Bayerisches Staatsministerium des
Innern, für Sport und Integration

Bayerisches Staatsministerium der
Finanzen und für Heimat

CYBERSICHERHEIT IN BAYERN 2023

Bericht zur Cybersicherheit in Bayern

VORWORT

Die Digitalisierung unserer Gesellschaft schreitet stetig voran und hat nahezu alle Lebensbereiche durchdrungen.

Die im Bericht „Cybersicherheit in Bayern 2022" bezüglich der Gefährdungslage prognostizierten Entwicklungen haben sich überwiegend bewahrheitet. Die Bedrohungen im Cyberraum haben im vergangenen Jahr weiter zugenommen und mit den Feindseligkeiten im Cyberraum im Kontext des russischen Angriffskriegs gegen die Ukraine auch neue Formen angenommen.

Mit diesem Bericht zur Cybersicherheit in Bayern wird diese Bedrohung konkret aufgezeigt. Erfolgreiche Cyberangriffe sind keine Bagatellen, sondern für die betroffenen Einrichtungen häufig mit längeren Ausfällen der IT-Systeme und oftmals hohen Kosten verbunden. Staat, Wirtschaft und Gesellschaft stehen daher weiterhin vor großen Herausforderungen, die nur gemeinsam bewältigt werden können.

Cybersicherheit ist ein zentrales Tätigkeitsfeld moderner Gefahrenabwehr. Entlang ihres verfassungsmäßigen Auftrags tragen die bayerischen Sicherheitsbehörden besondere Verantwortung für deren Gewährleistung.

Vor diesem Hintergrund gilt es, die strategische Ausrichtung staatlichen Handelns im Handlungsfeld Cybersicherheit fortwährend auf den Prüfstand zu stellen und die hierfür getroffenen Maßnahmen auf Vollständigkeit, Wirksamkeit und Verhältnismäßigkeit zu prüfen. Mit der Fortschreibung der Bayerischen Cybersicherheitsstrategie 2.0 haben wir uns dieser Verantwortung gestellt und tragen so den aktuellen Lageentwicklungen und zukünftigen Herausforderungen Rechnung.

Für eine nachhaltige Stärkung der Resilienz von Staat, Wirtschaft und Gesellschaft gegen Cyberangriffe in Bayern, gilt es, weiterhin die wesentlichen Bestandteile und Herausforderungen moderner Cybersicherheitspolitik zielsicher zu identifizieren und strukturiert zu bewältigen.

Damit weiterhin gilt: In Bayern leben, heißt sicherer leben!

Joachim Herrmann, MdL
Bayerischer Staatsminister
des Innern, für Sport und Integration

Albert Füracker, MdL
Bayerischer Staatsminister
der Finanzen und für Heimat

INHALT

I. AUSGANGSLAGE

Bayern zeichnet sich von jeher durch ein hohes Maß an innerer Sicherheit aus. Als ein zentrales Tätigkeitsfeld moderner Gefahrenabwehr gilt das auch für die Cybersicherheit.

Die geopolitischen Entwicklungen und insbesondere der Krieg in der Ukraine verschärfen die ohnehin dynamische Bedrohungslage und stellen Staat, Wirtschaft und Gesellschaft gleichermaßen vor große Herausforderungen, denen nur gemeinsam wirkungsvoll begegnet werden kann.

Neben den bekannten Erscheinungsformen von Cyberkriminalität und Cyberspionage, hat sich in diesem Kontext auch eine neue Dimension des „Hacktivismus" entwickelt. So werden mit Cyberangriffen z.B. auf Behörden-Webseiten oder Kritische Infrastrukturen (KRITIS) zunehmend auch ideologische oder politische Ziele verfolgt.

Bayern ist mit seinen hochspezialisierten Organisationseinheiten bei Polizei, Verfassungsschutz, Justiz und dem Landesamt für Sicherheit in der Informationstechnik (LSI) sowie seinen Datenschutzaufsichtsbehörden für den Kampf gegen diese Bedrohungen hervorragend aufgestellt.

Erfolgsmeldungen, wie der koordinierten Zerschlagung von cyberkriminellen Netzwerken durch die Sicherheitsbehörden oder auch einen verschiedentlich wahrgenommenen Rückgang von Schadprogrammen und erfolgreichen Angriffen, dürfen jedoch nicht zum Anlass genommen werden, sich auf dem Erreichten auszuruhen.

