UIMC: Was deutsche Unternehmen aus der Spähaffäre der NSA lernen sollten

UIMC: 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 Checkups 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.

UIMC Dr. Voßbein GmbH
 Co. KG
Dr. Jörn Voßbein
Nützenberger Straße 119
42115 Wuppertal
Tel.: 0202 / 265 74 - 0
Fax: 0202 / 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.uimc.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=548575" width="1" height="1">

Pressekontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Firmenkontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Die UIMC DR. VOSSBEIN GmbH & Co KG, gegründet 1997, hat die damals seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und Dr. Jörn Voßbein in einer Beratungsgesellschaft vereint. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen.Kerngebiete ihrer Arbeit sind die IT-Sicherheit und der Datenschutz. Sie kann beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und hat eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Felder, auf denen ihre Erfahrungen branchenführend sind.Ihr Leistungsspektrum/Produktprogramm unterscheidet sich von dem anderer Beratungsunternehmen: Sie setzt ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für ihre Kunden generiert werden. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren.Sie führt Workshops, Schulungen sowie Fortbildungsmaßnahmen auf den Sektoren IT-Sicherheit und Datenschutz mit ihrer Marke UIMCollege auch als Inhouse-Veranstaltungen durch.