Pressemitteilung

Wien, 22.09.2021

KSÖ UND AIT VERANSTALTEN TRAINING FÜR DIE ABWEHR VON CYBERANGRIFFEN

Sicherheitsakteure aus der DACH-Region trainieren den Ernstfall im Rahmen einer hybriden Cybersicherheitsübung

Das Kuratorium Sicheres Österreich (KSÖ) veranstaltete am 20. und 21. September 2021 gemeinsam mit dem AIT Austrian Institute of Technology erstmals ein länderübergreifendes Cybersicherheits-DACH-Planspiel, in dem in hybrider Form die Abwehr von Cyberangriffen realitätsnahe durchgespielt wurde. Dieses Training rund um technische und kommunikative Prozesse lieferte wertvolle Erfahrungen für den Ernstfall.

Egal ob es sich um Unternehmen, Behörden oder andere Organisationen handelt: Der Prozess der Digitalisierung und Vernetzung eröffnet zwar viele neue Möglichkeiten, doch gleichzeitig bietet er auch immer mehr neuen Bedrohungen, etwa Datendiebstahl, Hackerangriffen oder Erpressungen mittels Ransomware ein Einfallstor. Cyberbedrohungen zählen mittlerweile zu den größten Geschäftsrisiken überhaupt. Ein Ausfall von IT-Systemen kostet nicht nur viel Zeit, Geld, Reputation und Nerven, sondern kann auch zum Produktionsstillstand von Fabriken oder zum Ausfall von Infrastrukturen führen, die Gesellschaft destabilisieren oder sogar lebensbedrohliche Konsequenzen haben. Das Kuratorium Sicheres Österreich (KSÖ) sieht es als eine seiner Aufgaben, die Cybersicherheit gemeinsam mit den Partnern aus Wirtschaft, Verwaltung, Wissenschaft und Politik zu stärken.

Grenzüberschreitende Herausforderung

Viele Unternehmen und Organisationen bereiten sich auf solche Angriffe vor, indem sie Pläne und Prozesse entwerfen, wie zu reagieren ist, wenn kritische Situationen eintreten. Um den Umgang mit den Bedrohungen auch realitätsnah trainieren zu können, veranstaltete das KSÖ gemeinsam mit dem AIT Austrian Institute of Technology auch in diesem Jahr ein „KSÖ Cybersicherheits-DACH-Planspiel“ – eine Cybersicherheits-Übung, die Ländergrenzen überwindet und den DACH-Raum (Deutschland, Österreich und Schweiz) im gemeinsamen Kampf gegen grenzüberschreitende Herausforderungen einbindet. Der Fokus des Planspiels lag auf cyber-physischen und begleitenden Informationsmaßnahmen.

Acht Teams kämpften gegen Angriff

Im Rahmen der Übung kamen am 20. und 21. September 2021 im Raiffeisen Forum in Wien sowie – online zugeschaltet – in der Schweiz und Deutschland die unterschiedlichsten technischen und strategischen Spieler:innen, Beobachter:innen und Multiplikator:innen zusammen, um sich einer hoch aktuellen Gemengelage zu stellen. Die Übung, die vom Bundesministerium für Inneres (BMI)

gefördert und von der Raiffeisen Holding NÖ-Wien, UNIQA Österreich Versicherungen AG sowie dem Enterprise Training Center (ETC) als Sponsoren unterstützt wurde, erfuhr erneut – wie schon bei der letzten gemeinsamen Übung im Jahr 2017 – einen sehr hohen Zuspruch von Seiten der Teilnehmenden. Getreu dem Motto „*train as you fight*“ bewährten sich die acht spielenden Teams in Wien gemeinsam mit einer nationalen Koordinierungsstruktur für die Cybersicherheit (IKDOK/OpKoord) als auch den Partner:innen vom schweizerischen nationalen Zentrum für Cybersicherheit (NCSC) und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem herausfordernden Szenario.

Training in einer der modernsten IT-Simulationsumgebungen, der „AIT Cyber Range“

Dieses Bedrohungsszenario wurde von Expertinnen und Experten des AIT in der „AIT Cyber Range“ umgesetzt. Dabei handelt es sich um eine flexible IT-Simulationsumgebung für Cybersicherheitsübungen. In der „AIT Cyber Range“ werden IT-Infrastrukturen und Kommunikationsprozesse realitätsnah simuliert, somit können die Erkennung und Abwehr unterschiedlichster Angriffe trainiert werden. Dadurch wird es möglich, die Abwehr von Cyberangriffen und Extremsituationen sogar in kritischen Infrastrukturen zu trainieren, bei denen „echte“ Tests in der realen Welt aus Sicherheits- oder Kostengründen nicht möglich sind. So können, Strukturen und Prozesse analysiert und Fehlerquellen eruiert werden. Die Wechselwirkungen von Auswirkungen und Handlungen sowie Reaktionen können somit sicher und transparent nachvollzogen werden.

