

Zukunft. Sicher. Digital.

Staat und Wirtschaft im Kampf gegen Cyberkriminalität
auf allen Ebenen stärken.

Cybercrime – die stark wachsende Gefahr.

Baden-Württemberg ist neben dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV), nicht zuletzt durch die erfolgreiche Einrichtung des Cybercrimezentrums an der Generalstaatsanwaltschaft Karlsruhe und der Cybersicherheitsagentur Baden-Württemberg (CSBW) für die Bekämpfung von Cyberstraftaten allgemein, Cyberspionage und -sabotage gut gerüstet. Dies wird eindrücklich durch die zunehmende Anzahl an Meldungen von Ermittlungserfolgen, auch dank internationaler Zusammenarbeit, belegt.

Wirtschaftliche Auswirkungen.

Unabhängig von einzelnen Erfolgen und Festnahmen sind die wirtschaftlichen Folgen von Cyberangriffen für das betroffene Unternehmen selbst, aber auch für die Gesamtwirtschaft oft erheblich. Gerade in Zeiten der Informationsüberflutung verlagern sich kriminelle Handlungen zunehmend in den digitalen Bereich. Immer häufiger haben es Angreifer auf die Informationssysteme von Unternehmen, Behörden und Einzelpersonen abgesehen – und gefährden damit auch den Wirtschaftsstandort BW. Deutschlandweit geben mehr als 70 Prozent der Unternehmen mit mehr als 5.000 Mitarbeitern an, bereits Opfer von Cyberangriffen geworden zu sein. Die FAZ fasste dies Ende August folgendermaßen zusammen: *„Die deutsche Wirtschaft hat in den vergangenen 12 Monaten durch digitale und analoge Spionage und Sabotage sowie Datendiebstahl einen Schaden von 266,6 Milliarden Euro erlitten. Rund zwei Drittel davon stammen aus Cyberattacken.“* Ein unvorstellbarer Schaden.

Aber längst nicht nur der wirtschaftliche Schaden in finanzieller Sicht, sondern auch der Verlust und die damit verbundene Weitergabe von Geschäftsgeheimnissen, Daten der Kundinnen und Kunden sowie anderen schützenswerten Daten schaden den Unternehmen oft in jeglicher Hinsicht. Durch sogenannte Phishing E-Mails oder sonstigen erschlichenen Zugriff auf Datensysteme von Unternehmen oder Behörden besteht die Gefahr, dass über längeren

Zeitraum Datenbestände ausgelesen werden können. Dies ist gerade im Fall der Spionage in Bereichen der kritischen Infrastruktur, der Rüstungs- oder Chemieindustrie, von Flughäfen oder Behörden ein Eingriff in den inneren Kernbereich deutscher Wirtschaft und Selbstverwaltung. Dabei handelt es sich um Angriffe, die auf das Schärfste zu verurteilen sind.

Deswegen unterstützt die CDU-Landtagsfraktion sämtliche Bestrebungen, die Abschöpfung von Vermögenswerten weiter auszubauen, dies vor allem auch in Bezug auf digitale Währungen. Hierzu ist eine enge und vertrauensvolle Zusammenarbeit mit nationalen wie internationalen Behörden unabdingbar. Denn ein Täter darf keinesfalls durch sein Handeln Profit machen. Dass dies gelingen kann, zeigt der Fall der Zerschlagung der ‚Hive‘ Gruppe im Zusammenhang mit Ransomware, bei welchem die Behörden aus Baden-Württemberg mit dem amerikanischen FBI kooperiert haben. Besonders erfreulich ist es, dass aufgrund der guten Zusammenarbeit auch Festnahmen erfolgen konnten. *Neben den meist öffentlich bekannten Fällen großer Wirtschaftssabotageakte gehen die Fälle der Cyberangriffe auf Privatpersonen, die häufig um ihr ganzes Erspartes gebracht werden, oft unter.*

Weitreichende Ermittlungserfolge.

