UIMCommunic@tion

03/2018

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

IT-Sicherheit beginnt beim Mitarbeiter

Ein digitaler Einbruch ist heute für viele Unternehmen mindestens so schwerwiegend wie ein herkömmlicher mit Dietrich und Brecheisen – wenn nicht sogar noch schlimmer. Er kann dazu führen, dass streng vertrauliche Daten in die falschen Hände geraten oder wichtige Daten nicht mehr zugänglich sind; aber auch der Imageschaden kann verheerend sein. Wer liest schon gerne über einen Geschäftspartner oder sein eigenes Unternehmen, dass sensible Kundendaten verlorengegangen oder sogar in kriminelle Hände gelangt sind. Kurz: Ein Hackerangriff kann das Renommee oder sogar die Existenz eines Unternehmens gefährden. Weil sich viele Unternehmer und Geschäftsführungen dieser Gefahr bewusst sind, wird seit Jahren viel in die digitale Sicherheit investiert. Milliarden Euro fließen in Firewalls, Virenscanner, Intrusion Detection Systeme oder Verschlüsselungsprogramme. Zeigen die eingesetzten Ressourcen den gewünschten Erfolg? „Zweifel sind angebracht, ob tatsächlich richtig und zielgerichtet investiert wird", gibt sich IT-Sicherheitsfachmann Dr. Jörn Voßbein nachdenklich. Tatsächlich lassen Berichte über Sicherheitslücken nicht nach.

Diverse Sicherheitsstudien zeigen mit regelmäßiger Konstanz, 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 häufig die Konsequenz aus Unwissenheit oder fehlender Sensibilität der Mitarbeiter.

Beispiel 1: Ransomware. Vielen Mitarbeitern ist nicht bewusst, was sie mit einem unbedachten Anklicken eines Anhangs einer Mail anrichten. Zumal viele Mitarbeiter unter Stress stehen und die Mails mit schädlichen Inhalten häufig „gut gemacht" sind. Auch wiegen sich viele Mitarbeiter aufgrund der ausgefeilten Sicherheitstechnik im Unternehmen in „falscher" Sicherheit, schließlich „kümmert sich ja eine ganze Abteilung um die IT-Sicherheit".

Beispiel 2: Passwörter. In der heutigen digitalen Welt müssen sich die Nutzer zunehmend mehr Passwörter merken. Dies führt dazu, dass Passworte „synchronisiert" werden, indem ein Nutzer für mehrere Dienste – ob privat oder dienstlich – das gleiche Passwort nutzt. Wenn, wie jüngst bei dem Chatportal knuddels.de geschehen, die Zugangsdaten durch Hacker entwendet werden, kann dies auch dazu führen, dass Unternehmenssysteme angegriffen werden, wenn der Nutzer beispielsweise eine dienstliche Mail-Adresse hinterlegt hat. Sie dient dem Hacker als Indiz dafür, wo der Nutzer ggf. das gleiche Passwort zum Zugang zu Systemen nutzt.

Dazu passt, dass die Erfahrungen der UIMC zeigen, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen, den Sinn nicht erkennen oder von ihnen gar nicht erst wissen. Soziale Netzwerke, private Smartphones oder Cloud-Speicher-Dienste reißen indes weitere Löcher in die Sicherheitsarchitektur.

Doch sollte hierbei 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". „Sensibilisieren, sensibilisieren und nochmals sensibilisieren für die IT-Sicherheit", empfiehlt Dr. Voßbein eine langfristige und nachhaltige Konzeption zur Mitarbeiterschulung. „Der Datenschutz mit hohen gesetzlichen Anforderungen durch die Datenschutz-Grundverordnung wird hierdurch ebenfalls verbessert."

Damit eine solche Schulungsmaßnahme kein einmaliges Projekt darstellt, sollte ein kontinuierlicher Prozess geschaffen werden, in dem laufend aktuelle Themen aufgegriffen werden. Hierzu eignen sich insbesondere E-Learning-Plattformen, auf die einerseits dezentral zugegriffen und auf denen andererseits Inhalte 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.

„Die Mitarbeiter sollten nicht nur auf Richtlinien verpflichtet werden, sondern auch über die Gefahren informiert und auf die Notwendigkeit der Maßnahmen hingewiesen werden", schlägt Dr. Voßbein vor, um einen hohen Wirkungsgrad für die IT-Sicherheit des Unternehmens zu erreichen.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, 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

Save the Date!

Die Informationstage der UIMC und UIMCert finden traditionell im Maternushaus in Köln (Raum Ursula) statt. Hier können Sie sich über die ersten Erfahrungen mit der „neuen" Datenschutz-Grundverordnung informieren und mit uns diskutieren. Neben den Informationspflichten, prognostizierten Abmahnwellen, vermehrten Auskunftsersuchen und Anfragen der Datenschutz-Aufsichtsbehörden sind insbesondere die Risikobewertung und die Datenschutz-Folgenabschätzung aktuelle Themen. **Auch werden wir eine kleine Besonderheit für Sie bereithalten.**

Der Eintritt ist wie gewohnt natürlich frei (dies gilt nicht für die parallel stattfindende DAFTA). Nutzen Sie unsere Informationstage auch für fachliche Gespräche in angenehmer Atmosphäre. Selbstverständlich ist für uns, dass wir mit Ihnen ein kostenloses Beratungsgespräch führen und Sie als unsere Gäste bewirten.

Köln, 14./15. November 2018

Datenschutz-Folgenabschätzung

Veröffentlichung der „Muss-Liste" durch die Datenschutzkonferenz (DSK)

Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so ist eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO vorzunehmen. Die Aufsichtsbehörden haben aber die Möglichkeit, eine Liste der Arten von Verarbeitungsvorgängen zu erstellen, für die zwingend eine oder keine Datenschutz-Folgenabschätzung erforderlich ist. Dies hat die Datenschutzkonferenz nun getan: Innerhalb einer Liste sind jene Datenverarbeitungen angeführt, für die zwingend eine Datenschutz-Folgenabschätzung durchzuführen ist. Hierbei werden 16 maßgebliche Kriterien aufeführt. Die Regel ist: Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und eine Datenschutz-Folgenabschätzung durch den Verantwortlichen durchzuführen (ein Auftragsverarbeiter ist nicht verpflichtet).

Wenn eine Verarbeitung diesen Kriterien nicht unterliegt, bedeutet dies im Umkehrschluss nicht, dass zwingend keine Datenschutz-Folgenabschätzung durchzuführen ist. Vielmehr ist eine Risikobewertung durchzuführen. Ist das Ergebnis, dass voraussichtlich ein hohes Risiko für die Rechte und Freiheiten besteht, so ist eine Datenschutz-Folgenabschätzung vorzunehmen.

111 Tage Datenschutz-Grundverordnung: Was ist noch zu tun?

Mit diesem Titel haben wir am 13.09.2018 im Rahmen der Roadshow „Cybercrime" einen Vortrag gehalten. **Falls Sie es nicht einrichten konnten, am Vortrag teilzunehmen,** lassen wir Ihnen gerne die Vortragsunterlagen zukommen. Kommen Sie einfach formlos auf uns zu.

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

- ☐ IT-Sicherheit beginnt beim Mitarbeiter
- ☐ Informationen zum Online-Formular-Center und zum eCollege
- ☐ **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: https://communication.UIMC.de

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