Bayerisches Staatsministerium des
Innern, für Sport und Integration

Bayerisches Staatsministerium der
Finanzen und für Heimat

CYBERSICHERHEIT IN BAYERN 2024

Bericht zur Cybersicherheit in Bayern

VORWORT

Die Bayerische Staatsregierung räumt der Gewährleistung eines hohen Sicherheitsniveaus von je her einen hohen Stellenwert ein. Diesem Anspruch stellen wir uns auch im Cyberraum. In unserer zunehmend digitalisierten Welt ist die Cybersicherheit somit mehr denn je ein zentrales Tätigkeitsfeld moderner Gefahrenabwehr.

Die digitale Transformation hat nahezu alle Lebensbereiche erfasst. Von der persönlichen Kommunikation bis zur Arbeit im Homeoffice, von stark automatisierter Fertigung bis zum Smart Home. Nicht zuletzt hat sich auch die Arbeit der öffentlichen Verwaltung dadurch stark verändert. Digitalisierung bietet die Chance effizienter zu arbeiten und bequemer zu leben.

Auf der anderen Seite gehen mit der rasanten Technologieentwicklung aber auch Risiken für Staat, Wirtschaft und Gesellschaft einher, denen es entschlossen zu begegnen gilt. Dabei müssen wir insbesondere die wachsende Abhängigkeit von digitaler Technik als auch die Zunahme von Angriffsflächen und die damit einhergehenden potenziellen Auswirkungen- insbesondere für Cyberkriminalität im Blick behalten. Aktuelle Entwicklungssprünge etwa im Bereich der Künstlichen Intelligenz senken darüber hinaus die Einstiegshürden für Cyberangriffe und können dauerhaft deren Umfang, Geschwindigkeit und Schlagkraft erhöhen.

Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe. Sie ist ein Schlüsselfaktor, um die Chancen der Digitalisierung zu realisieren.

Um eine fortlaufende behördenübergreifende Beobachtung und Bewertung der Bedrohungslage durch die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben zu gewährleisten, sind diese in der Cyberabwehr Bayern institutionell vernetzt. Auf Grundlage dieser 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 ordnet die aktuellen Aktivitäten der Behörden mit Cybersicherheitsaufgabe entsprechend ein.

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

Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 01.01.2023 bis zum 31.12.2023 (Berichtszeitraum). Die Behörden und Einrichtungen mit Cybersicherheitsaufgaben haben im Berichtszeitraum neben einer quantitativen und qualitativen Steigerung an Fällen im Bereich der Cyberkriminalität ebenso beobachtet, dass sich bestehende und neue globale Konflikte als „Brandbeschleuniger" im Bereich der gezielten Verbreitung von Desinformation sowie anderer hybrider Bedrohungen erwiesen haben.

Um diesen Herausforderungen zu begegnen, ist Bayern stark aufgestellt. Die bayerische Cybersicherheitsarchitektur sticht bundesweit nicht nur durch fortschrittliche Maßnahmen, wie beispielsweise die Errichtung des Landesamts für Sicherheit in der Informationstechnik, sondern auch durch die etablierte, institutionalisierte Zusammenarbeit aller Behörden und Einrichtungen mit Cybersicherheitsaufgaben hervor. Deren Vernetzung untereinander und zu den wichtigen Akteuren beim Bund und in anderen Ländern ist ein wesentlicher Erfolgsfaktor. Nur durch gemeinsame Anstrengungen kann die steigende Bedrohung erfolgreich eingedämmt und Sicherheit in der digitalen Welt gewährleistet werden.

II. ALLGEMEINES LAGEBILD ZUR CYBERSICHERHEIT IN BAYERN

Die bereits angespannte Lage spitzte sich im Berichtszeitraum weiter zu. Die Spannbreite der Angriffe reichte von Erpressungslagen mittels DDoS-Angriffen, E-Mail-Manipulation und Ransomware-Angriffen bis hin zur Industrie- und Wirtschaftsspionage.

Besorgniserregend ist, dass nach wie vor nicht mehr nur große Unternehmen, sondern vermehrt auch kleine und mittelständische Unternehmen sowie Behörden von derartigen Vorfällen betroffen waren. Auch bayerische Kommunen waren im Berichtszeitraum das Ziel von verschiedenen Cyberangriffen, wie beispielsweise Phishing, Malware oder im Bereich Social Engineering[1].

1 Beim Social Engineering nutzen Angreifer den „Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um ihre kriminellen Absichten zu verwirklichen. Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyberkriminelle verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, zum Beispiel durch Hacktivismus und Verbreitung von Desinformation oder Propaganda durch ausländische Nachrichtendienste. Wie auch im vergangenen Jahr stand Bayern daher auch im Fokus staatlicher Cyberspionage.

