Kauf des Gerätes Ihre Hausaufgaben gemacht und vertrauen dem Hersteller. Was wäre also gegen die regelmäßige Zusendung eines E-Mail-Newsletters einzuwenden? Wenig.

### Die technische Seite

Anders stellt sich die Sachlage dar, wenn man sich in die Situation eines Unternehmens versetzt, dessen Mitarbeiter sich derartige Newsletter ins Büro schicken lassen. Dieses Unternehmen kann naturgemäß kein Interesse daran haben, dass die Kollegen sich während der Arbeitszeit über neue Kameras, aktuelle Handys oder Sonderangebote bei Druckertinte informieren. Aus Unternehmenssicht handelt es sich also zweifellos um unerwünschte Werbesendungen – auch wenn diese von den Mitarbeitern ausdrücklich gewünscht wurden. Hinzu kommt, dass diese Newsletter die Kommunikations-Infrastruktur eines Unternehmens nicht weniger belasten als klassische Spam-Mails.

So einfach sich die Situation aus Unternehmenssicht auch darstellen mag, so schwierig ist es doch, sie zu beheben: Dies beginnt schon auf der technischen Seite, denn Unternehmensnewsletter unterscheiden sich signifikant von den üblichen Spam Mails: Als Absender finden Spam-Filter normale, leicht verifizierbare Unternehmens-Adressen. Als Adressaten sind einzelne valide E-Mail Adressen angegeben, die üblichen Versuche, auf Basis einer bekannten Anschrift weitere Anschriften automatisch zu generieren, fehlen. Spam-typische Inhalte, die sich über eine Suche nach bestimmten Schlüsselwörtern (Rolex, Viagra etc.) entdecken lassen, können – naturgemäß – nicht ermittelt werden. Doch technische Probleme sind in aller Regel lösbar und professionelle Mail-Dienste sind durchaus in der Lage, auch seriöse Newsletter von elektronischer Geschäftspost zu trennen und in die entsprechenden Spam-Verzeichnisse umzuleiten.

### Die menschliche Seite

Sehr viel komplexer stellt sich – wie so oft – die menschliche Seite des Problems dar. Hier gilt es rechtmäßige, aber auch soziale Bedenken zu adressieren. Juristisch gesehen ist ein Arbeitgeber, der seinen Mitarbeitern die Nutzung von E-Mail Services gestattet, ein Anbieter von Telekommunikations- beziehungsweise Telemediendiensten und daher verpflichtet, auch angemessene technische Vorkehrungen zum Schutze des Fernmeldegeheimnisses zu treffen. Darüber hinaus ist es ihm nicht gestattet, private E-Mails zu lesen – und dazu zählen im juristischen Sinne auch Spam-Mails, in denen etwa die Vergrößerung bestimmter Körperteile beworben wird. Ausnahmen bestehen hier lediglich bei Virengefahr oder einem Verdacht auf Verrat von Dienstgeheimnissen.

Das bedeutet, dass selbst die übliche Spam-Mail nicht ohne weiteres gelöscht werden darf: Stattdessen muss sie gespeichert werden, sodass der Adressat sie bei Bedarf abrufen kann. Dies gilt umso mehr für Newsletter, die der Mitarbeiter schließlich bewusst bestellt hat. Um eine für alle Beteiligten befriedigende Lösung zu finden, ist ein offener und transparenter Umgang mit dem Problem unerlässlich: Arbeitgeber- und Arbeitnehmervertreter müssen sich einvernehmlich darauf einigen, wie mit solchen Newslettern umgegangen werden soll. Dabei sollten möglichst die Interessen beider Seiten gewahrt bleiben. Hier kann die Zusammenarbeit mit einem erfahrenen Anbieter von Managed Mail Services deutliche Vorteile bieten, denn diese Unternehmen kennen sich nicht nur mit der technischen, sondern auch mit der juristischen Seite der Problematik aus: So werden Newsletter nicht einfach pauschal gelöscht, sondern – ebenso wie Spam-Mails – für eine definierte Zeitdauer unter Quarantäne gestellt. So bleibt es schließlich dem Adressaten selbst überlassen, ob er sich die jüngsten Informationen über Sonderangebote für Druckertinte aus der Quarantäne abruft – oder ob er es lässt, weil ihm diese Informationen lästig werden.

