Bayern

Wichtige Schritte gegen Cybercrime

[14.11.2022] Die Cyberabwehr Bayern, in der die bayerischen Behörden mit Cyber-Sicherheitsaufgaben zusammenarbeiten, hat neue Räume bezogen. Zudem erschien der erste bayernweite Bericht zur Cyber-Sicherheit, der belegt, dass sich Cyber-Angreifer immer weiter professionalisieren.

Bayerns Innenminister Joachim Herrmann hat gemeinsam mit Finanzminister Albert Füracker und Justizminister Georg Eisenreich die neue Räumlichkeiten der Cyberabwehr Bayern (wir berichteten) sowie den Cyberlagebericht 2022 vorgestellt.
Die 2020 gegründete Cyberabwehr Bayern fungiert als behördeninterne Informations- und Kooperationsplattform für alle bayerischen Landesbehörden mit Cyber-Sicherheitsaufgaben und soll den engen und schnellen Austausch zwischen den staatlichen Akteuren im Bereich Cyber-Sicherheit garantieren. Beteiligte Behörden werden schnellstmöglich über relevante IT-Sicherheitsvorfälle informiert und können im Krisenfall rasch über erforderliche Maßnahmen entscheiden. Verbessert wird laut Ministeriumsangaben auch der Überblick über die Gefährdungslage im Cyber-Raum, denn die Informationen der bayerischen Behörden mit Cyber-Sicherheitsaufgaben werden zu einem bayernweiten Cyber-Lagebild gebündelt. Zudem ist die Cyberabwehr Bayern die zentrale Ansprechstelle für das Nationale Cyber-Abwehrzentrum (NCAZ).
Nun hat das Lagezentrum neue, „hochprofessionell ausgestattete“ Räume im Bayerischen Landesamt für Verfassungsschutz bezogen. Rund vier Millionen Euro hatte das Land für die neuen Räumlichkeiten der Cyberabwehr ausgegeben. Innenminister Hermann sprach von einer „guten Investition“. Das neue Lagezentrum sei ein Musterbeispiel für eine erfolgreiche ressortübergreifende Zusammenarbeit und angesichts der stetig zunehmenden Bedrohungen im Cyber-Raum wichtiger denn je.

Ransomware-Angriffe und Cyber-Sabotage auf dem Vormarsch

Der erste bayernweite Lagebericht vom Innen- und Finanzministerium zur Cyber-Sicherheit im Freistaat bestätigt diese Einschätzung. Die Angreifer nutzen fortwährend neue Angriffsstrategien und organisieren sich zum Teil hochprofessionell in der Anonymität des Darknets, so die Minister während der Vorstellung des Berichts. Ransomware sei mittlerweile zum größten Problem der Cyber-Kriminalität geworden, nicht zuletzt wegen der zunehmenden Verbreitung von Kryptowährungen wie etwa Bitcoin. Durch die Begleichung von Lösegeldforderungen in einer Kryptowährung können die Täter weitgehend anonym und ohne eigenes Risiko vollständig aus dem Ausland agieren. 2021 war in Bayern einen Anstieg von Krypto-Ransomware-Fällen von über 25 Prozent gegenüber dem Vorjahr zu verzeichnen, so Herrmann.
Aber auch Cyber-Angriffe durch so genannte APT-Gruppen (Advanced Persistent Threat, übersetzt: hochentwickelte beständige Bedrohung) auf Forschungseinrichtungen und Wirtschaftsunternehmen wurden vom Landesamt für Verfassungsschutz vermehrt registriert. Durch ausländische Nachrichtendienste gelenkt, seien diese Gruppierungen bestens ausgestattet und können Cyber-Spionage und Cyber-Sabotage entsprechend professionell betreiben.
Nach wie vor seien Software-Schwachstellen das Einfallstor für Cyber-Angriffe – auch, weil längst verfügbare Sicherheitsupdates zum Teil nicht eingespielt würden, wie Finanzminister Füracker berichtete. Er mahnte, die Bedrohungen ernst zu nehmen und IT-Sicherheit zur Chefsache zu machen.

(sib)

Stichwörter: IT-Sicherheit, Bayern, Cyber-Sicherheit