06/2015

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Ob Bundestag oder Wirtschaftsunternehmen – Reicht ein Update der IT-Sicherheitstechnik aus?

Aktuell wird das IT-System des Bundestags komplett neu aufgesetzt, um nach dem Hackerangriff die Sicherheitstechnik zu aktualisieren. Hierdurch soll der Stand der Sicherheit maßgeblich verbessert werden. Dr. Jörn Voßbein, mehrfach bestellter IT-Sicherheitsbeauftragter, weist darauf hin, dass dies nur ein Baustein zur Verbesserung der Sicherheit ist; vielmehr muss auch der User in die Überlegungen und Maßnahmen viel stärker einbezogen werden.

Nicht erst seit den Enthüllungen rund um die NSA oder dem Angriff auf das Netzwerk des Bundestages ist vielen (nicht nur großen) Unternehmen bewusst, dass sie sich um die Sicherheit der IT-Systeme und ihrer vertraulichen Daten kümmern müssen. Hierzu werden den IT-Abteilungen entsprechende Budgets für die Anschaffung und den Betrieb von Sicherheitssystemen zur Verfügung gestellt.

Doch wenn über IT-Sicherheit, Informationssicherheit oder auch über Datenschutz gesprochen wird, liegt der Hauptaugenmerk oftmals auf den Aktivitäten der IT-Abteilung. Es werden Firewalls, Virenscanner, Intrusion Detection Systeme oder Verschlüsselungsprogramme angeschafft und eingesetzt, so dass die IT-Systeme dadurch „gehärtet“ werden. Dass es trotzdem immer wieder zu Virenbefall, Spionagefällen oder anderen Vorfällen kommt, ist aber insbesondere auch in einem Faktor begründet: dem Menschen bzw. dem User.

Trotz der technischen Aufrüstung müssen immer wieder Sicherheitsvorfälle registriert werden, wodurch z. T. hochvertrauliche Informationen nach Außen dringen, Systeme „lahmgelegt“ oder Compliance-/Datenschutz-Probleme bekannt werden. Vertrauensverlust, Vertraulichkeitsverlust bei Betriebsgeheimnissen wie Produktionsverfahren oder Preiskalkulationen oder die Nicht-Verfügbarkeit von Systemen oder Daten: Durch solche Vorfälle ist die Wettbewerbsfähigkeit des Unternehmens gefährdet.

Doch woran liegt dies, wo doch soviel in die Sicherheit investiert wird? Grund hierfür sind nicht ausschließlich Hacker. So zeigen diverse Sicherheitsstudien, dass über zwei Drittel der Sicherheitsvorfälle im Unternehmen durch die eigenen Mitarbeiter verschuldet werden. Dabei handelt es sich oftmals nicht um bewusste oder mutwillige Verstöße. Vielmehr sind sie vielmehr die Konsequenz aus Unwissenheit oder fehlender Sensibilität der Mitarbeiter.

Die Erfahrungen der UIMC zeigen dabei, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen, den Sinn nicht erkennen oder von ihnen gar nicht erst wissen. Auch wiegen sich viele Mitarbeiter aufgrund der ausgefeilten Sicherheitstechnik in „falscher“ Sicherheit, schließlich „kümmert sich ja eine ganze Abteilung um die IT-Sicherheit“. Soziale Netzwerke, private Smartphones oder Cloud-Speicher-Dienste reißen indes weitere Löcher in die Sicherheitsarchitektur.

Doch sollte der User nicht als Täter oder „Feindbild“ gesehen werden. Vielmehr sollte man ihn als Teil der Sicherheitsarchitektur sehen und auch diesen Bereich – analog zu den technischen Sicherheitsmaßnahmen – „härten“. Beginnen sollte man nach einer kurzen Risikoanalyse zunächst mit verbindlichen Regelungen, um Transparenz und einen Rahmen zu schaffen, in dem sich die Mitarbeiter sicher bewegen können. Danach sollten praxisorientierte Schulungen und Sensibilisierungsmaßnahmen gestartet werden. So muss der Mitarbeiter nicht nur auf die Richtlinien verpflichtet, sondern auch über die Gefahren informiert und auf die Notwendigkeit der Maßnahmen hingewiesen werden. Denkbar sind persönliche Schulungen, E-Learning-Plattformen und/oder Informationsmaterialien wie interne Newsletter, Blogs oder Flyer. Solche Maßnahmen sollten aber nicht als einmaliges Projekt, sondern als ein kontinuierlicher Prozess verstanden werden, in dem laufend auch aktuelle Themen aufgegriffen werden.

