



Inhaltsverzeichnis ++ Tipps für mehr Sicherheit ++ Umgang mit Data Privacy Framework ++ Freikarten für Cybersecurity Day ++ Podcast: UIMC zu Gast bei CYBR Dates ++ Spruch des Monats ++ **Inhaltsverzeichnis**



Gefahren durch Admins, Dienstreisen und Home Office?!

Cybersecurity: Wertvolle Tipps für mehr Sicherheit

Ob Funke Medien Gruppe, die Universität Duisburg-Essen oder die Stadt Witten: Hackerangriffe auf Unternehmen und Institutionen sorgen immer wieder für Schlagzeilen und Beeinträchtigungen des Geschäftsbetriebs. Die IT-Sicherheit wird für Unternehmen immer wichtiger, was auch die Zahlen des Digitalverbandes Bitkom belegen: In Deutschland wird für IT-Sicherheit so viel Geld ausgegeben wie noch nie zuvor. Die Ausgaben im Bereich IT-Sicherheit dürften sich im vergangenen Jahr auf rund 7,8 Milliarden Euro belaufen, ein Wachstum von 13 Prozent gegenüber dem Vorjahr. „Cyberangriffe können alle treffen. Die Frage ist nicht, ob eine Attacke passiert, sondern wann. Die Belegschaft ist ein beliebtes Einfallstor für Cyberkriminelle“, weiß der erfahrene Experte für Informationssicherheit, Dr. Jörn Voßbein. Umso wichtiger sind wertvolle Tipps und Hinweise vom UIMC-Expertenteam.

Die UIMC geht in einer fünfteiligen Reihe auf verschiedene Themen der Informationssicherheit ein. Im dritten Teil geht es um das mobile Arbeiten und die besonderen Anforderungen bei Admin-Usern.

In der Regel ist das Unternehmensnetz besser geschützt als der Mitarbeitende zu Hause. Vorsicht sollten Unternehmen auch rund um das Home Office walten lassen. „Das mobile Arbeiten, ob von zu Hause oder von unterwegs, wird geschätzt. Es birgt aber auch Risiken“, so Dr. Jörn Voßbein. Risikobehaftet ist grundsätzlich die Verbindung von IT-Anwendungen mit dem Internet. Die Risiken in Stichworten: Datenexfiltration, Identitätsdiebstahl, Missbrauch des Unternehmensinformationssystems oder Ransomware dringt ein und verschlüsselt ganze Systeme.

Einige Handlungsempfehlungen sind hierbei leicht umzusetzen:

- » Daten sollten immer verschlüsselt gespeichert werden,
- » Geräte sollten auf Geschäftsreisen mit Blickschutzfiltern ausgerüstet sein,
- » Passwörter sollten nicht gespeichert werden,
- » der Zugriff auf das Unternehmensnetzwerk sollte ausschließlich über VPN (Virtual Private Network) erfolgen;
- » eine lokale Firewall sollte ebenfalls auf jedem Rechner aktiviert sein.

Aber: Das Vorhandensein einer lokalen Firewall reicht bei weitem nicht aus. Vielmehr empfiehlt die UIMC hier, in eine „menschliche“ Firewall zu investieren und Security Awareness-Schulungen zur Mitarbeitersensibilisierung zu etablieren (mehr dazu in Teil 4 der UIMC-Serie). Auch Administratoren sollten entsprechend geschult und sensibilisiert werden, auch oder weil sie viel stärker in der digitalen Welt leben.

Ferner gibt es auch bei Administratoren klare und konkrete Hinweise für einen besseren Schutz vor den Gefahren:

- » Jede Mitarbeiterin und jeder Mitarbeiter besitzt ein eigenes Nutzerkonto.
- » Admin-Konten bleiben nur den Verantwortlichen vorbehalten und sind ansonsten für niemanden zugänglich.
- » Auch Administrationsrechte sind soweit wie möglich zu beschränken und zu differenzieren.
- » Besonders zu beherzigen ist der folgende Tipp: Kein Surfen im Internet von einem Administratorenkonto!
- » Unverzüglicher Entzug von Administrationsrechten bei Verlassen des Unternehmens.

