luca

Berlin, 26.5.2021

Hinweis auf einen potentiellen MIssbrauch des luca Systems im Zusammenhang Microsoft Excel Code Injection

Durch eine Medienanfrage und per Twitter haben wir heute von einem möglichen Missbrauch im Zusammenhang mit der Verwendung von luca und Microsoft Excel erfahren, der ab jetzt auch systemseitig verhindert wird.

Dies gilt im Übrigen auch für Excel Dateien, die per E-Mail empfangen werden. Daher gibt es vom BSI Empfehlungen zur Konfiguration von Excel. Im behördlichen Umfeld werden solche Makros im Regelfall deaktiviert. Wir weisen diesbezüglich auf die BSI Empfehlungen hin: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/Empfehlungen_Microsoft_190619.html

Laut den auf Twitter erhobenen Vorwürfen wäre es unter Umständen möglich gewesen, durch das luca-System schadhaften Code an die Gesundheitsämter zu übertragen. Hintergrund ist eine sogenannte CSV Injection, ein in Excel bekanntes Problem, weshalb Excel auch generell Dateien auf solchen Schadcode bei Öffnung prüft und die Nutzer:innen darauf hinweist. Diese Schwachstelle in Excel kann es theoretisch ermöglichen, schadhaften Code in Excel auszuführen. Mithilfe von bestimmten Formeln können Angreifer:innen beispielsweise Daten auslesen oder andere schädliche Aktionen ausführen.

Um den potentiellen Missbrauch durch die Übertragung der luca-Daten an Excel über die dort implementierten Sicherheitsmaßnahmen hinaus zu verhindern, werden im luca-System verschiedene Filter angewendet, welche im Vorfeld die CSV/Excel Dateien nach Zeichen und Formeln scannen.

Das luca-System berücksichtigt die Empfehlungen von OWASP bezüglich CSV Injection, die hier https://owasp.org/www-community/attacks/CSV_Injection aufgelistet sind. Entsprechende Zellen werden wie empfohlen “escaped”. Heute Vormittag haben wir diesen Filter noch zusätzlich um eine sogenannte “Allow List” an Zeichen erweitert, damit böswillige Angreifer:innen diese Excel Lücke nicht mehr ausnutzen können.

Wir haben uns das Szenario angeschaut:

Was ist theoretisch passiert?
Ein simulierter Angreifer hat schadhaften Code in seinen Kontaktdaten angegeben. Diese werden verschlüsselt und daher nicht im luca-Backend überprüft. Beim Abruf der Daten im Infektionsfall wird dieser potentiell schadhafte Inhalt angezeigt.

Was bedeutet das für luca?
Das luca-System selbst ist davor geschützt, dass durch schadhafte oder missbräuchliche Daten ein Schaden entsteht.

Was bedeutet das für andere Systeme?
Eine Übertragung von schadhaftem Code in beispielsweise SORMAS ist ausgeschlossen, da SORMAS über einen Datenfilter verfügt, der genau dieses Szenario verhindert. Im gezeigten Fall ging es um Makros in Excel, welche bei falscher Konfiguration von Excel ausgeführt werden konnten, sofern Nutzer:innen die Sicherheitshinweise missachten.

Es ist unwahrscheinlich, dass ein entsprechender Vorgang im Gesundheitsamt bei einem Excel-Import ausgelöst wird, da die Möglichkeit der Ausführung eines schadhaften Makros im Rahmen eines Excel-Imports im behördlichen Umfeld im Regelfall deaktiviert ist (BSI Empfehlung BSI-CS 136). Sollte dies wider Erwarten nicht der Fall sein, erhalten Nutzer:innen in jedem Fall eine Sicherheitswarnung, bevor ein schadhafter Code ausgeführt wird.

Was bedeutet das für die Arbeit in Gesundheitsämtern?
Generell ist es ratsam, Makros in Excel nur mit Bedacht zu aktivieren. Beim Öffnungsversuch entsprechender schadhafter Dateien erfolgt eine Warnung über ein Pop-up-Fenster, welches vor dem Öffnen der Dateien auf dem Bildschirm angezeigt wird. Es ist sehr wichtig, diese Hinweise sorgsam zu lesen und nicht direkt wegzuklicken. Darüber hinaus ist es ratsam zu überprüfen, inwiefern die Empfehlungen des BSI im jeweiligen Gesundheitsamt bereits umgesetzt werden (BSI Empfehlung BSI-CS 136).

Es ist unwahrscheinlich, dass Schaden durch einen derartigen Angriff entstanden ist, wenn Mitarbeiter:innen nicht aktiv die Sicherheitswarnungen des Systems missachtet haben. Uns ist kein dementsprechender Sicherheitsvorfall im Zusammenhang mit dem luca System bekannt.

Durch weitere Maßnahmen, die heute im luca-System umgesetzt worden sind, wird in Zukunft ein solcher Missbrauch in Zusammenhang mit Makros in Excel verhindert.