Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg

07.02.2019

CYBERSICHERHEIT

1. CyberSicherheitsForum 2019 mit rund 350 Teilnehmern in Stuttgart

© Steffen Schmid

„Cyberattacken zerstören das Vertrauen der Menschen in digitale Anwendungen und bedrohen die Existenz unserer Unternehmen. Die Cybersicherheit ist ganz entscheidend bei der Frage, wie erfolgreich wir beim digitalen Wandel sein werden. Die Cybersicherheit ist damit ein bedeutender Standortfaktor, gerade für die Weltmarktführer und Hidden Champions in Baden-Württemberg. Wir, das Land, setzen daher auf Cybersicherheit. Wir wollen Vorreiter und Taktgeber in diesem Bereich sein. Daran arbeiten wir mit aller Kraft – und leisten dafür mit Projekten wie der Cyberwehr auch Pionierarbeit in Europa“, so der Stv. Ministerpräsident und Innenminister Thomas Strobl am Donnerstag, den 7. Februar 2019, bei der Eröffnung des ersten CyberSicherheitsForums von Baden-Württemberg in Stuttgart.

Das Innenministerium und Landeskriminalamt haben zum ersten CyberSicherheitsForum ins Haus der Wirtschaft eingeladen. Unter dem Motto „Wirtschaft. Digital. Sicher“ trafen sich Vertreter aus Wirtschaft, Wissenschaft und Sicherheitsbehörden zum interdisziplinären Austausch. Gerade auch mittelständische Unternehmen sollten für das Thema Cybersicherheit sensibilisiert und über Maßnahmen im Umgang mit Cyberkriminalität informiert werden. Über 350 Teilnehmerinnen und Teilnehmer sind der Einladung zum CyberSicherheitsForum gefolgt. „Wir wollen damit ganz gezielt Entscheider, Sicherheitsexperten und Unternehmerinnen und Unternehmer zusammenbringen“, so Digitalisierungsminister Thomas Strobl.

Die Referenten waren hochkarätig, darunter der ehemalige BND-Präsident Dr. August Hanning und der Cyber-Experte von EUROPOL, Dietrich Neumann. „Der Cyberspace ist Teil des Staatsgebietes geworden“, argumentierte Neumann. Dementsprechend müssen Regierungen weltweit reagieren. Dr. Hanning beschrieb das internationale Gefährdungspotenzial insbesondere durch China, Russland und Iran: „Wir brauchen im staatlichen Bereich in Deutschland eine engere Bündelung der Kräfte, eine engere Abstimmung zwischen Bund und Ländern und einen intensiveren Informationsaustausch mit befreundeten Nationen. Im Unternehmensbereich muss die Förderung leistungsfähiger deutscher Unternehmen im Bereich Cybersicherheit deutlich erhöht werden.“

Cybersicherheit als Standortfaktor gerade für Baden-Württemberg

In den vergangenen zwei Jahren waren laut einer Studie des Branchenverbandes Bitkom bereits sieben von zehn Industrieunternehmen Opfer von Sabotage, Datendiebstahl oder Spionage . Das Bundesamt für Verfassungsschutz beziffert den Schaden für deutsche Unternehmen in den vergangenen beiden Jahren auf mindestens 43 Milliarden Euro . „Wir sind das Land der Hidden Champions, nirgendwo sonst in Deutschland gibt es so viele wie bei uns. Wir sind der Innovationsmotor Europas und beheimaten damit unfassbar viel Knowhow, das geschützt werden muss“, so der Digitalisierungsminister. „Wir sind aber auch das Land der KMU, der kleinen und mittleren Unternehmen – sie alleine stellen rund 60 Prozent der Arbeitsplätze. Und gerade sie sind gegen Cyberangriffe nicht immer ausreichend gewappnet“, so der Minister.

Ausweitung der erfolgreichen polizeilichen Strukturen

Deshalb hat das Land die bereits erfolgreichen Strukturen bei der Polizei ausgeweitet. Die Polizei Baden-Württemberg verfügt beim Landeskriminalamt und den regionalen Polizeipräsidien flächendeckend über spezialisierte Einheiten zur Bekämpfung der Cyberkriminalität. Baden-Württemberg ist damit das erste Bundesland mit einem solchen ganzheitlichen Ansatz. „Gerade weil die Cybersicherheit für ein Technologieland wie Baden-Württemberg ein so bedeutender ökonomischer Faktor ist, hat das Land hier jetzt auch ganz gezielt Maßnahmen und Programme angestoßen. Die Polizei kümmert sich seit einigen Jahren sehr erfolgreich um die Strafverfolgung im Bereich Cybercrime. Die Wiederherstellung der Daten geht dabei allerdings weit über den polizeilichen Auftrag hinaus. Bislang konnte die Polizei die betroffenen Unternehmen lediglich auf eine Liste zertifizierter IT-Unternehmen des Bundesamtes für Informationssicherheit verweisen – auf der aber nur ein Dienstleister aus Baden-Württemberg gelistet war. Diese Lücke schließen wir jetzt – mit Projekten wie der Cyberwehr oder gezielten

Förderprogrammen, die Start-Ups das nötige Rüstzeug an die Hand geben, um sich erfolgreich im IT-Sicherheitsmarkt zu etablieren“, so der Digitalisierungsminister. Aber auch gezielte Präventions- und Informationsmaßnahmen stünden verstärkt im Fokus.

Beim ersten CyberSicherheitsForum wurden etwa Maßnahmen vorgestellt, mit denen sich Unternehmen vor Cyberattacken auch auf kritische Infrastruktur schützen können. Darüber hinaus gab das Landeskriminalamt als Mitveranstalter Einblick in die Ermittlungsarbeit der auf Cyberkriminalität spezialisierten Abteilung „Cyberkriminalität/Digitale Spuren“. Über 130 Spezialisten sind dort unter anderem für die IT-Beweissicherung, Ermittlungsunterstützung, Telekommunikationsüberwachung und forensische Datenträgeranalyse rund um die Uhr im Einsatz. Hinzukommen rund 280 Ermittler, Datenauswerter und IT-Beweissicherer bei den regionalen Präsidien.

Pionierarbeit mit der Cyberwehr

Auf dem CyberSicherheitsForum wurde auch die Cyberwehr näher vorgestellt und stieß auf großes Interesse. Im August 2018 gestartet, steht sie zurzeit rund 11.000 Unternehmen im Großraum Karlsruhe zur Verfügung. „Mit der Cyberwehr haben wir eine bundesweit einmalige Anlaufstelle für kleine und mittlere Unternehmen geschaffen. Eine Feuerwehr, die den Brand bei kleinen und mittleren Unternehmen nach einem Cyberangriff löscht“, erklärt Minister Thomas Strobl. Bislang konnte die Cyberwehr in fast 50 Fällen Hilfe leisten. In vielen Fällen konnte bereits die telefonische Ersthilfe den Schaden einschränken oder ausreichende Handlungsempfehlungen geben. Aber auch die Task-Force, ein Spezialisten-Team der Cyberwehr, war schon mehrfach im Einsatz vor Ort, um den Schaden zu beheben. Bislang konnten die Systeme bei allen bearbeiteten Fällen wieder zum Laufen gebracht werden. Eine Wiederaufnahme der Geschäftsprozesse war möglich und die Systeme wurden zudem für künftige Angriffe abgesichert. Seit diesem Monat ist die Cyberwehr auch an sieben Tagen die Woche rund um die Uhr erreichbar.