Cyber Security Status Quo und Herausforderungen
Agenda itWatch GmbH - Inhouse Event 13. und 14. Mai 2022

Impulsvorträge und Paneldiskussionen

Prof. Udo Helmbrecht teilt seine Einschätzung zur aktuellen Lage aus Sicht seiner Erfahrungen als BSI Präsident und ENISA Präsident und seiner Tätigkeiten an der Universität der Bundeswehr.

Albrecht Broemme spricht über seine Erfahrungen bei Katastrophenbewältigung, Nachschub und Unterstützung als THW Präsident und in seiner Rolle als Vorstandsvorsitzender des Zukunftsforums Öffentliche Sicherheit

Frau Bubendorfer-Licht, Mitglied des Deutschen Bundestages, Obfrau im Ausschuss für Inneres und Heimat, Religionspolitische Sprecherin der FDP-Bundestagsfraktion, Mitglied im Landesvorstand der FDP Bayern, spricht zu uns über Ihre Einschätzung der aktuellen Lage und der weiteren Entwicklungen

Prof. Dr. Ingo J. Timm, international ausgewiesener KI-Forscher und Wirtschaftsinformatiker mit Forschungsschwerpunkt auf Theorie, Methoden und Anwendungen der (Verteilten) Künstlichen Intelligenz und der Simulation, spricht über autonome Softwaresysteme, Intelligente Assistenzsysteme, kognitive Entscheidungsmodelle, soziale Interaktion autonomer Systeme und (Sozial-) Simulation im Fokus. Seine aktuelle Forschung beinhaltet bspw. Informationsmanagement und kognitive Sozialsimulation für das kommunale Krisenmanagement auch in der COVID-19-Pandemie.

Klaus-Peter Treche General a.D. kennt die digitale Entwicklung der Streitkräfte in Deutschland, Europa und der NATO aus seiner aktiven Zeit und seinen verschiedenen Funktionen wie der Führung der AFCEA Chapter Bonn und Brüssel.

Herr Andreas v. Büren, Geschäftsführer des BDSV – Bundesverband der deutschen Sicherheits- und Verteidigungsindustrie, diskutiert mit einem politischen Sprecher aus dem Bundestag die industrielle und politische Sicht zum Thema der aktuellen EU Taxonomie, wonach Unternehmen, die zu einem größeren Teil Umsatz als militärische Zulieferer – z.B. mit Cyber Security Produkten – erzielen, von Krediten und der Finanzwirtschaft ausgeschlossen werden sollen.

Frau Barbara Hofmann, Vice President Global Strategic Operations Government SAMSUNG, stellt die Gedanken zu der Zukunft der mobilen Cyber Security der Firma Samsung vor. Dieser Vortrag ist in englischer Sprache.

Jürgen Storbeck Direktor Europol a.D. berichtet über die aktuelle Sicherheitsstruktur in Europa auf Grundlage seiner Tätigkeiten und des Grünbuchs sowie aktueller nationaler und internationaler Erkenntnisse.

Frau **Prof. Dr. Angela Sasse**, Inhaberin des Lehrstuhls für Human-Centred Security am Horst-Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum, gilt als Pionierin der Usable Security ist Forscherin an der Nordrhein-Westfälischen Akademie der Wissenschaften und der Künste und spricht zum Thema Security Awareness. In ihrem Vortrag erfahren sie die neuesten Erkenntnisse zu Security Awareness und benutzerzentrierter Cyber Security.

Herr Arno Fiedler, Nimbus Technologieberatung, berichtet zum Thema eIDAS und dem Stand der Technik der sicheren Authentisierung eIDAS (electronic IDentification, Authentication and trust Services), in Deutschland auch IVT (elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen) bezeichnet die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Sein Vortrag ist eingebettet in weitere Statements zu dem Thema Vertrauensketten und der Frage, was Vertrauen ist und wie es hergestellt wird, ergänzt durch einen Workshop mit praktischen Inhalten.

Michael Bartsch , Gründer und Geschäftsführer der Deutor Cyber Security Solutions GmbH, ist Krisenmanager, Berater und Trainer für Cybersicherheit. Seit vielen Jahren berät er Staaten und Unternehmen in den Bereichen der Risikovorsorge und der Umsetzung technischer- und organisatorischer- (Cyber-) Sicherheitsmaßnahmen während und nach einem Cyberangriff. Er wird uns mit Berichten aus verschiedenen Krisenmanagement Szenarien begleiten. Warum ist Krisenmanagement und Krisenkommunikation bei einem Cyberangriff wichtig? Welche Schäden können bei falschem Verhalten entstehen? Do´s und Dont´s. Außerdem bekommen Sie Tipps für ein erfolgreiches Management während eines Cyberangriffs.

Frau Dr. Stefanie Frey, Trainerin für Cybersicherheit, Geschäftsführerin der Deutor Cyber Security Solutions, Buchautorin. Frau Dr. Frey ist auf die Entwicklung von Strategien und Lösungen gegen kriminelle Handlungen spezialisiert, wobei sie eng mit Strafverfolgungsbehörden und anderen relevanten Gremien zusammenarbeitet. Als Militärhistorikerin beobachtet Stefanie Frey seit Jahren die sicherheitspolitischen Entwicklungen in den Bereichen Öffentliche Sicherheit, Verteidigung und insbesondere im Bereich der Cybersicherheit. Sie hat mehrere Bücher und Publikationen zu Cybersicherheit, dem Kalten Krieg und dem Zweiten Weltkrieg veröffentlicht und wird uns einen orientierten Beitrag zur Ukrainekrise geben.

