unbefugte Benutzung ist.

Wie sollten Druckereien handeln?

Jede Druckerei sollte das Thema Datensicherheit sehr ernst nehmen. In Sachen IT-Sicherheit sollten Druckereien die Initiative ergreifen statt nur zu reagieren – damit ihr Betrieb bestmöglich geschützt ist. Wissen ist Macht. Dies gilt auch für die Abwehr neuartiger Bedrohungen von außen und innen.

Ernennen Sie einen Sicherheitsbeauftragten

Als Erstes sollten Sie einen Mitarbeiter aus dem Betrieb zum Sicherheitsbeauftragten machen. Diese Person ist zuständig für die Festlegung der Richtlinien und Verfahren, an die sich die gesamte Druckerei halten muss, um Schwachstellen auszumerzen. Der Sicherheitsbeauftragte nimmt an der Entscheidungsfindung teil und leitet die IRT-Eingreiftruppe (Incident Response Team). Das IRT untersucht und dokumentiert vermutete Verstöße und andere gemeldete Vorfälle und klärt sie auf.

Gefährdungsdiagnose

Die Gefährdungsdiagnose ist ein weiteres nützliches Instrument zur Erkennung verbesserungswürdiger Bereiche. Sie sollte von unabhängiger Seite und nicht in Eigenregie durchgeführt werden. Prinect Security Analysis® bietet die Möglichkeit, dass Heidelberg Ihren Betrieb unter die Lupe nimmt, etwaige Schwachstellen identifiziert und Empfehlungen zu deren Behebung ausspricht. Auf Wunsch kümmern wir uns auch um die Umsetzung dieser Empfehlungen.

Regeln für die zulässige Nutzung

Legen Sie Regeln für die zulässige Nutzung fest. Beim Zugriff auf Dienste und Daten sind Mitarbeiter und vor Ort anwesende Kunden und Anbieter auf das Internet angewiesen. Um das ganze Spektrum des Internets ohne Einschränkungen nutzen zu können, müssen Druckereien potenzielle Bedrohungen in den Griff bekommen und auf ein Minimum reduzieren. Die Frage, welche Personen mit welchen Einschränkungen Zugriff auf welche Inhalte haben sollen, muss sorgfältig erwogen werden. Regeln für die zulässige Nutzung sind ein wichtiges Instrument für die Steuerung des Zugriffs auf das Internet. Sauber formulierte Regeln machen deutlich, welches Serviceniveau Mitarbeiter und Besucher erwarten können, und liefern eine klare Beschreibung der Rolle, die das Internet in Ihrem Betrieb spielt.

Beseitigen Sie unerwünschte Software

Unerwünschte Software ist Software, die nicht vom jetzigen Benutzer installiert wurde. Meist handelt es sich um Programme, die auf gekauften Rechnern vorinstalliert sind. Diese Programme sollten nach Möglichkeit gelöscht werden.

Server, Workstations und Drucker widerstandsfähiger machen

Halten Sie sich an die Richtlinien von Anbietern wie Microsoft, Apple und HP, was das „Aushärten“ ihrer Betriebssysteme bzw. Drucker/Proofer betrifft.