Am 1. Januar 2024 hat das Cybercrimezentrum in Karlsruhe seine Arbeit aufgenommen. Auch wenn insbesondere die IT-Ausstattung gerade noch in der Aufbauphase ist und das Cybercrimezentrum erst seit wenigen Monaten existiert, konnten bereits einige bedeutende Verfahren abgeschlossen werden. Gerade durch die enge Zusammenarbeit des Cybercrimezentrums mit dem LKA, den regionalen Polizeipräsidien und sonstigen nationalen wie internationalen Behörden, kann schnell und effektiv gearbeitet werden. Dies alles zeigt, dass die Konzeption des Cybercrimezentrums funktioniert. Für die CDU-Landtagsfraktion ist klar: die Einrichtung des Cybercrimezentrums kann bereits heute als Erfolg verbucht werden. Die von der CDU-Landtagsfraktion vorangetriebene Einstellungsoffensive der Polizei sowie die durch uns unterstützte kontinuierliche Stärkung der Staatsanwaltschaften in den letzten Jahren schafft die Grundlage dafür, diesen Weg auch in Zukunft erfolgreich fortzusetzen.

Cybertechnologien als Ermittlungsansatz – auch zum Schutz von Kindern.

„Verdacht auf Kinderpornografie: 17 Wohnungen durchsucht“ – Meldungen wie diese gehen durch Mark und Bein. Unschuldige Kinder vor grausamsten Missbrauchserfahrungen zu schützen, ist eine wesentliche Aufgabe des Staates und der Strafverfolgungsbehörden. Dies kann durch den Einsatz moderner Technik um einiges schneller und oft auch für die

ermittelnden Beamtinnen und Beamten schonender erfolgen als durch menschliche Sichtung. Moderne Technologien geben uns für die Aufdeckung und Verhinderung von Straftaten starke Instrumente an die Hand. Dazu gehört bspw. die Zusammenarbeit mit der US-amerikanischen Organisation National Center for Missing and exploited Children (NCMEC), durch welche Kinderpornographie in den sozialen Netzwerken aufgedeckt und gemeldet wird. Die gemeldeten Fälle müssen sodann in Deutschland weiterverfolgt werden. Die CDU-Landtagsfraktion setzt sich daher dafür ein, dass die Justiz die ihr zur Verfügung gestellten Digitalisierungsmittel auch für KI-unterstützte Anwendungen zur schnelleren Erfassung von großen Datenmengen in diesem Bereich nutzt. Darüber hinaus gilt es für die Zukunft die Schaffung einer landeseigenen Stelle zur Koordinierung von Sperrungen illegaler Inhalte in den Blick zu nehmen.

Die Rechtsprechung des EUGH lässt unter anderem bereits eine anlasslose Speicherung von IP-Daten bei sämtlichen Straftaten grundsätzlich zu. Hieran müssen wir endlich anknüpfen und die rechtlichen wie technischen Voraussetzungen in Deutschland schaffen. Alle Speicherung bringt aber nur dann einen echten Mehrwert, wenn Daten auch abgeglichen werden können. Deshalb fordern wir eine verfahrensübergreifende Recherche und Analyseplattform, um durch eine möglichst schnelle automatisierte Analyse den polizeilichen Umgang mit immer größer werdenden Datenbeständen aus unterschiedlichen Quellen zu erleichtern und so effektiv Gefahren abzuwehren. Wie beispielsweise in unserem Nachbarland Frankreich ist es auch in Deutschland grundsätzlich möglich, Gesichtserkennungssoftware einzusetzen. Die KI-Verordnung der EU lässt dies für Sicherheitsbehörden ausdrücklich zu.

