OTS0091 5 WI 0772 MST0002 CI Di, 07.Nov 2017
Sicherheit/Kriminalität/EU/IT/Notfälle

KSÖ: Sicherheit im Netz als Nagelprobe im Kampf gegen ausufernde Kriminalität

Helmut Leopold, AIT; Erwin Hameseder, KSÖ

Credit: AIT / Johannes Zinner
Fotograf: Johannes Zinner

KSÖ-Cybersecurity-Planspiel - Praxistest für EU-Richtlinie

Credit: AIT / Johannes Zinner
Fotograf: AIT / Johannes Zinner

v.l.n.r. Spanner, Linhard, Hammeseder, Kardeis, Kaponig, Leopold, Ledinger

Credit: AIT / Johannes Zinner
Fotograf: AIT / Johannes Zinner

Utl.: KSÖ-Cybersecurity-Planspiel - Praxistest für EU-Richtlinie. =

Wien (OTS) - Bereits zum vierten Mal veranstaltete das Kuratorium Sicheres Österreich (KSÖ) von 6. bis 7. November ein Cybersecurity-Planspiel. Dabei wurde einmal mehr die Fitness Österreichs im Kampf gegen Cyberattacken, Spionage und Onlinebetrug einer Nagelprobe unterzogen. Gemeinsam mit dem Bundesministerium für Inneres (BMI) und dem AIT Austrian Institute of Technology probten rund 200 heimische IT-Sicherheitsexpertinnen und IT-Sicherheitsexperten aus 32 namhaften Organisation, bestehend aus Behörden, Wirtschaft und Wissenschaft den Ernstfall und stellten die

aktuelle EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) und die Datenschutzgrundverordnung interaktiv auf die Probe.

Zwtl.: Staat und Wirtschaft proben technische Cybersecurity Zusammenarbeit

Nach den organisatorischen und rechtlichen Aspekten der letzten drei Jahre stand beim diesjährigen Planspiel der technische Charakter im Mittelpunkt. So wurden in den letzten beiden Tagen die Teilnehmerinnen und Teilnehmer mit Angriffsszenarien auf Betreiber kritischer Infrastrukturen konfrontiert. Besonderes Augenmerk galt dem Zusammenspiel zwischen Staat (BMI, BMLVS, BKA, BMeiA) und Wirtschaft sowie den interorganisatorischen Bindegliedern (CERT.at, GovCERT und erstmals Austrian Energy CERT). „Das KSÖ will dabei zeigen, wie praxisfit sich die Cybersecurity-Zusammenarbeit hinsichtlich der NIS-Richtlinie erweist“, betont KSÖ-Präsident Mag. Erwin Hameseder. „Nur in der praxisnahen Simulation können Schwachstellen herausgearbeitet und in Zukunft auch beseitigt werden. Ein funktionierender Austausch zwischen Wirtschaft, Wissenschaft und Behörden kann eine weitreichende digitale Sicherheit gewährleisten.“

Das AIT gestaltete als Spielleiter die technische Komponente des Planspiels mittels ihres modernen Cyber Security Trainingszentrums, der AIT „Cyber Range“. „Das Ausmaß und die Professionalität von Cyber-Bedrohungen haben sich in den letzten Jahren wesentlich verändert. Diese massive Entwicklung stellt die Industrie und die Gesellschaft vor neue Herausforderungen. Es braucht daher ein umfassendes Bewusstsein aller Stakeholder, um eine gemeinsame sichere, globale Infrastruktur für unsere digitale Gesellschaft zu bauen und unsere Privatsphäre umfassend zu schützen. In diesem Kontext hat das AIT eine besondere IT-Trainingsplattform aufgebaut, um Cyber Security Übungen für Unternehmen anbieten zu können.“ so Helmut Leopold, Head of Center for Digital Safety & Security, AIT (www.ait.ac.at/cyberrange/).