Die Angreifer professionalisieren sich zunehmend, gehen zum Teil arbeitsteilig vor und agieren über Landesgrenzen hinweg in der Anonymität des Darknets. Sie verursachen hohe Schäden und stellen eine reale Gefahr für die wirtschaftlichen Grundlagen unserer Gesellschaft dar.

Daneben sind vermehrt auch gegen Bayern gerichtete Desinformationskampagnen und andere hybride Bedrohungen geeignet unsere demokratische Gesellschaft zu destabilisieren.

Vor diesem Hintergrund muss der Kampf gegen diese Bedrohungen weiter konsequent, professionell und von allen Akteuren gemeinsam geführt werden.

Um eine fortlaufende behördenübergreifende Beobachtung und Bewertung der Bedrohungslage durch die genannten bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sowie den Strafverfolgungs- und Datenschutzaufsichtsbehörden zu gewährleisten, sind diese in der Cyberabwehr Bayern institutionell vernetzt. Auf Grundlage dieser mittlerweile bewährten behördenübergreifenden Zusammenarbeit veröffentlichen das Staatsministerium des Innern, für Sport und Integration und das Staatsministerium der Finanzen und für Heimat jährlich diesen Bericht zur Cybersicherheit in Bayern. Als gemeinsamer Lagebericht führt dieser die Erkenntnisse und Einschätzungen der mit Cybersicherheit befassten Stellen zusammen und ordnen die aktuellen Aktivitäten der Behörden mit Cybersicherheitsaufgabe entsprechend ein.

II. ALLGEMEINES LAGEBILD ZUR CYBERSICHERHEIT IN BAYERN

Cybercrime ist weiterhin eine der größten Herausforderungen in unserer digitalen Welt. Diesbezüglich war 2022 ein vorfallstarkes Jahr bezogen auf Fake-E-Mails – meist mit Zielrichtung Erpressung, Identitätsdiebstahl oder Phishing – und beinahe monatlichen Meldungen über gestohlene Nutzerdaten aus den Beständen großer Unternehmen. Zunehmend wurden auch staatliche Institutionen Ziel von Angriffen durch Cyberkriminelle.

Dem langjährigen Trend folgend ist die Bedrohungslage für Staat, Wirtschaft und Gesellschaft sowie Kommunen in Bayern auch im Berichtsjahr 2022 auf einem anhaltend hohen Niveau.

Im Jahr 2022 bestimmten vor allem folgende Phänomene die digitale Sicherheitslage in Bayern:

A SCHWACHSTELLEN UND KONFIGURATIONSFEHLER

Schwachstellen in Software stellen nach wie vor eine erhebliche, aber leider weiterhin unterschätzte Gefährdung dar. Die vorliegenden Erkenntnisse lassen darauf schließen, dass eine erhebliche Verwundbarkeit von Systemen in Bayern bestand bzw. weiterhin besteht, weil verfügbare Patches nicht umgehend eingespielt werden. Selbst noch Monate nach Veröffentlichung entsprechender Sicherheitspatches werden noch erfolgreiche Angriffe verzeichnet. Gerade bei weit verbreiteten Softwareprodukten führt diese Leichtsinnigkeit zu letztlich überflüssigen Cybervorfällen.

Es gilt als gesichert, dass solche Schwachstellen auch von ausländischen Akteuren genutzt werden, um unauffällig einen langfristigen Zugang zu Systemen zu erhalten.

Ungepatchte Schwachstellen bieten allerdings nicht nur hochprofessionellen Cyberkriminellen ein offenes Einfallstor, sondern ermöglichen auch niederschwellige Cyberkriminalität und somit eigentlich leicht vermeidbare Schäden. So wurden im Berichtszeitraum beispielsweise auch Telefonanlagen kompromittiert und Auslandsgespräche auf Kosten der Opfer geführt.

Es ist zudem eine Zunahme der Meldungen von erfolgreichen Angriffen auf Cloud-Systeme festzustellen, wobei in den bekannten Fällen fast ausschließlich Angriffe über die Entwendung von Zugangsdaten mittels Social Engineering (z.B. E-Mail mit

Link auf gefälschte Login-Seite) erfolgten. Mit 312 Meldungen haben Angriffe auf Cloud-Dienste, insbesondere mit dem Zweck einer missbräuchlichen Verwendung der damit verbundenen E-Mail-Infrastruktur, weiterhin ein hohes und ernstzunehmendes Niveau erreicht. Es fehlt häufig noch das Bewusstsein, dass solche Cloudumgebungen sorgsam konfiguriert und geschützt werden müssen.