Die CDU-Landtagsfraktion fordert die Landesregierung auf, sich auf Bundesebene dafür einzusetzen, alle rechtlichen Möglichkeiten zur Datenauswertung und Gesichtserkennung einzurichten und zu nutzen. Derzeit ist es der Landespolizei zwar möglich, Online-Durchsuchungen durchzuführen, allerdings nur zur Verfolgung von Straftaten, nicht jedoch zur Prävention. Durch das LfV kann zwar in Einzelfällen die Telekommunikation insbesondere zu präventiven Zwecken abgehört werden. Zur effektiven Terrorabwehr spricht sich die CDU-Landtagsfraktion jedoch für eine umfassende präventive Kontrolle von Onlineaktivitäten bei Tatverdächtigen nach bayerischem Vorbild aus.

Notwendige Maßnahmen aus Sicht der CDU-Landtagsfraktion.

Die Verhinderung von Cybercrime beginnt mit guter Prävention. Durch die gezielte Information von Bürgerinnen, Bürgern, Behörden und Unternehmen über Maßnahmen, um

Angriffsversuche abzuwehren, wird ein wirkungsvoller erster Schutz errichtet.

Präventionsangebote, wie sie beispielsweise das LfV und die Cybersicherheitsagentur Baden-Württemberg auch in Zusammenarbeit mit den Industrie- und Handelskammern Baden-Württembergs bietet, müssen dazu ausgebaut werden. Aber auch strukturelle Maßnahmen zur gezielten nationalen und internationalen Reaktion bei Cyberangriffen sind zu stärken und zu erweitern, um den Betroffenen bei der Behebung der Folgen eines Cyberangriffs möglichst schnell zu helfen. Bei strafbaren Handlungen sind Cyberverfahren weiterhin mit großem Nachdruck zu verfolgen. Hierbei ist auch auf nationale und internationale Zusammenarbeit und Erfahrung zurückzugreifen. Ein stetiger Austausch der Behörden ist hierfür immanent.

Das Cybercrimezentrum bei der Generalstaatsanwaltschaft Karlsruhe leistet bereits im ersten Jahr einen großartigen Beitrag zu mehr Ermittlungserfolgen im Cyberraum. Die CDU-Landtagsfraktion wird sich daher weiterhin dafür einsetzen und im Rahmen künftiger Haushaltsverhandlungen dafür aussprechen, das Cybercrimezentrum konsequent weiter auszubauen und die Arbeit voranzutreiben. Den Tätern darf kein Vorteil aus den Straftaten entstehen. Die CDU-Landtagsfraktion spricht sich daher für eine konsequente Abschöpfung sämtlicher erbeuteter Vermögenswerte aus den Taten aus, gerade in Zusammenhang mit digitalen Währungen. Eine Notveräußerung der Kryptowährung um eine Haftung wegen eines etwaigen Kursverfalls zu verhindern, ist zu überprüfen. Es sollen zudem Methoden gefunden werden, die Geltendmachung, auch für die Geschädigten zu vereinfachen.

Bei der Strafverfolgung stehen unsere Ermittlerinnen und Ermittler vor einer immensen Herausforderung. Nicht selten stellt die Abfrage der IP-Adresse des mutmaßlichen Täters bei einem Telekommunikationsanbieter die einzige Identifizierungsmöglichkeit dar. Die Strafverfolgungsbehörden warten daher dringend auf eine gesetzliche Regelung des Bundes, welche die Telekommunikationsanbieter zur vorübergehenden internen Speicherung der vergebenen IP-Adressen verpflichtet. Die gesetzlichen Regelungen in Deutschland dürfen nicht hinter den Möglichkeiten zurückbleiben, welche der Europäische Gerichtshof in sorgfältiger Abwägung der widerstreitenden Positionen zur Vorratsdatenspeicherung von IP-Adressen eröffnet hat. Insbesondere um die Schwächsten in unserer Gesellschaft zu schützen, dazu zählt vor allem der Schutz von Kindern und Jugendlichen vor sexuellem Missbrauch, benötigen wir auf Bundesebene eine Neuregelung der Vorratsdatenspeicherung.