Bayerisches Staatsministerium des
Innern, für Sport und Integration

Rede des Bayerischen Staatsministers des Innern,
für Sport und Integration, Joachim Herrmann,

anlässlich der Pressekonferenz zur Vorstellung des
Berichts zur Cybersicherheit in Bayern 2023

am Montag, 4. September 2023 in Nürnberg

Es gilt das gesprochene Wort!

- Anrede -

Einleitende Worte

Ich freue mich, dass wir unseren **Bericht zur Cybersicherheit in Bayern 2023** wieder gemeinsam vorstellen, dieses Mal im LSI in Nürnberg – herzlichen Dank für die Einladung!

Cybersicherheitslage allgemein

Die von uns im **Vorjahres-Bericht prognostizierten Entwicklungen** haben sich überwiegend **bewahrheitet**. Die Bedrohungen im Cyberraum haben 2022 **weiter zugenommen** und mit den **Feindseeligkeiten im Cyberraum** im Kontext des **russischen Angriffskrieg** gegen die Ukraine auch **neue Formen** angenommen.

Dabei bestimmten 2022 vor allem folgende **Methoden** die Sicherheitslage in Bayern:

Schwachstellen

Wie Kollege Füracker bereits erwähnt hat, gehören **Schwachstellen in Softwareprodukten** weiterhin zu einer **erheblichen und** oft **unterschätzten Gefahr**. Offene

Schwachstellen bieten nicht nur **ausländischen Nachrichtendiensten** ein **Einfallstor**, um unaufällig **langfristige Zugänge zu Servern** zu erhalten. Sie ermöglichen auch **niederschwellige Cyberkriminalität**. Wichtig ist daher stets eine **umgehende Aktualisierung von Software**.

Überlastungsangriffe (sog. DDoS-Angriffe)

Zudem haben **russlandfreundliche**, **mutmaßlich politisch motivierte Gruppierungen** verstärkt **Überlastungsangriffe** auch auf **Websiten bayerischer Behörden** verübt. Nennenswerte **Schäden** wurden jedoch **nicht verursacht**. Die Angriffe zielten vor allem auf **Verun-sicherung und Propagandawirkung** ab.

Lieferkettenangriffe (sog. Supply-Chain-Angriffe)

Aufgrund des häufig **schwächeren Sicherheitsniveaus** von kleineren Zulieferbetrieben stellen erneut auch Cyberangriffe, die nicht direkt auf das Unternehmen erfolgen, sondern **indirekt über die Lieferkette durchgeführt** werden, **zunehmend** ein **großes Risikopotenzial** für

bayerische Unternehmen dar. Zu den häufig beobachteten Methoden zählen das **Einschleusen manipulierter Software-Updates** über Schwachstellen bei Softwareherstellern oder die **Ausnutzung von Sicherheitslücken in Fernwartungszugängen** von IT-Dienstleistern.

Ransomware-Angriffe

Das größte Problem der Cyberkriminalität stellen aber nach wie vor **Ransomware-Angriffe** *(Schadsoftware zur Verschlüsselung von Daten und dem Ziel der Lösegeldepressung)* dar. Neben **Unternehmen** waren erneut auch **öffentliche Stellen und Einrichtungen** im Freistaat betroffen. Wir beobachten hier immer häufiger ein Geschäftsmodell, bei dem diese Schadsoftware weiterverkauft oder vermietet wird und der Anbieter nach einem erfolgreichen Angriff einen vorher festgelgten Anteil des erbeuteten Lösegelds erhält – also quasi **Lösegelderpressung als Dienstleistung** angeboten wird.

PKS Bayern
Zahlen ausschließlich Straftaten mit Tatort im Inland

Zahlen in Klammer betreffen ausschließlich Krypto-Ransomware

Straftaten:
2022: 580 (320)
2021: 680 (380)
2020: 330 (300)
2019: 390 (340)
2018: 368 (244)

Zwar verzeichnen die Sicherheitsbehörden in **2022** im Vergleich zum Vorjahr *(2021: 680, davon 380 Fälle Krypto-Ransomware und 300 Fälle Sperrbildschirme)* einen **leichten Rückgang** der **angezeigten Ransomware-Fälle** von 680 auf 580. *(2022 ca. 580 Fälle, davon 320 Fälle Krypto-Ransomware und 260 Fälle Sperrbildschirme)*. Der **Trend seit 2018** zeigt jedoch eine **ansteigende Tendenz**.

Ursachen für Nichtanzeige: nur geringer Schaden verursacht und/oder Opfer versprechen sich aus strafrechtlicher Ermittlungen keinen Erfolg oder fürchten geschäftsschädigende Reputationsschäden.