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

A SCHWACHSTELLEN UND KONFIGURATIONSFEHLER

Schwachstellen in Software stellen nach wie vor eine gleichermaßen erhebliche wie unterschätzte Gefährdung dar.

Die Vorfälle im Berichtszeitraum zeigen, dass die Angreifer weiterhin verstärkt auf nicht oder nicht schnell genug gepatchte Schwachstellen in zentralen und nach außen exponierten Softwarekomponenten abzielen. Dabei nehmen Cyberkriminelle zunehmend auch Schwachstellen bei externen Dienstleistern in den Fokus, um dort- z.B. im Zuge von Wartungsarbeiten- Zugang zu sensiblen Daten zu erlangen oder Systeme zu kompromittieren.

B ANGRIFFE AUF CLOUD-DIENSTE

Eine weitere Entwicklung ist die Zunahme der Meldungen von erfolgreichen Angriffen auf Cloud-Systeme, wobei in den bekannt gewordenen Fällen fast ausschließlich Angriffe über die Entwendung von Zugangsdaten mittels Social Engineering (z.B. E-Mail mit Link auf gefälschte Login-Seite) erfolgten. Es fehlt häufig noch das Bewusstsein, dass solche Cloudumgebungen sorgsam konfiguriert und geschützt werden müssen. Dabei sollte Multi-Faktor-Authentifizierung sowohl bei Anwendungen in der Cloud als auch bei anderen Anwendungen standardmäßig eingesetzt werden.

C RANSOMWARE[2]

Ransomware stellt- trotz der rückläufigen Zahlen des Bayerischen Landeskriminalamtes (BLKA)- weiterhin eine der größten Cyber-Bedrohungen dar.

Für das nach wie vor sehr hohe Gefahrenpotential von Ransomware-Angriffen sind insbesondere auch Angriffsmethoden wie Leakware (Drohen mit Veröffentlichung geleakter Daten) und Wiper-Ransomware (dauerhafte Beschädigung oder Löschung von Daten) verantwortlich. Davon betroffen sind gleichermaßen Unternehmen, kritische Infrastrukturen, Forschungseinrichtungen sowie die öffentliche Verwaltung.

Bei den vielen Gruppierungen, die sich Angriffe mit Ransomware zum Geschäftsmodell gemacht hatten, dominierten im Berichtszeitraum u.a. Black Basta, LockBit 3.0, Alphv/BlackCat und Royal. Neben der Verschlüsselung der Daten ist aus datenschutzrechtlicher Sicht besonders schwerwiegend zu bewerten, dass die Daten in aller Regel vor der Verschlüsselung von den Angreifern abgegriffen werden. Diese Variante wird auch Double Extortion (doppelte Erpressung) genannt. Sie bietet den Angreifern nicht nur die Möglichkeit, ein Lösegeld für die Entschlüsselung der Daten zu verlangen, sondern auch damit zu drohen, die oftmals sensiblen Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird.

Die Hoffnung, dass angesichts geringer Zahlungsbereitschaft und nach der Auflösung der Ransomware-Gruppierung „Conti“ sowie anderer größerer Gruppierungen eine Konsolidierung im Bereich Ransomware eintreten würde, hat sich bedauerlicherweise nicht erfüllt. So traten in der zweiten Jahreshälfte 2023 fast zwei Dutzend neue Gruppen mit erstmaligen Angriffen im bayerischen Raum auf.

2 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.

Dabei hat sich die Tendenz verstärkt, vermehrt auf technische Angriffe zu setzen. So nutzen die Täter schnell und gezielt Schwachstellen in Software oder Systemen aus, um zum Ziel zu gelangen und setzen nicht nur auf den menschlichen Faktor (etwa E-Mails mit Schadcode).

Das BLKA registrierte in 2023 erneut einen Rückgang der Ransomwarefälle gegenüber den Vorjahren 2022 (ca. 580 Fälle) und 2021 (680 Fälle) auf ca. 340 angezeigte Fälle.

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 sowie das hohe Bedrohungspotenzial der Cyberkriminalität auf.

D DDOS[3]-ANGRIFFE (DISTRIBUTED DENIAL OF SERVICE)

Im Berichtszeitraum kam es immer wieder zu DDoS-Angriffen, die von den jeweiligen Tätergruppierungen im Vorfeld pressewirksam angekündigt wurden. Eine dieser Gruppen ist die seit März 2022 bekannte prorussische Gruppe NoName057(16). Sie führt Angriffe gegen die Ukraine und NATO-Staaten sowie gegen Personen durch, die sich öffentlich kritisch gegenüber Russland äußern. Ihre Angriffe proklamiert die Gruppe stets in einem ihrer Telegram-Kanäle.

