Warnung des Landeskriminalamts Baden-Württemberg vor Schadsoftware durch angebliche E-Mail-Rechnungen von vermeintlich bekannten Absendern

Das Landeskriminalamt Baden-Württemberg warnt davor, dass aktuell ein stark erhöhtes Aufkommen elektronisch versandter angeblicher Rechnungen zu verzeichnen ist. In diesem Zusammenhang geht eine Gefahr von den der E-Mail angehängten Word-Dokumenten aus. Im deutschen oder englischen Text der E-Mail wird teils ein angeblich zu begleichender Rechnungsbetrag angegeben, teils auch eine Änderung von beispielsweise Rechnungsanschrift oder Bankverbindung vorgegeben. Für Details wird auf den Anhang verwiesen. Um die E-Mail vertrauenswürdig erscheinen zu lassen, wird mit technischen Hilfsmitteln der wahre Absender verschleiert und so verfälscht, dass er als ein dem Adressaten bekannter Versender erscheint.

Das Dokument in der Anlage enthält sogenannte „Makros“. Makrofunktionen sind bei neueren Versionen der Office-Programme aus Sicherheitsgründen zwar standardmäßig nicht aktiviert, es erscheint dann aber eine Abfrage, ob sie aktiviert werden sollen. Wird diese trotz Hinweis auf möglicherweise – und vorliegend tatsächlich – bestehende Sicherheitsrisiken bejaht, wird im Word-Dokument enthaltener Programmcode ausgeführt, der über das Internet Schadsoftware unterschiedlicher Art auf den betroffenen Rechner herunterlädt und startet. E-Mails mit derartiger Schadsoftware im Anhang sind kein neues Phänomen, erscheinen nunmehr aber verstärkt von angeblich bekannten Absendern, um die Adressaten in Sicherheit zu wiegen.

Um sich vor derartigen Angriffen zu schützen, empfehlen wir entsprechend den Hinweisen des Landeskriminalamts Baden-Württemberg:

- Im Umgang mit Word-Dokumenten, die als E-Mail-Anhang zugeschickt werden, ist auch bei vermeintlich bekannten Absender-Adressen äußerste Vorsicht notwendig. Im Zweifel kann eine Nachfrage bei dem vermeintlichen Versender angezeigt sein, ob dieser ein Dokument zugesandt hat. Besteht beispielsweise keine geschäftliche Verbindung, kann auch keine Rechnung geschickt werden.
- Wenn eine derartige Anlage dennoch geöffnet wird, muss eine Aktivierung der „Makros“ im Textverarbeitungsprogramm unbedingt unterbleiben, auch wenn dazu aufgefordert wird.
- Ältere Office-Versionen aktivieren „Makros“ innerhalb von Dokumenten automatisch. In diesen Fällen ist die automatische Aktivierung in den Programmeinstellungen grundsätzlich manuell zu deaktivieren.
- Wenn es trotz aller Vorsicht zu einer Infizierung mit Schadsoftware kommt, muss der betroffene Rechner unverzüglich vom Netz genommen werden, um das Nachladen zusätzlicher Schadsoftware aus dem Internet sowie eine Infizierung weiterer Rechner im Netzwerk möglichst zu vermeiden.
- Das Rechnersystem muss durch den Einsatz aktueller Anti-Viren-Software ständig geschützt und regelmäßig überprüft werden.
- Für den Fall, dass es dennoch zu einem Befall mit Schadsoftware kommt, ist es wichtig, regelmäßig Backups der Benutzerdokumente und -vorlagen zu erstellen und diese auf externen Systemen zu sichern.

Technische Rückfragen hierzu klären Nutzer des diözesanen Intranets bitte mit der Service-Hotline unter Telefon 07472/169-961, E-Mail: service@drs.de. Sollte bereits Schadsoftware eingeschleust worden sein, wird dazu geraten, Strafanzeige bei der örtlichen Polizeidienststelle oder bei der Zentralen Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts Baden-Württemberg, Tel. 0711/5401-2444, E-Mail: cybercrime@polizei.bwl.de, zu erstatten.