Zwtl.: Das Szenario: Terrorbedrohung während EU-Ratspräsidentschaft

Das Rahmenszenario orientierte sich an einer fiktiven Bedrohung während der bevorstehenden EU-Ratspräsidentschaft Österreichs und den Brexit-Verhandlungen. Annahmefall: Drohungen terroristischer Gruppen gegen Betreiber kritischer Infrastrukturen in Österreich um politische Ziele zu erreichen. Dabei wurde darauf geachtet, dass nicht nur spezielle IT Fachleute, sondern auch klassische Anwender

von IT Systemen insofern eingebunden werden, sodass die gestellten Aufgaben ohne besondere Vorkenntnisse zu bewerkstelligen waren und dennoch ein maximaler Lerneffekt geboten wurde.

Der erste Tag (6. November) zielte auf die Schulung und Übung von aktuellen Cyberangriffen, -techniken und -lösungen anhand eines praxisnahen Beispiels von modernen digitalen industriellen Steuerungssystemen wie z.B. in der Energieversorgung ab. Gruppengrößen von etwa 3 Personen (10 Teams) und die Betreuung durch Expertinnen und Experten mit weitreichender Erfahrung im Cybersecurity Kontext gewährleisten das rasche Erlernen, Erkennen und Analysieren von Cyber-Angriffen. Zielgruppe des ersten Tages waren vor allem technische Expertinnen und Experten (Security Spezialisten, CERT-Mitarbeiter) sowie interessierte Manager und Behördenvertreterinnen und -vertreter.

Der zweite Tag (7. November) knüpfte an die Tradition der vorherigen Planspiele an und behandelte Kommunikationswege und Prozesse zwischen allen Beteiligten. Das Szenario beinhaltete im Kern Interaktionselemente zwischen den Akteurinnen und Akteuren (d.h. kritische Infrastrukturbetreiber, CERT.at und Austrian Energy CERT, Behörden) und technische Aufgaben anhand von Beispielen aus der Energieversorgung. Die Akteurinnen und Akteure analysierten im Zuge des Tages, welche organisationsinternen Maßnahmen möglich und welche Inhalte auszutauschen und zu berichten sind, um die Schadensreichweite diverser Störfälle (als Aufgaben in unterschiedlichen Schwierigkeitsgraden) so gering wie möglich zu halten. Im Fokus standen folglich auch das gegenseitige Verstehen der unterschiedlichen Perspektiven und Handlungsdimensionen von Unternehmen, Behörden und CERTs.
Zielgruppe dieses Tages waren die technischen Expertinnen und Experten des ersten Tages plus das deren Management bzw. die Führungsebene. An diesem Tag gab es auch für externe Beobachterinnen und beobachter die Möglichkeit das Planspielgeschehen und ergänzende Vorträge zu verfolgen.

Zwtl.: Kuratorium Sicheres Österreich (KSÖ)

Das KSÖ ist ein gemeinnütziger, unabhängiger Verein, der es sich als nationale Vernetzungs- und Informationsplattform für Themen der inneren Sicherheit zum Ziel gesetzt hat, Österreich sicherer zu machen. Das Kuratorium fungiert als Schnittstelle zwischen Wirtschaft, Forschung, Behörden und Gesellschaft. Gemeinsam mit dem

Bundesministerium für Inneres (BMI) führt das KSÖ seit 2011 eine Initiative für Cybersecurity. Es trägt als Kompetenznetzwerk dazu bei, die relevanten Akteure zusammenzuführen, um gemeinsam an diesem Ziel zu arbeiten. Unter dem Motto „Potenziale heben & Risiken minimieren“ hat sich das KSÖ für 2018 im Rahmen des neuen „Sicherheitsforum Digitale Wirtschaft Österreich“ - einer Vernetzungsplattform zwischen Wirtschaft, Wissenschaft und Behörden - die sichere Digitalisierung der österreichischen Wirtschaft als neue Herausforderung zum Ziel gesetzt. Mehr dazu auf unserer Homepage unter https://kuratorium-sicheres-oesterreich.at

Bild(er) zu dieser Aussendung finden Sie im AOM / Originalbild-Service sowie im OTS-Bildarchiv unter http://bild.ots.at

~

Rückfragehinweis:
KSÖ - Kuratorium Sicheres Österreich
Dr. Alexander Janda
Mobil: +43 (0)664 55 66 800
E-Mail: janda@kuratorium-sicheres-oesterreich.at

~

OTS0091 2017-11-07/11:10

071110 Nov 17

Link zur Aussendung:
https://www.ots.at/presseaussendung/OTS_20171107_OTS0091