E PHISHING[4] UND SOCIAL ENGINEERING

Im Bereich Social Engineering stellt das sog. Phishing nach wie vor die prominenteste Methode dar. Mittels in gefälschten E-Mails oder SMS-Nachrichten enthaltenen Links oder Dateianhängen soll das potentielle Opfer meist zur Preisgabe von Nutzer- und Bankdaten verleitet werden. Häufig handelt es sich um gezielte Kampagnen, sog. Spear-Phishing, als Basis für Cyber- oder Internetkriminalität. Mit

3 Unter Distributed Denial of Service (DDoS)-Angriffen versteht man die mutwillige Überlastung eines Internetdienstes durch eine Flut von Anfragen, mit dem Ziel, dass dieser die Menge der Anfragen nicht mehr bewältigen kann und den Dienst verweigert bzw. im schlimmsten Fall zusammenbricht. Hierfür kommt eine Vielzahl von unterschiedlichen Systemen in einem großflächig koordinierten Angriff zum Einsatz. Durch die hohe Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam. Ein DDoS-Angriff ist daran zu erkennen, dass sie deutlich mehr Netzressourcen als der normale Netzwerkverkehr beansprucht.

4 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.

den neuen Möglichkeiten generativer KI (Künstlicher Intelligenz) können sich Phishing-Kampagnen von den Angreifern noch einfacher planen und überzeugender vortragen lassen.

Zwar zeigen breit angelegte Schulungs- und Sensibilisierungsmaßnahmen bei Unternehmen, Behörden und der Bevölkerung insgesamt mittlerweile Wirkung. Die fortschreitende Entwicklung der KI führt jedoch dazu, dass das Risiko durch professionelles Phishing wächst und kontinuierliche Wachsamkeit sowie die Anpassung an neue Bedrohungen erforderlich sind.

Eine besonders ausgefeilte Methode, die in den letzten Jahren an Popularität gewonnen hat, ist das Phishing mittels Outlook Web App (OWA). Diese Methode nutzt die Vertrautheit vieler Benutzer mit der Microsoft Outlook-Umgebung aus, um sie zu täuschen und sie zu veranlassen, sensible Informationen preiszugeben. Der öffentliche Sektor ist besonders anfällig für Phishing-Angriffe, die auf OWA abzielen. Aufgrund der umfangreichen Nutzung von E-Mail-Plattformen wie Microsoft Outlook für die Kommunikation zwischen Behörden, Bürgern und anderen Interessensgruppen bieten öffentliche Institutionen ein attraktives Ziel für Cyberkriminelle.

F APT[5]-ANGRIFFE/CYBERSPIONAGE

Insbesondere vor dem Hintergrund des russischen Angriffskriegs gegen die Ukraine beobachteten Europäische Nachrichtendienste vermehrt großangelegte und gut

5 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.

koordinierte Angriffskampagnen gegen Unternehmen verschiedenster Bereiche, insbesondere aus dem Sicherheits- und Verteidigungssektor, sowie gegen Forschungseinrichtungen.

Zudem mehren sich die Hinweise auf weitergehende, längerfristige Ansätze chinesischer Cyberspionage, deren Ziel es ist, die digitale Souveränität der westlichen Staaten durch das Schaffen von Abhängigkeitsstrukturen zu unterwandern. Hierfür werden sämtliche Bereiche des Internets, aber auch Kooperationen – insbesondere zwischen Unternehmen und Forschungseinrichtungen –, Joint Ventures und soziale Netzwerke intensiv genutzt.

G HACKTIVISMUS

Im Berichtszeitraum wurde beobachtet, dass prorussische Gruppierungen wie Killnet und NoName057(16) DDos-Angriffe insbesondere auf die Webseiten von kritischen Infrastrukturen, Behörden und Kommunalverwaltungen weiter fortsetzten bzw. zu derartigen Angriffen aufriefen. Erfolgreiche Angriffe werden als propagandistisches Mittel genutzt, um die vermeintliche Schwäche westlicher Ziele und zugleich russische Stärke zu demonstrieren. Durch die Auswahl medienwirksamer Ziele erlangt „Killnet“ in Russland eine breite Aufmerksamkeit und besitzt dort, insbesondere unter Jugendlichen, einen gewissen Kultstatus.

Bisher haben registrierte DDoS-Angriffe pro-russischer Aktivisten („Hacktivismus“) nur geringe oder keine bleibenden Schäden verursacht. Die bayerischen Sicherheitsbehörden bewerten diese Angriffe eher als Propagandaaktionen, die darauf abzielen, Verunsicherung zu verbreiten und das Vertrauen in staatliche Institutionen zu untergraben. Erkenntnisse aus der globalen Sicherheitslage der vergangenen Jahre zeigen jedoch, dass sich einerseits die Strategie schnell ändern kann und andererseits die möglichen Schäden kaum absehbar sind.

