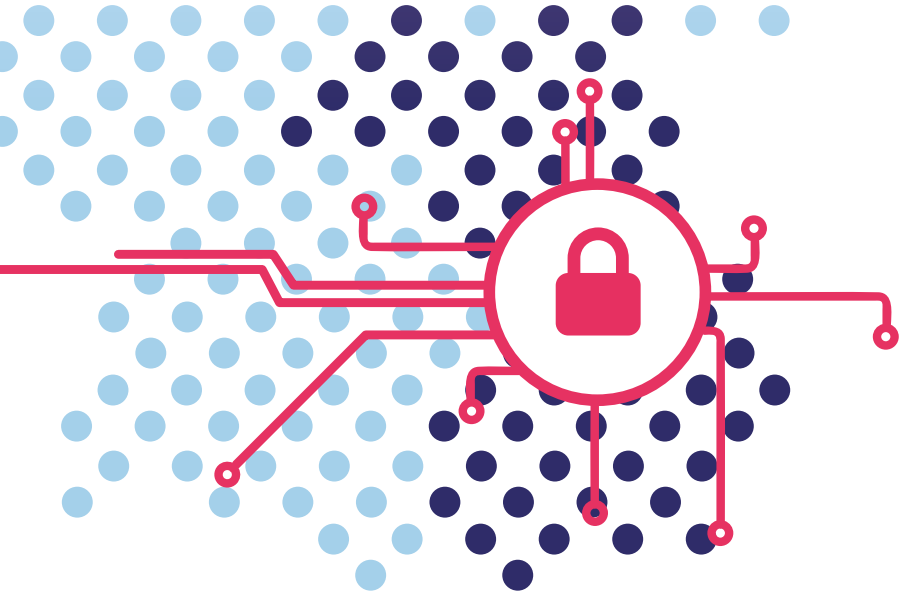
Bayerisches Staatsministerium des
Innern, für Sport und Integration

Bayerisches Staatsministerium der
Finanzen und für Heimat

CYBERSICHERHEIT IN BAYERN 2022

Bericht zur Cybersicherheit in Bayern



VORWORT

Die Digitalisierung unserer Gesellschaft schreitet stetig voran und hat nahezu alle Lebensbereiche durchdrungen. Damit wachsen aber auch die Herausforderungen an die Sicherheit von IT-Systemen und für die innere Sicherheit.

Vor allem Cyberkriminalität ist schon längst keine abstrakte Gefahr mehr, sondern zur alltäglichen Bedrohung von Staat, Kommunen und Wirtschaft, aber auch der Bürgerinnen und Bürger geworden. Schwachstellen in Software und Kryptowährungen, wie Bitcoin, erleichtern es den Tätern, insbesondere mithilfe des Einsatzes von Ransomware teilweise verheerende Schäden zu verursachen.

Cybersicherheit ist daher unstreitig einer der Schlüsselfaktoren der digitalen Transformation und eine wichtige gesamtgesellschaftliche Aufgabe geworden.