B RANSOMWARE

Ransomware[1] war, wie bereits 2021, ein bestimmendes Thema der Cybersicherheitslage und stellt weiterhin das Leitphänomen der Cyberkriminalität dar. Dabei beobachten die bayerischen Sicherheitsbehörden immer häufiger ein Geschäftsmodell (Cybercrime-as-a-Service), bei dem Ransomware weiterverkauft oder vermietet wird. Nach einem erfolgreichen Angriff erhält der Anbieter einen vorher festgelegten Anteil des erbeuteten Lösegelds. Die eigentlichen Täter benötigen hierfür selbst nur wenige technische Kenntnisse. Dadurch wird Ransomware als Begehungsweise für mehr Kriminelle zugänglich und bleibt ein dynamisches Phänomen.

Der durch die Zerschlagung des Ransomware-Netzwerkes „Emotet" erreichte Rückgang der Sicherheitsvorfälle Ende 2021 war nur vorübergehend. Die Lücke füllten Cyberkriminelle insbesondere mit der „QakBot-Kampagne", die im 4. Quartal 2022 sowohl quantitativ als auch qualitativ das gleiche Niveau wie bei „Emotet" im Jahr 2020 erreichten.

Der entscheidende Erfolgsfaktor war, dass die Angreifer permanent ihre Angriffsvektoren erweiterten bzw. an neue Schutzmechanismen anpassten. Ebenso konnte die Schadcodekampagne „LockBit 2.0" erheblichen Aufschwung erlangen. Auch das Netzwerk „Emotet" steht vor einem möglichen Comeback und steht unter kritischer Beobachtung.

Der Kampf gegen Cyberkriminelle ist daher keinesfalls erfolglos, muss aber nachhaltig und entschlossen geführt werden. Der gut funktionierende und enge Schulterschluss der Behörden mit Cybersicherheitsaufgaben, national wie international, ist hierbei ein entscheidender Erfolgsfaktor.

1 Bei Ransomware handelt es sich um Schadsoftware, bei der Daten der Opfer auf deren IT-Systemen verschlüsselt und damit unbrauchbar gemacht werden. Der Entschlüsselungs-Key wird im besten Falle nach Zahlung einer Lösegeldforderung durch die Täter zur Verfügung gestellt.

Die bayerischen Fallzahlen, Lösegeldforderungen und Lösegeldzahlungen stellen sich im Jahr 2022 wie folgt dar:

- Das BLKA registrierte in 2022 einen leichten Rückgang der Ransomwarefälle gegenüber dem Vorjahr 2021 (ca. 680 Fälle) auf ca. 580 angezeigte Fälle. Der Mehrjahres-Trend zeigt jedoch weiterhin eine ansteigende Tendenz. In diesem Deliktsfeld muss zudem von einer hohen Dunkelziffer ausgegangen werden.
- Auch öffentliche Stellen im Freistaat wurden erneut zum Opfer von Ransomware-Attacken. Im Berichtszeitraum sind wiederum Angriffe auf Kommunalverwaltungen zu verzeichnen. Die den Behörden bekannt gewordenen Fälle zeigen die teils schweren Folgen das hohe Bedrohungspotenzial der Cyberkriminalität auf.

Abschießend ist zu betonen, dass die Verschlüsselung in vielen Fällen nur die letzte Stufe eines Angriffs mit Ransomeware ist. Zuvor eignen sich die Angreifer häufig die Daten der Opfer an. Diese Daten werden nicht nur zur Erpressung des Opfers genutzt, sondern auch für weitere Angriffe verwertet oder im Darknet verkauft. Während die Folgen einer Verschlüsselung von den meisten Organisationen noch bewältigt werden können, stellen gerade diese Datenverluste einen bleibenden, nicht mehr beseitigbaren Schaden und eine Bedrohung für Dritte dar. Darauf lassen die den bayerischen Behörden bekannten Vorfälle und die spezifische Beobachtung des Darknets schließen.

C DDOS-ANGRIFFE (DISTRIBUTED DENIAL OF SERVICE)

Zwar gingen DDos-Angriffe in 2022 zahlenmäßig leicht zurück, erfolgten aber mit einer höheren Durchschnitts- und Maximalbandreite. Insofern konnte hier im Berichtszeitraum eine Professionalisierung der Angriffsmethodiken aber auch eine verstärkte Koordinierung (vgl. Ausführungen zu „Hacktivismus“) beobachtet werden.