Alexander Hüls
*retarus*

Datensicherheit

# Zutrittskontrolle nach neuem PAuswG – **Der elektronische Identitätsnachweis**

*Zum 01. November 2010 wurde der neue Personalausweis eingeführt und mit ihm auch gravierende Änderungen. Eine Preissteigerung um rund 20 Euro, ein kleineres Scheckkartenformat und ein RFID-Chip zur Speicherung von elektronischen Daten - aber auch neue Regeln für nicht-öffentliche Stellen zum Umgang mit dem elektronischen Personalausweis.*

### Überblick

Den neuen Personalausweis gibt es in verschiedenen Varianten - unterschieden nach Alter der Ausweisinhaber allerdings immer im gleichen Format und nach allgemeinem Muster.

| Alter des Ausweisinhabers | Gültigkeit | Besonderheiten |
|---|---|---|
| Ab der Geburt bis zur Vollendung des sechsten Lebensjahres | 6 Jahre | Der Antrag ist freiwillig und muss durch die Sorgeberechtigten erfolgen. Auf dem Chip werden nur das Lichtbild und die Daten des sichtbaren maschinenlesbaren Teils gespeichert und keine Fingerabdrücke abgenommen. Keine Unterschrift des Kindes. |

© DATAKONTEXT

| Alter des Ausweisinhabers | Gültigkeit | Besonderheiten |
|---|---|---|
| Bis zur Vollendung des zehnten Lebensjahres | 6 Jahre | Der Antrag ist freiwillig und muss durch die Sorgeberechtigten erfolgen. Fingerabdrücke sind möglich. Keine Unterschrift des Kindes. |
| Ab Vollendung des zehnten Lebensjahres bis Vollendung des 16.Lebensjahres | | Der Antrag ist freiwillig und muss durch die Sorgeberechtigten erfolgen. Fingerabdrücke sind möglich (Entscheidung durch die Sorgeberechtigten). Unterschrift des Kindes ist Pflicht. |
| Ab Vollendung des 16. Lebensjahres bis Vollendung des 24. Lebensjahres | | Der Antrag ist Pflicht und kann durch den Jugendlichen selbst erfolgen. Es besteht die Möglichkeit des elektronischen Identitätsnachweises (Entscheidung des Jugendlichen). Die Kosten betragen für alle Personalausweise (ab Geburt bis zur Vollendung des 24. Lebensjahres) 22,80 EUR. Der erste Personalausweis ist nicht mehr – wie ursprünglich vorgesehen - kostenlos. |
| Ab Vollendung des 24. Lebensjahres | 10 Jahre | Die Kosten betragen nun 28,80 EUR. |

## Elektronischer Identitätsnachweis

Hauptmerkmal des neuen Personalausweises ist der RFID-Chip mit der Möglichkeit den Ausweis auch im elektronischen Rechtsverkehr als Identitätsnachweis zu nutzen. Voraussetzung für den elektronischen Identitätsnachweis (eID) ist die Freischaltung durch den Ausweisinhaber. Ansonsten ist der neue Ausweis weiterhin nur als Sichtausweis nutzbar. Die Erklärung über die Freischaltung ist bei Antragstellung abzugeben und kann während der Gültigkeitsdauer des Ausweises jederzeit schriftlich geändert werden. Ist die Funktion des eID freigeschaltet können die Daten, die auf dem Chip gespeichert sind elektronisch übermittelt werden. Die Übermittlung erfolgt ausschließlich, wenn der Empfänger über ein gültiges Berechtigungszertifikat. Der Chip prüft das Zertifikat und der Ausweisinhaber startet die Übermittlung mit der Eingabe der Geheimnummer. Aus Datenschutzgründen unterscheiden sich die Berechtigungszertifikate nach Datenkategorien. So soll gewährleistet werden, dass eine nicht-öffentliche Stelle nur die Daten übermittelt bekommt, die wirklich notwendig sind.

## Was ist erlaubt?

Wie dürfen nicht-öffentliche Stellen den neuen Personalausweis nutzen?

| Art der Kontrolle/Maßnahme | Zulässigkeit | Bemerkung |
|---|---|---|
| Sichtung des Ausweises durch nicht-öffentliche Stellen | ✓ | Keine Verpflichtung des Ausweisinhabers, allerdings ist die nicht-öffentliche Stelle berechtigt den Zutritt zu verweigern, sofern eine Identitätsfeststellung notwendig ist, aber verweigert wird (Hausrecht). |
| Hinterlegung des Ausweises bei nicht-öffentlichen Stellen | × | **§ 1 Abs. 1 S. 3 PAuswG:** Vom Ausweisinhaber darf die Hinterlegung oder Aufgabe des Gewahrsams in anderer Weise nicht verlangt werden. |
| opto-elektronische Erfassung (Scannen / Kopieren) durch nicht-öffentliche Stellen | × | **§ 14 Nr. 2 PAuswG:** nicht-öffentliche Stellen dürfen Daten aus dem Ausweis oder mit Hilfe des Ausweises ausschließlich nach Maßgabe der §§ 18-20 PAuswG (elektronischer Identitätsnachweis) erheben und verwenden. **Begründung zu § 14 PAuswG (Bundesratsdrucksache 550/08 vom 8. August 2008):** „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die dafür vorgesehenen Wege erfolgen darf. Dies sind für nichtöffentliche […] Stellen der elektronische Identitätsnachweis […]. Weitere Verfahren, so etwa über die opto-elektronische Erfassung (das Scannen) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden. […]“ |



