Jedes System ist verwundbar

DATENSCHUTZ ■ Wie gehen wir mit den eigenen, vor allem aber mit den geschäftlichen und personenbezogenen Daten unserer Kunden um? Tun wir wirklich alles für deren Sicherheit? Datenschutz ist heute, mehr denn je, Chefsache. Doch trotz gesetzlicher/vertraglicher Regelungen agieren viele Mediendienstleister immer noch viel zu blauäugig.

Datenschutz ist Chefsache und nichts, was man einfach so nebenbei machen kann! Denn Datenschutz macht richtig Arbeit und erfordert ein hohes Maß an Disziplin.

■ Gewisse Nachrichten werden von manchen Zeitgenossen zur Rationalisierung des eigenen unvernünftigen Handels herangezogen. Die Kenntnis vom skandalösen Umgang von Unternehmen und Regierungsstellen mit Daten oder gar deren illegale Beschaffung lösen beim Nachrichtenempfänger nicht etwa verstärkte Gegenmaßnahmen zum Schutz der eigenen Daten, sondern ein resigniertes „Da kann man nichts gegen machen“ oder „Ich habe nichts zu verbergen“ aus. Das Gegenteil aber ist wahr: Gegen Ausspähangriffe sollte man sich bestmöglich schützen und selbstverständlich haben Unternehmen etwas zu verbergen: Geschäftsgeheimnisse und personenbezogene Daten! Während der Schutz der Geschäftsgeheimnisse im Interesse der Unternehmen liegt, ist der Schutz personenbezogener Daten gesetzlich geregelt.

BUNDESDATENSCHUTZGESETZ. Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit personenbezogenen Daten. Dabei gilt der Grundsatz, dass die Verarbeitung von personenbezogenen Daten verboten ist, aber vom Betroffenen erlaubt werden kann. Wenn Ihnen also ein Kunde den Auftrag zur Erstellung einer Visitenkarte erteilt, sollten der durch den Auftrag entstehende Werkvertrag in irgendeiner Weise eine Erlaubnis enthalten, die personenbezogenen Daten der Visitenkarte verarbeiten und für einen Nachdruck speichern zu dürfen. Bei der Vergabe von Aufträgen, bei denen regelmäßig personenbezogene Daten verarbeitet werden, zum Beispiel in der Mailingproduktion, werden Medienunternehmen von Auftraggebern mittels Verträgen zur Auftragsdatenverarbeitung detailliert auf den Schutz der personenbezogenen Daten nach BDSG verpflichtet. In der Regel wird die datenschutzgerechte Löschung der Daten nach Auftragsabschluss gefordert. Im Gegensatz zu der erlaubten Archivierung der Visitenkarte ist das Aufbewahren von Adressdaten nicht gestattet. In der betrieblichen Praxis hat sich vielerorts durchgesetzt, personenbezogene Daten nach zum Beispiel drei Monaten zu löschen. Die sofortige Löschung, zum Beispiel direkt nach Postauflieferung, wäre realitätsfremd, schließlich könnten zum Beispiel im Reklamationsfall Fragen entstehen, die nur durch Einsichtnahme in die angelieferten Daten geklärt werden können.

In den Anhängen zu Verträgen werden typischerweise auch technisch organisatorische Maßnahmen (TOM) beschrieben. Diese Maßnahmen sollen sicherstellen, dass die Verarbeitung der Daten lückenlos protokolliert wird, Zugangs- und Zugriffskontrollen stattfinden und Daten unterschiedlicher Aufträge getrennt verarbeitet werden. Systemadministratoren müssen also sicherstellen, dass die bei der Verarbeitung eingesetzten Systeme mit Zugangskontrollen arbeiten, also zum Beispiel den Login mit Benutzer und Passwort fordern oder mittels Single Sign On auslesen. Selbstverständlich müssen sich die Zugangskontrollen auch auf den Zutritt zum Betriebsgelände und zu besonders schützenswerten Räumen wie Rechenzentren, IT oder zu den Produktionsräumen erstrecken. Diese Maßnahmen werden im Gesetz gefordert, ohne dass dafür Ausführungsbestimmungen genannt werden. In den TOM werden die Maßnahmen präzisiert. Die Folge: Verträge müssen geändert werden, wenn sich Maßnahmen ändern, die User sich also etwa nicht mehr mit User- und Password, sondern mit Key Card oder Finger-Print-Scanner Zugang verschaffen.