H ONLINEBETRUG IM FINANZBEREICH (IDENTITÄTSDIEBSTAHL)

Das Umleiten von Zahlungsströmen („Payment Diversion Fraud") per E-Mail ist eine Betrugsmasche, die sich des Identitätsdiebstahls und des Social-Engineerings bedient. Die Betrüger geben sich als Geschäftspartner aus. Mit gefälschten oder „gephishten" Informationen wird die vorgetäuschte Identität glaubhaft gemacht und im weiteren Verlauf darauf hingewiesen, dass sich Zahlungsmodalitäten oder Bankdaten geändert hätten. Die Betrugsmasche ist relativ simpel und für die Täter äußerst lukrativ, da es sich bei den Opfern meist um Unternehmen handelt und der Beuteschaden häufig im fünf- bis sechsstelligen Bereich liegt. Aufgedeckt wird der Betrug häufig erst mit erheblicher zeitlicher Verzögerung, wenn Mahnungen für die vermeintlich bezahlte Ware oder Dienstleistung eingehen. Für das Versenden solcher Mahnungen lassen sich die Firmen oft Zeit, um zum Beispiel das Verhältnis zwischen den Geschäftspartnern nicht zu belasten. Somit ist die Möglichkeit einer Rückbuchung meist nicht mehr gegeben.

Im Berichtszeitraum wurden vom BLKA 380 derartiger Fälle verzeichnet. Nach 2022 (310) und 2021 (130) bedeutet das einen erneuten deutlichen Anstieg der Fallzahlen.

I DESINFORMATIONSKAMPAGNEN UND HYBRIDE BEDROHUNGEN

Im Zusammenhang mit dem Russland-Ukraine-Krieg wird weiterhin ein vermehrtes Auftreten von Desinformations- und Einflussnahmeaktivitäten beobachtet. Diese zielen darauf ab, das Vertrauen der deutschen Öffentlichkeit in die Verlässlichkeit von Politik und Medien zu untergraben und den gesellschaftlichen Zusammenhalt zu schwächen.

Die russische Cybergruppierung „Ghostwriter" hat in diesem Kontext Desinformations- und Einflussnahmeaktivitäten mit Cyberangriffen kombiniert. Betroffen waren erneut E-Mail-Konten von Personen im politischen Raum. „Ghostwriter" versucht auf diese Weise Passwörter zu erbeuten, um damit Zugang zu persönlichen Informationen in E-Mail-Postfächern und in den sozialen Medien zu erlangen und diese für Desinformation und Propaganda zu missbrauchen. Betroffene Personen wurden informiert und sensibilisiert.

Auch im Bereich der hybriden Bedrohungen eröffnet KI den Akteuren neue Möglichkeiten. Mittels KI können Desinformationskampagnen mittlerweile überzeugender gestaltet und mit deutlich reduzierten Aufwänden in den sozialen Medien verbreitet werden. Der Kostenfaktor wird hier durch KI quasi auf null gesetzt.

J CYBERTRADING, TRADING-SCAM, FAKE-SHOPS[6]

Wirtschaftliche Schäden von enormem Ausmaß werden weiterhin im Bereich des „Trading-Scam" (auch in Form des sog. „Pig Butchering") verursacht. Die Täter nutzen hierbei Fake-Profile auf Dating-Plattformen, bauen eine Beziehung zu ihren Opfern auf und verleiten diese dazu, ihr Geld bei betrügerischen Krypto-Plattformen zu investieren. Im Berichtszeitraum wurden bei der Zentralstelle Cybercrime Bayern (ZCB) ca. 170 Fälle mit einem Gesamtschaden von ca. 17 Millionen Euro angezeigt. Darüber hinaus sind Fake-Shops eine sehr aktuelle Kriminalitätsentwicklung, die – auch wenn die Schäden im Einzelfall vergleichsweise gering sind – in der Masse zu immensen Schäden führen. Fake-Shops treffen breite Schichten der Bevölkerung und führen zu einer tiefgreifenden Verunsicherung der Opfer. In einem maßgeblich im Jahr 2023 ermittelten Fall wurde von der ZCB im Februar 2024 der Betrieb von 52 Fakeshops zur Anklage gebracht, durch den die Täter einen Schaden von ca. 1,4 Millionen EUR verursacht haben.

