Baden-Württemberg

LANDESKRIMINALAMT

Warnmeldung für Firmen und Behörden

Aktuelle Angriffswelle: Schädliche E-Mail-Anhänge .one und .html

Stuttgart, 16.03.2023

Das Landeskriminalamt Baden-Württemberg warnt vor einer aktuellen Angriffswelle im E-Mail-Verkehr. Computer und IT-Netzwerke werden mit Schadsoftware infiziert. Anschließend werden Daten ausgespäht und sabotiert. Auch in Baden-Württemberg ansässige Unternehmen und Institutionen sind betroffen.

Hintergrund

IT-Fachkräfte haben die von Office-Dateien ausgehende Gefahr erkannt und die IT-Netzwerke vor der Ausführbarkeit nicht signierter Makro-Elemente gesichert. Cyberkriminelle weichen aus und verwenden zunehmend auch andere präparierte Dateitypen, die Sie mit E-Mails oder Download-Links in die Computersysteme potentieller Opfer einzubringen versuchen.

Wie gehen die Angreifer vor?

Die Absender verwenden so genannte OneNote-Dateien. Diese Dateien besitzen in der Regel die Dateiendung **.one** und können bösartig programmierte Bestandteile enthalten. Die Manipulation der Dateien ist für Empfänger nicht erkennbar. Führen die Anwender die manipulierte One-Datei aus, initialisiert sich ein enthaltenes Skript (Programm), das unbemerkt zum Download von Schadsoftware führt.

Andere Cyberkriminelle versenden schädliche Datei-Anhänge im Format **.htm** oder **.html**. Die Aktivierung der Dateien kann zur Ausführung enthaltener schädlicher Skripte wie beispielsweise JavaScript führen.

Besonderheiten

Die Absender täuschen oftmals die Identität und die E-Mail-Adresse von bekannten E-Mail-Kontakten vor. Der Text der E-Mail weist plausible Inhalte auf und soll den Empfänger der E-Mail zum Aktivieren der beigefügten Datei-Anlage oder Download-Links verleiten.

Empfehlungen der Polizei

- Veranlassen Sie unverzüglich die Einrichtung technischer Gegenmaßnahmen durch die IT-Fachkräfte Ihrer Institution. Diese Maßnahmen sollten im Alltag dauerhaft eingerichtet sein und sich auch auf andere kritische Dateitypen beziehen.
- Blockieren Sie E-Mail-Anhänge und Downloads, die OneNote-Dateien (.one, .onetoc2, onepkg) enthalten und deren Ausführbarkeit.
- Sofern Sie reguläre OneNote-Dateien verwenden: Richten Sie technische Gruppenrichtlinien ein, die in OneNote-Dateien enthaltene unsignierte Skripte blockieren.
- Verwenden Sie für Microsoft-Systeme unbedingt Schutzfunktionen wie WDAC, SRP und AppLocker.
- Blockieren Sie die Möglichkeit des Downloads ausführbarer und sonstiger kritischer Dateien aus dem Internet und die Aktivierung dieser Dateitypen durch Anwender (insbesondere .js, .hta und .dll). Beziehen Sie auch die Benutzerprofile der Anwender ein. Ausschließlich von IT-Fachkräften geprüfte und freigegebene Dateien sollten ausführbar sein (Whitelist).
- Deaktivieren oder beschränken Sie unbedingt die Verwendung von PowerShell.
- Deaktivieren oder beschränken Sie Windows Script Host und MSHTA.
- Prüfen Sie die Möglichkeit der Deaktivierung von Skripten wie JavaScript in allen verwendeten Browsern Ihrer Institution. Deinstallieren oder deaktivieren Sie veraltete Browser wie den Internet Explorer.
- Der Hersteller Microsoft hat Updates zur Reduzierung des Risikos angekündigt. Wie für alle zur Verfügung stehenden Updates gilt: Installieren Sie Sicherheitsupdates zeitnah nach der Veröffentlichung.

- Die übergangsweise Umleitung aller E-Mails und Downloads, die OneNote-Dateien beinhalten, in gesicherte Bereiche, ist empfehlenswert. Die IT-Fachkräfte sollten diese Dateien vor der Weiterleitung an die Anwender einer intensiven Prüfung unterziehen.
- Unabhängig der aktuellen Problematik ist die Deaktivierung aktiver Inhalte in E-Mails sinnvoll.

Die Zentrale Ansprechstelle Cybercrime für Unternehmen und Behörden beim Landeskriminalamt Baden-Württemberg hat polizeiliche Handlungsempfehlungen gegen Verschlüsselungsangriffe veröffentlicht und erläutert mit dem Dokument weitere empfehlenswerte Schutzmaßnahmen zur Abwehr von Cyberangriffen:
Informationen

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg

Die ZAC dient als zentraler Ansprechpartner für die Wirtschaft und Behörden in allen Belangen des Themenfeldes Cybercrime.

Erreichbarkeit der ZAC:
Telefon: +49 (0)711 5401 2444
E-Mail: **cybercrime@polizei.bwl.de**
Website: www.lka-bw.de/zac

