UIMCommunic@tion
praxisnah.gut.informiert.

10/2022

Ausgabe für Deutschland

BSI-Lagebericht als Weckruf für Behörden und Wirtschaft

UIMC: Trotz Krise sollte in Informationssicherheit investiert werden

Noch nie war die Gefahr so groß, im Cyberraum Opfer krimineller Machenschaften zu werden wie derzeit. Tatsächlich werden seit Beginn des russischen Angriffskrieges auf die Ukraine immer mehr Menschen, Unternehmen und öffentliche Einrichtungen Opfer von Cyberattacken. Dieses aktuelle Bild liefert der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), der erst vor wenigen Tagen in Berlin präsentiert wurde. „Aufwachen ist das Gebot der Stunde. Dieser aktuelle Lagebericht lässt die Alarmglocken schrillen. Öffentliche Institutionen, Unternehmen und letztlich wir alle sind gefordert, unsere Sicherheit im Cyberraum zu verbessern und zu optimieren“, erklärt UIMC-Geschäftsführer Dr. Jörn Voßbein anlässlich der Vorstellung des BSI-Lageberichtes. Die wesentlichen Ergebnisse, IT-Problemlagen und mögliche Handlungsempfehlungen müssen in den Blick genommen werden.

Hinter den Cyberattacken stehen überwiegend finanzielle Motive. Der Identitätsdiebstahl, die Erpressung mit kompromittierenden Fotos („Sextortion“) und Fake-Shops im Internet stellen aktuell die größten Risiken für Nutzerinnen und Nutzer dar. Bei Fake-Shops muss online die bestellte Ware bezahlt werden, die dann aber nie geliefert wird. Beim Identitätsdiebstahl nutzen Kriminelle persönliche Daten anderer Personen, um damit unter anderem Online-Konten zu eröffnen, Verträge abzuschließen oder Waren und Dienstleistungen zu bestellen. Die Geschädigten erfahren davon oftmals erst, wenn ihnen vom Konto Geld abgebucht wird oder Rechnungen in den Briefkasten flattern. Allerdings macht die Bundesbehörde auch auf eine erhöhte Bedrohungslage im Zuge des russischen Angriffskrieges aufmerksam.

Im Cyberbereich werden Angriffe durch Ransomware als größte Bedrohung identifiziert. Darunter versteht man Cyberattacken auf Unternehmen, Verbände und Behörden, mit dem Ziel, Lösegeld zu erpressen. In den letzten Monaten ist es zu mehreren Ransomware-Vorfällen gekommen, bei denen Kommunen (u.a. die Stadt Witten) oder Firmen (Heizkostendienstleister ISTA, Funke Medien Gruppe) angegriffen wurden.

Im Lagebericht des Bundesamtes wird beklagt, dass in vielen Fällen eine unzureichende Qualität von IT- und Softwareprodukten die kriminellen Attacken begünstigt. Im Jahr 2021 wurden laut Lagebericht zehn Prozent mehr Schwachstellen in Software-Produkten bekannt als im Vorjahr. Das Bundesamt fordert aufgrund der Ergebnisse und Feststellungen auch eine Zeitenwende für „Cyber-Sicherheit made in Germany“. Aus Sicht von UIMC muss der Lagebericht eine Motivation sein, um die Anstrengungen für mehr Cybersicherheit in allen Bereichen zu maximieren. „Ohne Informationssicherheits-Managementsystem wird es für Unternehmen schwer. Sicherheitslücken müssen geschlossen werden. Die Überprüfung der IT-Systeme, die regelmäßige Schulung der Mitarbeiterschaft, sowie ein wirksames Notfallmanagement verbessern die Informationssicherheit von Unternehmen und Behörden“, empfiehlt Dr. Jörn Voßbein als erfahrener Informationssicherheits-Fachmann. Mit diesen drei Maßnahmen ließe sich die IT-Sicherheitsarchitektur in Wirtschaft und Verwaltung erheblich verbessern. „Auch kleine Maßnahmen helfen. Es müssen nicht immer riesige Investitionen sein. Eine Bestandsaufnahme ist dabei ein guter Anfang.“

Mehr Informationen unter www.uimc.de/news

FAQ / Umgang mit dem EuGH-Urteil zum Drittlandtransfer

Auf der zweiten Seite diese Infobriefs weisen wir auf die ablaufende Umsetzungsfrist zum Neuabschluss von Standardverträgen hin. Doch: Was ist ansonsten bei einem Drittlandtransfer zu beachten? Hierzu haben wir im Rahmen unserer E-Learning-Plattform „eCollege“ im FAQ-Bereich eine Praxishilfe zum Umgang mit dem Urteil zusammengestellt: **www.uimcollege.de** > FAQ und Wissenswertes (geschützter Bereich).

