Baden-Württemberg
LANDESKRIMINALAMT

Warnmeldung für Unternehmen und Behörden

PRESSESTELLE LKA BW
TELEFON 0711 5401-2012 ODER -3012 FAX 0711 5401-1012
PRESSESTELLE-LKA@POLIZEI.BWL.DE WWW.LKA-BW.DE

Stuttgart, 18. April 2019

Hintertür (sog. Backdoor) in mehreren Unternehmen festgestellt

Das Landeskriminalamt Baden-Württemberg, Inspektion 510 Cybercrime, führt aktuell Ermittlungen zu mehreren Fällen der gewerbs- und bandenmäßigen Erpressung mittels einer Ransomware zum Nachteil von Wirtschaftsunternehmen. Die bisherigen Angriffe auf betroffene Firmen führten zur Verschlüsselung sämtlicher Daten. Für eine mögliche Entschlüsselung der Daten wird eine Lösegeldzahlung gefordert.
Eine Analyse der bislang betroffenen IT-Systeme zeigt einen gemeinsamen Angriffsvektor, dessen Merkmale der Anlage "Indikatoren" entnommen werden können. Diese Indikatoren können von IT-Verantwortlichen genutzt werden, um eine mögliche Betroffenheit durch eine sog. Backdoor zu überprüfen und entsprechende Maßnahmen einzuleiten.
Sollten Sie bei Ihrer IT-Infrastruktur feststellen, dass die genannten Indikatoren zutreffen, ist nach derzeitigem Stand davon auszugehen, dass Angreifer unberechtigt Zugang zu Ihren IT-Systemen haben.

In diesem Fall empfehlen wir eine vollständige Überprüfung aller IT-Systeme. Bitte berücksichtigen Sie dabei auch, dass aktuell genutzte Passwörter eventuell ausgespäht wurden. Wir empfehlen darüber hinaus, zu überprüfen, ob unberechtigt Benutzerkonten bzw. Passwörter verändert oder hinzugefügt wurden.
Bei der Bereinigung Ihrer IT-Systeme kann es mitunter sinnvoll sein, entsprechende IT-Sicherheitsdienstleister hinzuzuziehen.
Sollten Sie eine Kompromittierung Ihrer IT-Systeme feststellen, empfehlen wir Ihnen Strafanzeige bei der für Sie zuständigen Zentralen Ansprechstelle Cybercrime (ZAC) zu erstatten.

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg

Erreichbarkeit der ZAC:
Telefon: +49 (0)711 5401 2444
E-Mail: cybercrime@polizei.bwl.de