Cybersecurity-Planspiel: Helmut Leopold (AIT), Guido Jestädt (BAWAG Group), Andreas Reichhardt (BMF), Markus Popolari (BMI), Alexander Janda (KSÖ)

Cyber-Angriffe abwehren

Österreichische und internationale Unternehmen sowie Behörden trainierten den Ernstfall eines hybriden Angriffs auf den Bankensektor in einer der modernsten digitalen Simulationsumgebungen.

Das *Kompetenzzentrum Sicheres Österreich (KSÖ)* veranstaltete am 6. und 7. November 2024 in Wien gemeinsam mit dem *AIT Austrian Institute of Technology* und der *BAWAG Group* das bereits siebente Cyber-Planspiel. Die auf modernster IT-Infrastruktur stattfindende Cyber-Sicherheitsübung zielte darauf ab, dass Vertreterinnen und Vertreter österreichischer, aber auch internationaler Unternehmen und Behörden den Ernstfall anhand eines fiktiven hybriden Angriffs auf Staat, Wirtschaft und Gesellschaft trainierten. „Der Austausch zwischen der öffentlichen Verwaltung und der Wirtschaft ist gerade beim Thema Cyber-Sicherheit von entscheidender Bedeutung“, sagte Markus Popolari, Leiter der Direktion Digitale Services (DDS) im Bundesministerium für Inneres.

Beim Cyber-Sicherheitstraining übernahmen etwa 100 Teilnehmerinnen und Teilnehmer verschiedene Rollen von Verantwortungsträgern fiktiver Unternehmen wie „Optiteq“ oder „OeBank“. Ihre Aufgabe war es, Angriffe krimineller Organisationen zu erkennen und mit der Einleitung von Gegenmaßnahmen abzuwehren. Das Spektrum der sicherheitsgefährdenden Aktivitäten an den IT-Strukturen von Behörden, der kritischen Infrastruktur und Großkonzernen ist jedoch breit und es lauern auch Gefahren wie Desinformationskampagnen oder Diebstähle. Auch diese wurden durch den Einsatz der neuesten technischen Software beim Cyber-Sicherheitstraining berücksichtigt.

Das Ziel dieses Trainings war es, die Geschäftsaktivitäten der bedrohten Behörden und Betriebe sicherzustellen. „Bei solchen Planspielen gibt es ‚Table-Top-Exercises‘, das heißt, es liegt ein Zettel auf dem Tisch, auf dem steht, was passiert ist. Die Teilnehmerinnen und Teilnehmer müssen rasche Lösungen finden“, erklärte KSÖ-Generalsekretär Dr. Alexander Janda. Die bisherigen sechs Übungen hatten theoretischen Charakter, ohne auf technischer Ebene einzuschreiten. Partner für das siebente Planspiel war das *Austrian Institute Of Technology*, das die Übungsinfrastruktur zur Verfügung stellte. Daraus entstand ein Szenario mit einer technisch realistischen Infrastruktur, um das Planspiel spannend zu gestalten.

„Wir haben zwar die technische Umgebung, aber es geht bei der Übung nicht darum, dass allein die IT-Spezialisten eine Lösung finden, sondern es soll gezeigt werden, wie wichtig die Zusammenarbeit von Vertretern verschiedener Fachbereiche in einem Unternehmen ist und dass sie zur Problemlösung beiträgt“, bekräftigte Janda. Die bisherigen Planspiele brachten Erfahrungen, wie sich Informationsprozesse entwickeln, worauf Entscheidungen beruhen oder auf welche Weise Entscheidungsprozesse innerhalb von Unternehmen verteilt sind. Auch inner-

Foto: Katharina Schiffl

halb von Unternehmen braucht es eine bessere Vernetzung. „Es kann sein, dass in einem Unternehmen die betroffene Abteilung nicht über die Handlungsprozesse einer anderen wichtigen Abteilung informiert ist“, erläuterte der KSÖ-Generalsekretär. Natürlich ist es möglich, dass in bestimmten Branchen, wie Banken, Energieversorger oder den Versicherungen Ungewissheit herrscht, welche verwertbaren Informationen man von Kollegen in einem Krisenfall bekommt.

Kooperation mit den Behörden. Ein wesentlicher Faktor ist die Kooperation mit Behörden, die im Fall eines Cyber-Angriffes und einer daraus resultierenden Krise entsprechende Maßnahmen setzen. Dazu kommen Vorschriften, die im Krisenfall berücksichtigt werden müssen, wie das NIS-1 (Netz- und Informationssicherheitsgesetz) und das NIS-2 Gesetz, das zwar seit 17. Oktober 2024 in der Europäischen Union gültig ist, aber in Österreich noch in nationales Recht umgesetzt werden muss. Bei dieser Übung werden die Meldeprozesse berücksichtigt, die gesetzlich vorgeschrieben sind. In den jeweiligen Bereichen, wie Banken, müssen eigene legislative Vorgaben berücksichtigt werden. Bei einem umfangreichen Cyber-Angriff wäre eine Vernetzung zwischen Behörden, Betrieben der kritischen Infrastruktur, dem Finanzwesen sowie großer Industriebetriebe notwendig.

Die Bekämpfung von Cyber-Angriffen bedingt nicht nur technische Kenntnisse, die auf dem neuesten Stand sein müssen, sondern auch andere Aspekte, wie psychologisches Wissen und analytische Fähigkeiten mit denen eine Informationsstruktur geschaffen werden kann.

Im Szenario gab es eine fiktive Bank, die in verschiedenen Regionen in Österreich Geschäftsstellen betreibt, sowie ein fiktives Industrieunternehmen, das ebenfalls in mehreren Regionen tätig ist. Die Bank wird angegriffen und daraufhin entsteht eine für die Bank dramatische Entwicklung, die Auswirkungen auf das Industrieunternehmen hat. Mit diesem Szenario wurden die Teilnehmerinnen und Teilnehmer konfrontiert. „Es ist ein klassisches Angreifer-Verteidiger-Spiel, eine Art Wettbewerb. Hier sind Vertreterinnen und Vertreter der Republik Österreich von Ministerien und Behörden versammelt, ebenso wie IT-Betreiber und Serviceanbieter, Repräsentanten der kritischen Infrastruktur sowie der Banken“, erklärte Dipl.-Ing. Helmut Leopold, der Leiter des Zentrums für digitale Sicherheit des *Austrian Institute of Technology (AIT)*. Es nahmen auch Mitarbeiterinnen und Mitarbeiter des Bundesministeriums für Inneres (NIS-Behörde) teil.

Bei dieser Simulation wurden die digitale Struktur und Aktionskreisläufe bestimmter Betriebe realistisch dargestellt. Für Planspiele dieser Art werden digitale Zwillinge echter Angriffs- und Abwehrszenarien entwickelt, die das Know-how und die darauf beruhenden Erfahrungen der Spielteilnehmerinnen und -teilnehmer erweitern sollen. „Bei dieser Übung wird viel Information zwischen Personen und Firmen ausgetauscht. Es ist wie eine Prüfung und die Beteiligten müssen sich fragen: Weiß ich etwas? Kann ich etwas? Es stellt sich auch die Frage, ob die Teilnehmenden bereit sind, ihren Mitspielern zu vermitteln, was sie nicht wissen“, sagte Helmut Leopold. *Michael Ellenbogen*