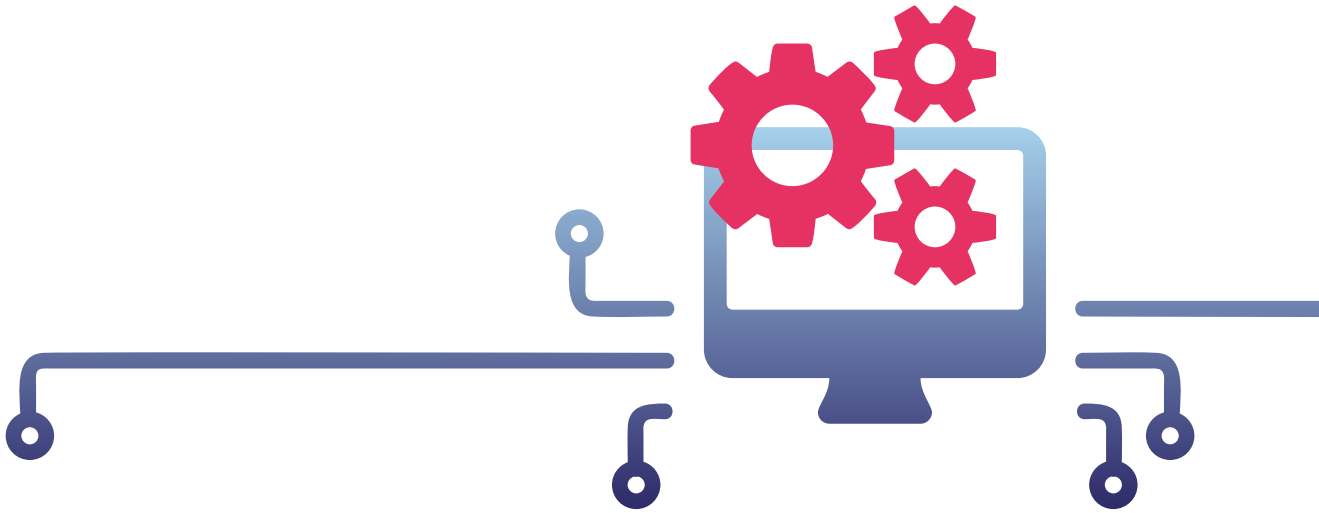
Bayern ist in Sachen Cybersicherheit bereits hervorragend aufgestellt. Das ist das Ergebnis einer konsequenten und erfolgreichen Sicherheitspolitik. Um entschlossen und wirkungsvoll auf aktuelle Bedrohungen reagieren zu können, hat Bayern starke, hochspezialisierte Einheiten bei Polizei, Staatsanwaltschaften und Verfassungsschutz geschaffen sowie das bundesweit erste Landesamt für Sicherheit in der Informationstechnik gegründet.

Eine enge Zusammenarbeit der Behörden mit Cybersicherheitsaufgaben, insbesondere eine gemeinsame Beurteilung der Cybersicherheitslage wird durch die behördenübergreifende Informations- und Kooperationsplattform „Cyberabwehr Bayern" gewährleistet. Wie dieser Bericht zur Cybersicherheit in Bayern aufzeigt, bleiben wir mit einer steigenden Bedrohungslage konfrontiert. Wir dürfen uns deshalb nicht auf dem bereits Erreichten ausruhen, sondern sind gemeinsam gefordert, die Resilienz unserer Wirtschaft, Gesellschaft und Verwaltung gegen Cyberangriffe zu verbessern, um ein höchstmögliches Schutzniveau in der Cybersicherheit zu erreichen.

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

Albert Füracker, MdL
Bayerischer Staatsminister
der Finanzen und für Heimat

INHALT



I. AUSGANGSLAGE

Die Bedrohungen im Cyberraum nehmen weiter rasant zu. Allein im vergangenen Jahr hat ein unabhängiges Forschungsinstitut für IT-Sicherheit in Deutschland täglich mehr als 450.000 neue Schadprogramme (Malware) und andere potentiell unerwünschte Anwendungen registriert.[1]

Die Angreifer nutzen fortwährend neue Angriffsstrategien und organisieren sich zum Teil hochprofessionell in der Anonymität des Darknets. Sie agieren über Landesgrenzen hinweg, verursachen hohe Schäden und stellen mitunter eine reale Gefahr für unsere Demokratie und die wirtschaftlichen Grundlagen unserer Gesellschaft dar.

Auf diese dynamische Bedrohungslage hat Bayern bereits 2013 mit einer eigenen Cybersicherheitsstrategie reagiert und in deren Umsetzung eine schlagkräftige Cybersicherheitsarchitektur errichtet sowie bedarfsorientiert fortentwickelt. Zu den bei Polizei, Justiz und Verfassungsschutz auf Cyberkriminalität und Cyberspionage spezialisierten Einheiten gehören u.a. die Zentrale Ansprechstelle Cybercrime (ZAC) im Bayerischen Landeskriminalamt (BLKA), das Cyber-Allianz-Zentrum Bayern (CAZ) beim Landesamt für Verfassungsschutz (BayLfV) sowie die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg.

