

Cybersecurity Konferenz 2024

Unternehmenssicherheit im Fokus: Prävention, Detektion
und Reaktion auf Cyberangriffe

11. Juli 2024 | Atos Information Technology GmbH | Fürth

BVMW Cybersecurity Konferenz 2024

Liebe BVMW-Mitglieder, liebe mittelständische Unternehmerinnen und Unternehmer,

Unternehmen aus Mittelstand und KMU sind täglich vielfältigen Sicherheitsrisiken ausgesetzt. Eine besondere Herausforderung sind Cyberangriffe. Malware, Advanced Persistent Threats (APT) und DDoS-Angriffe (Distributed Denial of Service), die schnelle Entwicklung der KI und andere Bedrohungen stellen Unternehmen vor ungeahnte Probleme.

Der BVMW in der Metropolregion Nürnberg unterstützt daher kleine und mittlere Unternehmen aller Branchen sowie Start-ups bei der Prävention, Detektion und Reaktion auf Cyberangriffe.

Mit unserer Cybersecurity Konferenz 2024 am 11. Juli 2024 wollen wir dazu beitragen, das Cybersicherheitsniveau bei Mittelstand und KMU in unserer Region zu erhöhen und die Unternehmen so resilienter zu machen. Kleine und große Mittelständler erhalten wertvolle Informationen, Impulse und Handlungsempfehlungen. Und es bleibt auch viel Raum für Austausch und Vernetzung.

Ich freue mich, wenn Sie dabei sind wünsche Ihnen wertvolle Impulse!

Edgar Jehnes

BVMW in der Metropolregion Nürnberg



Programm



- **Grußwort**
Christian Ernst | Geschäftsführer Atos Information Technology GmbH



- **IT-Sicherheit ist Chefsache - Gewappnet sein für einen Cyberangriff**
Siegfried Plommer | Managing Director beyond SSL
Frederik Heller | Sales Manager beyond SSL



- **NIS-2 – Anforderungen für eine höhere Cybersecurity**
Regina Stoiber | Geschäftsführerin Datenbeschützerin GmbH



- **Cybersecurity Frameworks - Wie Unternehmen Informationen, Know-how und Intellectual Property schützen**
Uwe Rühl | Geschäftsführer Resilience Operations Center



- **Cyber Recovery – Business Continuity nach einem Ransomware-Angriff**
Dr. Christian Hillebrand | Atos Information Technology GmbH



- **IT-Sicherheitsrecht: Was Unternehmen unbedingt beachten müssen**
Tomas Krause | Fachanwalt für IT-Recht

Impulse

IT-Sicherheit ist Chefsache - Gewappnet sein für einen Cyberangriff

Siegfried Plommer | Managing Director beyond SSL

Frederik Heller | Sales Manager beyond SSL

Siegfried Plommer und Frederik Heller führen Sie ein in die Welt der digitalen Sicherheit für KMUs. Freuen Sie sich auf fundierte Einblicke in umsetzbare Sicherheitslösungen für den Mittelstand, die darauf abzielen, Ihr Unternehmen effektiv zu schützen und zu stärken, während Sie gleichzeitig Kosten und Komplexität minimieren. Die beiden Experten zeigen Ihnen verbesserte Methoden, um Ihre Sicherheit zu optimieren. Es erwarten Sie praxisnahe Beispiele und innovative Perspektiven, die Sie dazu inspirieren werden, Ihre IT-Sicherheitsstrategie neu zu überdenken.

Die beyond SSL GmbH wurde 2015 gegründet und arbeitet weltweit mit über 1700 Kunden, von KMU bis zu Weltkonzernen, sowie zahlreichen Partnern zusammen. Ziel des Unternehmens ist es, Kunden vor unbefugtem Zugriff auf ihre Netzwerke zu schützen und Datenlecks zu verhindern.

NIS-2 – Anforderungen für eine höhere Cybersecurity

Regina Stoiber | Geschäftsführerin Datenbeschützerin GmbH

Die Unsicherheit bei vielen Unternehmen ist groß: Sind wir von NIS-2 betroffen? Wenn ja, was bedeutet das für uns? Welche Vorgaben müssen wir bis wann umsetzen? Regina Stoiber gibt einen Überblick über die von der NIS-2 Richtlinie betroffenen Kategorien von Organisationen. Zudem zeigt sie auf, wie sich die Anforderungen der EU-Richtlinie im deutschen NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz wiederfinden, wie Sie sich darauf

vorbereiten können und welche Maßnahmen Sie ergreifen sollten. Sie erhalten einen praxisorientierten Leitfaden, um bestmöglich für die Anforderungen gewappnet zu sein, sowie einen Fahrplan für Ihre nächsten Schritte.

Regina Stoiber tauchte bereits 2007 in die Materie Informationssicherheit ein. Als Gründerin und Geschäftsführerin der Datenbeschützerin® GmbH unterstützt sie gemeinsam mit ihrem Expertenteam KMUs und große Unternehmen dabei, ihre Informationssicherheit und den Datenschutz aktuell zu halten.

Cyber Recovery – Business Continuity nach einem Ransomware-Angriff

Dr. Christian Hillebrand | Atos Information Technology GmbH

In der von Cyberbedrohungen geprägten Welt ist Cyber Recovery entscheidend für die schnelle Wiederherstellung nach Angriffen. Es nutzt fortschrittliche Technologien wie Isolation, Immutable Storage und KI-Analyse, die in traditionellen Backups oftmals nicht eingesetzt werden. Isolation schützt Backups in einer separaten Umgebung, Immutable Storage verhindert Datenmanipulation, und KI beschleunigt die Erkennung von Bedrohungen und die Wiederherstellungsprozesse. Diese Maßnahmen minimieren Ausfallzeiten und sichern die Betriebskontinuität, indem sie eine rasche Wiederaufnahme des Normalbetriebs nach einem Cyberangriff ermöglichen.