D PHISHING[2] UND SOCIAL ENGINEERING

Beim Versand von Phishing-Mails sollen potentielle Opfer mittels gefälschter E-Mails oder SMS-Nachrichten über enthaltene Links oder Dateianhänge meist zur Preisgabe von Nutzer- oder Bankdaten verleitet werden. Zwar zeigen breit angelegte Schulungs- und Sensibilisierungsmaßnahmen mittlerweile Wirkung. Im Bereich „Social Engineering" stellt das sog. „Phishing" jedoch nach wie vor die prominenteste Methode dar. Häufig handelt es sich um gezielte Kampagnen, sog. „Spear-Phishing", als Basis für Cyber- oder Internetkriminalität. In Bayern standen im Berichtszeitraum erneut insbesondere Hochschulen und Forschungseinrichtungen im Fokus der Angreifer.

E IDENTITÄTSDIEBSTAHL

Das Umleiten von Zahlungsströmen („Payment Diversion Fraud") per E-Mail ist eine Betrugsmasche, die sich wiederum des Identitätsdiebstahls und des Social Engineerings bedient. Die Betrüger geben sich als Geschäftspartner aus. Im Jahr 2022 wurden ca. 310 derartiger Fälle verzeichnet, im Jahr 2021 waren es noch etwa 130 Fälle weniger. Mit gefälschten oder „gephishten" Informationen wird die vorgetäuschte Identität glaubhaft gemacht und im weiteren Verlauf darauf hingewiesen, dass sich Zahlungsmodalitäten oder Bankdaten geändert haben.

F APT[3]-ANGRIFFE

Für Unternehmen und Forschungseinrichtungen in Bayern besteht die Gefährdungslage bzgl. APT-Angriffen unverändert fort. Wie bereits im Bericht aus dem Vorjahr ausführlich dargestellt, liegen weiterhin zumeist Organisationen aus dem öffentlichen Sektor, KRITIS-Betreiber, innovative Wirtschaftsunternehmen und Forschungseinrichtungen im Fokus der ATP-Gruppierungen.

2 Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln') versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es z. B. an persönliche Daten eines Internet-Benutzers zu gelangen oder ihn z. B. zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge werden dann beispielsweise Kontoplünderung oder Identitätsdiebstahl begangen oder eine Schadsoftware installiert.

3 Advanced Persistent Threat (APT; dt.: „fortgeschrittene andauernde Bedrohung") ist ein häufig im Bereich der Cyber-Bedrohung (Cyber-Attacke) verwendeter Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen aller Branchen, welche aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können

G DESINFORMATIONSKAMPAGNEN UND HYBRIDE BEDROHUNGEN

Im Zusammenhang mit dem Russland-Ukraine-Krieg ist ein vermehrtes Auftreten von Desinformationskampagnen zu verzeichnen. Diese zielen darauf ab, Unterstützung für die außenpolitische Position Russlands zu generieren sowie westliche Sanktionen zu diskreditieren.

Die Akteure versuchten beispielsweise, Internetauftritte von Politikerinnen und Politikern durch Übernahme ihrer Social-Media-Konten zu fingieren und Falschinformationen zu streuen. Diese Vorgehensweise und gewünschte Einflussnahme auf die Politik deuten auf staatlich gesteuerte Cyberakteure hin.

H SUPPLY-CHAIN-ANGRIFFE

Bei sog. „Supply-Chain-Angriffen" machen sich der oder die Täter oft die weniger geschützten Systeme bei Zulieferbetrieben größerer Konzerne und das Vertrauensverhältnis zwischen Unternehmen innerhalb einer Lieferkette für ihre Zwecke zunutze.

Aufgrund von meist vielen beteiligten betroffenen Unternehmen stellen Supply-Chain-Angriffe in der Gesamtschau zunehmend eines der größten Risiken für bayerische Unternehmen dar. Die Fallzahlen von Supply-Chain-Angriffen wurden zwar in 2022 noch nicht systematisch erfasst. Einzelfälle, wie der Cyberangriff auf einen IT-Dienstleister mit 130 betroffenen Unternehmen in Bayern, zeigen schon jetzt das Risikopotential dieser Angriffsart.

Zu den häufig beobachteten Methoden zählen die Kompromittierung von Software über Schwachstellen bei den Herstellern von Software, um über die bestehenden Software-Verteilungsmechanismen manipulierte Software(-Updates) in IT-Infrastrukturen von Zielunternehmen einzuschleusen, oder die Ausnutzung von Sicherheitslücken in bestehende Fernwartungszugänge von IT-Dienstleistern, um direkten Zugriff auf Zielsysteme zu erhalten.

