CDU BW
Fraktion

Cyberattacken abwehren. Prävention fördern. Sicherheit stärken.

Positionspapier zur Cybersicherheit
der CDU-Landtagsfraktion Baden-Württemberg
Beschlossen in der Fraktionssitzung am 10.10.2023

Unser Leben wird immer digitaler – Smartphones, Streaming, vernetzte Küchengeräte, smart homes oder selbstfahrende Autos sind nur einige Begriffe, die im 20. Jahrhundert noch „Neuland“ waren. Aus dem digitalen Wandel ergeben sich viele Chancen, aber auch Risiken. Schulen, Krankenhäuser, Unternehmen, Behörden, Privatpersonen – kaum ein Bereich ist vor Cyberangriffen wie Identitäts- und Datendiebstahl, Erpressung oder Wirtschaftsspionage sicher. Auch wenn das Problembewusstsein und die Sensibilität in den letzten Jahren – nicht zuletzt wegen des völkerrechtswidrigen Angriffs Russlands auf die Ukraine – zugenommen hat, müssen wir dennoch hier noch mehr tun.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Gefährdungslage im Cyberraum so hoch wie nie zuvor. Besonders kleine und mittlere Unternehmen (KMU) – das Herzstück unserer heimischen Wirtschaft – sind häufig im Visier von Cyberkriminellen. Im Vergleich zu größeren Unternehmen und Konzernen ist ihre digitale Verwundbarkeit größer, da oft die personellen wie finanziellen Ressourcen zur Absicherung fehlen.

Baden-Württemberg hat in der letzten Legislaturperiode mit dem Cybersicherheitsgesetz – dem deutschlandweit ersten Gesetz, das einen ganzheitlichen Ansatz zur Verbesserung der Cybersicherheit verfolgt – Pionierarbeit geleistet und eine neue Cybersicherheitsstruktur geschaffen. In dessen Rahmen wurde die Cybersicherheitsagentur Baden-Württemberg (CSBW) als zentrale Koordinierungs- und Meldestelle ins Leben gerufen und eine Cybersicherheitsstrategie entwickelt, die bis 2026 umgesetzt werden soll. Damit diese Umsetzung bis 2026 erfolgreich verläuft, ist es uns als CDU-Landtagsfraktion zur „Halbzeit“ dieses Zeitraums ein Anliegen, zu eruieren, welche Punkte künftige besonderer Aufmerksamkeit bedürfen.

1. Bessere Vernetzung

Angesichts der wirtschaftlichen Schäden von Cyberkriminalität brauchen wir eine Intensivierung der Vernetzung aller im Bereich Cybersicherheit tätigen Akteure, Gremien, Behörden und Ebenen – national wie international. Nur wenn wir eng zusammenarbeiten, Informationen austauschen und Synergien nutzen, gelingt es uns, gegen weltweit agierende und bestens vernetzte Hacker etwas auszurichten. Dazu gehört auch eine sinnvolle Vernetzung mit dem BSI. Gerade im Hinblick auf Personalknappheit auch in dieser Branche gilt es, Synergien zu nutzen. Künstliche Intelligenz ist auch bei der Cybersicherheit auf dem Vormarsch – sowohl Angreifer als auch Verteidiger nutzen modernste Methoden. Dies stellt insbesondere KMU und auch Kommunen vor erhebliche Herausforderungen. Gleichzeitig besteht der Bedarf, Daten auszutauschen, die nur mehrere Unternehmen gemeinsam liefern können, um „Machine Learning-Modelle“ trainieren zu können. Für staatliche Stellen gibt es Möglichkeiten das für diesen Datenaustausch erforderliche Vertrauen zwischen den Unternehmen zu schaffen.

2. Stärkung von Frühwarnsystemen

Große Datenmengen sind das A und O, um Mustererkennung zu betreiben. Der Warn- und Informationsdienst der CSBW, mit dem staatliche Stellen und Kommunen in Echtzeit mit Warnungen und Handlungsempfehlungen versorgt werden, soll ausgebaut und auch für Dritte (z.B. KMU) erschlossen werden. Perspektivisch wollen wir „vor die Lage“ kommen – z.B. mit einer „Wetterkarte“ für die Risiko-Analyse von Cyber-Attacken. Um Gefahren

frühzeitig feststellen und abwehren zu können, unterstützen wir Frühwarnsysteme für unsere Netze. Voraussetzung für ein solches Frühwarnsystem ist die umfangreiche Sammlung und der Austausch von Daten. Mit Hilfe eines rechtzeitigen Lagebilds möglicher Cyberbedrohungen steigt die Wahrscheinlichkeit, dass kritische Infrastrukturen, Behörden, Unternehmen usw. nicht unvorbereitet getroffen werden.

3. Bekanntheit der Cybersicherheitsagentur steigern

Die CSBW ist das Herzstück der neuen Cybersicherheitsstruktur des Landes Baden-Württemberg. Sie fungiert als zentrale Koordinierungs- und Meldestelle und ist damit Anlaufpunkt für Kommunen, Bürgerinnen und Bürger, Wirtschaft und Wissenschaft. Leider wissen gerade kleinere und mittlere Unternehmen (KMU) und diejenigen, die sich nicht explizit mit dem Thema Cybersicherheit befassen, oft nichts von ihrer Existenz und ihren vielfältigen Angeboten. Dem wollen wir entgegenwirken und mit einer Werbekampagne Abhilfe schaffen – idealerweise in Kooperation mit Verbänden und Kammern, um die Betriebe zielgerichtet zu erreichen. Regelmäßige Mailings und/oder eine Roadshow wären eine Möglichkeit.