K DEEPFAKE – MISSBRAUCH GENERATIVER KI

Auch die Bürgerinnen und Bürger in Bayern nutzen immer stärker moderne Kommunikationswege und müssen sich daher auch immer stärker vor kriminellen Übergriffen im Cyberraum schützen. Mit Tools wie ChatGPT, Bard, LLaMa und zahlreichen weiteren Anwendungen hat KI nun auch die technikferne Öffentlichkeit erreicht. Diese Tools sind benutzerfreundlich und liefern qualitativ hochwertige Ergebnisse, wodurch sie jedoch auch anfällig für kriminellen Missbrauch sind. Sie ermöglichen die Erstellung authentisch wirkender manipulierter Bilder, Videos und Stimmen – sog. Deepfakes – die immer schwieriger zu entlarven sind.

6 Bei Fake-Shops handelt es sich um einen Modus Operandi, bei dem mit Hilfe des Internets in kürzester Zeit eine große Anzahl an Warenbetrügereien zu begehen und ein Maximum an Beute zu erzielen ist. Hierzu richten die Täter scheinbar echte Online-Shops ein, in denen meist höherpreisige elektronische Geräte, Schmuck oder Markenkleidung zu besonders günstigen Preisen angeboten werden. Dann sorgen die Täter dafür, dass ihre vermeintlich seriösen Online-Shops bei den Treffern von einschlägigen Online-Such-maschinen relativ weit oben auf der Trefferliste erscheinen, um eine möglichst große Anzahl an Kaufwilligen zu erreichen. Als Zahlungsmöglichkeiten werden in den Shops meistens Vorkasse per Überweisung oder Kreditkartenzahlung angeboten. Nach erfolgter Zahlung warten die Käufer allerdings vergeblich auf die Lieferung der bezahlten Ware und bleiben aufgrund einer ggf. für sie unsicheren Zahlungsweise meist auf dem Schaden sitzen.

Die so erstellten Inhalte können dann bei vielen der oben geschilderten Angriffsszenarien zum Einsatz kommen. Die fortschreitende Entwicklung von KI verdeutlicht, dass das Risiko durch die modernen technischen Möglichkeiten sprunghaft anwächst und kontinuierliche Wachsamkeit sowie die Anpassung von Sicherheitsprozessen und Bekämpfungsstrategien an die neuen Bedrohungen erforderlich sind.

L DUNKELFELD

In allen oben aufgeführten Phänomenbereichen ist von einer erheblichen Dunkelziffer auszugehen. Als empirische Grundlage wird die Dunkelfeldbefragung des bundesweiten Viktimisierungssurvey des Bundeskriminalamts und der Polizei der Länder „Sicherheit und Kriminalität in Deutschland- SKiD 2020" herangezogen. Im Ergebnis wurden demnach nur 17,9 % der Straftaten angezeigt.

Als mögliche Ursachen für die Nichtanzeige kommen in Betracht, dass kein oder nur geringer Schaden verursacht wurde und/oder die Opfer durch ein öffentliches Bekanntwerden eines Angriffs geschäftsschädigende Reputationsschäden fürchten.

Zudem ist zu berücksichtigen, dass der Fokus der Betroffenen regelmäßig auf der schnellen Wiederherstellung der Verfügbarkeit der betroffenen IT-Systeme liegt.

III. MASSNAHMEN

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

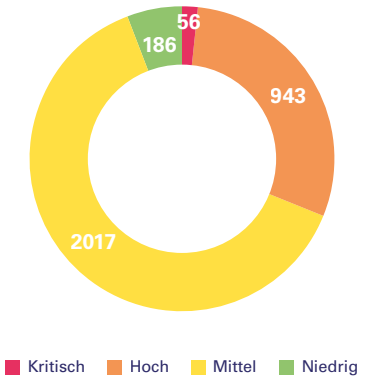
A PRÄVENTION & CYBERSICHERHEITSBERATUNG

Nach Maßgabe der Bayerischen Cybersicherheitsstrategie 2.0 wurden die unterschiedlichen, aufeinander abgestimmten Präventionsangebote von Polizei, Justiz und Verfassungsschutz für den Bereich Wirtschaft und Gesellschaft bedarfsgerecht weiterentwickelt.