Oft erkennt man erst beim Durchspielen einer Situation, welche Fähigkeiten einer Organisation zur Abwehr eines Cyberangriffs noch fehlen. Die „AIT Cyber Range“ wird beispielsweise auch von der Internationalen Atomenergiebehörde IAEA als Trainingsumgebung eingesetzt, um eine hohe Cybersicherheit in kritischen Teilen von Atomkraftwerken sicherzustellen: In Österreich werden in ihr auch Großübungen für den Fall einer Cyberkrise durchgeführt – analog zu klassischen Großübungen im Krisen- und Katastrophenmanagement.

Übungsszenario: Angriff auf ein Pharmaunternehmen

Das Übungsszenario beim diesjährigen KSÖ Cybersicherheits-DACH-Planspiel bestand darin, dass ein fiktiver internationaler Pharmakonzern, der eine Schlüsselfunktion in der Bekämpfung einer Pandemie innehat, von einer Gruppe von Akteuren mittels cyber- und informationsfokussierter Attacken angegriffen wird, um die geschäftlichen Tätigkeiten des Unternehmens zu stören.

Die teilnehmenden Akteure agierten u.a. als technisch-operative Mitarbeitende des Pharmakonzerns sowie als strategische Spielerinnen und Spieler und hatten zwei Aufgabenbereiche zu erfüllen: Zum einen übten sie auf Basis der „AIT Cyber Range“ die Erkennung und Abwehr der besagten Angriffe. Zum anderen trainierten sie die Kommunikation und Koordination mit den jeweils involvierten und zuständigen Behörden und Ansprechpartnerinnen bzw. Ansprechpartnern in diesem Szenario.
Darüber hinaus konnten Entscheidungsträger:innen sowie Multiplikatorinnen und Multiplikatoren begleitend in einem Beobachter:innenprogramm (auch online) am Planspiel teilnehmen.

Zitate:

Mag. Erwin Hameseder, Präsident KSÖ
„An beiden Tagen haben Cybersicherheitsexpert:innen aus Österreich, der Schweiz (NCSC) und Deutschland (BSI) erfolgreich an einer Übung – dem KSÖ Cybersicherheits-DACH-Planspiel 2021 – teilgenommen. Diese Veranstaltung, die sowohl vor Ort in Wien als auch im digitalen Raum stattfand, wurde möglich, weil die richtigen Partner:innen zusammengekommen sind.
Ich möchte den nationalen und internationalen Partner:innen und Organisationen, den beteiligten Unternehmen und auch den zahlreichen Interessierten für ihre Teilnahme und Unterstützung meinen Dank ausdrücken. Aber auch beim AIT und dem KSÖ-Team möchte ich mich für die Umsetzung des Planspieles bedanken. Nur wer in der Lage ist – im Rahmen solcher Übungen gemeinsam zu trainieren – kann auch im Ernstfall bestehen, das wurde hier eindrucksvoll gezeigt."

Dr. Helmut Leopold, **Head of Center for Digital Safety & Security, AIT:**
„Durch die enge Kooperation zwischen Unternehmen, Wissenschaft und Behörden und dem Einsatz einer speziellen neuen Trainingsplattformen für Cybersicherheit – der AIT Cyber Range – konnten wir eine der modernsten Übungen umsetzen, um effektivst einerseits Weiterbildungs- und Trainingseffekte bei den Expertinnen und Experten zu erzielen, aber auch um wertvolle Erfahrungen für die Erhöhung des Cybersicherheitsschutzes für den Ernstfall zu sammeln. Damit konnten wir uns erneut als internationales Vorzeigebeispiel positionieren und einen wichtigen Beitrag für die Sicherstellung der digitalen Souveränität Europas leisten."

Mag. Dr. Franz Ruf, MA, Generaldirektor für die öffentliche Sicherheit, des Bundesministeriums für Inneres, besuchte persönlich das KSÖ Cybersicherheits-DACH-Planspiel 2021 und zeigte sich von dem kooperativen und effektiven Verlauf der Übung positiv beeindruckt: „Solche Übungen helfen uns dabei Prozesse im Rahmen der Abwehr von Cybervorfällen auch länderübergreifend gemeinsam abzustimmen und die Kommunikation für den Ernstfall kooperativ beherrschen zu können."

Weitere Informationen über die AIT Cyber Range: https://cyberrange.at/

Pressekontakt:

Mag. (FH) Michael W. Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)664 235 17 47
michael.muerling@ait.ac.at I www.ait.ac.at

Dr. Alexander Janda
KSÖ – Kuratorium Sicheres Österreich
T +43 (0)676 556 68 00
janda@kuratorium-sicheres-oesterreich.at | www.kuratorium-sicheres-oesterreich.at/