IT-Sicherheit

Angriffen Paroli bieten

[26.01.2021] Baden-Württemberg will bei der Abwehr von Internet-Kriminalität schlagkräftiger werden und gründet dazu eine eigene Cyber-Sicherheitsagentur. Diese soll künftig als zentrale Koordinierungs- und Meldestelle fungieren.

Ob Mitteldeutscher Rundfunk, die Uniklinik Düsseldorf, das Robert-Koch-Institut, Handwerkskammern oder Industrieunternehmen – sie alle wurden bereits Opfer von Cyber-Angriffen. In einer Umfrage des Branchenverbands Bitkom gaben drei Viertel aller befragten Unternehmen an, Ziel von Cyber-Kriminalität geworden zu sein. Auch Verwaltungen und Behörden, Forschungseinrichtungen oder Einzelpersonen geraten in den Fokus von Cyber-Kriminellen. Die Schäden gehen allein wirtschaftlich betrachtet in die Milliarden. Menschen, Institutionen und Unternehmen im digitalen Raum bestmöglich zu schützen, ist Aufgabe der Politik. In Baden-Württemberg trägt das Ministerium für Inneres, Digitalisierung und Migration daher nicht nur für die klassischen Themen der inneren Sicherheit wie Polizei und Bevölkerungsschutz Verantwortung, sondern auch für die Cyber-Sicherheit. Eine größtmögliche Sicherheit in diesem Bereich ist ein entscheidender Faktor für die nachhaltige Entwicklung und Wettbewerbsfähigkeit und somit auch ein wichtiger Standortfaktor. Denn Baden-Württemberg ist ohne Zweifel ein lukratives Ziel für Cyber-Kriminelle. Die vielen erfolgreichen Unternehmen im Land, Forschungseinrichtungen, aber auch Verwaltungen und öffentliche Einrichtungen stehen im Fokus. Bei den Angriffen geht es um ganz unterschiedliche Dinge: den Diebstahl von Wissen und Know-how, Angriffe aus finanziellen Motiven oder auf sensible Infrastrukturen.

Herz der Sicherheitsinfrastruktur

Baden-Württemberg hat das erkannt und setzt entsprechende Maßnahmen um. Dazu gehört unter anderem die Gründung einer eigenen Cyber-Sicherheitsagentur. Sie wird das Herz der neuen Cyber-Sicherheitsinfrastruktur sein und soll potenziellen Angriffen auf die digitalen Infrastrukturen Paroli bieten. Im September 2020 hat das Kabinett den Entwurf für das „Gesetz zur Verbesserung der Cyber-Sicherheit“ verabschiedet, der die Cyber-Sicherheitsagentur auf den Weg bringt. Es folgten Wochen im Oktober und November mit viel Lesestoff, denn im Rahmen der Verbandsanhörung und eines Bürgerbeteiligungsverfahrens gingen zahlreiche Stellungnahmen ein. Die Auswertung dieser Meinungen und Anregungen ergab: Ein großer Teil der eingebrachten Impulse bewertet das Vorhaben positiv. Mit den Kritikpunkten haben sich die Verantwortlichen auseinandergesetzt und an der ein oder anderen Stelle den Gesetzestext nachjustiert. Wichtig ist es dem Land, alle Beteiligten früh einzubeziehen und gemeinsam mit den anderen Akteuren im Bereich der Cyber-Sicherheit zusammenzuarbeiten. Um schlagkräftiger zu werden, soll die bisher dezentral organisierte Abwehr von Gefahren aus dem Internet besser vernetzt werden. Bisher müssen noch alle öffentlichen Stellen im Land eigene Strukturen schaffen und die erforderlichen technischen Voraussetzungen aufbauen. Für die neue Cyber-Sicherheitsarchitektur stellt das Land Baden-Württemberg im Staatshaushalt 2020/2021 Mittel in Höhe von 13 Millionen Euro zur Verfügung. Innerhalb dieses finanziellen Rahmens hat der Gesetzgeber insgesamt 83 Stellen für die neu gegründete Agentur genehmigt. Von den 32 Stellen, die bereits seit Anfang 2020 zur Verfügung stehen, waren trotz der pandemiebedingten schwierigen Rahmenbedingungen Stand Anfang Dezember 2020 bereits 22 besetzt.