2017 hat Bayern als erstes Land ein Landesamt für Sicherheit in der Informationstechnik (LSI) mit gesetzlich geregelten Aufgaben und Befugnissen zum Schutz der staatlichen IT-Infrastrukturen, kommunaler IT-Sicherheit und für kritische Infrastrukturen (KRITIS) errichtet. Damit war Bayern zudem das erste Land mit einem IT-Sicherheitsgesetz. Das seit 2003 bestehende Bayern-CERT [2] wurde in das LSI integriert.

Als neue zentrale Informations- und Koordinationsplattform der genannten Behörden untereinander sowie dem Landesbeauftragten für den Datenschutz (BayLfD) und dem Landesamt für Datenschutzaufsicht (LDA), wurde im Januar 2020 die „Cyberabwehr Bayern“ etabliert.

Bayern ist mit den spezialisierten Stellen bei Polizei und Verfassungsschutz, dem LSI als Fachbehörde für IT-Sicherheit und der institutionalisierten Vernetzung in der Cyberabwehr Bayern gut aufgestellt. Zur weiteren Stärkung der Cybersicherheit ist eine fortlaufende Beobachtung und Bewertung der Lage sowie eine entsprechende Anpassung der Maßnahmen erforderlich.

Das im folgenden dargestellte Lagebild fußt einerseits auf den Erkenntnissen und Einschätzungen der mit Cybersicherheit befassten Stellen in den Geschäftsbereichen von StMI und StMFH. Zu Grunde liegt andererseits das im Rahmen der Cyberabwehr Bayern durch den kontinuierlichen operativen Austausch der Behörden mit Cybersicherheitsaufgaben entstandene behördenübergreifende Cyberlagebild aus dem Berichtsjahr 2021.

1 Quelle: AV Test GmbH- https://www.av-test.org/de/statistiken/malware/

2 Ein Computer Emergency Response Team (CERT), deutsch Computersicherheits-Ereignis- und Reaktionsteam ist eine Gruppe von EDV-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen (z. B. Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebssystemen, neuartige Virenverbreitung, bei Spam versendenden PCs oder gezielten Angriffen) als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst, Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet.

II. ALLGEMEINES LAGEBILD ZUR CYBERSICHERHEIT IN BAYERN

Die Bedrohungslage für Wirtschaft, Staat und Gesellschaft sowie Kommunen in Bayern war in 2021 – entsprechend dem Trend im Bund – auf einem anhaltend hohen Niveau. Dies schlägt sich auch in tendenziell steigenden Angriffszahlen nieder.

Im Jahr 2021 bestimmten vor allem folgende Phänomene die Sicherheitslage in Bayern[3]:

A SCHWACHSTELLEN UND KONFIGURATIONSFEHLER

Kritische Schwachstellen in der Java-Bibliothek log4j:

Herausragend in Bezug auf das mögliche Schadenspotential war die Schwachstelle in der Java-Bibliothek log4j, die im Dezember 2021 bekannt wurde. Bei einer Bibliothek handelt es sich um einen Codebaustein, der in einer Vielzahl von Programmen und Produkten verwendet wird. Entsprechend aufwändig war die Bewältigung allein für die staatlichen IT-Systeme durch die Behörden. So hat das LSI 7.500 Webserver, die dem Freistaat Bayern zugeordnet werden konnten, auf Auffälligkeiten gescannt. Bisher wurden im Bereich der öffentlichen IT in Bayern keine auf der log4j-Schwachstelle beruhenden Schäden bekannt.

Kritische Schwachstellen in Microsoft-Produkten:

Schwachstellen in Microsoft-Produkten wie dem Verzeichnisdienst Active-Directory oder Exchange führten zu einer erheblichen Gefährdung, insbesondere, wenn notwendige Patches nicht zeitnah eingespielt wurden. Vorliegende Erkenntnisse lassen darauf schließen, dass eine erhebliche Verwundbarkeit von Systemen in Bayern bestand bzw. weiterhin besteht und die entscheidende Bedeutung des zeitnahen Patchens zu häufig unterschätzt wird. Daraus resultieren, selbst noch ein Jahr nach Veröffentlichung entsprechender Sicherheitspatches, zahlreiche gravierende Sicherheitsvorfälle bei Einrichtungen in Bayern.