I „HACKTIVISMUS"

Im Berichtszeitraum bestimmten verschiedene Gruppierungen die Schlagzeilen, deren Angriffe unter der Überschrift Hacktivismus zusammengefasst werden können. Diese Kampagnen werden häufig von einer pro-russischen Positionierung begleitet. Erwähnenswert sind insbesondere sog. DDoS-Angriffe, die zum Ziel haben die Internetseiten von Behörden und kritischen Infrastrukturen lahmzulegen.

Hier ist beispielsweise die Gruppierung „Killnet“ in Erscheinung getreten. Derartige Gruppierungen verursachen bisher keinen nachhaltigen Schaden und scheinen auf Verunsicherung der Öffentlichkeit sowie auf Propagandawirkung in Russland abzuzielen.

Im zeitlichen Zusammenhang mit dem Angriff auf die Ukraine stehende erhöhte Scanaktivitäten staatlicher IT-Systeme lassen vermuten, dass auch diese gezielt im Fokus von Angreifern stehen.

In neuesten Bewertungen westlicher Sicherheitsbehörden und IT-Sicherheitsunternehmen werden – neben „Killnet“ – auch andere Gruppierungen in unmittelbaren Zusammenhang mit russischen Nachrichtendiensten gebracht. Dabei wird davon ausgegangen, dass sie von russischen Diensten mit Informationen für ihre Angriffe versorgt werden. Die Medienpräsenz von „Hacktivismus“ hat nach Erkenntnissen der bayerischen Polizei auch dazu geführt, dass Betrüger sich als ukrainische Hacker ausgegeben haben und mit Angriffsdrohungen „Spenden“ erpressen wollten. Zudem haben Cyberkriminelle ihre Lösegeldforderung als „Spende“ beschönigt.

J DUNKELFELD

Aufgrund der Erkenntnisse der Behörden und Einrichtungen mit Cybersicherheitsaufgaben ist in allen oben aufgeführten Phänomenbereichen von einer erheblichen Dunkelziffer auszugehen.

Insbesondere im Bereich Ransomware ist von einer deutlich höheren Betroffenheit bei kleinen und mittleren Unternehmen (KMU) sowie Privatpersonen, die im Berichtszeitraum Opfer breit angelegter Ransomware-Kampagnen wurden, auszugehen.

Häufig werden diese Fälle nicht erkannt (z.B. wegen Missbrauchs von digitalen Identitäten oder technischen Geräten) oder nicht zur Anzeige gebracht.

Als mögliche Ursachen für die Nichtanzeige kommen in Betracht, dass kein oder nur geringer Schaden verursacht wurde und/oder die Opfer sich aus der strafrechtlichen Ermittlung keinen Erfolg versprechen oder geschäftsschädigende Reputationsschäden fürchten.

Zudem ist zu berücksichtigen, dass der Fokus der Betroffenen regelmäßig auf der schnellen Wiederherstellung der Verfügbarkeit der betroffenen IT-Systeme liegt. Forensische Maßnahmen der Ermittlungsbehörden werden hier häufig als hinderlich bewertet.

In der Praxis von Polizei und LSI hat sich hingegen gezeigt, dass Verdachtsfälle von Cyberangriffen weiterhin sorgsam aufgeklärt werden müssen, um einerseits Angriffstechniken zu verstehen und so Risiken für andere IT-Systeme verringern zu können sowie andererseits um Täterspuren forensisch zu sichern.

III. MASSNAHMEN

Die anhaltend hohe Cybergefahr erfordert weiterhin eine Intensivierung der individuellen Anstrengungen als auch ein starkes behördenübergreifendes Zusammenwirken. Dies ist insbesondere mit folgenden Maßnahmen gewährleistet:

A PRÄVENTION & CYBERSICHERHEITSBERATUNG

Die unterschiedlichen, aufeinander abgestimmten Präventionsangebote von Polizei und Verfassungsschutz für den Bereich Wirtschaft und Gesellschaft wurden bedarfsgerecht weiterentwickelt.