Dr. Christian Hillebrand, Doktor in Informatik von der TU München, ist mit einer Erfahrung von über 20 Jahren in den Bereichen Softwareentwicklung, Sicherheit und Cloud-Technologien, insbesondere für kleine und mittelständische Unternehmen tätig.

Impulse

Cybersecurity Frameworks - Wie Unternehmen Informationen, Know-how und Intellectual Property schützen

Uwe Rühl | Geschäftsführer Resilience Operations Center

Informationssicherheit, Cybersecurity, Datenschutz, Know-how-Schutz - viele Schlagwörter, hinter denen sich meist komplexe Themen verstecken. In der Praxis stellt sich die Frage: wie umsetzen? Und wie mit den Überschneidungen zwischen den Aufgabenfeldern umgehen? Dazu kommen „neue“ Themen und rechtliche Anforderungen auf EU-Ebene zu Digitalen Märkten, Data Governance oder KI. Wie Unternehmen bewährte Standards und Ansätze nutzen und kombinieren können, beleuchtet dieser Kurzvortrag. Alle, die ein Informationssicherheitsmanagementsystem betreiben oder aufbauen, werden von diesem Vortrag profitieren und praktische Tipps für ihr Managementsystem erhalten.

Uwe Rühl ist Gründer des Resilience Operations Centers mit Sitz in Nürnberg. Mittelständische Unternehmen überlebens- und zukunftsfähig machen, ist der Auftrag. Um das zu erreichen, müssen Unternehmen für Resilienz konfiguriert sein und ihre Lage im Blick behalten.

IT-Sicherheitsrecht: Was Unternehmen unbedingt beachten müssen

Tomas Krause | Fachanwalt für IT-Recht

In seinem Impuls beschäftigt sich Tomas Krause mit den derzeit geltenden gesetzlichen Verpflichtungen im Bereich der IT-Sicherheit, vor allem im Bereich Datenschutz. Er arbeitet die Unterschiede zwischen Datenschutz und Datensicherheit heraus, gibt Hinweise zur Implementierung geeigneter technischer und organisatorische Maßnahmen (TOM) sowie

Empfehlungen zum richtigen Umgang mit Datenpannen und Cybervorfällen. Weiterhin beleuchtet er die rechtlichen Rahmenbedingungen des Einsatzes von KI im Unternehmen. Zum Schluss wirft er noch einen Blick auf den Cyber Resilience Act (CRA), mit dem die Cybersicherheit von Produkten mit digitalen Elementen verbessert werden soll.

Tomas Krause ist Rechtsanwalt und Fachanwalt für IT-Recht mit langjähriger Berufserfahrung. Er berät in seiner volldigitalisierten Kanzlei vor allem kleine und mittelständische Unternehmen zu allen Fragen des Wirtschaftsrechts. Des Weiteren steht er seinen Mandanten als externer Datenschutzbeauftragter (DSB-TÜV) zur Verfügung.

Im Foyer:

Eye-Tracker

Warum fallen immer wieder Menschen auf Phishing-E-mails rein? Unsere Augenbewegungen verraten viel über Vorgänge in unserem Gehirn. Mit Eye-Tracking können wir diese Vorgänge sichtbar machen und herausfinden, wie Nutzer mit Phishingmails interagieren und wie wir uns besser vor Phishingattacken schützen können. Am interaktiven Infostand des **EU-Projekts Digitale Innovation Ostbayern** stellen wir die Technologie vor: Sie können selbst die mobilen Tobii Pro Fusion Eye-Tracker ausprobieren und Ihr Wissen über Phishingmails testen. Nebenbei erfahren Sie auch, wie Sie Eye-Tracking bei sich im Unternehmen sinnvoll einsetzen können.

Termin | Ort |Anmeldung

Termin

Donnerstag, 11. Juli 2024

16:00 – ca. 19:30 Uhr, Einlass ab 15:15 Uhr

Ort

Atos Information Technology GmbH, Wehlauer Straße 3, 90766 Fürth

Anfahrt und Parken

Kostenfreie Parkmöglichkeiten direkt am Eingang zu Atos sowie einige Meter weiter Richtung Flamme Möbel auf der linken Seite (markierte Atos-Parkplätze).

ÖPNV: U1 Haltestelle Klinikum, Busse 126/171/172 Haltestelle Klinikum West

Teilnahmegebühr

Die Teilnahme ist kostenfrei.

Teilnehmerzahl

Die Teilnehmerzahl ist begrenzt. Bitte melden Sie sich daher möglichst frühzeitig an.

Anmeldung

Bitte ausschließlich verbindliche Anmeldungen über unser [Online-Formular](#).

Informationen

Alle aktuellen Informationen, das Anmeldeformular sowie die Teilnahmebedingungen finden Sie auf der Veranstaltungsseite www.bvmw.de/nuernberg.

Kontakt

Der Mittelstand.BVMW

BVMW in der Metropolregion Nürnberg

Edgar Jehnes

Schopenhauerstraße 21

90409 Nürnberg

Telefon: +49 911 287 90 46

Mobil: +49 174 94 89 133

E-Mail: edgar.jehnes@bvmw.de

Web: www.bvmw.de/nuernberg

LinkedIn: <https://www.linkedin.com/in/edgarjehnes/>

Der BVMW unterstützt u.a. folgende Projekte

Netzwerkpartner der

CYBERSicher

Transferstelle.
Cybersicherheit.
Mittelstand.



MIT Sicherheit
ausbilden