DATENSCHUTZBEAUFTRAGTER. Das BDSG schreibt bereits ab neun Personen, die in einem Betrieb mit der Verarbeitung personenbezogener Daten beschäftigt sind oder Zugriff auf diese Daten haben, die Bestellung eines Datenschutzbeauftragten (DSB) vor. In der Praxis spielt diese Grenze häufig keine Rolle, weil in den Verträgen zur Auftragsdatenverarbeitung regelmäßig die Benennung des DSB gefordert wird, es also unabhängig vom gesetzlichen Zwang auch den aus einzelvertraglichen Regelungen gibt. Zum DSB kann ein Mitarbeiter bestellt werden, es kann auch ein externer DSB beauftragt werden. Der DSB ist – ähnlich wie ein Betriebsrat – in seinen Tätigkeiten nicht weisungsgebunden, Mitarbeiter unterliegen einem weitreichenden Kündigungsschutz. Der DSB muss die notwendige Fachkunde und Zuverlässigkeit besitzen. Er beschreibt die organisatorischen Maßnahmen zur Durchsetzung des Datenschutzes und soll ggf. Verbesserungsvorschläge unterbreiten, ein Weisungsrecht steht ihm allerdings nicht zu. Bei Verstößen gegen Datenschutzbestimmungen haftet in Folge dessen auch die Geschäftsführung.

GRUNDSÄTZLICH VERWUNDBAR. „Es gibt nur zwei Arten von Unternehmen: Diejenigen, die wissen, dass sie gehackt wurden, und diejenigen, die nicht wissen, dass sie gehackt wurden“, wird ein Verantwortlicher eines großen Softwareherstellers zitiert. Wenn Angriffe und das Eindringen Unberechtigter ins System schon nicht gänzlich zu verhindern sind, ist es die Aufgabe der für die Sicherheit der Systeme Verantwortlichen, potentiellen Angreifern die Arbeit wenigstens zu erschweren. Dafür gilt es, ein unternehmensweites Sicherheitskonzept zu entwickeln, das natürlich vom Geschäftsmodell des jeweiligen Betriebs abhängig ist. Wer Schnittstellen zu Kunden unterhält, über die unternehmenskritische Daten, zum Beispiel Kundenadressen und Marketingdaten, übermittelt werden, wird andere Anforderungen an sein Sicherheitskonzept stellen, als ein Unternehmen, das lediglich E-Mail und lesenden Internetzugriff über Netzwerkdienste nutzt.
Das Sicherheitskonzept wird üblicherweise mit einer Sicherheitsrichtlinie durchgesetzt, die in Windows-Netzwerken als Group-Policy die Beregelung der Userrechte, -aktivitäten und die Konfiguration der Programme und Workstations bis ins letzte Detail ermöglicht. Systemadministratoren sollten darauf achten, dass alle Standardsysteme, die Netzwerkdienste bereitstellen, beständig mit den aktuellsten Sicherheitspatches versorgt werden, damit zumindest bekannte Sicherheitslücken geschlossen werden. Zu den wichtigsten Komponenten einer Sicherheitsarchitektur zählt die Firewall, mit der die Systemadministratoren die externe Kommunikation zulassen. Hier ist darauf zu achten, dass nur berechtigte und benötigte Netzwerkdienste freigeschaltet werden und zum

DD-SERIE

DATENMANAGEMENT IN DER PRAXIS

In enger Zusammenarbeit mit dem Prepress-Spezialisten CTRL-S GmbH (Stuttgart) zeigt *Deutscher Drucker* auf, wie ein professionelles Datenmanagement bei Mediendienstleistern heutzutage aussehen kann.

- Teil 1 (Desaster Recovery/Business Continuity) erschien in DD 4/2015,
- Teil 2 (Datenschutz) in dieser Ausgabe,
- Teil 3 (Produktionssicherheit/Datenqualität) folgt in DD 8/2015

