Baden-Württemberg

Viertes CyberSicherheitsForum

[22.04.2022] Hauptthema des diesjährigen CyberSicherheitsForums Baden-Württemberg war die Prävention von Cyber-Angriffen. Mit dem Sicherheitspreis 2022 wurden Unternehmen ausgezeichnet, die besonders viel für die Sensibilisierung ihrer Mitarbeiter tun.

Bereits zum vierten Mal fand die Konferenz CyberSicherheitsForum Baden-Württemberg mit rund 500 Teilnehmern – vor Ort in Stuttgart und online – statt. Veranstalter waren das Ministerium des Inneren, für Digitalisierung und Kommunen sowie als Partner das Ministerium für Wirtschaft, Arbeit und Tourismus, das Ministerium für Ernährung, ländlichen Raum und Verbraucherschutz sowie die drei baden-württembergischen Sicherheitsbehörden: die Cybersicherheitsagentur, das Landeskriminalamt und das Landesamt für Verfassungsschutz.
Innenminister Thomas Strobl betonte in seiner Eröffnungsrede mit Blick auf den Krieg in der Ukraine die Bedeutung der Abwehr von Cyber-Angriffen, Propaganda und Desinformation. Der Krieg habe sich auch ins Netz verlagert. Es gelte, künftig nicht nur für die territoriale Souveränität, sondern auch für die digitale Souveränität Sorge zu tragen. Nur mit vereinten Kräften aus Staat, Wirtschaft, Forschung und Gesellschaft sei es möglich, eine digitale Unabhängigkeit herzustellen. Dazu müsse Baden-Württemberg seine technologischen Kernkompetenzen bündeln und weiterentwickeln, so Strobl.

Cyber-Sicherheit ist essenziell

Der IT-Unternehmer Hans-Christian Boos, der auch Mitglied im Digitalrat der Bundesregierung ist, beschrieb in seiner Keynote Baden-Württemberg als Standort mit idealen Voraussetzungen, um die digitale Souveränität weiter zu stärken. Technologien wie künstliche Intelligenz und Cyber-Sicherheit seien essenziell für die wirtschaftliche Zukunftsfähigkeit Deutschlands und ganz Europas. Auch Irene Bertschek, die als Mitglied der Expertenkommission Forschung und Innovation die Bundesregierung zu technologischer und digitaler Souveränität berät, sieht Cyber-Sicherheit als ein wesentliches Element der digitalen Souveränität. Deutsche und europäische Unternehmen müssten Herstellungs- und Entwicklungskompetenzen auf- und ausbauen, um mehr digitale Souveränität zu erreichen. Auch gelte es, digitale Kompetenzen in der akademischen Bildung sowie in der Aus- und Weiterbildung zu stärken. Kontinuierliches Monitoring solle die Fortschritte in diesen Bereichen verfolgen. Neben Diskussionsrunden und Vorträgen gab es auch konkrete Anleitungen und Workshops für die Praxis.

(sib)

Stichwörter: IT-Sicherheit, Baden-Württemberg, CyberSicherheitsForum