

Landesweiter Ausbau des Pilotprojekts Cyberwehr Baden-Württemberg

Die Cyberwehr Baden-Württemberg wurde als zentrale Anlaufstelle für kleine und mittlere Unternehmen im Falle eines IT-Sicherheitsvorfalls ins Leben gerufen. Nach der erfolgreichen ersten Pilotphase in Karlsruhe, Baden-Baden und Rastatt ist die Cyberwehr ab sofort auch landesweit kostenlos über die Hotline erreichbar. Das Ministerium für Inneres, Digitalisierung und Migration unterstützt und fördert das Projekt bis Ende 2021.

Karlsruhe, 08.09.2020 – Ab heute erweitert die Cyberwehr Baden-Württemberg den Pilotbetrieb ihrer kostenlosen Hotline und macht diese nun auch landesweit für alle kleinen und mittleren Unternehmen aus Baden-Württemberg verfügbar. Bei allen Formen von ungewöhnlichen Aktivitäten auf Computern oder Servern können sich die Unternehmen jederzeit rund um die Uhr an die kostenlose Hotline **0800-292379347** beziehungsweise **0800-CYBERWEHR** wenden. Die Vorfälle werden dann von einem Mitarbeiter der Cyberwehr vertraulich entgegengenommen und gemeinsam mit einem IT-Sicherheitsexperten analysiert. Auf Basis dessen werden dann schnellstmöglich sinnvolle Schritte für das weitere Vorgehen geklärt. "Das Ziel der Cyberwehr Baden-Württemberg ist, das Einfallstor zu finden, zu schließen und darauffolgend Handlungsoptionen aufzuzeigen", so Projektleiter Dr. Dirk Achenbach vom FZI Forschungszentrum Informatik. „Mit der Cyberwehr gehen wir systematisch an die Bedrohungen des digitalen Raums heran. Wir sind damit Vorreiter und zeigen: Baden-Württemberg hat die Zukunft fest im Blick – die Chancen, aber auch die Risiken!“ so der Stv. Ministerpräsident und Minister für Inneres, Digitalisierung und Migration Baden-Württemberg Thomas Strobl, und ergänzt „die Reaktionen und Nachfragen von Bund und anderen Ländern zeigen uns, dass wir mit der Cyberwehr Baden-Württemberg den richtigen Weg eingeschlagen haben. Diesen Service wollen wir nun auch landesweit zur Verfügung stellen. Wir investieren damit aktiv in die digitale Sicherheit in unserem Land!“

Vertraulichkeit als Eckpfeiler der Kooperation

Grundsätzlich gilt, dass die Gespräche zwischen Cyberwehr und Betroffenen vertraulich behandelt werden. Informationen oder Daten werden nicht an Dritte weitergegeben. Liegt der Verdacht einer Straftat vor, so rät die Cyberwehr zur Anzeige, übermittelt Informationen aber nur mit dem Einverständnis des Betroffenen an die Ermittlungsbehörden. Bei Bedarf und nach Abklärung der möglichen Handlungsoptionen vermittelt die Cyberwehr überdies ein IT-Sicherheitsteam, um auch weitere Hilfe unmittelbar vor Ort anbieten zu können. Die anfallenden Kosten für diesen Service vor Ort werden vorab mit den Unternehmen besprochen.

Pilotphase mit Erfolg abgeschlossen

"Die erste Pilotphase der Cyberwehr in der Region Karlsruhe, Baden-Baden und Rastatt war ein voller Erfolg", reflektiert Achenbach den bisherigen Projektverlauf. "Dies zeigt sich für uns nicht nur in den durchweg positiven Rückmeldungen der Unternehmen, die sich bisher an uns gewandt haben. In den ersten zwei Jahren konnten wir wichtige Erkenntnisse über das Anforderungsprofil der Hotline gewinnen und unser Partnernetzwerk mit IT-Experten sukzessive erweitern. Nun gehen wir einen Schritt weiter. Sehr früh gab es bereits Anfragen von außerhalb unserer Pilotregion, die wir nun mit der landesweiten Verfügbarkeit der Hotline beantworten können. Wir freuen uns auf die nun kommenden Herausforderungen und sind gespannt auf die neuen Erkenntnisse für das Projekt", so Achenbach mit Blick in die Zukunft. Hierzu wird die Fortsetzung und Erweiterung der Pilotphase bis Ende 2021 auch weiterhin durch das Ministerium für Inneres, Digitales und Migration Baden-Württemberg gefördert.