Für den kommunalen Bereich bietet das LSI neben dem Siegel „Kommunale IT-Sicherheit", technischen Orientierungshilfen, Unterlagen für ein Notfallmanagement, laufenden Angriffswellen und anderen Bedrohungen, einem für die öffentliche Verwaltung – Staat und Kommunen – kostenfrei nutzbaren Online-Mitarbeitersensibilisierungskurs vor allem konkrete technische Beratung zu allen Fragen der IT-Sicherheit. Neben der öffentlichen Verwaltung werden auch Unternehmen der kritischen Infrastruktur beraten und unterstützt. Dabei werden die Sektoren sukzessive mit branchenspezifischen Informationen und Handlungsanleitungen sowie einem individuellen Beratungsangebot versorgt. Nach Angeboten für Krankenhäuser und Wasserversorger wurden zuletzt entsprechende Formate für Abwasserentsorgung sowie Siedlungsabfallentsorgung geschaffen.

Großer Nachfrage erfreut sich das neue Portal des Warn- und Informationsdienst des LSI mit dem zu konkreten Sicherheitslücken und allgemeinen Bedrohungen umfassend informiert wird. Bisher haben sich alleine im kommunalen Bereich rund 1.400 Stellen registriert.

B BEWÄLTIGUNG VON VORFÄLLEN

Straftaten in Zusammenhang mit Cyberkriminalität können bei jeder Polizeidienststelle in Bayern angezeigt werden. Beginnend bei Schwerpunktsachbearbeitern bei den lokalen Polizeiinspektionen bis hin zu hochspezialisierten Ermittlern und IT-Forensikern bei den Kriminalpolizeidienststellen sowie beim BLKA stehen auf allen polizeilichen Ebenen kompetente Ansprechpartner für Cyberkriminalität zur Verfügung. Neben der Konstituierung des Fachdezernats Cybercrime beim BLKA wurden zudem flächendeckend „Cybercrime"-Kriminalfachdezernate und -Kommissariate in ganz Bayern eingerichtet, an welche die Dienststellen der „Digitalen Forensik" angegliedert sind. Über die sog. Cybercrime Quick-Reaction-Teams der Bayerischen Polizei ist eine Rund-um-die-Uhr Einsatzfähigkeit der polizeilichen IT-Spezialisten für herausragende bzw. schwerwiegende Cyberangriffe gewährleistet. Ergänzend wurden das mobile Forensik Labor PALADIN beim Polizeipräsidium Oberfranken sowie die Hotline für IT-Notfälle und der dazugehörige Chatbot beim BLKA in Betrieb genommen.

In komplexen und schwerwiegenden Fällen von Cybercrime, dazu zählen auch Cyberangriffe auf Unternehmen, ermittelt die im Jahr 2015 gegründete Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg.

Bei dem Verdacht eines Cyberangriffs mit nachrichtendienstlichem Hintergrund steht das CAZ als vertraulicher Ansprechpartner für Unternehmen, Hochschulen, Forschungseinrichtungen und KRITIS zur Verfügung.

Meldungen von IT-Sicherheitsvorfällen im Aufgabenbereich des LSI werden dort im Lagezentrum aufgenommen und bearbeitet. Das Labor wurde im Berichtszeitraum weiter ausgebaut. Damit steht eine Infrastruktur für statische und dynamische Schadcodeanalyse, forensische Untersuchungen, sowie Erprobungen aller Art zur Verfügung. Somit können durch Schadcode verursachte Sicherheitsvorfälle in realer Umgebung in einer isolierten und sicheren Umgebung nachgestellt und analysiert werden.

IT-Sicherheitsexperten des LSI unterstützen auch bei Vorfällen in Kommunen oder Unternehmen der kritischen Infrastruktur. Hierbei ist eine enge Abstimmung mit der Polizei ein entscheidender Erfolgsfaktor. Aus der Bearbeitung der Vorfälle erfolgt eine konkrete, technische Beratung für alle anderen Institutionen der jeweiligen Zielgruppe durch das LSI. Das LSI verzahnt sich über die Zusammenarbeit mit den Behörden hinaus weiter mit der IT-Sicherheitscommunity, sei es durch Kooperationen im wissenschaftlichen Umfeld oder durch die Mitarbeiter in CERT-Verbunden. Im Berichtszeitraum wurde das LSI als erstens CERT eines Bundeslandes im Netzwerk „Trusted Introducer" akkreditiert.

Die Behörden mit Cybersicherheitsaufgaben raten allen betroffenen Stellen, Vorfälle anzuzeigen, Meldepflichten einzuhalten und nicht auf Lösegeldforderungen einzugehen.