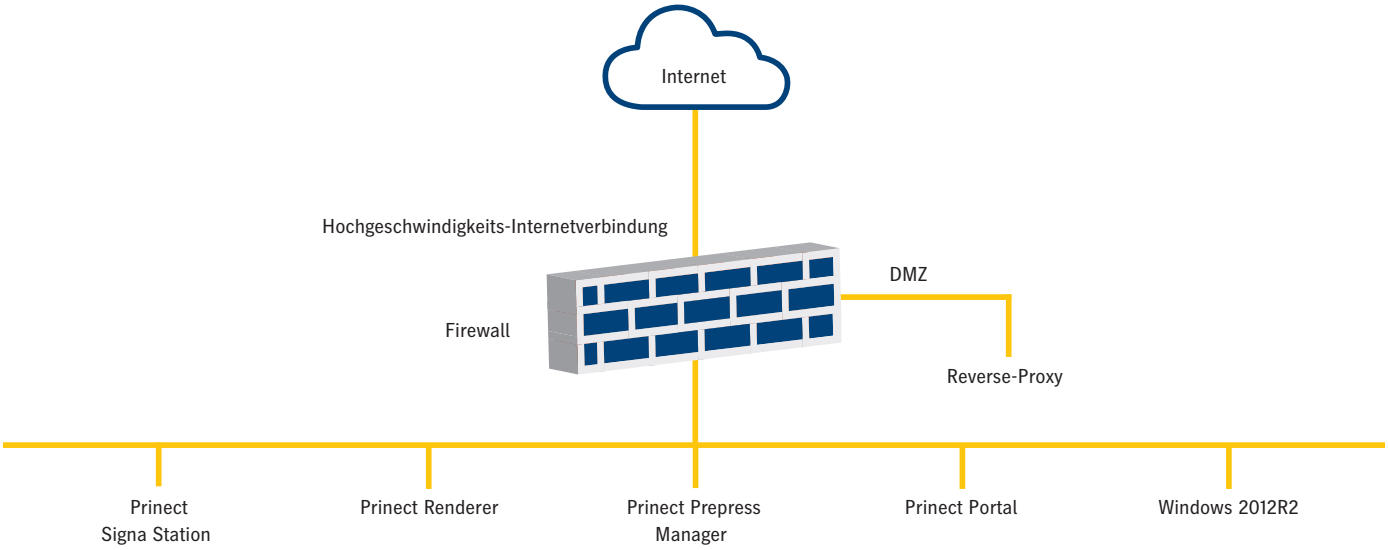
Installieren Sie Virenschutzsoftware

Wichtig ist nicht nur, dass eine Virenschutzsoftware auf einem System läuft, sondern auch, dass sie immer auf dem aktuellen Stand ist.

Einhaltung von Standards

Druckereien, die Kreditkarten akzeptieren, müssen darauf achten, dass ihr Netzwerk und Ihr Betrieb PCI- (Payment Card Industry) und DSS-konform sind (Data Security Standard).

DMZ (entmilitarisierte Zone)



Verzichten Sie auf FTP

In vielen Druckereien ist FTP noch immer gängige Praxis. Das Problem: FTP basiert auf Quellcode aus den 1980er-Jahren, und die Schwachstellen des Protokolls sind Hackern bestens bekannt – daher auch der Spitzname „Failure To Protect“, was frei übersetzt „schutzlos ausgeliefert“ bedeutet. Druckereien, die Kreditkarten akzeptieren, müssen darauf achten, dass ihr Netzwerk und Ihr Betrieb PCI-(Payment Card Industry) und DSS-konform sind (Data Security Standard).

FTP bringt zahlreiche Probleme mit sich, um die sich eine Firewall nicht kümmert:

- Für die Datenübertragung werden zusätzliche TCP/IP-Verbindungen genutzt.
- Datenverbindungen werden möglicherweise an beliebige Port-Nummern weitergereicht.
- Datenverbindungen können sowohl vom Server zum Client als auch vom Client zum Server aufgebaut werden.
- Die Zieladressen von Datenverbindungen werden ad hoc zwischen Client und Server ausgehandelt, und zwar auf dem Kanal, der für die Steuerungsverbindung verwendet wird.

FTP verschlüsselt keine Anmeldedaten:

- Anfällig für Lauschangriffe und den Diebstahl von Passwörtern und anderen vertraulichen Informationen.
- Verbindungen können gekapert werden.

Anonymes FTP ist wirklich anonym:

- Es gibt keinerlei Aufzeichnung darüber, wer welche Informationen abgefragt hat.

Moderne Lösungen wie Prinect Portal sind in den Workflow eingebunden und damit sowohl sicherer als auch zuverlässiger.

DMZ und Reverse Proxy implementieren

Bei der Bereitstellung von Online-Diensten für ihre Kunden sollten sich Druckereien einer „entmilitarisierten Zone“ (DMZ, De-Militarized Zone) und eines umgekehrten Proxys bedienen.