4. Verstärkte Sensibilisierung der Endanwender (Risikofaktor Mensch)

Auch wenn die Sensibilität für das Thema wächst, sind Einfallstore für Hacker nach wie vor schwache Passwörter oder Phishing Mails, mit denen Nutzer dazu gebracht werden sollen, auf schadhafte Links zu klicken. Hier gilt es, die Endanwenderinnen und Endanwender sowohl im beruflichen als auch im privaten Kontext stärker zu sensibilisieren. Zugleich braucht es für Mitarbeiterinnen und Mitarbeiter niederschwellige Angebote, um Fehler und Verdachtsfälle einfach und sicher melden zu können. Je früher die jeweilige IT-Abteilung weiß, dass ein möglicherweise schadhafter Link in einer verdächtigen E-Mail angeklickt wurde, desto schneller kann sie reagieren. Im Zweifelsfall kommt es auch hier auf jede Minute an!

5. Mehr Präventionsmaßnahmen

Die Zunahme von Sicherheitsvorfällen macht die Dringlichkeit von Präventionsmaßnahmen deutlich. Klassische Schulungsangebote erreichen in der Regel vergleichsweise wenige Menschen bei relativ hohem Aufwand. Es braucht daher alternative Lehrformen wie Lernvideos und Web-Based-Trainings und in Applications integrierte Tests. Um den Aufwand gerade für Schulen, Behörden und KMU überschaubar zu halten, soll die CSBW entsprechende Tools soweit möglich zentral bereitstellen und regelmäßig aktualisieren. Unser Ziel ist auch eine Sensibilisierung der KMU, um die von Cyberattacken ausgehenden Risiken für die eigene Firma ins Bewusstsein der Unternehmen zu rücken. Finanzielle Schäden durch Cyberattacken können schnell sehr hoch werden, wenn z. B. der Geschäftsbetrieb von durch Attacken blockierten Daten abhängt. Damit sind auch kleine Betriebe durch entsprechende Angriffe in ihrer Existenz bedroht. Wir empfehlen daher den Unternehmen in Baden-Württemberg neben mehr Präventionsmaßnahmen sowie der Sensibilisierung der Beschäftigten auch den Abschluss einer entsprechenden Cyber-Versicherung zu prüfen, die neben Vermögensschäden zum Beispiel auch die Datenrettung abdeckt. Dabei gilt allerdings: Es ist in höchstem Maße

problematisch, wenn Versicherungen Lösegeldzahlungen im Versicherungsschutz mit abdecken.

6. Mehr Aus-, Um- und Weiterbildung

Laut Branchenverband BITKOM fehlten im vergangenen November in Deutschland 137.000 IT-Fachkräfte quer durch alle Branchen. Dieser Mangel macht sich auch im Bereich Cybersicherheit bemerkbar. Wir müssen die berufliche Aus-, Um- und Weiterbildung im Bereich der IT-Sicherheit fördern und die Ausbildungsinhalte auf Aktualität prüfen. Mit Blick auf die fortschreitende Digitalisierung der Lebens- und Arbeitswelt muss informatische Bildung in der Schule beginnen. Damit Kinder und Jugendliche selbstbestimmt und verantwortungsvoll an der digitalen Welt teilnehmen können und frühzeitig für das Thema Cybersicherheit sensibilisiert werden, sprechen wir uns für ein durchgängiges Pflichtfach Informatik an den weiterführenden Schulen aus. Die grundständige Ausbildung von Informatik-Lehrkräften und die Fortbildung der Bestandslehrkräfte sollen dazu weiter gestärkt werden.

7. Cyberstrategien für Behörden und Unternehmen

Kommunalen Behörden und Einrichtungen sowie Landesbehörden, Unternehmen usw. wird empfohlen, eine individuelle, an bestehenden Standards ausgerichtete Cyberstrategie zu erarbeiten und umzusetzen. Neben einer Risikoanalyse und entsprechenden Sicherheitsmaßnahmen halten wir in diesem Zusammenhang auch einen Maßnahmenplan (Notfallplan) zur Bewältigung etwaiger Sicherheitsvorfälle für geboten. Diese Cyberstrategie gilt es kontinuierlich zu überwachen und zu aktualisieren. Die Erstellung einer Cyberstrategie ist eine Investition in die künftige Existenz und erfolgreiche Arbeit von Unternehmen und Behörden. Eine Cyberstrategie mit einer Risikoanalyse stellt eine gute Grundlage dar, um abzuwägen, ob und in welcher Höhe eine Cyber-Versicherung sinnvoll ist. Wir sehen es als Aufgabe der CSBW, mit einem Leitfaden zur Erstellung einer Strategie die Behörden und KMU zu unterstützen. Generell sehen wir die CSBW auch künftig als Ansprechpartner der KMU bei der Cyber-Ersthilfe mit einem 24/7 besetzten Service.

8. Zukunft und Ausblick

Die CSBW ist eine hervorragende Ausgangsbasis für die Bewältigung der Herausforderungen der IT- und Cybersicherheit, die sich in den kommenden Jahren noch deutlich verschärfen werden. In der Strafverfolgung unterstützen wir es ausdrücklich, dass mit dem neuen Cybercrime-Zentrum in Karlsruhe intensiv gegen Cyberkriminalität vorgegangen wird. Beides sind wichtige Aufgaben und erfordern politische Unterstützung. Um sowohl die CSBW als auch das Cybercrime-Zentrum als kraftvolle Akteure weiterhin anforderungsgerecht aufstellen zu können, sind personelle Verstärkungen und zusätzliche finanzielle Mittel in künftigen Haushalten erforderlich.