03/2013

UIMCommunic@tion

Dies ist keine stille Post:
Um interne Verteilung wird gebeten!

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Der Mensch hebelt als Layer 8 teure Sicherheitssoftware aus

[Pressemitteilung vom 03.04.2013] In vielen Unternehmen werden zum Teil hohe Summen für durchaus erforderliche Sicherheitssoftware investiert. Nichtsdestotrotz müssen immer wieder Sicherheitsvorfälle registriert werden, wodurch z. T. hochvertrauliche Informationen nach Außen dringen, was wiederum auch die Wettbewerbsfähigkeit gefährdet.

Neben den öffentlich sehr stark wahrgenommenen Hacking-Attacken werden unzählige Vorfälle in den Unternehmen verzeichnet, die weniger durch Kriminelle als vielmehr durch die eigenen Mitarbeiter verschuldet sind. So zeigte beispielsweise die neueste KES-Sicherheitsstudie, dass über 70 % der Sicherheitsvorfälle im Unternehmen durch die eigenen Mitarbeiter verschuldet werden. Die weitaus meisten sind jedoch keine bewussten oder mutwilligen Verstöße, sondern vielmehr Konsequenzen aus Unwissenheit oder fehlender Sensibilität.

Dies legt die Vermutung nahe, dass die Mitarbeiter – also die Nutzer, die in Technikerkreisen auch scherzhaft „Layer 8“ genannt werden – im Rahmen der Sicherheitspolitik im Unternehmen vergessen werden.

Die Erfahrungen der UIMC decken sich hierbei mit den Ergebnissen der besagten KES-Studie, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen oder weil sie die Erfordernis einer bestimmten Maßnahme nicht erkennen. Hinzu kommt, dass sich viele Unternehmen durch die Sicherheitssoftware und -produkte in „falscher“ Sicherheit wiegen. Hinzu kommt eine modernere Form der Gefahr: Die Mitarbeiter nutzen soziale Netzwerke und geben dadurch entweder Unternehmensinterna direkt preis, indem sie geheime Informationen auf Fotos von Arbeitsplätzen einsehbar machen, oder geben in „Plauderlaune“ andere Interna indirekt einem relativ großen Empfängerkreis „versehentlich“ bekannt.

Dies zeigt, dass nicht nur die Layer 1 bis 7 des OSI-Modells durch die IT-Abteilung „gehärtet“ werden sollten, sondern auch die achte Schicht selbst. Dies kann einerseits durch klare Vorgaben im Rahmen eines Informationssicherheits-Managementsystems erreicht werden. 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 geschaffen werden.

Dabei sollte eine solche Schulungsmaßnahme kein einmaliges Projekt darstellen, sondern vielmehr ein kontinuierlicher Prozess sein, in dem laufend auch aktuelle Themen aufgegriffen werden. Hierzu eignen sich insbesondere E-Learningplattformen, auf die einerseits dezentral zugegriffen werden und auf denen andererseits Inhalte kontinuierlich aktualisiert werden können, ohne großen Organisationsaufwand zu erzeugen. Innerhalb der Kurse können neben (rechtlichen) Grundlagen insbesondere praktische Themen diskutiert und Tipps zur Einhaltung gegeben werden. Die Möglichkeit, durch Tests das erlernte Wissen zu überprüfen, kann die Mitarbeiter zusätzlich motivieren.

Auch wenn der Frage, ob Sicherheitssoftware ohne Betrachtung von Layer 8 nutzlos ist, sicherlich nicht kommentarlos zugestimmt werden kann, so wird die Effektivität solcher Maßnahmen durch die Kompetenz und die Sensibilisierung der Mitarbeiter maßgeblich bestimmt.

Mehr Pressemitteilungen finden Sie hier:

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

Vorherige Info-Briefe einsehen?
www.UIMC.de/Communication

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Tipps für die Beantwortung telefonischer Anfragen/Auskünfte

Jeder kennt diese Situation: Es ruft ein Schulungsanbieter an und möchte bestimmte Informationen über einen Ihrer Kollegen erhalten („Ich brauche zur Seminaranmeldung *noch eben schnell* die private Anschrift und Geburtsdatum Ihres Kollegen“) oder ein Kunde ruft an und möchte eine (vermeintliche) Selbstauskunft haben („Sind meine Daten noch aktuell? Sagen Sie mir doch eben mal, was Sie im System stehen haben!“) oder der Nachmieter ruft beim Versorger an oder ein Angehöriger auf der Krankenhaus-Station oder oder oder... **Doch dürfen Sie diese Informationen überhaupt weitergeben?**

Nachfolgende Tipps und Denkanstöße sind dabei sicherlich unterstützend:

1. Vergewissern Sie sich, ob der Anrufer auch derjenige ist, für den er sich ausgibt (ggf. Rückruf vereinbaren und/oder Telefonnummer im Internet prüfen).
2. Sofern es möglich ist, sollten Sie beim Betroffenen nachfragen („Einwilligung einholen“).
3. Bei polizeilichen/staatsanwaltlichen Anfragen:
   - Scheuen Sie nicht davor zurück, nach der Rechts-/Gesetzesgrundlage für die gewünschte Übermittlung zu fragen.
   - Es sollte die Schriftform gewahrt werden (Fax inkl. Übermittlungrund/Rechtsgrundlage).
4. Prüfen Sie gewissenhaft die Rechtmäßigkeit, schließlich tragen Sie die Verantwortung dafür (im Zweifelsfall beim Datenschutzbeauftragten nachfragen).
5. **Last but not least:** Die Ablehnung einer Anfrage muss nicht unhöflich sein; vielleicht ist es ja höflich dem Betroffenen gegenüber.

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

Bisher erschienene Hinweise/Tipps:
„Sichere Nutzung von Smartphones“ (01/2013)
„Nutzung von sozialen Netzwerken“ (02/2013)

Testen Sie das eCollege

Das eCollege der UIMC ist eine sinnvolle Alternative zu klassischen Schulungen. Innerhalb der Kurse des eColleges werden neben Grundlagen insbesondere praktische Tipps zur Einhaltung gegeben. Schwerpunkt ist hierbei die Sensibilisierung.

Über den Browser kann via Internet zugegriffen werden, so dass von „überall“ gelernt werden kann; auch mobil und ohne VPN-Zugang.

☐ Bitte ermöglichen Sie mir einen kostenfreien Demo-Zugang!

Social Media

Innerhalb der UIMCollege-Praxis-Workshops diskutieren wir mit Ihnen die Risiken von Social Media (also von sozialen Netzwerken und weiteren Web 2.0-Diensten) im Hinblick auf den Datenschutz und die Informationssicherheit.

Auch werden Ihnen entsprechende Hinweise gegeben, wie diesen Risiken begegnet werden kann. Hierbei betreiben wir keine Systemberatung, sondern zeigen vielmehr Risikominderungsstrategien auf.

17.04.2013, 13:30 Uhr

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

☐ Praxis-Workshop „IT-Trends Sicherheit“ (24.04.2013 im rewirpower-Stadion des VfL Bochum)

☐ 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