Anmeldung

Bitte melden Sie sich über folgenden Link an:
https://events.ihk-siegen.de/termine/525/
Die Teilnahme ist kostenlos.

Agenda

Sascha Skudelny
17:30 KontiKat
IT Sicherheit & Cyber-Crime

Roland Schwalm
18:00 bits+bytes it-solutions
Cyber-Attacken und Sensibilisierung von Mitarbeitern

Dr. Jürgen Hartung
18:30 Oppenhoff & Partner
Rechtliche Perspektive der KMU-Sicherheit

19:00 Möglichkeit zur Diskussion im Nachgang

Nächste UKUS: 03. September 2020

Wichtige Information für die Teilnehmer: Wenn Sie nach der UKUS-Veranstaltung eine weitere Kontaktaufnahme wünschen, so können Sie an info.smi@uni-siegen.de eine E-Mail schreiben.

Organisation

Industrie- und Handelskammer Siegen
Referat 22 Hochschule/Wirtschaft
Marco Butz
Koblenzer Straße 121
57072 Siegen
Telefon: 0271 / 3302-2 22
E-Mail: marco.butz@siegen.ihk.de
Internet: www.ihk-siegen.de

SMI - Siegener Mittelstandsinstitut
Sekretariat
Silke Rosenthal
Unteres Schloß 3
57072 Siegen
Telefon: 0271 / 740-39 95
E-Mail: info.smi@uni-siegen.de
Internet: www.uni-siegen.de/smi

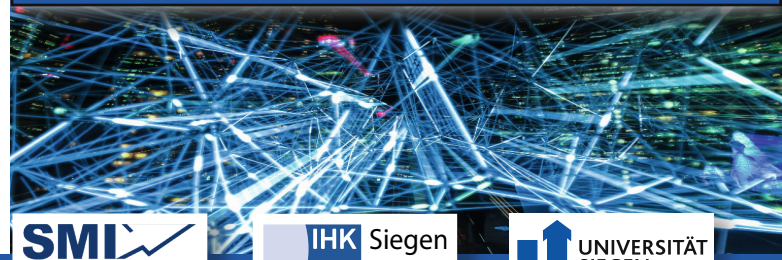
Mittelstand 4.0 - Kompetenzzentrum Siegen
Dr.Martin Stein
Kohlbettstr. 15
57072 Siegen
Telefon 0271 / 740-4763
E-Mail: info@kompetenzzentrum-siegen.digital
Internet: www.kompetenzzentrum-siegen.digital

Mittelstand 4.0 Kompetenzzentrum Siegen
Mittelstand-Digital
Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
EUROPÄISCHE UNION Investition in unsere Zukunft Europäischer Fonds für regionale Entwicklung
EFRE.NRW Investitionen in Wachstum und Beschäftigung

UKUS
UNTERNEHMERKOLLOQUIUM DER UNIVERSITÄT SIEGEN & DER INDUSTRIE- UND HANDELSKAMMER SIEGEN

Sicherheit in KMU

Donnerstag, 04. Juni 2020,
ab 17:30 Uhr
Webinar



SMI SIEGENER MITTELSTANDSINSTITUT
IHK Siegen
UNIVERSITÄT SIEGEN

T-SICHERHEITS- UND RISIKOMANAGEMENT MODELLE

Die zunehmende Digitalisierung und Vernetzung führen dazu, dass IT-Sicherheit immer wichtiger wird. Besonders wichtig ist dies auch für kleine und mittlere Unternehmen (KMU), denn sie spielen in der deutschen und weltweiten Wirtschaft eine beachtliche Rolle. Auch wenn sie meist sehr innovativ sind, sind die zum Schutz des Unternehmens notwendigen Prozesse eines IT-Sicherheitsmanagements oftmals weder vorhanden noch standardisiert. Dieses häufig auftretende Problem hat seine Wurzeln darin, dass kleine und mittlere Unternehmen im Gegensatz zu großen Unternehmen oftmals nur über eingeschränkte Ressourcen hierfür verfügen. Gängige IT-Sicherheits- und Risikomanagementmodelle sind überwiegend für größere Unternehmen konzipiert.