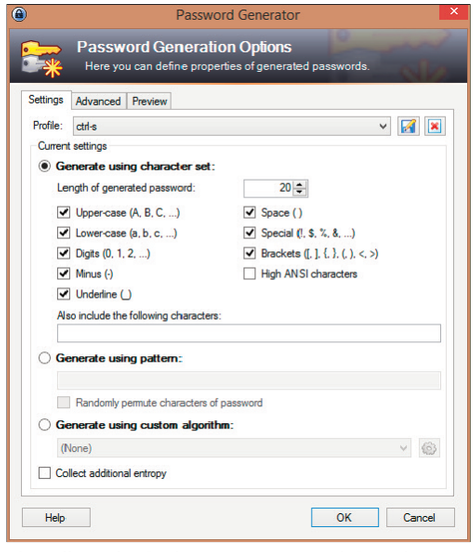
Beispiel Ports und Filter, die zu Testzwecken geöffnet wurden, auch wieder geschlossen werden. Sicherheitskonzepte umfassen regelmäßig neben der Firewall und den Sicherheitsrichtlinien ein Intrusion Detection System (IDS), Virenscanner, VPN etc.

SCHNITTSTELLEN VERSCHLÜSSELN. Nahezu jedes Unternehmen ist im Internet erreichbar. Eine wachsende Anzahl von Medienunternehmen stellt darüber hinaus Schnittstellen zur Verfügung. Dabei ist zwischen den öffentlich zugänglichen Schnittstellen wie zum Beispiel für FTP-Server oder Webshops und privaten Schnittstellen zu unterscheiden. Öffentlich erreichbare Schnittstellen garantieren mit TLS/SSL (im Browser erkennbar durch „https://“) und entsprechenden Zertifikaten nicht nur die Identität des Empfängers, sondern erlauben auch die verschlüsselte Übertragung von Daten. So wird beispielsweise die Übertragung von Passwords oder Kreditkartendaten vom Browser verschlüsselt, verschlüsselt im Internet übertragen und erst wieder beim Empfänger entschlüsselt. TLS/SSL ist ein Beispiel für die immer wieder auftretende Unsicherheit auch von sehr verbreiteten Sicherheitsprotokollen. Der Heartbleed-Bug und die Freak-Attacke zeigten anschaulich, wie wichtig die beständige Aktualisierung der bestehenden Sicherheitskonzepte ist.

Private Schnittstellen sind in der Unternehmenskommunikation typisch bei der Verbindung von Standorten, bei der überwiegend VPN (Virtual Private Network) eingesetzt wird. Bei VPNs wird sozusagen ein privater Tunnel im Internet aufgebaut, über den verschlüsselt kommuniziert werden kann. Damit erreichen VPNs eine ähnliche Sicherheit wie private LANs (Lokal Area Network). Private Schnittstellen sind aber auch zunehmend bei der Vernetzung von Geschäftspartnern zu finden. Über EDI (Electronic Data Interchange) werden Bestellungen, Liefernachweise, Rechnungen und Zahlungen abgewickelt, bei der Anbindung von Dienstleistern an ERP (wie zum Beispiel SAP) hat sich OCI (Open Catalog Interface) durchgesetzt, in der grafischen Industrie ist das in Kürze zu erwartende XJDF dabei, den Austausch zwischen Kunden und Medienunternehmen aber auch zwischen verschiedenen Medienunternehmen zu vereinfachen und zu automatisieren. Die privaten Schnittstellen sind aus verständlichen Gründen besonders schützenswert.

SICHERHEIT VS. PRODUKTIVITÄT. Große Unternehmen neigen dazu, den Datenschutz administrativ durchzusetzen. Das leidige Sperren des Computers zum Beispiel wird dort durch eine Sicherheitsrichtlinie durchgesetzt, die nach kurzer Untätigkeit am Computer die Sperrung erzwingt. Natürlich ist das dadurch erforderliche häufige Eingeben des Passwords der Produktivität nicht förderlich. Der den Datenschutz verantwortende Systemadministrator kann sich dann allerdings keine Untätigkeit vorwerfen lassen. Wenn dagegen in einem kleineren Unternehmen das Sperren des Computers der Disziplin der Mitarbeiter überlassen wird, ist das – neben der geringeren Aufmerksamkeit, die dem Datenschutz bei abnehmender Unternehmensgröße zukommt –, sicherlich auch der Absicht geschuldet, die Produktivität jedes Einzelnen zu erhöhen. Im Extremfall können überzogene Sicherheitsrichtlinien die Produktivität der Mitarbeiter ersticken; aber wie beim Arbeitsschutz gilt auch beim Datenschutz, dass mindestens alles getan werden muss, was gesetzlich vorgeschrieben ist und sinnvollerweise das, was wirtschaftlich und aus anderen Vernunftgründen geboten ist.