Zudem müssen wir in diesem Bereich auch von einer hohen **Dunkelziffer** ausgehen. Eine **frühzeitige Anzeige lohnt sich aber:** Sie kann helfen, den **Schaden zu begrenzen** und die **Spuren der Täter zu sichern**. Erst vor wenigen Tagen ist deutschen Strafverfolgungsbehörden zusammen US-Ermittlern erneut ein **großer Schlag gegen die internationale Cyberkriminalität** gelungen: Mit der Zerschlagung von „Qakbot“ konnte ein weiteres Schadsoftware-Netzwerk gestoppt werden, das mit über 700.000 infizierten Systemen als eines der gefährlichsten Schadsoftwares weltweit galt.

Prominentes Fallbeispiel

Ein **prominentes Beispiel**, das uns die Gefahren von Cyberangriffen zeigt, ist der Angriff auf ein **schwäbisches IT-Systemhaus** *(Reitzner AG mit Sitz in Dillingen)* am Ostermontag letzten Jahres *(18. April 2022)*. Eine mutmaßlich **russische**, unter dem **Namen** „**Lockbit 2.0**“ bekannte **Hackergruppe** hatte die IT-Systeme des **IT-Dienstleisters** lahmgelegt und eine Lösegeldforderung gestellt. Von dem Ransomwareangriff waren auch **Kundensysteme** des Dienstleisters betroffen, darunter die **Donau-Stadtwerke Dillingen-Lauingen**. Zwar waren die **örtliche Versorgung** mit Strom und Wasser sowie die Abwasserentsorgung durchgehend **gewährleistet**. Der Vorfall führt uns aber **warnend** vor Augen, dass Staat, Wirtschaft und Gesellschaft vor **großen Herausforderungen** stehen. Diese können wir nur **gemeinsam bewältigen**.

Fortschreibung Bayerische Cybersicherheitsstrategie

Als Antwort auf die wachsenden Herausforderungen im Cyberraum und zur Stärkung **der Resilienz** von Staat, Wirtschaft und Gesellschaft **gegen Cyberangriffe** in

Bayern, wollen wir gemeinsam mit allen Ressorts die **Bayerische Cybersicherheitsstrategie** bedarfsorientiert fortentwickeln und in den nächsten Wochen im Ministerrat beschließen.

Leitmotiv „modern. präventiv. resilient“

Unter dem **Leitmotiv „modern.präventiv.resilient**“ soll diese neue „**Cybersicherheitsstrategie 2.0**“ den strategischen Kompass für das **zukünftige staatliche Handeln im Bereich Cybersicherheit** im Freistaat bilden.

Hierbei wollen wir einen **noch stärkeren Fokus** auf staatliche Schutz- und Vorsorgemaßnahmen für **Kleine und mittlere Unternehmen** *(KMU)*, **Kritische Infrastrukturen** *(KRITIS)* **und Kommunen** richten. Neben **strategischen Zielen** werden in der **neuen Strategie** auch praxistaugliche **Maßnahmen festgeschrieben**.

Leuchtturmprojekt Cybertrainings

Wir wollen etwa **ressort- und sektorenübergreifende Cyber-Trainings etablieren**, um so unsere bestehenden Strukturen

und Prozesse im Cyberbereich **regelmäßig auf den Prüfstand zu stellen**.

Meine **Damen** und **Herren**, **Cybersicherheit** ist eines der zentralen Tätigkeitsfelder **moderner Gefahrenabwehr**. Die **Sicherheitsbehörden der Länder** tragen hierfür eine besondere Verantwortung.

Kritik am Bund

Der Aussage der **Bundesinnenministerin** *(PK vom 12.07.2022)*, die **Länder seien mit dieser Aufgabe** *(Gewährleistung der Cybersicherheit)* langfristig „**überfordert**“, widerspreche ich ganz entschieden!

Die **Erfolgsbilanz Bayerns** im Kampf gegen Cyberkriminalität und Cyberspionage ist der **eindeutige Gegenbeweis**:

- Zur **Stärkung** der **Abwehrfähigkeit gegen Cyberangriffe** hat die Bayerische Staatsregierung in den letzten Jahren **starke**, **hochspezialisierte Einheiten** bei Polizei, Staatsanwaltschaften und Verfassungsschutz geschaffen,

- das **bundesweit erste Landesamt** für Sicherheit in der Informationstechnik gegründet
- und die Vernetzung **aller** wichtigen **Akteure im Freistaat** durch die Informations- und Kooperationsplattform „**Cyberabwehr Bayern**“ sichergestellt.

Vernetzung zum Bund

Zu einer schlagkräftigen Cybersicherheitsarchitektur gehört aber auch eine **intelligente Vernetzung und Intensivierung der Zusammenarbeit zwischen Bund und Ländern**. Wir sehen das **Bundesamt für Sicherheit in der Informationstechnik** *(BSI)* daher als wichtigen **Kooperationspartner auf Augenhöhe** *(so auch BSI-Präsidentin Plattner im SZ-Interview vom 06.07.2023)*.