Während bei den technischen Maßnahmen zumeist eine zufriedenstellende Basis erreicht ist, auf dessen Grundlage das IT-Sicherheitsniveau künftig weiter erhöht werden sollte, besteht jedoch im Hinblick auf die personellen und organisatorischen Maßnahmen ein deutlich höherer Handlungsbedarf. Diese werden oftmals als ausreichend empfunden, obwohl sie häufig gar nicht oder nur ansatzweise vorhanden sind.

Referenten

Sascha Skudelny: Im Zeitalter zunehmender Digitalisierung und Vernetzung nimmt das Thema IT-Sicherheit und Cyberkriminalität einen stetig wachsenden Stellenwert ein. Kleine und mittlere Unternehmen (KMU) machen auch im Jahr 2020 den größten Anteil der deutschen Wirtschaft aus, verfügen jedoch im Gegensatz zu großen Unternehmen meist über nur eingeschränkte Ressourcen für IT-Sicherheit. Oft werden daher selbst essentielle Geschäftsprozesse trotz hohem Gefährdungspotenzial und Anfälligkeitsrisiko nur unzureichend geschützt. Erkenntnisse über die eigene IT-Sicherheitslage können daher wesentlich dazu beitragen, eigene Handlungsoptionen zu entwickeln und die IT-Sicherheit auch in Ihrem Unternehmen wirksam zu erhöhen.

Roland Schwalm: Das Internet ist nur eine der Gefahren, wodurch Datenmissbrauch entstehen kann. Der Umgang mit vertraulichen Informationen innerhalb eines Unternehmens lässt sehr oft zu wünschen übrig. Es passiert oft, dass auf Geschäftsreisen in Zug oder Flugzeug vertrauliche Informationen bearbeitet werden - jeder könnte mitlesen!
Wussten Sie, dass 70% der IT-Sicherheitsvorfälle durch Menschen verursacht werden? Teils durch böse Absicht - meist jedoch durch Fahrlässigkeit und Unkenntnis. Wir glauben, dass uns eine Antivirensoftware oder eine Firewall ausreichend vor Cyberkriminalität schützt. Ein Trugschluss, wie man es mittlerweile fast jeden Tag in der Presse liest. Daten kommen abhanden – Computersysteme werden als Botnetzwerk missbraucht. Menschen geben freiwillig und gutgläubig Informationen an Dritte weiter. Lernen Sie in dem Vortrag welche Möglichkeiten Unternehmen und Behörden haben, um ihre Mitarbeiter fit für diese Bedrohungen zu machen.

Dr. Jürgen Hartung: Die rechtliche Verantwortung für die Vermeidung von Risiken liegt bei der Geschäftsführung, die durch eine Verletzung dieser Pflicht auch in eine persönliche Haftung geraten kann. Bei Cyberrisiken gibt es verschiedene Rechtsvorschriften zu beachten. Zunächst der Datenschutz; mit der Datenschutzgrundverordnung sind Unternehmen verpflichtet, ein Datenschutz Management System einzuführen. Dann unterliegen bestimmte Unternehmen im Bereich kritischer Infrastrukturen besonderen Sorgfalts- und Meldepflichten nach dem BSI-Gesetz. Schließlich hat die EU aber mit der Cybercrime Richtlinie auch einen strafrechtlichen Schutz für Unternehmen gegen Angriffe eingeführt.

Insbesondere in Bezug auf die sichere Archivierung und Verschlüsselungsmaßnahmen zum Schutz von Unternehmensdaten sind Vernachlässigungen nachweisbar. Mit der Digitalisierung steigt vor allem die Kriminalitätsentwicklung im Internet kontinuierlich. Anhand von verschiedenen Möglichkeiten wie beispielsweise die Infizierungen des Computers durch Trojaner, Viren, Ransomware oder Phishing (Identitätsdiebstahl) gelingt es Cyberkriminellen, die Daten von Unternehmen zu sammeln und gewinnbringend zu verkaufen.

Unternehmen müssen hier aktiv werden, Vorkehrungen treffen, um sich zu schützen, und Pläne ausarbeiten, wie zu agieren ist, wenn das Worst-Case-Szenario eintritt.

In unserer Veranstaltung werden Experten aus verschiedenen Bereichen erzählen, auf was KMU beispielsweise bei Maschinen und dessen Vernetzung, bei ihren Mitarbeitern und im rechtlichen Bereich achten müssen.

T SICHERHEIT & CYBER-CRIME