C BEHÖRDLICHE IT-SICHERHEIT

Im Lagezentrum des LSI werden Daten der Monitoringsysteme im Bayerischen Behördennetz (BYBN) sowie den staatlichen Rechenzentren zusammengefasst überwacht und auf verdächtige Aktivitäten untersucht. Alle gewonnenen Erkenntnisse werden nahezu in Echtzeit mit anderen Teilnehmern geteilt. Hierdurch konnten Infektionen in anderen Bundesländern und Firmen verhindert bzw. entdeckt werden. Es werden täglich rund 2 Milliarden Datensätze analysiert. Die Sicherheitsmechanismen am Internetübergang werden auf der Grundlage verschiedenster Erkenntnisse sehr schnell zusammen mit den Rechenzentren nachgeschärft, um Angriffe möglichst automatisiert abzuwehren.

Im Jahr 2022 hat das LSI über 4.000 Angriffsversuche auf das bayerische Behördennetz registriert, von denen rund 1.500 zu schwerwiegenden Auswirkungen hätten führen können. In keinem dieser Fälle ist es den Angreifern gelungen, erfolgreich Schadcode im Behördennetz zur Ausführung zu bringen. Die technischen und operationellen Mechanismen im Lagezentrum des LSI und am IT-DLZ konnten alle Angriffsversuche erfolgreich abwehren.

Ein funktionierendes Informationssicherheitsmanagement (ISMS) ist dabei ein entscheidender Faktor für die IT-Sicherheit einer Organisation. Dementsprechend unterstützt das LSI die Ressorts bei der Erstellung und Pflege der jeweiligen ISMS. Im kommunalen Bereich unterstützt das ISMS-Förderprogramm für bayerische kommunale Gebietskörperschaften. Hierbei werden die Kommunen insbesondere auch unterstützt, das Siegel „Kommunale IT-Sicherheit“ des LSI zu erwerben. Bei der Beratung der Kommunen arbeiten LSI und die Regierung von Oberfranken als zentrale Förderstelle für ganz Bayern eng zusammen.

D BEHÖRDENÜBERGREIFENDE ZUSAMMENARBEIT

Ein regelmäßiger und schneller Austausch von Informationen und Erkenntnissen ist wesentlicher Erfolgsfaktor bei der Bewältigung von Cybersicherheitsvorfällen. Innerhalb Bayerns wurden hierfür mit der Errichtung der CAB bereits zum Jahresanfang 2020 der notwendige organisatorische Rahmen geschaffen. Die gemeinsame Aufarbeitung konkreter Vorfälle in der CAB nutzt beispielsweise der Bayerische Landesbeauftragte für den Datenschutz, um die Stellen in seinen Zuständigkeitsbereich zu zusätzlichen Maßnahmen zum Schutz personenbezogener Daten aufzufordern.

Mit der pilotweisen Entsendung von bayerischen Verbindungsbeamten aus der CAB in das Nationale Cyber-Abwehrzentrum (Cyber-AZ) hat Bayern außerdem eine wichtige Scharnierfunktion zum Bund geschaffen. Ebenso ist die GenStA Bamberg, ZCB als einer der Vertreter der Länderstaatsanwaltschaften beim Cyber-AZ vertreten. Ausgehend von den in Pilotphase identifizierten Mehrwerten für die Arbeit der CAB ist es ein wichtiges Anliegen, diese horizontale Vernetzung zu verstetigen.

Auch im Bereich der öffentlichen IT-Sicherheit ist die ebenübergreifende Kooperation zwischen LSI und BSI sowie anderen Länder-IT-Sicherheitsbehörden ein entscheidender Erfolgsfaktor. Der schnelle, technische und konkrete Informationsaustausch im Verwaltungs-CERT-Verbund (VCV) hat sich sehr bewährt. Die weitere Vertiefung der Zusammenarbeit bzw. der Ausbau dieses Formats werden von bayerischer Seite aktiv unterstützt. Auch hier wird das LSI mit positiven Beispiel des Länderengagements vorangehen.

Hinsichtlich des Austausches von Information setzt das LSI hier sowie in der Zusammenarbeit mit den Zielgruppen auf eine Malware-Information-Sharing-Plattform (MISP). MISP ist eine in Europa entwickelte offene Arbeitsumgebung für den schnellen und automatisierten Austausch von Bedrohungsinformationen, die sich hinsichtlich der in der Praxis erforderlichen hohes Reaktionsfähigkeit sehr bewährt hat. Ziel ist insbesondere die Etablierung einer bayerischen „Sharingcommunity", um die Abwehrmechanismen schnell fortzuentwickeln.

