Pressemitteilungen

FÜRACKER: CYBER DEFENCE CENTER DES LSI SORGT FÜR IT-SICHERHEIT IM FREISTAAT! Kontinuierlich wachsende Bedrohungslage bei IT-Sicherheit // seit LSI-Gründung: stetiger Ausbau des ‚Lagezentrums' zum ‚Cyber Defence Center'

7. April 2025

„Das ‚Cyber Defence Center' im LSI sorgt als ‚ZentrumBayern für digitale Sicherheit' rund um die Uhr für IT-Sicherheit in der bayerischen Verwaltung, bei bayerischen Kommunen und im Bereich kritischer Infrastrukturen: Täglich werden hier rund 2,5 Milliarden Datensätze analysiert und aktiv Maßnahmen zur Abwehr von Cyberangriffen ergriffen. Der Fachkompetenz, den etablierten Abwehrmechanismen und dem beherzten Eingreifen des LSI verdanken wir, dass 2024 nur wenige konkrete IT-Sicherheits-Vorfälle verzeichnet wurden – und das trotz der hohen Anzahl von über 140.000 Benutzern im Bayerischen Behördennetz. Potenzielle Schäden wie beispielsweise ein Abgreifen oder eine Verschlüsselung von Daten wurden so aktiv und erfolgreich verhindert", freut sich Finanz- und Heimatminister Albert Füracker beim Pressetermin am Montag (7.4). im Landesamt für Sicherheit in der Informationstechnik (LSI).

„Im Freistaat haben wir früh erkannt, dass staatliche IT-Sicherheit vor dem Hintergrund der wachsenden Bedrohungslage eine entscheidende Rolle spielt: Bayern hat 2017 mit der Gründung unseres LSI als erstes Bundesland eine eigene Fachbehörde für IT-Sicherheit eingerichtet. Das bereits seit 2003 bestehende Bayern-CERT ging mit der Gründung des LSI als Keimzelle auf und wurde dort zu einem Lagezentrum. Es galt bereits zu dieser Zeit als wegweisend – gleichwohl es anfangs als eher reaktive Einheit startete. Das Lagezentrum hat sich seitdem nach und nach zu einem echten, proaktiven ‚Cyber Defence Center' weiterentwickelt", so Füracker weiter.
Das Cyber Defence Center (CDC) des LSI bündelt verschiedene interne Fachkompetenzen in einer Einheit und erkennt Angriffe frühzeitig mithilfe der vorhandenen Sicherheitsmechanismen. Das CDC bekämpft die Angriffe aktiv und analysiert sie anschließend IT-forensisch. Daraus werden wichtige Erkenntnisse gewonnen, die zur Verbesserung der Sicherheitsmechanismen genutzt werden. Darüber hinaus nutzt das CDC „Open Source Intelligence", also in öffentlichen und halböffentlichen Quellen verfügbare Informationen über geplante Angriffe, um auf zukünftige Ereignisse bestmöglich vorbereitet zu sein. Aber auch aktuelle Trends wie beispielsweise der Einsatz von Künstlicher Intelligenz oder langfristige Entwicklungen wie Quantencomputing werden berücksichtigt, um immer auf dem neuesten Stand zu sein und bestmöglichen Schutz zu bieten.

Das CDC verhindert monatlich rund 1,2 Milliarden potenziell schädliche Internetaufrufe. Im Jahr 2024 wurden von über 500 Millionen empfangenen E-Mails rund 390 Millionen als schädlich erkannt und noch vor der Zustellung automatisch blockiert, da sie als Spam oder Phishing identifiziert werden konnten.

Pressemitteilung auf der Seite des Herausgebers