Angriff ins Leere

22.04.2022, Unternehmens-Blog

Ende November 2021 erschütterte ein Fehler die IT-Welt: Durch eine Schwachstelle im Java-Baustein LOG4j gab es Angriffspotenzial auf die Systeme zahlreicher Unternehmen. Auch in oscare® steckt jede Menge an LOG4j. Damit war die GKV-Branchenlösung grundsätzlich betroffen – bis eine schlagkräftige Taskforce kam.
LOG4j ist ein populärer und häufig verwendeter Baustein für Java, den vor allem Entwickler:innen nutzen. LOG4j sammelt Login-Informationen sowie Protokolle und speichert sie oder führt aus diesen Informationen heraus Kommandos aus. In diese Sammlungen könnten durch eine Schwachstelle ausführbare Befehle unbemerkt nachgeladen werden. Beispielsweise „kontaktiere einen Server“ oder „rufe eine Internetseite auf“. Oder auch „lade Schadsoftware herunter und installiere sie“. Dadurch wäre es Cyberkriminellen potenziell möglich, ganze Unternehmensnetzwerke zu infiltrieren, Schadsoftware zu installieren und in der Folge sensible oder unternehmensinterne Daten herunterzuladen oder Server-Einstellungen zu manipulieren. So bestand also Ende des vergangenen Jahres hier höchste Gefahr – und die Auswirkungen waren weltweit spürbar. Forscher hatten zwar die LOG4j-herausgebende Apache-Stiftung bereits im November informiert. Doch zu diesem Zeitpunkt hätte die Schwachstelle schon weidlich ausgenutzt werden können. Kaum lief die Berichterstattung an, versuchten weitere Cyberkriminelle rund um den Globus, die ihnen nun plötzlich bekannte Möglichkeit zu verwenden. Es begann der übliche Wettlauf zwischen den Unternehmen, die mit einem Patch die Schwachstelle beheben wollten, und Hacker:innen, die einen kleinen Vorsprung hatten.

Suche und Lückenschließung liefen parallel

„Bei uns ergriffen die Geschäftsbereiche Services und Entwicklung sofort nach Veröffentlichung der Informationen gemeinsam die Initiative“, erinnert sich Werner Meier, Geschäftsbereichsleiter Services und Leiter der unmittelbar gegründeten Taskforce. „Wir informierten unsere Kunden und IT-Dienstleister umfassend und transparent über unser Kundenportal sowie im weiteren Fortgang in täglichen Videokonferenzen. Wir recherchierten umgehend in allen eingesetzten Systemen und IT-Diensten und dokumentierten alle Fundstellen – mehr als 1.000. Wir führten eine Risikobetrachtung durch und erstellten eine Prioritätenliste.“ Die Geschäftsbereiche Entwicklung und Services arbeiteten hier Hand in Hand. Als Erstes behandelten die Mitarbeiter:innen aus der Entwicklung der AOK Systems alle Systeme mit Kundenbezug, die Java verwenden und auf das Framework LOG4j setzen. Wurde eine Lücke gefunden, erfolgte mit den inzwischen verfügbaren Patches deren Schließung. Um die notwendigen Updates bei uns und den IT-Dienstleistern einspielen zu können, musste für jedes System ein passendes Wartungsfenster gefunden werden – zum Beispiel eine Tageszeit, in der möglichst wenige Mitarbeiter das jeweilige System verwenden. Nach dem Einspielen war zu überprüfen, ob jedes der 1.000 Systeme wieder fehlerfrei läuft. Während des Abarbeitens kamen neue Findings

hinzu, was die Arbeit erschwerte. Den Kunden entstand jedoch durch die LOG4j-Schwachstelle kein Schaden.

Jederzeit zentrale Sicht auf die Dinge

Für die Recherche nutzten die Geschäftsbereiche externe Quellen wie das Bundesamt für Sicherheit in der Informationstechnik und das IT-Nachrichtenportal Heise online. Auch Lieferanten von Soft- und Hardware gaben wichtige Hinweise. Darüber hinaus setzten wir spezielle Scripte ein, um die Systeme zu scannen. All das band intern sehr viele Ressourcen, was sich natürlich auf den Regelbetrieb der Softwareerstellung auswirkte. Information und die Bereitstellung der Dokumentation über das Kundenportal liefen sehr gut. Alle Beteiligten hatten jederzeit eine zentrale, verbindliche Sicht auf den Stand der Dinge. Das Angriffspotenzial über LOG4j wurde erfolgreich und ohne Schaden eingedämmt. Allerdings werden Cyberkriminelle weiterhin jede Gelegenheit für ihre dunklen Machenschaften nutzen, denn Sicherheitslücken lassen sich nie ganz ausschließen. Die AOK Systems stellt sich dieser Aufgabe täglich und routiniert. „Vor einer Auslieferung überprüfen wir unsere Software auf potenzielle Lücken und verhindern über die interne Qualitätssicherung bereits im Vorfeld, dass Schwachstellen überhaupt das Tageslicht beim Kunden erblicken“, fasst Werner Meier zusammen. Es ist davon auszugehen, dass vor allem kritische Infrastrukturen weiterhin Ziel krimineller Angreifer sein werden. Die AOK Systems bleibt beim Hase-Igel-Rennen wachsam.

Autor/in: Jürgen Röttgen, Entwickler Cloud Service