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

Unternehmen sehen Datenschutz als lästige Nebenpflicht

Die nordrhein-westfälische Landesdatenschutzbeauftragte Bettina Gayk hat kürzlich den 27. Landesdatenschutzbericht präsentiert und der Öffentlichkeit vorgestellt. Der Bericht bezieht sich auf das Jahr 2021 und liefert interessante Erkenntnisse zur Entwicklung des Datenschutzes. Unter anderem wurden bei Unternehmen der Energiewirtschaft – gerade in Zeiten von Gas- und Energiekrise von herausragender Bedeutung – Querschnittsprüfungen zu den Regeln und Vorschriften der DSGVO vorgenommen. Die ausgewählten Unternehmen wurden zufällig ermittelt. „Die Datenschutzprüfung der Unternehmen zeigt, dass die Datenschutzbehörden inzwischen nicht mehr nur auf Eingaben und Beschwerden reagieren, sondern pro aktiv arbeiten, um die Normen der DSGVO durchzusetzen“, erklärt UIMC-Geschäftsführer Dr. Jörn Voßbein mit Blick auf die Ergebnisse des Landesdatenschutzberichts 2021.

Wie wurde die Prüfung durchgeführt? Die Datenschutzprüfung fand bei den zufällig ausgewählten Energieversorgungsunternehmen in Nordrhein-Westfalen (NRW) mit Hilfe eines Fragebogens, bestehend aus unterschiedlichen Fragegruppen, statt. Unter anderem ging es um die Umsetzung der DSGVO im Betrieb, die Struktur und Organisation innerhalb des Unternehmens beim Datenschutz, aber auch konkret um die Beschwerde-Bearbeitung, sowie die Durchführung von Sensibilisierungsmaßnahmen und der Erfüllung der Rechenschaftspflicht.

Zu welchen Ergebnissen führte die Prüfung? In Kurzform: Wenig Licht, aber viel Schatten. Konkret und ganz offen schreibt die NRW-Landesdatenschutzbeauftragte in ihrem Bericht: „Datenschutz wird von den Unternehmen eher als lästige Nebenpflicht angesehen. Einige Unternehmen waren nicht in der Lage, die wesentlichen unternehmensspezifischen Datenverarbeitungen transparent darzustellen.“ Allerdings fiel das Ergebnis bei einigen wenigen Unternehmen der Energie- und Versorgungsbranche auch erfreulich aus. Sie werden als „Datenschutzleuchttürme“ bezeichnet. Hieraus hat die Landesdatenschutzbehörde sechs „Best Practices“ gebildet, die sogar von der Behörde als „bereichsübergreifend“ klassifiziert werden.

Die sechs „Best Practice“ finden Sie
unter www.uimc.de/news

Reminder: Abschluss von Standardvertragsklauseln bis zum 27.12.2022

Seit Sommer 2021 gibt es neue Standardvertragsklauseln, die einen Datentransfer in Drittländer außerhalb der EU ermöglichen. Hintergrund war ein Urteil des EuGH, welches die alten Standards für unzulässig erklärt hat. Zur Umsetzung der neuen Verträge gab die EU-Kommission eine Übergangsfrist von 18 Monaten, die am 27. Dezember 2022 abläuft.

Die UIMC rät: Prüfen Sie, ob alle Standardverträge für den Drittlandtransfer auf dem aktuellen Stand sind.

Mehr Infos unter www.uimc.de/drittlandtransfer

Download der Verträge unter
www.online-formular-center.eu (geschützter Bereich)

Aktuelles im Online-Formular-Center

Um über Neuerungen zeitnah informiert zu werden, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.

www.uimcollege.de