Datum: 17.12.2021
Verteiler: Pressestellen LHS, LUP

Presseupdate KW 50

Schwerin, 17. Dezember 2021 – Rückblickend war das Jahr 2021 und insbesondere das vierte Quartal mit vielfältigen Herausforderungen geprägt.

Seit Mitte des Jahres halten verschieden Hackerattacken Kommunen und öffentliche Unternehmen in Atem, auch in Schwerin und Westmecklenburg. Der Angriff auf uns als kommunalen IT-Dienstleister mit mehr als 4.000 Arbeitsplätzen bei unseren Kunden und Trägern war einer der schwersten Cyberangriffe in der jüngsten Vergangenheit, wobei die Dunkelziffer weiterhin sehr hoch sein dürfte. Seit nun mehr neun Wochen befinden wir uns auf dem Weg zu einem stabilen Notbetrieb.

Auch wenn jeder Angriff individuell zu betrachten ist, ist es uns im Vergleich zu anderen Fällen gelungen, in kürzester Zeit einen stabilen Notbetrieb aufzusetzen. „Hierfür möchte ich mich bei allen Beteilgten bedanken“, betont Matthias Effenberger das große und kräftezehrende Engagement in den vergangenen Wochen. „Natürlich hofft man, dass man als Unternehmen von derartigen Extremsituationen verschont bleibt. Doch es kann jeden treffen.“, so Effenberger weiter.

Risikomeldung des BSI: Sicherheitslücke in der Java-Logging-Bibliothek mit dem Namen „Log4j“

Um so mehr Aufmerksamkeit wurde in der IT-Welt auf die am 10. Dezember 2021 erfolgte Meldung des Bundesamts für Sicherheit in der Informationstechnik (BSI) gelegt, dass eine signifikante Schwachstelle in der Java-Logging-Bibliothek (in der sogenannten log4j Version 2) bekannt geworden ist, die Angreifer ausnutzen könnten. Betroffen sind eine Vielzahl von Fachanwendungen, quer durch das gesamte Anwendungsportfolio. Im Laufe der vergangenen Woche wurden daher deutschlandweit verschiedene Maßnahmen eingeleitet, um das Risiko einer Kompromittierung zu minimieren. Aufgrund der bei der SIS/KSM etablierten sehr hohen Sicherheitsmaßnahmen wägen wir im Einzelfall ab, ob wir bis zur Bereitstellung des entsprechenden Updates oder Patches die Nutzung der Anwendungen teilweise einschränken oder den entsprechenden Dienst vorübergehend vom Netz nehmen.

Somit lag der Fokus in der zurückliegendenen Woche verstärkt auf der Analyse der betroffenen Systeme.

Stabiler Notbetrieb

Dennoch konnten in der vergangenen letzten Woche weitere Fachverfahren und –anwedungen bei unseren Kunden und Träger im Notbetrieb zur Verfügung gestellt werden. Etwa neun Wochen nach dem Cyberangriff und dem kontrollierten Herunterfahren sämtlicher Systeme, stehen viele der für den Bürger- und Kundenservice relevanten Fachverfahren und Anwendungen wieder zur Verfügung. Die Kunden und Träger waren in den vergangenen Wochen verstärkt mit der Nacherfassung bzw. Bearbeitung von liegengebliebenen Fällen und Anfragen beschäftigt.

Die Einrichtung der jetzt noch ausstehenden und erforderlichen Fachverfahren sowie Nacharbeiten, wie beispielweise die Freischaltung von weiteren Schnittstellen und Zugriffsmöglichkeiten, wird noch einige Zeit in Anspruch nehmen. Parallel werden jedoch bereits wieder laufende Service- und Supportleistungen erbracht.

Insgesamt stehen bereits rund 95% der PC´s und Notebooks wieder zur Verfügung. An der Etablierung von HomeOffice-Lösungen wird weiterhin mit Hochdruck gearbeitet.

Presseupdate KW 50

Rückkehr zum Normalbetrieb

Technisch betrachtet befinden wir uns in den kommenden Wochen weiterhin im stabilen Notbetrieb, wobei es - wie bereits aufgezeigt - Unterschiede in der Verfügbarkeit der einzelnen Fachverfahren und Anwendungen geben wird. Unter stabilem Notbetrieb ist dabei zu verstehen, dass die Fachverfahren und Dienste für die Nutzer - also die Mitarbeiter/-innen in den Verwaltungen oder bei den Kunden - zwar mit den annähernd gleichen Parametern (Funktionalitäten, Verfügbarkeiten, Wartung, etc.) wie im normalen Tagesgeschäft bereitstehen, es jedoch im Hintergrund noch weitreichende technische Restriktionen gibt, die durchaus zu funktionalen Einschränkungen führen können.

Für die Bürger*innen als auch für die Mitarbeiter*innen in der jeweiligen Verwaltung sollte in der kurzfristigen Perspektive dennoch kaum ein Unterschied zum Normalbetrieb feststellbar sein, lediglich neue IT-Projekte u.a. zum weiteren Ausbau von Onlineservices und im laufenden Betrieb geplante Maßnahmen müssen neu terminiert werden.

Für den technischen Wechsel in den IT-Normalbetrieb werden in den kommenden Wochen infrastrukturelle und netzseitige Voraussetzungen konzipiert und geschaffen, bevor eine Migration aus dem Notbetrieb heraus erfolgen kann. Der vollständige Übergang in den IT-Normalbetrieb wird somit erst im Laufe des Jahres 2022 erfolgen.

Nächstes Update: 13.01.2022

In Anbetracht der anstehenden Feiertage erhalten Sie das nächste reguläre Presseupdate in der KW 2.

Wir wünschen Ihnen ein frohes Weihnachtsfest und einen guten Start ins Jahr 2022!