IV. AUSBLICK

PROGNOSE

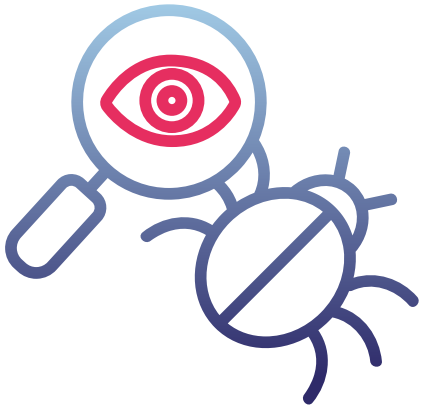
Für das Jahr 2023 ist mit einer weiteren Zunahme von Straftaten aus dem Bereich der Cybercrime zu rechnen. Für die Täter scheint die Begehung derartiger Delikte weiterhin ein so lohnendes Ziel zu sein, dass die Gefahr der Strafverfolgung in Kauf genommen wird. Es ist davon auszugehen, dass die Täter auch weiterhin aktuelle gesellschaftliche und politische Geschehnisse nutzen werden, um ihren Modus Operandi entsprechend anzupassen.

Es ist auch davon auszugehen, dass der Interessenkonflikt Russlands mit westlichen Staaten weiterhin von Cyberangriffen und Vorbereitungshandlungen für hybride Operationen und weitere Eskalationsoptionen begleitet werden wird. Zu diesem Zweck werden unter anderem Firmen- sowie Behördennetzwerke infiltriert, KRITIS-Strukturen aufgeklärt und Einflussnahmeversuche auf Personen in geeigneten wirtschaftlichen und politischen Positionen intensiviert.

Mit der rasanten Technologieentwicklung sowie der stetig voranschreitenden Digitalisierung und Vernetzung geht auch eine Veränderung von Staat, Wirtschaft und Gesellschaft einher. Nach wie vor erkennen Gesellschaft und Wirtschaft in der Digitalisierung und globalen Vernetzung eine große Chance, beispielsweise um persönliche Freiräume oder höhere Wertschöpfung zu schaffen. Die digitale Transformation erhöht gleichzeitig die Verwundbarkeit im Cyberraum.

Vor dem Hintergrund der dynamischen Bedrohungslage im Cyberraum gilt es, die strategische Ausrichtung staatlichen Handelns im Handlungsfeld Cybersicherheit fortwährend auf den Prüfstand zu stellen und die hierfür getroffenen Maßnahmen auf Vollständigkeit, Wirksamkeit und Verhältnismäßigkeit zu prüfen. Mit der neuen Bayerischen Cybersicherheitsstrategie 2.0 wird den aktuellen und zukünftigen Herausforderungen Rechnung getragen.

Das LSI wird den Schutz der staatlichen IT-Infrastruktur weiter intensivieren und die technischen Unterstützungsangebote an seine Zielgruppen weiter ausbauen. Im Fokus steht auch der sukzessive Ausbau von branchenspezifische Beratungsangeboten für KRITIS-Betreiber sowie der bayerischen „Sharingcommunity". Weiterer Schwerpunkt ist der Ausbau der Analysefähigkeit sowie die Intensivierung der Beratung zur sicheren Cloudnutzung. Die bestehende Zusammenarbeit mit unterschiedlichen Hochschulen wird weiter ausgebaut und gefördert. Die sich daraus ergebenen Kooperationen zu Forschungsprojekten und der direkte Wissenstransfer aus der Forschung in die Praxis tragen zu einer stetigen Steigerung der IT-Sicherheit in Bayern bei.



Impressum

Herausgeber: Bayerisches Staatsministerium des Innern, für Sport und Integration
Odeonsplatz 3, 80539 München
www.innenministerium.bayern.de

Bayerisches Staatsministerium der Finanzen und für Heimat
Odeonsplatz 4, 80539 München
info@stmfh.bayern.de, www.stmfh.bayern.de

Bildrechte: AdobeStock/vectorwin
Grafik: Saskia Kölliker
Stand: September 2023
Druck: Landesamt für Landesamt für Digitalisierung, Breitband und Vermessung,
Alexandrastraße 4, 80538 München
Gedruckt auf umweltzertifiziertem Papier (PEFC, FSC)

Das Bayerische Innenministerium im Internet:

www.innenministerium.bayern.de

www.twitter.com/BayStMI

www.instagram.com/BayStMI

www.facebook.com/BayStMI

www.youtube.de/BayerischesInnenministerium

„Let's talk Innenpolitik" mit Joachim Herrmann – unser Podcast auf allen großen Plattformen