… und es sind weitere Speaker angefragt.

Themenblöcke

Die Themenblöcke bestehen jeweils aus verschiedenen Impulsvorträgen und anschließenden Diskussionen in separierten Räumen mit Workshopcharakter. Ein im Thema erfahrener Moderator führt durch den jeweiligen Themenblock.

Sicherheitsanforderungen an Liefer- und Informationsketten – Status Quo, Herausforderungen und Lösungen

Moderation/Wrap up durch Oberstleutnant Franz Lantenhammer

Frau v. d. Leyen wies bereits 2017 darauf hin, dass die milliardenschweren Geräte der Bundeswehr zu Luft Land und See ihre Wirkfähigkeit nur entwickeln können, wenn die IT funktionsfähig ist. Zum Schutz der Funktionsfähigkeit müssen Maßnahmen aus der Cyber Security zum Einsatz kommen. Trotzdem könnten in einzelnen zugelieferten Bauteilen Schwachstellen (z.B. wie bei Log4j) oder sogar absichtliche Hintertüren verbaut sein.

Dieser Themenblock ist für alle Herstellungsprozesse mit längeren Lieferketten, in welchen digitale Elemente für ein End-Produkt angereichert werden.

Einzelne Themenblöcke sind aber für berechtigte Gruppen abgegrenzt:

_ Cyber Security für die militärische Lieferkette bei der Herstellung von dual Use oder Produkten mit rein militärischer Verwendung / Militärische Lieferkette / Resilienz

_ Digitale Souveränität

_ Resiliente Kommunikation – auch zwischen den verbauten digitalen Elementen

Sexualisierte Gewalt gegen Kinder verhindern – Das Potenzial digitaler Technologien für den Kinderschutz nutzen!

Sexualisierte Gewalt gegen Kinder nimmt stetig zu. Laut polizeilicher Kriminalstatistik ist die Zahl angezeigter Missbrauchsfälle 2020 gegenüber dem Vorjahr um knapp sieben Prozent gestiegen. Den stärksten Zuwachs (53 Prozent) verzeichnete die Herstellung und Verbreitung von Missbrauchsdarstellungen. Die Statistik umfasst jedoch nur die der Polizei bekannt gewordenen Delikte. Die Dunkelziffer wird höher eingeschätzt.

Herr von Heyden, Wissenschaftlicher Mitarbeiter der Charité – Universitätsmedizin Berlin wir einen Vortrag zum Thema „Sexualisierte Gewalt gegen Kinder verhindern – Das Potenzial digitaler Technologien für den Kinderschutz nutzen“ halten. Herr von Heyden arbeitet eng mit Prof. Dr. Dr. Klaus M. Beier, Direktor des Instituts für Sexualwissenschaft und Sexualmedizin an der Charité und auch im Therapie Netzwerk „Kein Täter werden“, zusammen. Das Projekt bietet pädophilen Menschen therapeutische Hilfe unter Schweigepflicht.

Herr Joachim Schneider, Polizeidirektor Landeskriminalamt Baden-Württemberg /Leiter Referat ProPK wird uns zum Thema polizeiliche Prävention berichten. Der Schutz vor Straftaten und die präventive Abwehr von Gefahren stellen eine gemeinsame Aufgabe der Polizeien der Länder und des Bundes dar. Ziel des ProPK ist es, die Bevölkerung, aber auch Multiplikatoren, Medien und andere Präventionsträger über Erscheinungsformen der Kriminalität und Möglichkeiten zu deren Verhinderung aufzuklären sowie die örtlichen Polizeidienststellen in ihrer Präventionsarbeit zu unterstützen.

Herr Mathias Bölle, Leitung der Abteilung „Cyber Crime und Digitale Spuren“ im Landeskriminalamt (LKA) Baden-Württemberg. Mathias Bölle ist ehemaliger leitender Verfassungsschutz-Mitarbeiter und stieg als Kripochef und Kommandoführer einer Spezialeinheit auf. Heute führt er 130 Spezialisten im Landeskriminalamt in Stuttgart, die gegen Kriminalität im Netz kämpfen. Grundsätzlich kann jedes Unternehmen Opfer einer Cyberattacke werden. Wie hoch die Bedrohungslage ist, welchen Schutz es gibt und wie man im Ernstfall reagieren sollte, erläutert Matthias Bölle in einem spannenden Vortrag.

Besondere Herausforderungen für Verschlusssache Umgebungen – insbesondere auch Netzübergänge in Forschungsnetze (VS-NfD)

Hinweis: einzelne Teile der Veranstaltung können nur für Zugehörige zu besonderen Berufsgruppen angeboten werden, um in diesen Gruppen eine offene Kommunikation zu ermöglichen.

Krisenmanagement

Warum ist Krisenmanagement und Krisenkommunikation bei einem Cyberangriff wichtig? Welche Schäden können bei falschem Verhalten entstehen? Wir sprechen über Do´s und Dont´s. Außerdem bekommen Sie Tipps für vorbereitende Maßnahmen, ein erfolgreiches Management während eines Cyberangriffs und das Aufräumen danach.

Technologieaustausch zwischen Kunden und mit unseren Technologiepartnern in einem Format „User & Partner Group“

Für Kunden der itWatch wird es eine USER GROUP Umfrage geben. Hier können Sie am Freitag während der Veranstaltung Ihr Voting abgeben, welche Themen Sie besonders interessieren, und wir gehen in einem Workshop am Samstag gerne auf diese Wünsche und Anfragen ein.

… und es sind weitere Themenblöcke angefragt.