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, 20. Dezember 2018

**Schadsoftware im E-Mail-Anhang von vermeintlich bekannten Absendern**
Ergänzende Informationen zur Warnmeldung vom 20. November 2018

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnet eine auffällige Häufung an Meldungen zu schwerwiegenden IT-Sicherheitsvorfällen, die im Zusammenhang mit der Schadsoftware Emotet stehen. Auch in Baden-Württemberg hat die Schadsoftware bereits bei mehreren Unternehmen zu Ausfällen der kompletten IT-Infrastruktur geführt.
Die Schadsoftware wird weiterhin über groß angelegte Spam-Kampagnen verteilt. Eine Infektion wird aktuell dadurch ausgelöst, dass ein per E-Mail erhaltenes Word-Dokument geöffnet wird. Andere Infektionswege sind jedoch nicht ausgeschlossen.
Emotet ist in der Lage, E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme auszulesen. Die abgezogenen Informationen werden in der Folge zur Weiterverbreitung der Schadsoftware genutzt, indem Empfänger fingierte Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen. Die Täter fälschen mit technischen Mitteln die Absender-E-Mail-Adresse und täuschen bekannte E-Mail-Kontakte vor, um die Empfänger in Sicherheit zu wiegen und zum Öffnen einer beigefügten Datei zu bewegen. Nach dem

Öffnen der häufig als "Rechnung" bezeichneten Datei mit der Endung „.doc“ wird ein Dialogfenster angezeigt, welches dazu auffordert sogenannte Makros oder die Bearbeitungsfunktion im Dokument zu aktivieren. Makrofunktionen sind bei neueren Versionen der Office-Programme aus Sicherheitsgründen standardmäßig deaktiviert.
Die E-Mail-Verfasser nutzen hier die Sorglosigkeit vieler Anwender im Umgang mit Word-Dokumenten aus und animieren die Adressaten zur Aktivierung einer der eben genannten Funktionen. Dies führt dazu, dass durch das manipulierte Word-Dokument die eigentliche Schadsoftware auf den betreffenden Rechner heruntergeladen und automatisch gestartet wird.

**Um sich vor derartigen Angriffen zu schützen, rät das Landeskriminalamt Baden-Württemberg:**

- Sensibilisieren und informieren Sie regelmäßig Nutzer für die Gefahren durch E-Mail-Anhänge oder Links.
- Seien Sie äußerst vorsichtig im Umgang mit Word-Dokumenten, die Ihnen als E-Mail-Anhang geschickt werden. Dies gilt auch bei bekannter Absender-Adresse.
- Wenn Sie eine derartige Anlage dennoch öffnen, unterlassen Sie unbedingt das Aktivieren von Makros oder der Bearbeitungsfunktion in Ihrem Textverarbeitungsprogramm, auch wenn Sie dazu aufgefordert werden.
- Ältere Office-Versionen aktivieren Makros innerhalb von Dokumenten automatisch. Deaktivieren Sie deshalb unbedingt in den Programmeinstellungen die automatische Aktivierung von Makros. Administratoren können die Makro-Verwaltung global über eine Gruppenrichtlinie reglementieren.[1]
- Verhindern Sie durch technische Maßnahmen die Annahme externer E-Mails mit scheinbar internem Absender.[2] Hierdurch soll verhindert werden, dass E-Mails mit gefälschten Absenderinformationen (Beispiel: Absender@IhreFirma.de) zugestellt werden.

[1] http://ct.de/y9hg
[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html
https://docs.microsoft.com/de-de/office365/securitycompliance/anti-spoofing-protection

- Überprüfen Sie Ihr Rechnersystem regelmäßig mit aktueller Anti-Viren-Software.
- Nutzen Sie eine zentral administrierte Anti-Viren-Software und prüfen Sie, ob Updates von AV-Signaturen auf alle Clients verteilt werden.
- Installieren Sie zeitnah Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme, sodass sich Emotet nicht mehr über bereits bekannte Schwachstellen wie die Windows-Lücke EternalBlue im Netzwerk weiterverbreiten kann.[3]
- Sorgen Sie dafür, dass Nutzerkonten nur über die minimal zur Aufgabenerfüllung notwendigen Berechtigungen verfügen.
- Erlauben Sie ausschließlich die Ausführung von bestimmten Programmen (Application-Whitelisting, z. B. mittels Microsoft AppLocker)
- Lassen Sie E-Mails im Plain-Text-Format (statt im HTML-Format) anzeigen. Ein Vorteil dieser Darstellung ist, dass verschleierte URLs in der Textdarstellung leicht erkannt werden können (in einer HTML-E-Mail könnte eine als "www.polizei.de" angezeigte URL z. B. tatsächlich auf "www.schadsoftware.de" verweisen).
- Erstellen Sie regelmäßig Backups und bewahren Sie diese auf externen Systemen auf bzw. stellen Sie sicher, dass diese nicht durch eine Schadsoftware manipuliert werden können.

Weitere Schutzmaßnahmen und aktuelle Informationen zu Emotet finden Sie auf folgender Internetseite des BSI:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

[3] https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html

Baden-Württemberg

LANDESKRIMINALAMT

**Wenn Sie bereits Opfer der Schadsoftware wurden, sollten Sie folgende Maßnahmen treffen:**

- Isolieren Sie potenziell infizierte Rechner unverzüglich vom Netzwerk.
- Ändern Sie sämtliche Passwörter von Nutzerkonten, die auf den infizierten Systemen hinterlegt sind.
- Melden Sie sich nicht mit privilegierten Nutzerkonten (Administrations-Konten) auf einem potenziell infizierten System an
- Betrachten Sie infizierte Systeme als vollständig kompromittiert und setzen Sie diese vor erneuter Inbetriebnahme neu auf.
- Unter Umständen kann es sinnvoll sein einen externen IT-Dienstleister hinzuzuziehen, der Sie bei der Wiederherstellung Ihrer Systeme unterstützt.
- Erstatten Sie als geschädigte Organisation Strafanzeige bei der Zentralen Ansprechstelle Cybercrime (ZAC) in Ihrem Bundesland.

Übersicht ZAC-Dienststellen:
https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

**Zentrale Ansprechstelle Cybercrime**
**beim Landeskriminalamt Baden-Württemberg**

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

Baden-Württemberg

LANDESKRIMINALAMT