Durch bekannte Einzelfälle gilt als gesichert, dass solche Schwachstellen auch von ausländischen Akteuren genutzt werden, um unauffällig einen langfristigen Zugang zu Systemen zu sichern.

B RANSOMWARE[4]

Ransomware ist nicht zuletzt wegen der zunehmenden Verbreitung von Kryptowährungen, wie z. B. Bitcoin, zum Leitphänomen der Cyberkriminalität geworden. Durch die Begleichung von Lösegeldforderungen in einer Kryptowährung können die Täter weitgehend anonym und ohne eigenes Risiko vollständig vom Ausland aus agieren.

Trotz der Zerschlagung des sog. Emotet-Netzwerkes durch die Europol-Operation „Ladybird" ist Ransomware auch in Bayern vorherrschend geblieben. Die weltweit dominierenden Schadcodekampagnen, wie Conti, Lockbit, QLocker, Phobos oder SquirrelWaffel wurden auch in Bayern festgestellt.

Die bayerischen Fallzahlen, Lösegeldforderungen und Lösegeldzahlungen steigen und erreichten im Jahr 2021 neue Höchststände:

- Das BLKA registrierte in 2021 einen Anstieg der Crypto-Ransomware von über 25 % gegenüber dem Vorjahr 2020 (ca. 300 Fälle) auf ca. 380 angezeigte Fälle.

- Beim LDA sind 315 Meldungen (2020: 221 Meldungen) von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-Grundverordnung bei Wirtschaftsunternehmen durch Ransomware bekannt geworden.

3 Hierbei handelt es sich um eine qualitative Auswahl nach Risiko/Kritikalität (Schadenshöhe, Eintrittswahrscheinlichkeit) und/oder medialer Aufmerksamkeit des jeweiligen Phänomen-/Deliktsbereichs. Die Kennzahlen hierfür wurden innerhalb der Cyberabwehr Bayern abgestimmt. Die Aufstellung weicht insoweit von den Fallzahlen der polizeilichen Kriminalstatistik (PKS) ab und erhebt auch keinen Anspruch auf quantitative Vollständigkeit. Die Reihenfolge der Auflistung stellt keine Wertung/Priorisierung dar.

4 Bei Ransomware handelt es sich um Schadsoftware, bei der nach erfolgreicher Infektion häufig die Daten des Opferns zuerst ausgeleitet und auf den IT-Systemen verschlüsselt werden. Um die Opfer zur Zahlung der Lösegeldforderungen zu bewegen, werden diese ggfs. sowohl mit einer beschädigten IT-Infrastruktur als auch mit der Drohung einer Veröffentlichung der gestohlenen Daten doppelt unter Druck gesetzt. Der Entschlüsselungs-Key wird im besten Falle nach Zahlung einer Lösegeldforderung durch die Täter zur Verfügung gestellt.

- Auch öffentliche Stellen im Freistaat waren vor Ransomware-Attacken nicht gefeit. Im Berichtszeitraum sind Angriffe auf öffentliche Stellen im unteren einstelligen Bereich bekannt geworden. Dazu gehören beispielsweise erfolgreiche Angriffe auf die Gemeinde Kammeltal oder die Verwaltungsgemeinschaft Aurachtal. LSI, BLKA sowie weitere Behörden waren unverzüglich eingebunden und konnten durch gute Zusammenarbeit zur Analyse, Lagebewältigung und präventive Beratung beitragen. In allen dokumentierten Fällen wurde Lösegeldforderungen seitens öffentlicher Stellen nicht nachgekommen.

