Vortrag von Marc T. Hofmann zu Cyberkriminalität und Cybersicherheit

Marc T. Hofmann hielt einen umfassenden Vortrag über die aktuelle Bedrohungslage durch Cyberkriminalität, die Methoden und Motive der Täter, den Einsatz von Künstlicher Intelligenz im Bereich Cybercrime sowie konkrete Schutzmaßnahmen für Unternehmen und Privatpersonen.

- **Bedrohungslage und wirtschaftliche Dimension:** Hofmann erläuterte, dass Cyberkriminalität weltweit Schäden in Billionenhöhe verursacht und als drittgrößte 'Volkswirtschaft' nach den USA und China gelten würde. Er betonte, dass auch kleine Unternehmen und Privatpersonen zunehmend Ziel von Angriffen sind.
- **Methoden und Motive der Täter:** Die Täter agieren professionell, nutzen Ransomware, Phishing und Deepfakes und sind international vernetzt. Die Hauptmotive sind finanzieller Gewinn, Spionage und das Ausreizen technischer Herausforderungen (Trolling, Thrill Seeking).
- **Einsatz von Künstlicher Intelligenz:** Hofmann zeigte, wie KI-Modelle wie ChatGPT von Tätern ausgetrickst werden, um Schadsoftware zu generieren, und wie spezialisierte KI-Tools wie WormGPT für Phishing und Malware eingesetzt werden. Er warnte vor der Entwicklung autonomer KI-Agenten für Cyberangriffe.
- **Deepfakes und Social Engineering:** Die Qualität von Deepfakes ist so hoch, dass Stimmen und Gesichter mit wenigen Sekunden Rohmaterial täuschend echt imitiert werden können. Dies wird für CEO-Fraud, Enkeltrick und andere Betrugsmaschen genutzt.
- **Schutzmaßnahmen und Awareness:** Hofmann empfahl technische Maßnahmen wie regelmäßige Updates, starke Passwörter, Multi-Faktor-Authentifizierung und den Einsatz von Passwortmanagern. Er betonte die Bedeutung von Awareness, Codewörtern in Familien und Rückfragen bei verdächtigen Anrufen. Für iPhone-Nutzer empfahl er dringend das Update auf iOS 26 oder höher.

Fragerunde zu Cybersicherheit und technischen Schutzmaßnahmen

Im Anschluss an den Vortrag beantwortete Marc T. Hofmann zahlreiche Fragen der Teilnehmenden zu Passwortmanagern, dem Umgang mit Datenlecks, Cloud-Lösungen, VPN-Anbietern, dem Bürger-Cert-Newsletter des BSI und dem Einsatz von KI zur Cyberabwehr.

- **Passwortmanager und Passwortsicherheit:** Hofmann empfahl die Nutzung von Passwortmanagern, insbesondere aus vertrauenswürdigen Ländern wie Deutschland oder der Schweiz, und riet von kostenlosen Apps ohne klares Geschäftsmodell ab. Er betonte, dass Passwortmanager sicherer sind als die Nutzung identischer oder einfacher Passwörter.
- **Umgang mit Datenlecks:** Bei Benachrichtigungen über im Darknet gefundene Daten empfahl Hofmann, das Passwort des betroffenen Accounts zu ändern, sah aber keine akute Gefahr, da Millionen von Datensätzen im Umlauf sind.
- **Cloud-Lösungen als Backup:** Für Unternehmen hält Hofmann Cloud-Lösungen für sinnvoll, da Anbieter wie Microsoft oder Amazon meist bessere

Sicherheitsstandards bieten als kleine Unternehmen selbst. Privat sollte die Cloud nur so viel wie nötig genutzt werden.

- **VPN-Anbieter und Sicherheit:** NordVPN wurde als seriöser Anbieter genannt, während von Anbietern aus Ländern mit fragwürdiger Rechtslage (z.B. Russland) abgeraten wurde. VPNs erhöhen die Sicherheit insbesondere in öffentlichen WLANs.
- **Bürger-CERT-Newsletter und Awareness-Materialien:** Hofmann empfahl den Bürger-CERT-Newsletter des BSI sowie die dort verfügbaren Awareness-Materialien und Spiele, um das Thema Cybersicherheit regelmäßig ins Bewusstsein zu rufen.
- **KI in der Cyberabwehr:** KI kann helfen, ungewöhnliche Muster im Netzwerkverkehr zu erkennen und Angriffe frühzeitig zu identifizieren. Auch die Analyse von sprachlichen Mustern (Idiolekt) wird als zukünftige Möglichkeit zur Täteridentifikation erforscht.