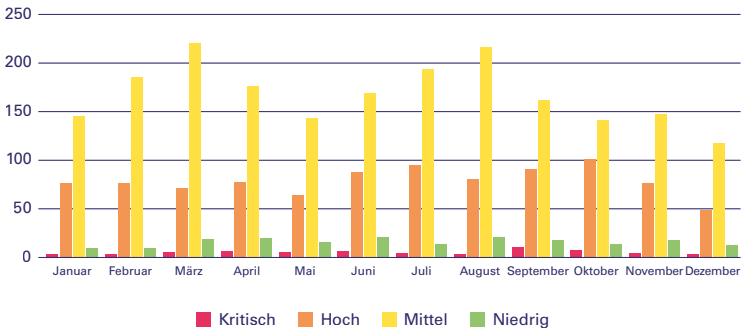
Beim BLKA wurde in der Vergangenheit die Zentrale Ansprechstelle Cybercrime (ZAC) als Single Point of Contact (SpoC) für Behörden, Unternehmen und Institutionen eingerichtet. Die ZAC ist unter der Hotline 089/1212-3300 erreichbar und steht als kompetenter Ansprechpartner bereit. Als einer der Schwerpunkte hat sich im Bereich der ZAC die Präventionsarbeit herauskristallisiert. So führte die ZAC im Berichtszeitraum 106 Präventionsveranstaltungen durch, in denen die Teilnehmer der verschiedenen Institutionen hinsichtlich der aktuellen Gefahren sensibilisiert und potentielle Lösungsmöglichkeiten dargelegt wurden. Das Credo ist hier „Hilfe zur Selbsthilfe" und das Heben des Themas IT-Sicherheit auf die höchsten Führungsebenen. Explizit für diese Hierarchieebenen bietet die ZAC die Möglichkeit, eventuelle Szenarien im Rahmen eines interaktiven Planspiels oder einer Krisenstabsübung (im Bereich KRITIS) zu beüben. Weiterhin konnten in zahlreichen Fällen Unternehmen aufgrund von Erkenntnissen aus laufenden polizeilichen Ermittlungsverfahren rechtzeitig vor einer unmittelbar bevorstehenden Verschlüsselung gewarnt werden.

Der kostenfreie Warn- und Informationsdienst des LSI informiert über die neuesten Gefährdungslagen und Risiken. Mit tagesaktuellen Warnmeldungen der IT-Sicherheitsexperten kann potentiellen Bedrohungen frühzeitig begegnet werden. Der Warndienst unterstützt damit Behörden und Kommunen in ganz Bayern, sich noch besser vor Cyberangriffen zu schützen. In den Warnmeldungen werden konkrete Anhaltspunkte zu dem jeweiligen Sicherheitsrisiko bzw. den bereits ermittelten Angriffen genannt. Flankiert werden die Warnhinweise oftmals auch durch direkte Information und Beratung der betroffenen oder potenziell betroffenen Institutionen. Im Berichtszeitraum wurden insgesamt 3202 neue Meldungen zu Schwachstellen veröffentlicht. Die jeweilige Kritikalität dieser Meldungen ist in den nachfolgenden Grafiken aufgeschlüsselt.

WARNMELDUNG NACH KRITIKALITÄT



WARNMELDUNGEN NACH MONAT



Neben Angeboten für staatliche Stellen bietet das LSI für den kommunalen Bereich das Siegel „Kommunale IT-Sicherheit". Zusätzlich werden technische Orientierungshilfen und Unterlagen für ein Notfallmanagement, laufende Angriffswellen und andere Bedrohungen bereitgestellt. Das LSI bietet einen kostenfreien Online-Mitarbeitersensibilisierungskurs für die öffentliche Verwaltung – Staat und Kommunen – und konkrete technische Beratung zu allen Fragen der IT-Sicherheit.

Zusätzlich 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.

Das Cyber-Allianz-Zentrum Bayern (CAZ) im Bayerischen Landesamt für Verfassungsschutz beteiligte sich im Berichtszeitraum an zahlreichen Informations- und Sensibilisierungsveranstaltungen. Dabei standen neben den Hinweisen auf allgemeine Spionageaktivitäten ausländischer Dienste, beispielsweise im Rahmen von Delegationsreisen in bestimmte Staaten, die Warnung vor Cyberangriffen gegen Parlamente und Mandatsträger im Vordergrund.

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.

Mit den im Jahr 2021 installierten Cybercrime „Quick-Reaction-Teams" (QRT) gewährleistet die Polizei eine Rund-um-die-Uhr-Verfügbarkeit qualifizierter Fachkräfte, um zeitnah auf die teilweise existenzbedrohenden Gefahren für die Unternehmen reagieren zu können. Durch den Einsatz der QRT kann der betroffenen Institution Unterstützung im technischen Bereich, z.B. bei der Netzwerkseparierung und im Rahmen eventueller Verhandlungen mit den Tätern gewährt werden. Die QRT kamen im Berichtszeitraum bayernweit in 127 Fällen zum Einsatz.

Die Bürgerhotline der Bayerischen Polizei für IT-Notfälle (089/1212-4400) wurde im Berichtszeitraum 1083-mal von Bürgerinnen und Bürgern in Anspruch genommen. 593 Telefongespräche hatten Cybercrime-Straftaten zum Inhalt. In 262 Fällen konnte der Anrufer präventiv beraten werden.

