

Viren, Würmer und Co: Wir müssen garantiert draußen bleiben

Die Offsetdruckerei Kuthal schützt ihre Informationstechnik mit einem für die Branche vorbildlichen Sicherheitskonzept

Das Fatale an Viren, Würmern und ihren Artgenossen ist, dass man sie erst bemerkt, wenn es zu spät ist: wenn die Druckmaschine stillsteht oder infizierte PCs Viren im Netzwerk der Geschäftspartner verbreiten. Das ist nicht nur ärgerlich, sondern kann auch sehr teuer werden. Der renommierte Offsetdruckbetrieb Kuthal im unterfränkischen Mainaschaff schützt seine Informationstechnik (IT) daher mit einem für die Branche vorbildlichen Sicherheitskonzept, in das sich auch die Heidelberg-Technologie integriert.



Main Distribution (RMD) eine gemeinschaftliche IT-Infrastruktur. An diese stellen die international operierenden Kunden von RMD, darunter Pharmakonzerne, Automobilunternehmen und Banken, strengste Sicherheitsanforderungen, da sie vertrauliche Daten weitergeben.

»I love you« – wer würde diesen Satz nicht gerne von seinen Kunden hören? Aber von einem Wurm, der sich mit dieser Betreffzeile per E-Mail in das Unternehmensnetzwerk einschleicht und von dort wahllos sensible Daten in alle Welt versendet oder auch das Betriebssystem am Hochfahren hindert? Für Uwe F.

Bauer, Leiter des IT-Dienstleisters EMS, einem Schwesterunternehmen des Druckspezialisten Kuthal und des Logistikzentrums RMD Rhein-Main-Distribution, wäre dieses Szenario der GAU schlechthin:

»Beispielsweise in der Vorstufe verschickt man enorme Datenmengen. Durch eine Infektion gestörte Prozesse hätten am Ende einen Produktionsstillstand zur

Blick in den Drucksaal: Im Vordergrund die Speedmaster XL 105 Sechsfarben plus Lack sowie im Hintergrund eine Speedmaster SM 102 Zwölffarben.

Folge. Im heutigen Verdrängungswettbewerb bedeutet Verzug rasch Verlust von Kunden.« Ganz zu schweigen von den Regressforderungen und Haftungsansprüchen, wenn die Druckerei sich ungewollt als »Virenschleuder« betätigt und die IT ihrer Kunden oder Geschäftspartner infizieren würde. »Das könnte für einige Unternehmen den finanziellen Ruin bedeuten«, ist der IT-Chef überzeugt.

Gepanzertes Netzwerk: Bauer hat daher eine der modernsten und wirkungsvollsten Sicherheitsinfrastrukturen der Druckbranche aufgebaut. Der vollstufige Betrieb, der rund um die Uhr produziert, darunter mit zwei Heidelberg Speedmaster XL 105 und einer Speedmaster SM 102-Zwölffarben, ist vom Auftragsingang über die Vorstufe und den Druck bis hin zur Weiterverarbeitung datentechnisch so gut wie unverwundbar. Das muss er auch sein. Denn um Synergien zu nutzen, betreiben Kuthal und die Logistikschwester Rhein-

Schlank und ohne Schlupfloch: Das Rückgrat des mehr als 47 Kilometer umspannenden Unternehmensnetzwerkes bildet ein Zentralverteilungssystem (Core

Info: Kontakt

EMS E-Mediaservice GmbH & Co. KG, Telefon 0 60 21/7 04-7 00, Fax 0 60 21/7 04-7 50, E-Mail u.bauer@e-mediaservice.com, Internet e-mediaservice.com



Uwe F. Bauer: Der Chef des IT-Dienstleisters EMS setzt mit seinem Sicherheitskonzept Maßstäbe.

Routing Switch), über welches alle Datenverbindungen autorisierbar und koordinierbar sind. Die innovative, von Bauer persönlich entworfene Architektur, die komplett auf Unterverteilungen verzichtet, reduziert nicht nur die Ausfallrisiken, sondern erhöht auch den Datendurchsatz. So lassen sich etwa an Arbeitsplätzen und Servern gewaltige Datenmengen von mehreren Hundert Gigabit simultan verarbeiten. Darüber hinaus wehren

mehrere täglich konfigurations-optimierte Softwaresysteme sowie Datenbanken, die stündlich aktualisiert werden, selbst außergewöhnlich komplexe Angriffe ab.