C PHISHING[5]

Der Diebstahl von Zugangsdaten durch sogenanntes „Phishing" tritt in Bayern nach wie vor häufig auf und ist regelmäßig Basis für Cyber- oder Internetkriminalität. Professionelle und gezielte Phishingangriffe, sogenanntes „Spear Phishing", wurde im Berichtszeitraum insbesondere im Bereich der bayerischen Hochschulen verzeichnet. Dabei wurden die Angehörigen der Hochschulen u.a. durch täuschend echt nachgemachte Internetseiten der Hochschulrechenzentren verleitet, dort deren Zugangsdaten einzugeben und somit dem Angreifer preiszugeben. An den Sicherheitsinstanzen des Bayerischen Behördennetzes wurden 2021 rund 280 Millionen Phishing-E-Mails geblockt, was die Dimension dieser Bedrohung unterstreicht.

D IDENTITÄTSDIEBSTAHL

Erhebliche Fallzahlen, insgesamt ca. 21.000 Anzeigen, hat die Bayerische Polizei beim Identitätsdiebstahl verzeichnet. So wurden ca. 16.000 Fälle von Accounteröffnungen (unter missbräuchlicher Verwendung fremder personenbezogener Daten) zur Anzeige gebracht (2020: ca. 14.000 Anzeigen/ +14,3 %). Dies dient häufig als Vorbereitungshandlung, um im Anschluss beispielsweise unter falscher Identität Bestellung auf Rechnung zu tätigen (Warenkreditbetrug). Die Übernahme bestehender Benutzerkonten (Account-Hijacking) ist im Berichtszeitraum hingegen zurückgegangen. Insgesamt kam es 2021 zu ca. 5.000 Anzeigen (2020: ca. 8.000 Anzeigen/- 37,5 %). Als Grund für den Rückgang ist neben einer höheren Sensibilität der Benutzer (z.B. Verwendung sicherer Passwörter) auch die zunehmende Implementierung fortgeschrittener Sicherheitsmerkmale, wie etwa die 2-Faktor-Authentifizierung oder OTP[6]-Mechanismen durch die Dienstebetreiber zu vermuten.

Bei der Bayerischen Polizei wurden ferner ca. 170 Fälle von „Payment Diversion Fraud" verzeichnet, einer Betrugsform, die insbesondere aufgrund der hohen erbeuteten Summen herausragt. Opfer sind hier meist (größere) Unternehmen, denen mit gefälschten oder durch vorgeschaltete Social Engineering-Kampagnen oder Cyberangriffe gewonnenen Informationen die Identität eines Geschäftspartners vorgetäuscht und dadurch Finanztransaktionen veranlasst werden.

E APT[7]-ANGRIFFE, CYBERSPIONAGE UND SUPPLY-CHAIN-ANGRIFFE

Im Bereich der Cyberspionage (Informationsbeschaffung) und Cybersabotage (Schädigung) stehen auch in 2021 gezielte Angriffe auf Wirtschaftsunternehmen durch sog. APT-Gruppierungen im Aufklärungsfokus des Verfassungsschutzes. Ziel ist hierbei regelmäßig die Gewinnung von Erkenntnissen zu den Zielvorstellungen der Täter sowie deren Infrastrukturen, Taktiken, Werkzeuge und Methoden sowie die Identifizierung der potenziellen Opferstrukturen.

Im Berichtszeitraum wurden durch das BayLfV vermehrt Cyberangriffe durch APT-Gruppen auf Forschungseinrichtungen und Wirtschaftsunternehmen in Bayern registriert. Durch staatliche Unterstützung erhalten derartige Gruppierungen Zugang zu modernsten Technologien und können mithilfe dieser Möglichkeiten ihre Aufgabe entsprechend professionell ausführen. Im Fokus der APT-Gruppierungen liegen zumeist Organisationen aus dem öffentlichen Sektor, KRITIS-Betreiber, innovative Wirtschaftsunternehmen und Forschungseinrichtungen.

Prominente Einfallstore sind regelmäßig Sicherheitslücken, die von den Akteuren gezielt gesucht und ausgenutzt werden. Im Zusammenhang mit der Ausnutzung einer Schwachstelle in Microsoft-Exchange standen zunächst Einrichtungen aus Forschung, Wissenschaft sowie Rüstung im Fokus. Aufgrund der angegriffenen Zielgruppen liegt die Vermutung einer durch ausländische Nachrichtendienste gesteuerten Kampagne nahe. Jedoch konnten auch Cyberkriminelle und kriminelle APT-Gruppen als Drahtzieher nicht ausgeschlossen werden.

