10/2013

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Gewinnspiel
Gewinnen Sie Voll-Lizenzen oder Fachliteratur (siehe Rückseite)

Was deutsche Unternehmen aus der Spähaffäre der NSA lernen sollten

Die Bundesregierung hat in der Vergangenheit viel Geld in abhörsichere Smartphones investiert. Dennoch konnte die NSA über Jahre führende Politiker ausspionieren, u. a. Bundeskanzlerin Merkel. Hierbei stellen sich natürlich die Fragen, wie dies trotz des großen Aufwands passieren konnte, aber auch, wie sich deutsche Unternehmen schützen können, die oftmals weder das Know How noch die finanziellen Mittel der Bundesregierung haben. Beim genaueren hinschauen zeigt sich, dass die Schaffung (sicherheits-) technische Infrastruktur meist nicht ausreichend ist.

Der Fall um die Handy-Überwachung vieler Regierungsverantwortlicher zeigt eines ganz offensichtlich: Technische Maßnahmen können einerseits nie eine vollständige Sicherheit herstellen und andererseits sind diese oftmals auch nicht nutzerfreundlich, so dass die Nutzer aus Bequemlichkeitsgründen hierauf verzichten. Ähnlich wie bei der Verschlüsselung der Sprachkommunikation der Bundeskanzlerin besteht das Problem beispielsweise auch bei vielen Unternehmen schon in der Mail-Kommunikatution. In der Regel funktioniert die Verschlüsselung nur, wenn beide Kommunikationspartner die gleiche Verschlüsselung nutzen. Auch ist die Performance und Bedienbarkeit meist schlechter als bei nicht verschlüsselten Vorgehensweisen. Vielleicht haben die überwachten Politiker deswegen entweder auf die Nutzung der Verschlüsselungsfunktion auf dem Dienstgerät verzichtet oder auf private bzw. andere Geräte zurückgegriffen.

Die Erfahrungen der UIMC zeigen dabei auch, dass auch die Mitarbeiter in Unternehmen und Nutzer von IT-Systemen oftmals aus Bequemlichkeit auf Sicherheit verzichten. Sei es der nicht gesperrte PC im Büro, der unbewachte Laptop im Zug, der schnelle Datenaustausch über dropbox oder der Besucher im Firmengebäude, der nicht angesprochen wird, sondern frei herumlaufen kann. Verschiedene Regelungen im Unternehmen können zwar technisch begleitet werden (automatische Sperre des Rechners, kryptografische Container auf mobilen Geräten, Mail-Verschlüsselung oder elektronische Zutrittssysteme), doch wenn Mitarbeiter weder um die Regelungen wissen noch um deren Bedeutung, bleiben diese meist wirkungslos. Leider können so viele Unternehmen zum Opfer von Wirtschaftsspionage werden.

Hinzu kommt, dass sich viele Mitarbeiter auch durch die Sicherheitssoftware und -produkte in „falscher“ Sicherheit wiegen („Die IT-Abteilung ist für Sicherheit verantwortlich!“). Dem kann einerseits durch klare Richtlinien entgegen gewirkt werden – idealerweise im Rahmen eines Informationssicherheits-Managementsystems. So sollte eine IT-Sicherheits-Organisation aufgebaut werden, so dass neben Dienstanweisungen auch Prozesse und Verfahrensverweisen festgelegt, Verantwortliche und Zuständige bekanntgegeben (z. B. Datenschutzbeauftragter) sowie der Ist-Zustand regelmäßig im Rahmen eines Check-ups oder Re-Audits festgestellt wird, um Verbesserungsmaßnahmen zu ergreifen.

Andererseits zeigt die Erfahrung der UIMC, dass ohne entsprechende Schulung und Sensibilisierung sowohl technische als auch organisatorische Sicherheitsmaßnahmen weit weniger effektiv sind. So muss der Mitarbeiter über Gefahren informiert, auf die Notwendigkeit von Maßnahmen hingewiesen und allgemein eine Aufmerksamkeit für das Thema Informationssicherheit und Datenschutz geschaffen werden.