Landesweites Lagebild

Die Cyber-Sicherheitsagentur soll künftig die zentrale Koordinierungs- und Meldestelle sein. In dieser Funktion sammelt sie Daten zur aktuellen Sicherheitslage und zu Angriffsszenarien im Land, dokumentiert diese und wertet sie aus. Anhand der gesammelten Daten soll ein landesweites Lagebild erstellt werden, das die Agentur zielgruppenorientiert weitergibt, gegebenenfalls durch Warnungen ergänzt und so das Niveau der Cyber-Sicherheit im Land erhöht. Außerdem soll die neue Institution Bürger, Wirtschaft, Wissenschaft und Verwaltung zum Thema Internet-Sicherheit sensibilisieren und beraten. Sie kann beispielsweise Kommunen dabei helfen, Schäden durch Cyber-Angriffe zu verhindern, sodass Verwaltungen im Falle eines Angriffs nicht komplett lahmgelegt werden. Das beginnt bei Workshops für die Mitarbeiter, geht über Schulungen für die IT-Administration bis hin zu konkreten Hinweisen auf Bedrohungs- und Gefährdungslagen. Alle Angebote haben letzten Endes das selbe Ziel: die IT-Infrastruktur des Landes und sensible Daten zu schützen. Doch auch, wenn es zu einem Angriff kam, kann die Cyber-Sicherheitsagentur unterstützen: Auf Ersuchen der betroffenen Stelle kann sie Maßnahmen treffen, die zur Wiederherstellung der Sicherheit und Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Das Kabinett hat das Gesetz im Dezember zur Behandlung in den Landtag eingebracht. Der Aufbaustab der neuen Landesoberbehörde soll – wenn alles nach Plan verläuft – im Frühjahr 2021 seine Arbeit aufnehmen. Dabei gilt es zunächst, Strukturen und Prozesse zu schaffen, die den operativen Betrieb ermöglichen. Die entsprechenden Vorbereitungen dafür laufen zum Teil schon jetzt. Zunächst wird sich die Agentur mit ihren Angeboten auf die Landesverwaltung und die Kommunen konzentrieren. Perspektivisch werden auch die Bürger, die Wirtschaft und die Wissenschaft einbezogen.

Zusammenarbeit mit anderen Behörden

Dass für ein sicheres und selbstbestimmtes Handeln in einer zunehmend digitalisierten Umgebung ein gesamtgesellschaftlicher Ansatz erforderlich ist, hat bereits die Cyber-Sicherheitsstrategie der Bundesregierung aus dem Jahr 2016 festgestellt. Bedeutsam ist deshalb vor allem die Zusammenarbeit der Cyber-Sicherheitsagentur mit anderen Sicherheitsbehörden, also den regionalen Polizeipräsidien, dem Landeskriminalamt und dem Landesamt für Verfassungsschutz. Diese sind weiterhin gemäß ihrem gesetzlichen Auftrag in der Ermittlung und Prävention von Cyber-Attacken aktiv. Betroffenen wird nahegelegt, immer auch Anzeige zu erstatten und im Falle eines erpresserischen Angriffs kein Lösegeld zu bezahlen. Besonders wichtig ist bei alldem der Faktor Mensch. Denn nur wer weiß, wo die Gefahren lauern und wie Angreifer agieren, kann sich wirksam schützen. Der Staat muss Sicherheit, Recht und Freiheit in unserem Land auch im digitalen Raum optimal gewährleisten. Hierzu bedarf es einer zeitgemäßen Cyber-Sicherheitsarchitektur, die die verschiedenen Akteure wirksam verzahnt. Nur mit einem ganzheitlichen Ansatz können die aktuellen und künftigen Herausforderungen, Bedrohungs- und Gefährdungslagen effektiv und effizient bewältigt werden.

()

Dieser Beitrag ist im Spezial der Ausgabe Januar 2021 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Baden-Württemberg, Cyber-Kriminalität, Cyber-Sicherheitsagentur