Sicherheit auch im digitalen Raum

Angriffe auf die IT-Infrastruktur von Unternehmen, Lösegelderpressungen oder der Verkauf von kritischen Firmendaten: IT-Sicherheitsvorfälle der letzten Monate haben aufgezeigt, wie professionell und organisiert Cyberkriminelle vorgehen. Beliebt sind dabei vor allem unzureichend abgesicherte Fernzugriffe auf die IT-Infrastruktur und authentisch wirkende E-Mails mit Schadsoftware-Anhängen. Das Gefahrenpotenzial hat sich in der Corona-Krise unter anderem durch den veränderten Arbeitsalltag erhöht: Nach dem erfolgreichen Zugriff auf die IT-Infrastruktur werden wichtige Daten für den Arbeitsalltag verschlüsselt und teilweise zum weiteren Verkauf kopiert. Nur gegen ein Lösegeld werden die Daten wieder für die Unternehmen zugänglich gemacht. Der fehlende Zugriff auf täglich notwendige Daten und die Lösegeldforderungen können nicht nur zu großen finanziellen Schäden führen, sondern existenzbedrohliche Ausmaße annehmen.

„Die Cyberwehr verschafft uns einen Wettbewerbsvorteil und echten Mehrwert für die digitale Sicherheit in unserem Land!“, resümiert der Stv. Ministerpräsident und Minister für Inneres, Digitalisierung und Migration Baden-Württembergs, Thomas Strobl, und setzt fort „die Cyberwehr rundet unser Portfolio weiter ab, sie ist unser Beitrag im Bereich der unmittelbaren Nachsorge solcher Attacken. Wir zeigen damit: Wir sorgen für Sicherheit, auch im digitalen Raum!“

Fünf Tipps zum Schutz digitaler Infrastruktur

Das Team der Cyberwehr Baden-Württemberg gibt allen Unternehmen unabhängig von der Branche fünf Tipps, um ihre IT-Infrastruktur vor Angriffen zu schützen oder im Ernstfall schnell wiederherstellen zu können.

1. Sichern Sie regelmäßig ihre Daten und bewahren Sie die Backups getrennt von Ihrem Firmennetzwerk auf.
2. Klicken Sie nicht auf unbekannte Links in E-Mails und überprüfen sie vorher die Ziel-Adressen.
3. Öffnen Sie keine Anhänge von unbekanntem Absendern.

4. Berücksichtigen Sie die Hinweise zu sicheren Passwörtern des [BSI Bundesamts für Sicherheit in der Informationstechnik](#).
5. Installieren Sie Software nur aus seriösen Quellen.

Das Bildmaterial in hoher Auflösung steht zum Download bereit unter:

<https://url.fzi.de/cw-bw-hotline>

<https://url.fzi.de/cw-bw-logo-claim>

Über die Cyberwehr Baden-Württemberg

Die Cyberwehr Baden-Württemberg ist ein bundesweit einmaliges Pilotprojekt: Kleine und mittlere Unternehmen unterstützt die Cyberwehr als zentrale Anlaufstelle im Falle eines IT-Sicherheitsvorfalls. In der Pilotphase richtet sich das Angebot zunächst an Unternehmen aus den Stadt- und Landkreisen Karlsruhe, Rastatt und Baden-Baden. Schon jetzt ist die Cyberwehr für sie an 7 Tagen der Woche und 24 Stunden am Tag erreichbar unter [0800-CYBERWEHR](#) oder [0800-292379347](#).

Langfristig will die Cyberwehr allen Unternehmen Baden-Württembergs bei IT-Sicherheitsvorfällen zur Seite stehen und IT-Experten vermitteln. Das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg fördert das Projekt als Teil der Digitalisierungsstrategie digital@bw.

Weitere Informationen unter: www.cyberwehr-bw.de

Über das Konsortium

Das Projekt wird von einem Konsortium bestehend aus FZI Forschungszentrum Informatik, DIZ | Digitales Innovationszentrum, CyberForum e.V. und der Secorvo Security Consulting GmbH umgesetzt.

Das **FZI Forschungszentrum Informatik** führt das Konsortium und bringt seine Expertise in der angewandten Forschung zur IT-Sicherheit in das Projekt ein. Das Team des FZI ist werktags an der Hotline für hilfeschende Unternehmen der erste Kontakt. In einem telefonischen Expertengespräch führt das FZI-Team zusammen mit einem Experten aus seinem Sicherheitsnetzwerk eine Vorfalldiagnose durch und spricht Handlungsempfehlungen aus.

Das **DIZ | Digitales Innovationszentrum** konzipiert Sensibilisierungsmaßnahmen sowie Community-Meetings und setzt diese gemeinsam mit den anderen Konsortialpartnern um.

Das **CyberForum e.V.** setzt die Presse- und Öffentlichkeitsarbeit für das Pilotprojekt in Abstimmung mit dem FZI um.

Die **Secorvo Security Consulting GmbH** entwickelt gemeinsam mit dem FZI den konzeptionellen Aufbau und die Prozesse der Cyberwehr Baden-Württemberg. Außerdem unterstützt sie das FZI bei der Schulung und Zertifizierung von Partnern der Cyberwehr Baden-Württemberg.

Weitere Informationen

Fabio Cusin
CyberForum e.V.
Haid-und-Neu-Str. 18
76131 Karlsruhe
Tel.: +49 721 602 897-620

und

Jerome Nguyen
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14
76131 Karlsruhe
Tel.: +49 721 9654-924

E-Mail: presse@cyberwehr-bw.de