DATENSCHUTZ ERFORDERT DISZIPLIN. Waren Sie schon in Betrieben, in denen Sie während der Wartezeit bequem alle Kundendaten des Unternehmens auf einen USB-Stick hätten spielen können? Weil der Mitarbeiter, der aufgebrochen ist, Ihren Ansprechpartner zu suchen, seinen Rechner, angemeldet und möglicherweise mit Zugriff auf alle Netzwerkressourcen, ungeschützt in Ihrer Reichweite zurücklässt? Dabei könnten einfachste Arbeitsanweisungen in Betrieben den Datenklau erschweren. „Windows-L“ ist das Tastaturkürzel für das Microsoft-Betriebssystem, mit dem das System den Zugriff erst nach Eingabe eines Passwords erlaubt. Mac-User haben es mit Bordmitteln etwas schwerer, dort muss zum Beispiel eine Bildschirmecke für den Bildschirmschoner und die Anforderung eines Passwords nach Beenden des Bildschirmschoners eingestellt werden, um den Rechner vor unbefugtem Zugriff zu schützen. Die Alternative am Mac ist ein Zusatzprogramm wie „Butler“, das ebenfalls einen Shortcut zur Verfügung stellen kann.



Einstellung der Optionen zur Password-Generierung in KeePass, einer Software zur Kennwortverwaltung.

Auch unverschlüsselt per Mail übergebene Passwörter stellen ein großes und leicht vermeidbares Sicherheitsrisiko dar, genauso wie das Verwenden von schwachen Passwörtern. Bei CTRL-S sorgt laut Geschäftsführer Martin Klein eine klare Anweisung, Passwörter immer über einen anderen Kanal als die übrigen Zugangsdaten zu übermitteln, dafür, dass keiner, der die Mailkommunikation mitliest, an die kompletten Zugangsdaten kommt. Ähnlich wird bei der Vergabe von Passwörtern verfahren. Kann der User ein eigenes Passwort wählen, sorgen Regeln dafür, dass das Passwort eine ausreichende Zahl an Zeichen enthält und aus einem großen Zeichenvorrat gewählt werden muss. Passwortgeneratoren helfen bei der Generierung von Passwörtern, für das Aufbewahren von vielen verschiedenen Passwörtern stehen Passwort-Manager, wie das kostenlose und in verschiedenen Tests sehr gut bewertete Open-Source-Projekt KeePass, zur Verfügung.

PENETRATIONSTEST. In den Verträgen zur Auftragsdatenverarbeitung sichern sich die Auftraggeber weitreichende Rechte zur Überprüfung der Einhaltung der vereinbarten Bestimmungen. Ein Versicherungskonzern nutzte gegenüber CTRL-S dieses Recht und führte vor der Freischaltung von Mailings, die online gestaltet und adressiert werden können, einen sogenannten Penetrationstest durch. Dabei wurde von einer auf IT-Security spezialisierten Firma Angriffe auf die IT-Infrastruktur und insbesondere die Schnittstellen zum Internet durchgeführt. Prüfkriterien waren dabei nicht nur das Eindringen ins System, um Adressen zu stehlen oder zu verändern, SQL-Injection (Einschleusen von Datenbankabfragen in erlaubte Kommunikation), sondern auch zum Beispiel die Abfrage, welche Technologie mit welchem Versionsstand benutzt wird. Dem Angreifer soll keinerlei Information geliefert werden, die den Angriff erleichtert. Wer um seine Datenschutz-Reputation bemüht ist, erwirbt Zertifizierungen nach der ISO 27000-Reihe oder gibt selbst Penetrationstests in Auftrag.

FAZIT. Das Thema Datenschutz macht richtig Arbeit und ist, wie alle anderen Themen, die unsere Artikelserie behandelt, nichts was man so nebenbei oder bei Bedarf machen kann, Rückendeckung durch die Geschäftsführung ist notwendig, in kleineren Unternehmen ist das Thema Chefsache. Insofern ist man gut beraten, entweder eigene Mitarbeiter mit dem entsprechenden Know-how auszurüsten und für Belange des Datenschutzes freizustellen oder aber auf externen Rat oder Unterstützung zurückzugreifen. Wer als Geschäftsführer Verträge zur Auftragsdatenvereinbarung „einfach so“ unterschreibt und die darin zugesagten Datenschutzmaßnahmen nicht aktiv lebt, begibt sich auf sehr dünnes Eis. **(ms)**