Abstracts

1. Vortrag – IT-Sicherheit ist Chefsache **14:40 Uhr**

Vortragende: Patrick Drögeler und Simon Koch

Sicherheit ist nicht alles, aber ohne Sicherheit ist alles nichts. IT-Sicherheit hat die Aufgabe, die Vertraulichkeit, Verfügbarkeit und Integrität von Daten und Informationen im Unternehmen sicherzustellen und dadurch wirtschaftliche Schäden durch technisches und menschliches Versagen, Spionage, Sabotage und Betrug zu verhindern. Neben dem Verlust von Daten und einem monetären Schaden kann das Unternehmensimage durch schwerwiegende Angriffe ebenfalls in Mitleidenschaft gezogen werden – ein Fauxpas, den sich kein Unternehmen heutzutage leisten kann. Doch welches Maß an Aufmerksamkeit kommt dem Thema der Sicherheit in der IT eigentlich zugute? Ist diese Thematik bereits auf Managementebene angekommen?

Dieser Vortrag stellt die Bedeutung der IT-Sicherheit heraus und zeigt, welchen unternehmerischen Stellenwert diese Disziplin im Zuge der fortschreitenden Digitalisierung branchenübergreifend einnimmt. Neben der Darstellung der allgemeinen Aufgaben und Eigenschaften der IT-Sicherheit, werden verschiedene Eingliederungsmöglichkeiten der IT-Sicherheit im Unternehmen sowie aktuelle Gefährdungen und Bedrohungen anhand von Beispielen vorgestellt. Es handelt sich dabei jedoch nicht ausschließlich um Gefahren, die von außen auf ein Unternehmen gerichtet sind, sondern ebenfalls um Gefahrenquellen, die innerhalb eines Unternehmens schlummern.

2. Vortrag – Social Engineering – Hacking the Human Operating System **15:10 Uhr**

Vortragende: Florian Drüen und Thomas Abeln

Viele Daten mit denen heutzutage gearbeitet wird, bewegen sich auf einem sehr hohen sicherheitskritischen Level. Dabei reicht es jedoch nicht mehr aus, einzig und allein die bestehende IT-Landschaft vor Angriffen von außen zu schützen. Vielmehr lauert Gefahrenpotenzial innerhalb des Unternehmens.

Kommunikationsmittel wie Email, Whatsapp oder der Auftritt auf sozialen Netzen wie Facebook bringen vermehrt den Menschen als Schwachstelle hervor. Dies führt dazu, dass die Verantwortung bei Unternehmen liegt, die einzelnen Mitarbeiter zu informieren und gegen cyberkriminelle Angriffe zu schulen. Bei Verfahren wie „Baiting“ oder „Phishing“ wird speziell nicht die technische Infrastruktur ausgenutzt, sondern der Mensch und sein soziales Handeln attackiert.

Dieser Vortrag stellt das sogenannte Social Engineering und seine Methoden genauer vor. Außerdem wird anhand von Beispielen verdeutlicht, wie sich diese Vorgehensweise in der Praxis zeigen kann. Zudem gibt der Vortrag einen Einblick darin, wie es einem Unternehmen oder auch einer Einzelperson möglich ist, sich gegen diese Maßnahmen erfolgreich zu wehren.

3. Vortrag – BYOD im betrieblichen Umfeld 15:40 Uhr

Vortragende: Lars Gausling und Jonas Fährmann

Mobile Endgeräte sind aus dem Alltag nicht mehr weg zu denken. Nutzer greifen heutzutage zu jeder Zeit und von nahezu jedem Ort auf Unternehmensdaten und -informationen zu. Einige Unternehmen profitieren bereits von dieser Art der Daten- und Informationsbeschaffung und -verarbeitung.

Bring Your Own Device (BYOD) ist ein anhaltender und weiter ansteigender Trend, der es den Mitarbeitern erlaubt, eigene, mit der Nutzung vertraute mobile Endgeräte dafür zu nutzen, um Zugriff auf unternehmensbezogenen Daten zu erhalten.

Dieser Vortrag setzt sich mit dem zukunftsorientierten, aber dennoch sehr kritischen Thema auseinander. Ergänzt durch einen kurzen Einblick in rechtliche und soziale Aspekte wie Datenschutz und Mitarbeiter-Sensibilisierung, liegt der Schwerpunkt auf Themen der IT-Sicherheit.

Es soll sich der Fragen angenommen werden, welche Bedrohungen durch BYOD entstehen, welche Risiken daraus resultieren und welche Lösungsansätze dem Unternehmen zur Verfügung stehen, um derartige Probleme gegenwärtig und zukünftig zu vermeiden.