Schon gewusst?

Viele Schulungen sind sinnvoll, weil sie die Qualität der Arbeit und/oder die Sicherheits- sowie Compliance-Situation innerhalb des Unternehmens verbessern. Zum Teil existieren ganz konkrete gesetzliche Auflagen für eine Schulung der Mitarbeiter. Hierbei sei exemplarisch der Datenschutz genannt, mit dem gemäß § 4g Absatz 1 Satz 4 Nr. 2 BDSG die Mitarbeiter vertraut gemacht werden sollen. Aber auch im Rahmen des Allgemeinen Antidiskriminierungsgesetzes sind nach § 12 Absatz 2 AGG Schulungen durchzuführen. Eine kombinierte Umsetzung von Datenschutz und Informations-/IT-Sicherheit ist hierbei durchaus sinnvoll.

Fragen Sie Ihren Datenschutzbeauftragten

UIMC® | in Datenschutz und Informationssicherheit stets gut beraten!

UIMC Dr. Vossbein GmbH & Co KG, Nützenberger Straße 119, 42115 Wuppertal

Tel.: (02 02) 2 65 74 - 0, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Sicheres Entsorgen bzw. Vernichten

Datenträger, die schützenswerte Daten enthalten (wie z. B. CDs, USB-Sticks, Festplatten, Multifunktionensgeräte, Smartphones) und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Analoges gilt für Papier-Unterlagen.

Hierbei sind beispielsweise folgende Maßnahmen zu ergreifen:

» Jedes Gerät, das entsorgt werden soll, ist daraufhin zu überprüfen, ob noch Speichermedien enthalten sind. Ist dies der Fall, sind o. g. Maßnahmen zu ergreifen.

» Funktionstüchtige Datenträger sind durch physikalisches Löschen der Daten zu bereinigen. Hierzu sind (je nach Vertraulichkeit der gespeicherten Daten) entsprechende Tools zu nutzen.

» Bei nicht mehr funktionierenden Datenträgern sollte dies durch mechanische Zerstörung erreicht werden. Die Datenträger sollten der IT-Abteilung übergeben werden.

» Belege und Druckausgaben, die sicherheitsrelevante Informationen beinhalten, sind vom übrigen Abfall getrennt zu entsorgen. Unter Umständen ist es einfacher, alle Datenträger zu sammeln und sicher beseitigen zu lassen, als zu versuchen, die sensitiven Elemente herauszusuchen. Dies gilt auch für Zwischen- und Fehldrucke.

» Zur Vernichtung von Unterlagen sind Datenschutz-Container oder Shredder zu nutzen.

» Größere Mengen sollten einem externen Vernichtungsunternehmen sicher übergeben werden (beachten Sie die datenschutzrechtlichen Anforderungen). Diese Unterlagen sind bis zur Vernichtung sicher in der Form zu verwahren, dass Unbefugte auf die Unterlagen nicht zugreifen können.

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

Wünschen Sie sich Tipps oder Wissenswertes zu einem bestimmten Thema? Dann schicken Sie uns eine Mail an communication@uimc.de.

E-Learning mit dem eCollege

Nicht nur in dezentralen Institutionen sind Präsenzschulungen durch Vorbereitung, Transferzeiten und starrer Zeitpunkte ineffizient. E-Learning kann eine sinnvolle Alternative oder Ergänzung zu klassischen Schulungen sein: Die Mitarbeiter erhalten umfassende, jederzeit verfügbare Informationen, die sie in den Zeiten durcharbeiten können, in denen es ihr Tagesgeschäft zulässt.

bis zum 31.09.2015 entfällt die Einrichtungsgebühr

Mehr unter eCollege.UIMC.de

Vortrag zum Faktor Mensch

Innerhalb unseres Vortrags gehen wir auf die auf der Vorderseite aufgeworfenen Probleme detaillierter ein und stellen die Risiken dar, die durch Mitarbeiter entstehen können... trotz technischer Sicherheitsmaßnahmen. Doch selbstverständlich stellen wir auch Lösungsmöglichkeiten vor, wie aufgeworfenen Gefahren begegnet werden kann. Nutzen Sie die Chance, im Anschluss mit dem Referenten im Plenum oder in einem persönlichen Gespräch zu diskutieren.

Düsseldorf, 29.09.2015

Mehr unter Termine.UIMC.de

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

☐ Reicht ein Update der IT-Sicherheitstechnik aus?

☐ Gesetzliche Schulungsanforderungen

☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

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

Mehr Informationen, Hinweise und Tipps finden Sie hier: www.UIMC.de/communication

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.