5 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.

6 one-time-password (Einmalpasswort): Kennwort zur einmaligen Autorisierung/Authentifizierung.

7 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.

Ein weiterer zu beobachtender Trend waren verstärkte Angriffe über Lieferketten. Bei sog. „Supply-Chain-Attacks" machen sich die Angreifer oft die weniger geschützten Systeme bei Zulieferbetrieben größerer Konzerne für ihre Zwecke zunutze.

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.

F DUNKELFELD

Aufgrund der Erkenntnisse der Behörden und Einrichtungen mit Cybersicherheitsaufgaben und von Studien (z.B. repräsentative Unternehmensbefragung des kriminologischen Forschungsinstituts Niedersachsens e.V. von 2018/19) 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 ohnehin sorgsam aufgeklärt werden müssen, um einerseits Angriffstechniken zu verstehen, damit so Risiken für andere IT-Systeme verringert werden können, und andererseits um Täterspuren forensisch zu sichern.

III. MASSNAHMEN

Die von den für Cybersicherheit zuständigen Behörden umgesetzten Maßnahmen orientieren sich neben dem gesetzlichen Auftrag an den jeweils bestehenden Gefährdungen.

Die oben dargestellte Lage erfordert sowohl eine Intensivierung der individuellen Anstrengungen als auch ein starkes behördenübergreifendes Zusammenwirken. Dies ist insbesondere mit folgenden Maßnahmen gewährleistet:

A PRÄVENTION & CYBERSICHERHEITSBERATUNG

Für den Bereich Wirtschaft und Gesellschaft stellen Polizei und Verfassungsschutz unterschiedliche, sich optimal ergänzende Präventionsangebote bereit, um bestmöglich auf Cyberangriffe vorbereitet zu sein. Hierzu gehört u.a. eine zielgruppenorientierte Verteilung von Warnmeldungen und Informationen zu Cybergefahren, aktuellen Kriminalitätsphänomenen (wie z.B. Phishing-Wellen) oder die Vermittlung sicherheitsbezogener Digitalkompetenz.

Für den kommunalen Bereich bietet das LSI neben dem Siegel „Kommunale IT-Sicherheit", technischen Orientierungshilfen, Unterlagen für ein Notfallmanagement, einem neuen Portal für den Warn- und Informationsdienst zu Sicherheitslücken, 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. Im Fokus stehen dabei neben der öffentlichen Verwaltung derzeit auch öffentliche Unternehmen der kritischen Infrastruktur wie Krankenhäuser und Wasserversorger.

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. Zudem ist mittlerweile bei jeder Kriminalpolizeiinspektion ein spezialisiertes Kommissariat „Cybercrime" 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 gewährleistet.

In komplexen und schwerwiegenden Fälle 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. Bei Vorfällen in Kommunen oder öffentlichen Unternehmen der kritischen Infrastruktur unterstützen IT-Sicherheitsexperten des LSI die Betroffenen bei der Abarbeitung. Hierbei ist eine enge Abstimmung mit der Polizei ein entscheidender Erfolgsfaktor. Notwendigenfalls kann auch mit Vor-Ort-Einsätzen Unterstützung geleistet werden. Aus der Bearbeitung der Vorfälle erfolgt eine konkrete, technische Beratung für alle anderen Institutionen der jeweiligen Zielgruppe durch das LSI. Gemäß dem Grundsatz „security is for sharing" verzahnt sich das LSI mit der IT-Sicherheitscommunity, sei es durch Kooperationen im wissenschaftlichen Umfeld oder durch die Mitarbeit in CERT-Verbünden.

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. Dabei 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.

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 Kommunen des StMI. Hiermit werden auch Kommunen unterstützt, die das Siegel „Kommunale IT-Sicherheit" des LSI anstreben. 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) seit Frühjahr 2021 hat Bayern außerdem eine wichtige Scharnierfunktion zum Bund geschaffen. Ebenso ist die ZCB seit Juni 2021 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. Herauszuheben ist dabei der schnelle, technische und konkrete Informationsaustausch im sog. Verwaltungs-CERT-Verbund (VCV).