Dabei sollten Schulungen kein einmaliges Projekt darstellen, sondern vielmehr ein kontinuierlicher Prozess sein, in dem laufend aktuelle Themen aufgegriffen werden. Dies kann durch die Schulung begleitende Plakate, Flyer, Mailings/Newsletter oder E-Learning-Plattformen/eCollege erreicht werden. So werden die Mitarbeiter einerseits sensibilisiert und Ihnen werden andererseits einfache Tipps zum richtigen Verhalten gegeben. Nur so kann der ungewollte Informationsabfluss im Unternehmen bekämpft werden; und das auch für „kleines“ Geld, was gerade für KMU wichtig ist.

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

Schon gewusst?

Es ist nicht nur sinnvoll und zweckdienlich, die Mitarbeiter im Rahmen der Informationssicherheit zu sensibilisieren. Es existieren auch **gesetzliche Verpflichtungen**, die Beschäftigten zu schulen: Gemäß § 12 AGG ist jeder Arbeitgeber verpflichtet, die Mitarbeiter im Hinblick auf die Anti-Diskrimierung zu schulen. Auch der Datenschutz beinhaltet eine Schulungskomponente!

Kurse zum AGG, Datenschutz und zur IT-Sicherheit finden Sie unter

eCollege.UIMC.de

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

Veröffentlichung von Mitarbeiterfotos

Im Rahmen des Marketings werden immer öfter Fotos von Mitarbeitern veröffentlicht, um dem Unternehmen „ein Gesicht zu geben“: Ob im Kontaktbereich der Internetpräsenz oder im Rahmen von Image-Videos bzw. -Broschüren. Auch hierbei sind verschiedene rechtliche Aspekte zu beachten:

1. Mit Ausnahme von Mitarbeitern, zu deren Kernaufgaben es auch gehört, das Unternehmen nach Außen darzustellen (Geschäftsführer, Vertriebsbereich oder Pressereferent), ist eine schriftliche Einwilligung einzuholen, wenn diese **namentlich mit den Kontaktdaten genannt** werden sollen.
2. Wenn diese Kontaktinformationen durch **Fotos** begleitet werden sollen, bedarf es in jeden Fall einer Einwilligung.
3. Diese **Einwilligung** muss freiwillig sein und kann künftig widerrufen werden. Auch sind alle Veröffentlichungsmedien darzustellen (z. B. Internetpräsenz, soziale Netzwerke, Imagebroschüre).
4. Wenn für die Fotos ein professioneller Fotograf engargiert wird, sollten unbedingt die **Urheberrechte** für die spätere Verwendung miterworben werden (andernfalls können Sie ggf. der Verantwortung gegenüber Ihren Mitarbeitern nur schwer nachkommen).
5. Wenn Videos oder andere Szene-/Gruppenfotos erstellt werden, können Mitarbeiter **nicht ohne Weiteres** die zuvor erteilte Einwilligung wieder zurückziehen. Hierauf sollten die Mitarbeiter entsprechend hingewiesen werden.
6. Ferner ist es **empfehlenswert**, auf eine „serisöse“ Darstellung zu achten (keine „Schnappschüsse“, die den Mitarbeiter ggf. lächerlich machen o. ä.).

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:
„Sichere Nutzung von E-Mails“ (09/2013)
„Umgang mit sozialen Medien“ (08 & 02/2013)
„Smartphone-Funktionen sicher nutzen“ (07/2013)
„Der richtige Umgang mit Besuchern“ (06/2013)
„Clean Desktop Policy“ (05/2013)

Informieren, testen, gewinnen, diskutieren

Unter diesem Motto stehen die diesjährigen Informationstage der UIMC/UIMCert, die traditionell neben dem Fachkongress „DAFTA“ im Maternushaus in Köln stattfinden. Nutzen Sie unsere Informationstage für fachliche Gespräche und **Informationen** sowie zum **Testen** unseres eColleges und des Vorabkontroll-Tools. Auch haben Sie die Möglichkeit, tolle Preise aus unserem Hause zu **gewinnen**:

- Vollversion eCollege „Basic“
- Einzelplatzlizenz des Vorabkontroll-Tools „light“
- Fachbuch „Datenschutz - Best Practice“.

Wir würden uns freuen, Sie zu einer interessanten **Diskussion** begrüßen zu können! Bei einer vorherigen Anmeldung bei uns können wir Ihnen auch einen Termin freihalten.

13. und 14. November 2013, Maternushaus Köln

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

☐ Was deutsche Unternehmen aus der Spähaffäre der NSA lernen sollten

☐ Gesetzliche Anforderungen zur Schulung und Sensibilisierung der Mitarbeiter

☐ **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