Damit dieses Hochleistungsnetz nicht perforiert und man jedes noch so kleine Schlupfloch vermeidet, gewährt EMS nur Geräten Netzzugang, die den strengen EMS-Anforderungen genügen. »Gemäß unserer Maxime – Flexibilität, Sicherheit, Performance – planen und realisieren wir hochverfügbare, robuste Lösungen, die sich ohne großen finanziellen oder zeitlichen Aufwand an zukünftige Geschäftsstrategien anpassen lassen«, bringt Bauer sein Erfolgskonzept auf den Punkt. »Diesen Anspruch erfüllen die Maschinen und Lösungen von Heidelberg. Das Sicherheitskonzept ist durchdacht und flexibel. Heidelberg nimmt unsere Vorschläge sehr ernst und hat alles getan, um seine Maschinen und Systeme so resistent wie möglich gegen Infektionen und Hackerangriffe zu machen.«

Sichere Produktion: Das Betriebssystem der bei Kuthal eingesetzten Heidelberg Speedmaster basiert auf dem höchsten verfügbaren Sicherheitsstandard, den auch internationale Großunternehmen verwenden. Doch das ist EMS und Heidelberg nicht sicher genug: Daher speckt Heidelberg das Betriebssystem um alle nicht notwendigen Funktionen ab und brennt es anschließend ein (embedded), so dass es weder überschreibbar noch von außen manipulierbar ist. »Weniger ungenutzte Funktionen vermindern nicht nur die Angriffsfläche, sondern steigern auch die Leistung der Druckmaschinen«, erläutert IT-Chef Bauer.

Einen weiteren Pluspunkt sieht er in der Offenheit: »Das Betriebssystem beherrscht alle

Standardprotokolle für die Datenübertragung. Und über offene Integrationslösungen können wir die betriebswirtschaftlichen Systeme unserer Wahl anbinden.« Das ist wichtig, weil Kuthal seinen Kunden künftig über ein Infosystem in Echtzeit Auskunft darüber geben möchte, bis wann der jeweilige Auftrag abgearbeitet ist. Dass bei diesen Online-Anfragen die Systeme von Heidelberg verlässlich mitspielen, daran zweifelt Bauer nicht: »Bislang hat sich nach meinem Kenntnisstand kein anderer Anbieter in der Branche in dieser Tiefe mit dem Thema Sicherheit befasst.«



Der IT-Experte: »Das Ergebnis unserer Kooperation hat gezeigt, dass Sicherheit im Druck technisch machbar und bezahlbar ist.

Als Referent auf internationalen Fachkonferenzen weiß Bauer, wovon er spricht. Nachdem er bereits vor 19 Jahren einen der ersten Virens Scanner erfand und auf den deutschen Markt brachte, gibt er sich auch heute nicht mit gängigen Lösungen zufrieden: »Mit Heidelberg haben wir den richtigen Partner. Gemeinsam werden die Lösungen, gerade auch im Bereich Sicherheit, fortlaufend weiterentwickelt und optimiert. Das Ergebnis unserer Kooperation hat gezeigt, dass Sicherheit im Druck technisch machbar und bezahlbar ist.«

Auch bei den Benutzeroberflächen punktet Heidelberg: Besonders beliebt bei den Anwendern ist die Möglichkeit, sich ihren Benutzerrechten entsprechend ein persönliches Cockpit

einzurichten und auf die individuellen Anforderungen hin zu konfigurieren. »State-of-the-Art-Technologie, Übersichtlichkeit

Schreiben Sie der Redaktion!

Senden Sie uns Ihre Briefe/Kommentare zum Thema oder allgemeine Fragen aus dem Bereich Publishing an folgende E-Mail-Adresse: redaktion_pp@publish.de

und Benutzerfreundlichkeit steigern Motivation und Produktivität unserer Mitarbeiter«, lobt Uwe F. Bauer.

Geschützter Remote-Zugriff:

Selbst bei kniffligen Themen wie dem Remote Service, bei dem Mitarbeiter des Heidelberg Systemservice über das Internet auf die Druckmaschinen zugreifen, um Fehler zu diagnostizieren und auch zu beheben, bleibt der IT-Experte gelassen. Denn hier setzt Heidelberg modernste Technologie ein. Diese erlaubt es über eine Firewall, nur dann einen Zugriff von außen ins Unternehmensnetz zuzulassen, wenn der Kunde eine Anfrage stellt (Request-Response-Prinzip) und sich die Heidelberg-Systems-service-Mitarbeiter mit einem für diese Anfrage eigens generierten Einmal-Passwort einloggen. »Die Wahrscheinlichkeit eines Angriffs tendiert hierdurch gegen Null. Es wäre wünschenswert, andere Anbieter würden dieser technischen Umsetzung folgen«, urteilt Bauer.

Fazit: Auch die haftungsrechtliche Sicherheit der Lösung lobt der IT-Chef, da Heidelberg als einziger deutscher Druckmaschinenhersteller mit einem vom TÜV zertifizierten Sicherheitskonzept beim Remote Service aufwarten kann. Der Sorgfaltspflicht ist damit Genüge getan. Dies ist zusammen mit dem umfassenden Schutz ein nicht zu unterschätzender Vorteil: »Ich schlafe ruhig, denn ich weiß, dass wir das Bestmögliche getan haben«, resümiert Bauer. Vermeintliche Liebesgrüße aus dem Cyberspace braucht er nicht zu fürchten. [Jürgen Ströbele/pe](#)

Info: Mögliche Schäden

USA: Konservativen Hochrechnungen des FBI Computer Crime Survey zufolge (Jahr 2005) verursachen Cyberkriminelle durch Viren, Würmer, Trojaner und Spyware in Firmen jährlich Schäden in Höhe von 67,2 Milliarden US-Dollar, das heißt 7,6 Millionen US-Dollar stündlich.