Verschlüsseln Sie Laptops nach der FDE-Methode (Full Disk Encryption)

Tragbare Rechner können abhanden kommen oder gestohlen werden. Möglicherweise enthält das Laptop vertrauliche Kunden- und Personaldaten oder Angaben zu Passwörtern und Konfigurationen für Netzwerke und Server.

Weiterführende Quellen.

Die nachstehend aufgeführten Websites informieren Sie über aktuelle Bedrohungen und Sicherheits-Tools.

Sicherheitsinfos und -ratgeber von Adobe
https://helpx.adobe.com/security.html

Sicherheits-Updates von Apple
https://support.apple.com/en-us/HT201222

Sicherheitsratgeber von Cisco
https://tools.cisco.com/security/center/publicationListing.x

European Cybercrime Center
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Flash Player: Sicherheit und Datenschutz
https://www.adobe.com/devnet/security.html

Sicherheitsratgeber von McAfee Labs
http://www.mcafee.com/apps/mcafee-labs/signup.aspx?region=us

Wichtige Patch-Updates & Sicherheitswarnungen von Oracle
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Sicherheitsratgeber von Microsoft
https://technet.microsoft.com/en-us/security/advisories

SANS (SysAdmin, Audit, Network, Security)
http://www.sans.org/

Sicherheitsratgeber von Symantec
http://www.symantec.com/avcenter/security/SymantecAdvisories.html

US CERT (Computer Emergency Response Team)
http://www.us-cert.gov/

US-Justizministerium
https://www.justice.gov/criminal-ccips/ccips-documents-and-reports

Resümee.

Wer Bedrohungen nach Kräften reduziert und beseitigt, sorgt für eine störungsfreie Produktion, die den Betrieb zuverlässiger und rentabler macht.

Druckereien, die ihren Kunden neue Internet-basierte Dienstleistungen und Produkte bieten möchten, sind zunehmend durch Hacker, Viren, Spyware, Adware, Malware etc. bedroht. Je nach Häufigkeit und Dauer der Vorfälle können den Druckereien Kosten entstehen, deren Ausmaß sich kaum abschätzen lässt. Manche Entscheidungen in Sachen Sicherheit werden schon beim Kauf oder bei der Installation getroffen, doch in Wirklichkeit erfordert das Thema Sicherheit permanentes Engagement und liegt letztlich in der Verantwortung des einzelnen Kunden. Wer Bedrohungen nach Kräften reduziert und beseitigt, sorgt für eine störungsfreie Produktion, die den Betrieb zuverlässiger und rentabler macht. Die beste Methode, einen Angriff zu überstehen, besteht darin, auf ihn vorbereitet zu sein.

Jeder Betrieb hat die Pflicht, die eigenen Sicherheitsrisiken einzuschätzen und über die zu ergreifenden Sicherheitsvorkehrungen zu entscheiden. Ganz gleich, ob ein Angriff absichtlich oder zufällig, von innen oder von außen erfolgt: Er stört die Produktion und kostet die Firma letztlich Geld. Die Zahl der Einbrüche in Netzwerke nimmt weiter zu, und mittlerweile ist nicht immer offensichtlich, dass ein Unternehmen kompromittiert wurde. Derzeit werden neue Gesetze formuliert, die Angriffe verhindern sollen, doch damit könnten auch Einschränkungen für Unternehmen verbunden sein. So hatte das Inkrafttreten des neuen DATA-Meldegesetztes (Data Accountability & Trust Act, H.R. 2221) im Jahr 2011 eine Veränderung der Geschäftsprozesse auch für Druckereien zur Folge. Angesichts der akuten Gefährdungslage und der zunehmenden Reglementierung müssen alle Mitarbeiter auf sämtlichen Ebenen wachsam sein, was die Sicherheit von Computern und Netzwerken betrifft. Ziel ist es, Schwachstellen auszumerzen und das Produktionsnetzwerk abzusichern.

Heidelberger Druckmaschinen AG
Kurfürsten-Anlage 52 – 60
69115 Heidelberg
Deutschland
Telefon +49 6221 92-00
Telefax +49 6221 92-6999
heidelberg.com