UIMCommunic@tion

Noch Fragen?
Treten Sie in einen Dialog ein!

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Ob fehlende Strukturen oder fehlendes Wissen:

Wer sich auf den (IT-) Dienstleister verlässt, kann schnell verlassen sein

Das Leasing von IT-Geräten ist heutzutage eine etablierte Form der Geschäftsausstattung. Hierbei werden die Geräte am Ende der Laufzeit an den Leasinggeber zurückgegeben und durch neue, modernere ersetzt. Wo bei klassischen Datenspeichern wie Festplatten, Laptops oder Smartphones noch an eine Löschung gedacht wird, wird dies bei Multifunktionsgeräten (Drucker, Scanner, Kopierer) oder Routern oftmals vergessen. Dies kann große Gefahren bergen, schließlich können auf den Geräten noch vertrauliche Informationen gespeichert sein.

Bei Multifunktionsgeräten ist es recht naheliegend, dass noch Daten gespeichert sind. So werden zu druckende oder kopierende Unterlagen in einem Zwischenspeicher abgelegt und dann rollierend gelöscht. Unter den kopierten Unterlagen können sich natürlich auch vertrauliche Angebote des Vertriebs, Protokolle der Geschäftsführung oder des Aufsichtsrats oder einfach „nur“ Teile aus Personalakten befinden.

Dass auch die Rückgabe eines Routers – also eine Netzwerk-Hardware ohne nennenswerten Datenspeicher – eine Gefahr darstellen kann, musste vor Kurzem ein großer deutscher Finanzdienstleistungskonzern feststellen. So wurden die Router ausgetauscht, jedoch die alten nicht vernichtet, sondern an den Händler zurückgegeben. Dieser hat sie dann bei ebay zu einem Preis von EUR 19,90 zum Sofortkauf angeboten, zuvor aber diese nicht auf Werkseinstellungen zurückgesetzt. Dadurch konnte sich der Käufer – ein klein wenig Fachkenntnis vorausgesetzt – in das Intranet des Finanzdienstleisters einwählen und sogar eine IPSec-Verbindung aufbauen sowie verschlüsselte Datenpakete mit einer Gegenstelle austauschen. Der VPN-Zugang hätte dafür genutzt werden können, im Intranet nach Hintertüren, nach unsicheren Systemen und nach „interessanten“ Daten zu suchen oder einfach Schad- und Schnüffelprogramme zu installieren. Der Finanzdienstleister hat somit quasi den Schlüssel für sein Netzwerk mit „aus der Hand gegeben“.

Was in diesem Fall schief gelaufen ist, liegt auf der Hand. Es sollte niemals IT-Sicherheits- bzw. Datenschutz-kritische Hardware nach dem eigenen Gebrauch – zumindest nicht ohne vorherige gewissenhafte Löschung der Daten – verkauft werden. Die Erfahrung der UIMC ist hierbei, dass entweder die internen Strukturen fehlen, die sicherstellen, dass vor Rückgabe sicherheitsrelevanter Hardware sämtliche Daten zu löschen sind, oder, dass das Wissen um diese Problematik nicht vorhanden ist.

Bei einer Vielzahl von IT-Sicherheitsschwachstellenanalysen oder Datenschutz-Checkups musste die UIMC feststellen, dass der Austausch von Hardware bzw. Datenträgern und die damit verbundene Entsorgung oder Rückgabe an den Dienstleister intern gar nicht oder nur unzureichend geregelt sind. Auch vertragliche Regelungen fehlten oftmals. Durch das strukturierte Prüfen der eigenen Organisation werden solche Schwachpunkte entdeckt. Diesen Mängeln kann dann durch verbindliche Regelungen begegnet werden, wie z. B. in einem IT-Sicherheits- und/oder Datenschutz-Handbuch.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Gemäß § 11 Absatz 2 Satz 4 f. BDSG ist ein Dienstleister im Rahmen einer Auftragsdatenverarbeitung (z. B. IT-Systemhaus, Personalabrechnung oder Lettershop) vor Beginn der Dienstleistung und sodann **regelmäßig zu prüfen**, ob die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG eingehalten werden. Dies ist laut BDSG zu dokumentieren.
Doch wie umsetzen? Hierzu hat die UIMC auf Basis des UIMC-Tools für Analyse und Berichterstellung ein Prüftool entwickelt. **Mehr unter:**

UIMC.de/Dienstleister-Audit

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Hinweise zur sicheren Nutzung von E-Mails

Die Nutzung des E-Mail-Dienstes ist mittlerweile nicht mehr wegzudenken. Das Gros an Kommunikation findet per E-Mail statt. Nachfolgend möchten wir daher ein paar Hinweise zur Nutzung geben:

1. Vertrauliche Daten sollten nur verschlüsselt oder passwortgeschützt versendet werden. Es ist zu beachten, dass ungeschützte E-Mails nicht nur während des Versands mitgelesen werden können, sondern beim Gegenüber auch eine automatische Weiterleitung eingerichtet sein kann (aufgrund von Krankheit oder Urlaubs), so dass die E-Mail auch von Unberechtigten gelesen werden könnte.
2. Bei einer automatischen Weiterleitung von E-Mails ist die Vertraulichkeit zu gewährleisten, indem sichergestellt wird, dass alle Empfänger die E-Mails auch lesen dürfen.
3. Sofern E-Mails – bspw. in Form eines Newsletters – an mehrere Empfänger versandt werden, sind Verteilerlisten oder die „BCC-Option“ zu nutzen, so dass der Empfänger nicht die komplette Empfängerliste einsehen kann.
4. Es sollten niemals dienstliche Daten und/oder E-Mails auf einen privaten E-Mail-Account um- oder weitergeleitet werden. Das Schutzniveau ist oftmals weit geringer und die Daten verlassen den Verantwortungsbereich des Unternehmens.
5. Insbesondere beim Empfang von E-Mails von Unbekannten sollte Anhängen und Hyperlinks stets misstraut werden. Im Zweifelsfall sollte die IT-Abteilung kontaktiert werden.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Nutzung von sozialen Netzwerken“ (08 & 02/2013)
„Smartphone-Funktionen sicher nutzen“ (07/2013)
„Der richtige Umgang mit Besuchern“ (06/2013)
„Clean Desktop Policy“ (05/2013)
„Beantwortung telefonischer Auskünfte“ (03/2013)

Informieren & gewinnen!

Wir werden auch 2013 unsere „traditionellen“ Informationstage am Rande der DAFTA im Maternushaus in Köln organisieren. Diesen Tag sollten Sie sich schon einmal vormerken: **Nutzen Sie unsere Informationstage für fachliche Gespräche.**
Auch haben Sie die Möglichkeit, tolle Preise aus unserem Hause zu gewinnen.
Wir würden uns freuen, Sie zu einem interessanten Gespräch begrüßen zu können!

13./14.11.2013, Köln

Sicher outsourcen!?

In unserer Reihe von Praxis-Workshops widmen wir uns als nächstes dem Thema „Outsourcing“. Mit der Auslagerung können z. B. Personalabrechnung oder IT-Support oft qualitativ besser und kostengünstiger umgesetzt werden. Dies birgt aber auch Risiken.

In unserem Workshop wollen wir dies und auch Lösungsansätze zum (rechts-) sicheren Outsourcing mit Ihnen diskutieren.

20.11.2013, Wuppertal

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Wer sich auf den (IT-) Dienstleister verlässt, kann schnell verlassen sein
- ☐ Dienstleister-Auditierungs-Tool: Auftragsdatenverarbeiter effektiv und effizient prüfen
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de