Pressemitteilungen

Herrmann, Füracker und Eisenreich: Geschlossen für mehr Cybersicherheit – Konflikte als Brandbeschleuniger bei Verbreitung von Desinformation – Auch kleine Unternehmen und Behörden im Visier von Cyberkriminellen – Bayern weiterhin stark …

24. September 2024

„Die Bedrohungslage im Bereich Cybersicherheit hat sich weiter zugespitzt. Neben einer quantitativen und qualitativen Steigerung an Fällen in der Cyberkriminalität beobachten wir, dass bestehende und neue globale Konflikte als regelrechte ‚Brandbeschleuniger' im Bereich der gezielten Verbreitung von Desinformation wirken." Das geht nach den Worten des bayerischen **Innenministers Joachim Herrmann** aus dem Bericht zur Cybersicherheit in Bayern 2024 hervor, den **Herrmann** heute gemeinsam mit **Finanzminister Albert Füracker** veröffentlicht hat. „Es ist besorgniserregend, dass nicht mehr nur große Unternehmen, sondern vermehrt auch kleine und mittelständische Unternehmen sowie Behörden Opfer von Cyberangriffen werden", sind sich **Innenminister Herrmann**, **Finanzminister Füracker** und **Justizminister Georg Eisenreich** einig. Darüber hinaus ist auch Cyberspionage, insbesondere vor dem Hintergrund des russischen Angriffskriegs auf die Ukraine, weiterhin eine große Bedrohung.

„Schwachstellen in Software stellen nach wie vor eine gleichermaßen erhebliche wie unterschätzte Gefährdung dar. Die Vorfälle im letzten Jahr zeigen, dass die Angreifer weiterhin verstärkt auf nicht oder nicht schnell genug geschlossene Schwachstellen in zentralen und nach außen exponierten Softwarekomponenten abzielen", so **Finanzminister Füracker**. „Dabei nehmen Cyberkriminelle zunehmend auch Schwachstellen bei externen Dienstleistern in den Fokus, um dort, etwa bei Wartungsarbeiten, Zugang zu sensiblen Daten zu erlangen oder Systeme zu kompromittieren."

Das sogenannte Phishing, also Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als ein vertrauenswürdiger Kommunikationspartner auszugeben, stellt weiterhin eine der prominentesten Methoden im Bereich Cybercrime dar. Häufig bilden gezielte Kampagnen, sogenanntes Spear-Phishing, die Basis für Cyber- oder Internetkriminalität. „Mit den neuen Möglichkeiten generativer Künstlicher Intelligenz können sich Phishing-Kampagnen von den Angreifern noch einfacher planen und überzeugender vortragen lassen", betont **Innenminister Herrmann**. Generell spielt KI im Bereich Cybercrime eine immer größere Rolle und ermöglicht durch Deepfakes, also mittels KI generierter Bilder, Videos oder Sprachinhalte, neue Kriminalitätsphänomene. **Justizminister Eisenreich**: „Es wird immer leichter, vor allem Frauen und Mädchen mit Deepfake-Technologie in pornografische Fotos oder Videos einzubauen. Der Bundesrat hat auf Initiative Bayerns eine neue Vorschrift zum Persönlichkeitsschutz im Strafgesetzbuch beschlossen. Die Bundesregierung ist aufgefordert, auf die Herausforderungen durch Deepfakes zu reagieren und das Strafrecht anzupassen. Für die Untätigkeit der Bundesregierung habe ich kein Verständnis."

„Die anhaltend hohe Bedrohungslage im Cyberraum erfordert weiterhin ein starkes behördenübergreifendes Zusammenwirken. Bayern ist hier sehr gut aufgestellt und wir werden uns weiterhin gemeinsam für mehr Cybersicherheit einsetzen“, betonen **Herrmann**, **Füracker** und **Eisenreich** übereinstimmend mit Blick auf die bereits ergriffenen Maßnahmen.

So wurde beim Bayerischen Landeskriminalamt die Zentrale Ansprechstelle Cybercrime für Behörden, Unternehmen und Institutionen eingerichtet, die als kompetenter Ansprechpartner bereitsteht. Mit den im Jahr 2021 installierten Cybercrime ‚Quick-Reaction-Teams‘ gewährleistet die Polizei zudem eine Rund-um-die-Uhr-Verfügbarkeit qualifizierter Fachkräfte, die rasch auf die teilweise existenzbedrohenden Gefahren für die Unternehmen reagieren können. Das Cyber-Allianz-Zentrum Bayern beim Bayerischen Landesamt für Verfassungsschutz unterstützt als vertraulicher Ansprechpartner Unternehmen, Hochschulen, Forschungseinrichtungen und KRITIS beim Verdacht eines Cyberangriffs mit nachrichtendienstlichem Hintergrund. Mit dem Landesamt für Sicherheit in der Informationstechnik (LSI) hat Bayern 2017 als erstes Bundesland eine eigenständige IT-Sicherheitsbehörde gegründet. Als kompetente Institution berät und unterstützt das LSI die Kommunen und öffentliche Betreiber kritischer Infrastrukturen in allen IT-Sicherheitsfragen. So informiert der kostenfreie Warn- und Informationsdienst des LSI mit tagesaktuellen Warnmeldungen über die neuesten Gefährdungslagen und Risiken.

Darüber hinaus wurde 2015 die Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg gegründet, die in komplexen und schwerwiegenden Fällen von Cybercrime ermittelt und in den vergangenen Jahren personell ausgebaut und verstärkt wurde. Um die ZCB technisch noch besser für Ermittlungen auf dem Gebiet der Fake-Shops zu rüsten, wurde im August 2023 zudem eine Kooperation mit dem Austrian Institute of Technology geschlossen, um gemeinsam den dort entwickelten KI-gestützten ‚Fake-Shop-Detector‘ für den Einsatz im Rahmen der Strafverfolgung zu optimieren.

Den Bericht zur Cybersicherheit in Bayern 2024, der die gewonnenen Lageerkenntnisse zur Cyberabwehr sowie die ergriffenen behördenübergreifenden Maßnahmen im Detail darstellt, ist abrufbar unter

https://www.stmi.bayern.de/sus/cybersicherheit/ sowie https://www.stmfh.bayern.de/digitalisierung/it_sicherheit/.

Pressemitteilung auf der Seite des Herausgebers