IV. AUSBLICK

LAGEENTWICKLUNG IM ZUSAMMENHANG MIT DEM KRIEG IN DER UKRAINE

Seit Beginn des russischen Angriffskriegs auf die Ukraine am 24. Februar 2022 werden die militärischen Auseinandersetzungen in der Ukraine verstärkt auch von Feindseligkeiten im Cyberraum begleitet. Dabei ist festzustellen, dass Cyberangriffe mit mutmaßlich russischem Ursprung im Rahmen von gezielten Angriffskampagnen oder durch hacktivistische Gruppierungen vorrangig gegen ausgewählte Unternehmen in der Ukraine als Mittel der hybriden Kriegsführung eingesetzt werden.

Damit einher geht eine erhöhte abstrakte Gefahr für bayerische Einrichtungen und Unternehmen. Nach Einschätzung der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sind sowohl Kollateralschäden dieser Angriffe als auch zielgerichtete Angriffe, beispielsweise auf Energieversorger und andere Betreiber kritischer Infrastrukturen möglich. Ebenso schließen sich, wie schon zu beobachten war, kriminelle Hackergruppierungen im virtuellen Raum einer der beiden Kriegsparteien an und beteiligen sich durch Cyberangriffe an dem Kriegsgeschehen mit Auswirkungen auf Deutschland und auch Bayern. Neben Cyberangriffen sind zudem Einflussnahmebemühungen gegen den politischen und medialen Raum im Netz festzustellen. Dazu gehört die gezielte Verbreitung von Desinformations- und Propagandaaktivitäten, um Einfluss auf das öffentliche Meinungsbild zu gewinnen. Hierbei bedient sich Russland verschiedener Narrativ- und Propaganda-Elemente, um eine moralische Unschuld oder Überlegenheit Russlands zu kommunizieren. Zusammenfassend ist derzeit jedoch festzustellen, dass sich das im Kontext des Ukrainekriegs vorhandene Bedrohungspotenzial durch Cyberangriffe im ersten Halbjahr 2022 bei Weitem noch nicht voll entfaltet hat.

PROGNOSE

Die Bedrohungslage durch Cyberangriffe wird stetig weiter steigen. Die Cyberangriffe im Zusammenhang mit dem Krieg in der Ukraine sind nur ein Indiz dafür. Mit Blick auf die weiter stark vorangetriebene Digitalisierung ist davon auszugehen, dass vor allem geschäftskritische Abhängigkeiten von funktionierenden IT-Systemen weiter zunehmen werden. Damit einher gehen breitere Angriffsmöglichkeiten, die von staatlichen Akteuren, vor allem aber auch von Cyberkriminellen ausgenutzt werden können.

Die staatlichen Maßnahmen zur Gewährleistung eines hinreichenden Cybersicherheitsniveaus dürfen deshalb nicht auf einem Stand verharren, sondern müssen ebenso wie die Gefährdungslage dynamisch weiterentwickelt werden. Die Staatsregierung wird daher ihre Anstrengungen noch weiter ausbauen. In einem nächsten Schritt soll hierfür die bayerische Cybersicherheitsstrategie aus dem Jahr 2013 evaluiert und fortgeschrieben werden.

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. Ein weiterer Baustein davon ist die Etablierung einer bayerischen „Sharingcommunity", in der maschinenlesbare Angriffskennzeichen ausgetauscht werden können, um die Abwehrmechanismen schnell zu laufenden Kampagnen fortzuentwickeln.

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: November 2022
Druck: Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung

Gedruckt auf: umweltzertifiziertem Papier

www.innenministerium.bayern.de
www.stmfh.bayern.de

www.twitter.com/BayStMI
www.twitter.com/finanzen_bayern

www.instagram.com/BayStMI
www.instagram.com/finanzen_heimat_bayern

www.facebook.com/BayStMI
www.facebook.com/BayerischesStaatsministeriumDerFinanzen

www.youtube.de/BayerischesInnenministerium
www.youtube.de/BayFinanzministerium

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