4. Vortrag – DDoS – vor dem Hintergrund von IoT und Industrie 4.0 16:30 Uhr

Vortragende: Jan-Oliver Brandt und Jan Lange

Das Thema Distributed Denial of Service (DDoS) ist in der nahen Vergangenheit vermehrt in den Medien aufgetaucht. Dabei standen stets aktuelle Themen wie das Internet der Dinge (IoT), Industrie 4.0 sowie die damit verbundenen Sicherheitsrisiken im Vordergrund.

Durch die Flut neuer netzwerkfähiger Geräte, welche oft unzureichend gesichert sind, nehmen die Gefahren für Unternehmen durch DDoS-Attacken bisher ungeahnte Ausmaße an. Jene stellen somit erhebliche Risiken dar, welche nicht ignoriert werden dürfen.

Ein Denial of Service Angriff beschreibt das Vorgehen einen Web-Service, wie beispielsweise einen Web-Shop, durch eine hohe Zahl eingehender Anfragen zu überlasten, um so den Service unbenutzbar zu machen. U. a. durch die Verteilung der gesendeten Anfragen mithilfe einer Vielzahl von Geräten (Distributed) lassen sich Angriffe noch verstärken. Das technische Wissen, welches für einen DDoS-Angriff benötigt wird, ist heute minimal. Die entsprechenden Kapazitäten lassen sich problemlos anmieten.

Die Gefahr für Unternehmen besteht dabei nicht nur durch Angriffe auf die eigenen Web-Services oder Anlagen. Durch die Kompromittierung eigener Geräte und Sensoren kann die eigene Infrastruktur schnell zum Teil des Angriffsnetzwerkes werden.

In diesem Zusammenhang müssen Schutzziele von zwei unterschiedlichen Ansatzpunkten betrachtet werden. Auf der einen Seite stehen der Schutz von (potenziellen) Opfern durch Technologien großer Anbieter (bspw. Cloudfare oder Google) sowie der strategisch richtige Aufbau der eigenen Infrastruktur.

Auf der anderen Seite steht der Schutz netzwerkfähiger Geräte. Im Fokus stehen hier bestehende Sicherheitslücken sowie eine Sensibilisierung bzw. ein Appell an die Nutzer und Hersteller.

5. Vortrag – Big Data und Datenschutz **17:00 Uhr**

Vortragender: Romaric Nzomwita

In den letzten Jahren hat das Interesse an Big Data im IT Bereich deutlich zugenommen. Das liegt daran, dass die Nutzung von Big Data durch deren Auswertung neue Möglichkeiten eröffnet, um große Datenmengen zu verarbeiten und neue Informationen zu gewinnen. Diese Technologie eröffnet Unternehmen neue Anwendungsgebiete, die durch herkömmliche Technologien unergründet geblieben wären. Das ist eine Entwicklung, die sowohl neue Herausforderungen als auch neue Gefahren mit sich bringen kann, zu denen auch das Datenschutzproblem gehört.

Das Ziel des Vortrages "Big Data und Datenschutz" ist, die Besonderheit des Datenschutzes von Big Data hervorzuheben. Dabei wird der Lebenszyklus von Big Data beschrieben und die Gefahr für den Datenschutz bei einzelnen Phasen der Big Data-Analysen aufgezeigt, was anhand von Beispielen verdeutlicht wird. Zum Schluss geht der Vortrag auf die Lösungsmöglichkeiten ein, wobei wirtschaftliche, rechtliche und technische Aspekte einbezogen werden, um eine Verbesserung der Sicherheitslage zu erzielen.

6. Vortrag – Vernetzt auf vier Rädern **17:30 Uhr**

Vortragende: Damian Denzel und Arthur Hofmann

Daten sind das neue Öl, welches von den heutigen Automobilen nicht nur zur Fortbewegung benötigt, sondern von diesen auch selbst in zunehmendem Maße generiert wird. Schon heute sind viele Automobile als fahrende Computer zu identifizieren, die mittels einer Vielzahl an Sensoren und Steuergeräten Daten zum Zustand des Fahrzeugs, zum Fahrverhalten der Fahrer, aber auch zum Umfeld erzeugen, zwischenspeichern und kommunizieren können. Dadurch können einerseits ganz neue Geschäftsfelder eröffnet und auf der anderen Seite die Sicherheit auf den Straßen erhöht werden. Informationen zum Fahrverhalten können beispielsweise für Versicherungsunternehmen zur Bemessung der Versicherungspolice von Interesse sein. Sicherheitsrelevante Themen sind bereits heute in einigen Navigationssystemen und Fahrzeugmodellen vorhanden, welche Informationen zu Staus, Unfällen oder Glatteis, direkt über Cloud-Services untereinander austauschen (Car2Car). Bei allen Vorteilen, die dadurch ermöglicht werden, sollten aber die Risiken hinsichtlich der IT-Sicherheit und des Datenschutzes der erfassten und kommunizierten Daten nicht vernachlässigt werden.