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

In komplexen und schwerwiegenden Fällen von Cybercrime, dazu zählen insbesondere Cyberangriffe auf Unternehmen und öffentliche Einrichtungen, ermittelt die im Jahr 2015 gegründete ZCB bei der Generalstaatsanwaltschaft Bamberg. Dort sind für die Schwerpunktbereiche des Cybertradings, der Fake-Shops und der Cyberangriffe auf Unternehmen und öffentliche Einrichtungen bereits in der Vergangenheit erfolgreiche Spezialeinheiten gebildet worden, die personell weiter ausgebaut und verstärkt wurden. Zur Verbreiterung der Ermittlungsmöglichkeiten auf dem Gebiet der Fake-Shops wurde im August 2023 zudem eine Kooperation mit dem Austrian Institute of Technology (AIT) geschlossen, um gemeinsam den dort entwickelten KI-gestützten „Fake-Shop-Detektor" für den Einsatz im Rahmen der Strafverfolgung zu optimieren. Da Cyberkriminelle nahezu ausschließlich aus dem Ausland operieren, pflegt die ZCB darüber hinaus seit Jahren unter anderem sehr gute Kontakte zu INTERPOL: So fand etwa am 10. und 11. Oktober 2023 das gemeinsam von INTERPOL und dem Staatsministerium der Justiz ausgerichtete "Interpol New Technologies Expert Forum 2023" in Erlangen statt, eine internationale Tagung, an der 73 Personen aus 32 Ländern teilnahmen.

IT-Sicherheitsvorfälle im Aufgabenbereich des LSI werden im Lagezentrum des LSI aufgenommen und durch die IT-Sicherheitsexperten des Bayern-CERTs bearbeitet. Bei größeren Vorfällen, sog. Major Incidents, wird eine Task Force eingerichtet, die sich ausschließlich um die Eindämmung, Behandlung und forensische Analyse des jeweiligen Vorfalls kümmert. Das LSI informiert in seinem täglichen IT-Sicherheitslagebericht über aktuelle Vorfälle, Auffälligkeiten sowie neueste Entwicklungen und Bedrohungen im Bereich der IT-Sicherheit, insbesondere in Bezug auf die IT-Sicherheitslage für die bayerische Staatsverwaltung.

Die IT-Sicherheitsexperten des LSI unterstützen auch bei Vorfällen in Kommunen oder Unternehmen der kritischen Infrastruktur. Hierbei ist eine enge Abstimmung mit der Bayerischen Polizei ein entscheidender Erfolgsfaktor.

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 Berichtszeitraum hat das LSI über 5.200 Auffälligkeiten und Angriffe auf das bayerische Behördennetz registriert, von denen rund 3.000 zu schwerwiegenden Auswirkungen hätten führen können. In keinem dieser Fälle ist es den Angreifern gelungen, ein System im Behördennetz in einer nachhaltig kritischen Weise zu kompromittieren. Die technischen und operationellen Maßnahmen im Lagezentrum des LSI und im IT-Dienstleistungszentrum des Freistaats Bayern (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 unterstützte das ISMS-Förderprogramm für bayerische kommunale Gebietskörperschaften. Hierbei wurden die Kommunen insbesondere auch bestärkt, das Siegel „Kommunale IT-Sicherheit" des LSI zu erwerben. Bei der Beratung der Kommunen arbeiteten das 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 Cyberabwehr Bayern (CAB) bereits zum Jahresanfang 2020 der notwendige organisatorische Rahmen geschaffen.

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. Ausgehend von den in der Pilotphase identifizierten Mehrwerten für die Arbeit der CAB ist es ein wichtiges Anliegen, diese horizontale Vernetzung zu verstetigen. Ebenso ist die GenStA Bamberg, ZCB, als einer der Vertreter der Länderstaatsanwaltschaften beim Cyber-AZ vertreten.

Auch im Bereich der öffentlichen IT-Sicherheit ist die ebenenübergreifende Kooperation zwischen LSI und BSI sowie anderen Länder-IT-Sicherheitsbehörden ein entscheidender Erfolgsfaktor. 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 den aktiven Austausch in CERT-Verbünden, wie beispielsweise dem Verwaltungs-CERT-Verbund (VCV).

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 hohen Reaktionsfähigkeit sehr bewährt hat.