© DATAKONTEXT

| Art der Kontrolle/Maßnahme | Zulässigkeit | Bemerkung |
|---|---|---|
| automatisierte Erfassung, Verarbeitung oder Nutzung der Daten des Personalausweises (ausgenommen eID) | × | Außer zum elektronischen Identitätsnachweis darf der Ausweis durch […] nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. |
| elektronischer Identitätsnachweis | ✓ | Sofern die nicht-öffentliche Stelle über ein gültiges Berechtigungszertifikat verfügt und die Übermittlung der Daten der Identifikation oder Legitimation des Ausweisinhabers dient. |

### Fazit

Zukünftig müssen nicht-öffentliche Stellen die Art der Zugangskontrolle dem neuen Personalausweisgesetz anpassen und sich gewaltig umstellen - denn vor allem die gängige Hinterlegung des Ausweises am Eingangsbereich oder das Kopieren des Ausweises sind nicht mehr zulässig. Der neue Personalausweis darf nur noch gelesen oder mittels elektronischen Identitätsnachweises genutzt werden. Unternehmen, die auf die Identifikation von Personen durch Personalausweis angewiesen sind, sollten dementsprechend in Lesegeräte und Berechtigungszertifikate investieren, um sich auch in Zukunft rechtskonform zu verhalten.

Barbara Broers
*Datenschutzberatung Broers*

Forensik

## Replizierung und Staging
# Das Sicherheits-Kosten-Dilemma lösen

*Mit erhöhten Anforderungen an die Ausfallsicherheit in Unternehmen stehen immer steigende Storage-Kosten in Verbindung.*

Die Techniken „Replizierung" und „Staging" können Unternehmen dabei unterstützen, die Faktoren Sicherheit und Kosten zu optimieren, ohne einen der beiden zu vernachlässigen. Das Thema Backup in Unternehmen geht heute weit über eine bloße Sicherung von Unternehmensdaten hinaus. Besonders kleine und mittelgroße Firmen verschenken in diesem Zusammenhang aber immer noch ungenutztes Potenzial, von der Datensicherung als Teil einer umfassenden IT-Strategie zu profitieren. Steigende Datenmengen, Aufbewahrungspflichten und die Notwendigkeit, Backups an mehreren Orten aufzubewahren, treiben die Storage-Kosten zwangsläufig in die Höhe. Aber gerade in Unternehmen mit stark begrenzten IT-Ressourcen führt dieses Sicherheits-Kosten-Dilemma zu einem Konflikt, der nicht selten auf Kosten der Sicherheit ausgetragen wird. Durch ein ausgewogenes und strategisches Backup-Management und den Einsatz von Technologien wie Replizierung und Staging kann diesem Dilemma professionell begegnet werden. Dabei geht es weniger darum, sich für mehr Sicherheit oder geringere Kosten zu entscheiden, sondern beide Bereiche vor dem Hintergrund der individuellen Anforderungen des Unternehmens zu optimieren: so viel Sicherheit wie möglich, so viel Kosten wie nötig.

### Replizierung: Sicherung mit doppeltem Boden

Damit die eigene Disaster-Recovery-Strategie im Ernstfall wirklich greift, setzen immer mehr kleine und mittlere Unternehmen gleichzeitig auf verschiedene Backup-Medien und verringern so das Risiko von Ausfallzeiten. Schließlich kann es sein, dass aufgrund von höherer Gewalt sämtliche Daten verloren gehen, selbst wenn sie sich in einem abgetrennten Serverraum befinden. Kein Betrieb kann sich einen längeren Produktionsausfall leisten. Wenige verfügen jedoch über die Ressourcen, in zusätzliche Rechenzentren mit hochredundanter Infrastruktur sowie Brand- und Hochwasserschutz zu investieren. Hier setzt die Technik der Replizierung an, wobei exakte Kopien der Backups an unterschiedlichen Speicherorten gleichzeitig abgelegt werden können. In den meisten Fällen wird die Replizierung eingesetzt, um Backups „On-site" zur sofortigen Wiederherstellung, wie auch „Off-site" zu sichern, um sie vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen. Unternehmen mit hohen Sicherheitsanforderungen und knappen Vorgaben für die Wiederanlaufzeit finden durch die Replizierung eine Möglichkeit, erhöhte Sicherheit unter überschaubaren Investitionen zu realisieren, zumal sie bei der Wahl der Backup-Medien schnellere Festplatten sowie günstigere Bandlaufwerke in die Strategie einbinden können.

### Staging: Dynamischer Lebenszyklus für Backups

Intelligentes Backup-Management priorisiert die Daten nicht nur, sondern ordnet diese auch dem passenden Backup-Medium zu. Während die Ausfallsicher-

© DATAKONTEXT