Baden-Württemberg

CYBERSICHERHEITSAGENTUR

Stuttgart, 05.11.2021

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

nachdem vor einigen Tagen bekannt wurde, dass die IT-Infrastruktur der Ransomwaregruppierung REvil durch eine Aktion US-amerikanischer Sicherheitsbehörden außer Betrieb gesetzt wurde, erfolgten in einschlägigen Hackerforen Drohungen und Aufrufe zum Angriff des öffentlichen Sektors der USA. Da durch Medienveröffentlichungen auch die erfolgreichen Ermittlungen des LKA BW gegen Hintermänner dieser Tätergruppierung bekannt wurden, ist nicht auszuschließen, dass auch die Landesverwaltung Baden-Württemberg in den Fokus solch einer Racheaktion geraten könnte.

Unabhängig hiervon möchten wir Sie auf Grund einer als „erhöht“ einzuschätzenden allgemeinen Gefahrenlage **dringend vor gefährlichen E-Mails warnen.** Hackerangriffe nehmen meist auf diesem Wege ihren Anfang. Zwar werden an unseren zentralen Schutz-Systemen täglich eine Vielzahl an schädlichen E-Mails herausgefiltert. Dennoch gelingt es Tätern durch technische Maßnahmen immer wieder, schädliche Mails einzuschleusen. Wenn die Technik an ihre Grenzen kommt, sind umso mehr wir Menschen als Nutzende gefragt.

Aktuell wird entweder versucht, über möglichst echt aussehende, mit gefälschter Absenderangabe versehene Mails Schadcode auf die Systeme zu bringen. Oder aber sollen Sie dazu bewegt werden, Ihre internen Benutzerdaten preiszugeben und sie auf einer externen Plattform / Webseite einzugeben. **Beides gilt es unbedingt zu verhindern.**

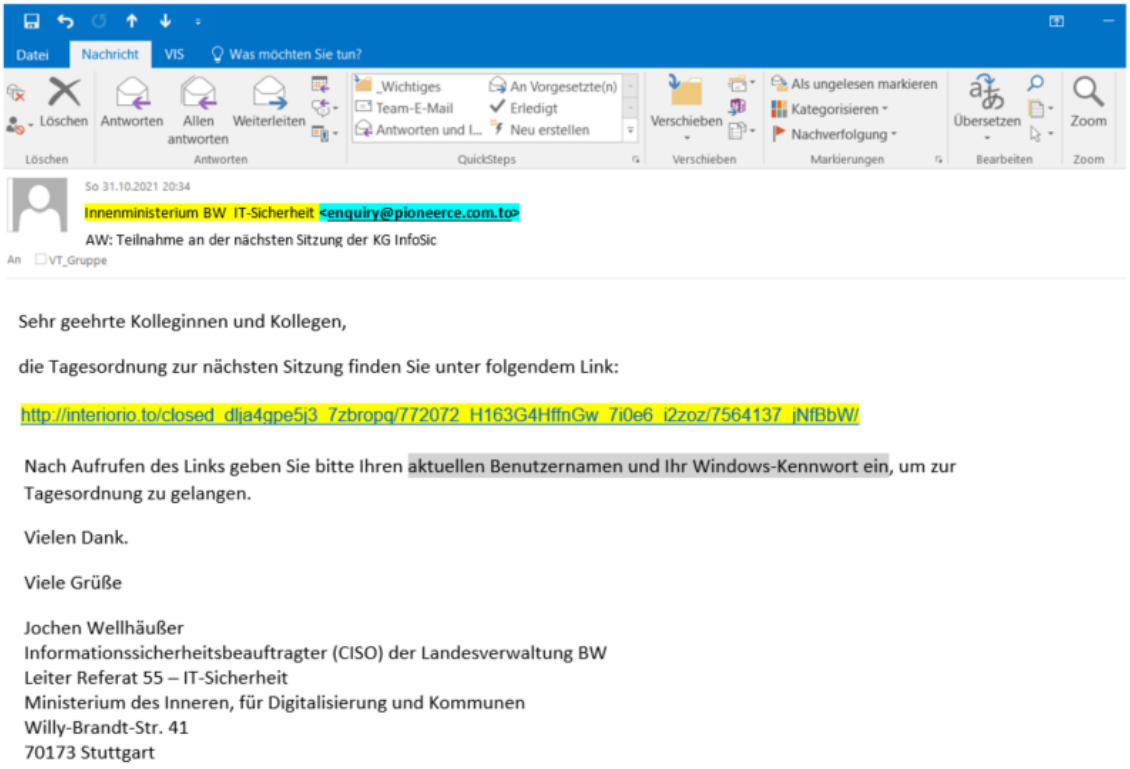
Was können Sie tun?

- ➔ **Vermeiden Sie es, auf Links in E-Mails zu klicken**. Achten Sie auf das Aussehen von Links. Beispiel: Beginnt ein externer Link mit „http“ anstelle von „https“ oder verweist er auf ein fremdes Land (im Beispiel unten: „.to“ steht für Tonga) oder sieht er kryptisch aus, so kann dies ein Indiz für Schadsoftware sein. Im Zweifelsfall empfiehlt sich ein manuelles Eintippen der Adresse der betreffenden Organisation.

- ➔ Geben Sie **niemals Ihre internen Benutzerdaten (Anmeldename und Passwort)**, mit denen Sie sich am Rechner anmelden, auf Ihnen unbekannten Webseiten ein. Professionelle Täter bauen mittlerweile auch zielgerichtet bekannte Webseiten sehr gut nach, um Zugangsdaten abzugreifen.

➔ **Achten Sie auf spam-verdächtige Inhalte in E-Mails** wie Fragen nach persönlichen Daten, sprachliche Ungenauigkeiten, auffällige Datei-Anhänge (insbesondere Office-Dokumente). Seien Sie bei Aufforderungen vorsichtig, die sich als dringend ausgeben.

➔ **Achten Sie auf die tatsächliche E-Mail-Adresse des Absenders**: Extern eingehende Mails zeigen in Outlook sowohl einen Namen als auch eine <E-Mail-Adresse> an. Die wirkliche E-Mail-Adresse ist in eckige Klammern <> gefasst. Der Name davor ist nahezu beliebig fälschbar, die E-Mail-Adresse dagegen nur schwer. Im untenstehenden Beispiel sieht man, dass <E-Mail-Adresse> nicht zum angezeigten Namen passt.



➔ **Auch am Smartphone lassen sich gefälschte Absender erkennen:** Tippen Sie auf die Ihnen angezeigte E-Mail-Adresse. Meist öffnet sich danach ein Kontakt-Fenster, in dem Sie die tatsächliche E-Mail-Adresse sehen. Passen diese zusammen?

➔ **Ist eine E-Mail im Betreff bereits mit „SPAM-Verdacht“ gekennzeichnet, ist besondere Vorsicht geboten.**

Wenn Sie bei der Beurteilung einer solchen Mail Unterstützung benötigen, **wenden Sie sich an Ihre Informationssicherheitsbeauftragten / CISOs oder an Ihre IT-Abteilung**. Jede im Vorfeld erkannte verdächtige Aktion kann Schäden und hohe Aufwände vermeiden!

Vielen Dank für Ihre Mithilfe.

Cybersicherheitsagentur Baden-Württemberg
Kompetenzzentrum für Sensibilisierung und Schulung

Willy-Brandt-Straße 41, 70173 Stuttgart
www.cybersicherheit-bw.de
E-Mail: schulungen@cybersicherheit.bwl.de