

# Landesweite Hilfe für Gesundheitsunternehmen bei IT-Sicherheitsangriffen

*Die Cyberwehr Baden-Württemberg erweitert ihren Aktionsradius: Aus ganz Baden-Württemberg können sich nun Einrichtungen aus den Bereichen der medizinischen und pflegerischen Versorgung sowie daran angrenzende Unterstützungsbereiche bei IT-Sicherheitsvorfällen an die kostenlose Hotline wenden.*

Karlsruhe, 23.04.2020 – Ab heute erweitert die Cyberwehr Baden-Württemberg den Pilotbetrieb ihrer kostenlosen Hotline landesweit für Einrichtungen, Unternehmen und Dienstleister aus den Bereichen der Medizin und Pflege. Insbesondere Krankenhäuser, Arztpraxen, Apotheken, Testlabore, Pflegeeinrichtungen und mobile Pflegedienste profitieren von dem erweiterten Service: Stellen sie einen IT-Sicherheitsvorfall fest oder beobachten ungewöhnliche Aktivitäten auf ihren Servern, können sie sich rund um die Uhr an die kostenlose Hotline **0800-292379347** wenden. Die Vorfälle werden aufgenommen und von einem IT-Sicherheitsexperten analysiert. Auf dieser Basis werden mögliche sinnvolle Schritte für das weitere Vorgehen geklärt. Die Gespräche werden dabei selbstverständlich vertraulich behandelt. Informationen oder Daten werden nicht an Dritte weitergegeben, können aber auf eigenen Wunsch hin mit den Ermittlungsbehörden geteilt werden. Bei Bedarf vermittelt die Cyberwehr ein IT-Sicherheitsteam, falls weitere Hilfe vor Ort notwendig ist. Die Kosten hierfür werden im Vorfeld besprochen und festgelegt.

Ursprünglich war ein stufenweiser Ausbau des Angebots der Cyberwehr für 2020 geplant. Mit der kurzfristigen Erweiterung des Aktionsradius, die zunächst für drei Monate gilt, reagiert das Konsortium des Forschungsprojekts auf das gestiegene Gefahrenpotenzial durch Angriffe auf die IT-Infrastruktur im Gesundheitswesen. "Wenn in der aktuellen Situation Anbieter aus den Bereichen Medizin und Pflege durch einen IT-Sicherheitsvorfall ausfallen, können unter Umständen Menschen nicht mehr versorgt werden", so der Projektleiter der Cyberwehr Dr. Dirk Achenbach vom FZI Forschungszentrum Informatik in Karlsruhe. "Das Ziel der Cyberwehr-Experten ist, die Systeme schnell wiederherzustellen und so das Unternehmen arbeitsfähig zu halten." Das Gefahrenpotenzial hat sich in der Corona-Krise unter anderem durch den veränderten Arbeitsalltag erhöht: Kommunikation findet vermehrt auf digitalen Wegen statt und mobiles Arbeiten erfordert häufig Fernzugriffe auf die IT-Infrastruktur. Cyberkriminelle nutzen diese Situation aus, um sensible Daten abzugreifen und Schadsoftware, wie etwa Verschlüsselungstrojaner zu installieren. Erst nach einer Lösegeldzahlung werden die Systeme eventuell wieder freigegeben.

"In der Corona-Krise ist die Cybersicherheit der Gesundheitsbranche von besonderer Bedeutung. Im Falle eines Angriffs nutzen wir alle Möglichkeiten für schnelle Hilfeleistungen", so Innenminister Thomas Strobl. Ermöglicht wird dies durch die fachliche Unterstützung des Sozialministeriums und eine schnelle Freigabe der Mittel durch das Finanzministerium. „Die Cyberwehr Baden-Württemberg erhält bis zu 850.000 Euro extra für drei Monate. Weil wir in guten Haushaltsjahren vorgesorgt haben, können wir jetzt auf die benötigten Reserven zurückgreifen, schnell reagieren und den besonders betroffenen Einrichtungen im Gesundheitswesen helfen“, unterstrich Strobl.

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 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](mailto:digital@bw.de).

Weitere Informationen unter: [www.cyberwehr-bw.de](http://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 hilfesuchende 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.de](mailto:presse@cyberwehr.de)