Fortsetzung unter www.uimc.de



Freikarten: Cybersecurity Day, 20.10.2023

Am 20. Oktober 2023 findet der Kongress rund um IT-Security, Compliance und Datenschutz traditionell in Saarbrücken statt. Die UIMC zeigt mit Ihrem Vortrag „Digitalisierung nutzen, aber sicher!“ pragmatische Wege für mehr Sicherheit im Mittelstand auf. **Und das Beste ist: Wir haben Freikarten.** Melden Sie sich einfach unter communication@uimc.de. Aber Beeilung: First order, first serve.



Datenschutz



Informationssicherheit



Organisation / Strategie

UIMC | pragmatisch.erfahren.verständlich.

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



Sorgt das DPF für Klarheit?

Ist das Data Privacy Framework (DPF) die Lösung bei der Datenübertragung in die USA und die dortige Datenverarbeitung? Oder nur eine weitere Etappe auf der Datenschutzbahn zwischen EU, USA und dem Europäischen Gerichtshof (EuGH)?

Am 10. Juli traf die EU-Kommission eine Entscheidung zur Datenübertragung in die USA und fasste einen Angemessenheitsbeschluss. Diese bedeutet konkret, dass der Datentransfer in die USA als unbedenklich

eingestuft wird, wenn die US-Unternehmen eine gültige DPF-(Selbst-) Zertifizierung besitzen. „Die EU zeigt mit diesem Beschluss, dass sie Geschäftshemmnisse reduzieren will. Wenn ich an die Schrems-Urteile denke, die die früheren Regelungen zur Datenübermittlung pulverisiert haben, bleibt die Frage, wie nachhaltig dieser Beschluss ist.“, erklärt UIMC-Datenschutzexperte Dr. Heiko Haaz.

Was Unternehmen sollten, um sich **nachhaltig** datenschutzkonform aufzustellen, zeigen wir unter

www.uimc.de/news

UIMC zu Gast bei CYBR Dates

CYBR DATES ist das etwas andere Podcastformat des Netzwerks CYBR 360 - die Initiative für digitale Sicherheit im Saarland. Im Podcast treffen sich immer zwei Teilnehmer:innen aus Wirtschaft, Wissenschaft oder Politik aus dem Saarland zu einem Blind Date. Das bedeutet, sie wissen vor der Aufnahme nicht, mit wem sie sich heute unterhalten werden. Eines bleibt allerdings immer gleich: das Thema! Fokus der Diskussion ist immer die digitale Sicherheit.

In der ersten Folge sind Tim Hoffmann (Berater der UIMC für Datenschutz und Informationssicherheit) und Roman Tabachnikov (Co-Founder der bitahoy GmbH) zu Gast. Gemeinsam sprechen sie über die Grundsätze der Cybersicherheit, ihren Blickwinkel darauf und dem Einfluss von Künstlicher Intelligenz auf die digitale Sicherheit.



Hören Sie gerne bei SPOTIFY rein: www.uimc.de/cybr-dates



Spruch des Monats: Oktober

1961 veröffentlichte der Kommunikationschef der BASF, Georg-Volkmar Graf Zedtwitz-Arnim, ein Buch mit dem Titel „Tu Gutes und rede darüber. Public Relations für die Wirtschaft“.

Was diese Redewendung bedeutet, was es übertragen auf Ihr Unternehmen sowie auf den Datenschutz und die Informationssicherheit heißt und welches „Goodie“ wir diesen Monat für Sie vorbereitet haben, finden Sie wie immer unter

www.uimc.de/kalendersprueche



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

Mehr Informationen, Hinweise & Tipps finden Sie hier: <https://www.UIMC.de/communication>

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