Um für Vorfälle im Cyberraum besser gewappnet zu sein, fand im Berichtszeitraum auch die Länder- und Ressortübergreifende Krisenmanagementübung LÜKEX 23 statt. Bei diesem zum neunten Mal stattfindenden Planspiel übten Bundesbehörden sowie Bundes- und Landesregierungen gleichzeitig. Das Übungsszenario war ein großangelegter Cyberangriff auf Regierung und Verwaltung, bei dem ein großflächiger Stromausfall in einem der bayerischen staatlichen Rechenzentren simuliert wurde. Die Projektleitung für Bayern hat das LSI übernommen.

Dem Ziel aus der Bayerischen Cybersicherheitsstrategie 2.0 folgend, sind auch für die Zukunft gemeinsame Übungen der Bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben geplant, um die effektive operative Zusammenarbeit bei großen Cyber-Lagen stetig weiterzuentwickeln und mit praxisnahen Anwendungsfällen in behördenübergreifenden Szenarien zu trainieren.

IV. AUSBLICK

Nach Einschätzung der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben wird die Cyber-Sicherheitslage in Bayern auch in Zukunft von mehreren dynamischen und teils besorgniserregenden Trends geprägt sein.

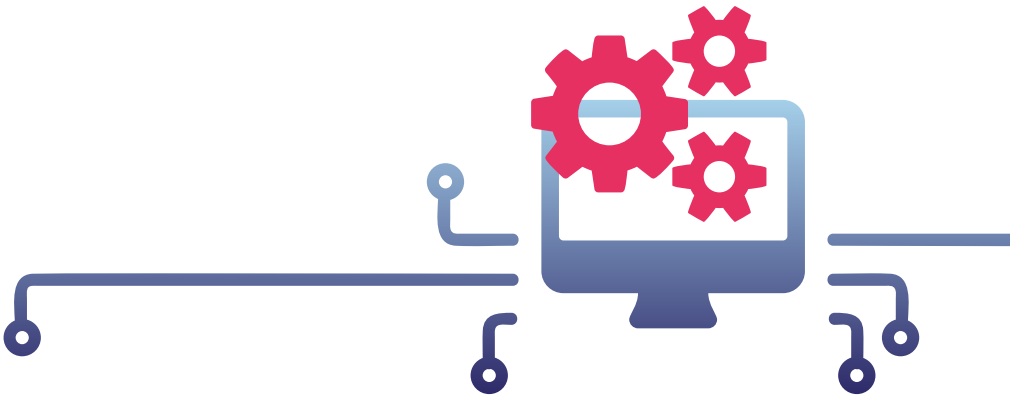
Es wird eine weiter zunehmende Komplexität und Frequenz von Cyberangriffen erwartet. Cyberkriminelle nutzen immer raffiniertere Techniken und Werkzeuge, um Sicherheitslücken auszunutzen. Insbesondere Ransomware-Angriffe werden als eine der größten Bedrohungen angesehen, da sie kritische Infrastrukturen und Unternehmen erheblich schädigen können. Kritische Infrastrukturen wie Energieversorgung, Gesundheitswesen, und Transportwesen müssen damit rechnen, verstärkt in den Fokus von Angreifern zu geraten. Diese Sektoren sind besonders anfällig für Angriffe, die auf eine Störung oder Sabotage abzielen.

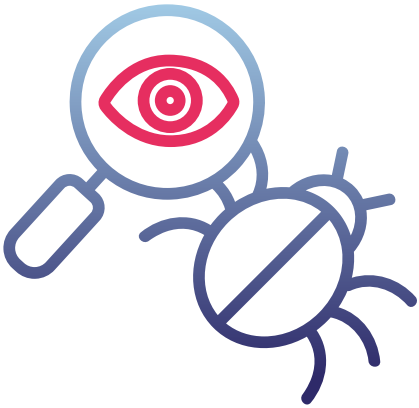
Eine effektive und nachhaltige Absicherung der IT-Infrastrukturen wird daher immer wichtiger, insbesondere angesichts der zunehmenden digitalen Vernetzung. Sowohl Angreifer als auch Verteidiger werden weiter zunehmend KI und Automatisierung einsetzen. Angreifer nutzen KI, um Phishing-Angriffe zu personalisieren und Malware zu entwickeln, die traditionellen Erkennungsmethoden ausweicht. Gleichzeitig setzen Verteidiger KI ein, um Anomalien zu erkennen und auf Bedrohungen schneller zu reagieren.

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 in diesem Kontext von der Bayerischen Staatsregierung im November 2023 verabschiedeten Bayerischen Cybersicherheitsstrategie 2.0 wird den aktuellen und zukünftigen Herausforderungen Rechnung getragen.

WEITERFÜHRENDE INFORMATIONEN

CYBERSICHERHEIT IN BAYERN – BROSCHÜREN ZUM DOWNLOAD





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 2024
Druck: 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.x.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