Log4J und die Folgen

INFOKOM überprüft stetig die Sicherheitssysteme

Unsere Welt ist zunehmend vernetzt, speziell in den letzten Jahren wurde die Digitalisierung und Vernetzung stark getrieben. Wir alle profitieren – geschäftlich und privat – von den Annehmlichkeiten des möglichst ungehinderten Datenaustauschs zwischen Menschen, Institutionen und Unternehmen. Leider hat die Vernetzung auch zu einer ganz neuen Kategorie der Kriminalität geführt. Hacker nutzen Sicherheitslücken konsequent aus und erbeuten so gewaltige Summen.

Für die Betreiber von IT-Systemen ist das eine permanente Herausforderung. Im Falle der IT-Systeme im EUROBAUSTOFF-Rechenzentrum ist dafür die INFOKOM zuständig. „Aktuelle Sicherheitssysteme ermöglichen ein Systemdesign, das möglichst wenig Angriffsfläche bietet und es Angreifern entsprechend schwermacht", erklärt Christian Kraus, Bereichsleiter Einkauf und Technik. „Penetrationstest von unabhängigen Dritten, die regelmäßig beauftragt werden, um mit den Methoden und Werkzeugen von Hackern die Schutzmaßnahmen der INFOKOM zu unterlaufen, sorgen für eine regelmäßige Überprüfung der Sicherheitssysteme", betont Kraus.

Weltweite Angriffe

Eine besondere Herausforderung ergab sich Mitte Dezember durch das Bekanntwerden einer Sicherheitslücke in der sehr häufig genutzten Softwarekomponente „Log4J". „Plötzlich hatten Hacker die Chance, weltweit Computersysteme mit der gleichen Strategie anzugreifen. Als sich abzeichnete, dass das bereits im größeren Stil passiert, wurde die Sicherheitslücke öffentlich gemacht, wodurch das Thema auch außerhalb der Fachpresse publik wurde", erinnert Kraus. Das sei außergewöhnlich gewesen, denn meist würden Sicherheitslücken entdeckt, bevor sie großflächig ausgenutzt werden. „Das ermöglicht es den Softwareherstellern, ihre Produkte stillschweigend zu korrigieren und den Anwendern Updates zukommen zu lassen", so Kraus.

Bei der INFOKOM galt es nun, das Rechenzentrum zu untersuchen und abzusichern. „Es wurde daher direkt nach Bekanntwerden der Lücke noch am Wochenende ein Krisenteam zusammengestellt, das automatisiert alle über 1.500 verschiedenen Systeme und Anwendungen überprüfte", schildert der Bereichsleiter. Am Folgetag konnten die gefährdetsten Systeme abgesichert werden, im Laufe der folgenden Woche wurden sukzessive alle weiteren Fälle bearbeitet. „Teilweise war die Komponente auch in Software von Drittanbietern integriert, die nicht so schnell Abhilfe schaffen konnten. Hier war aufgrund der sonstigen Sicherheitsarchitektur ein Angriff jedoch sehr unwahrscheinlich", erläutert Kraus. Inzwischen seien alle Arbeiten längst abgeschlossen.

„Durch die schnelle und konsequente Reaktion wurde ein Schadensfall in der EUROBAUSTOFF Cloud verhindert", betont Christian Kraus abschießend. Alleine in Deutschland wurden in den Tagen nach Bekanntwerden der Sicherheitslücke allerdings mehr als die Hälfte aller Firmennetzwerke angegriffen. „In vielen Fällen waren die Hacker erfolgreich – bei uns nicht", ist Kraus ebenso erleichtert wie stolz.

Davon profitierten neben den zentralen Anwendungen der EUROBAUSTOFF auch die INFOKOM-Kunden, die für Wawi, Fibu, CRM oder sogar die Arbeitsplatz-PCs die EUROBAUSTOFF-Cloud nutzen. „Der professionelle Rechenzentrumsbetrieb ermöglicht ein wesentlich höheres Sicherheitsniveau, als es in den Räumen eines Baustoffhändlers typischerweise möglich ist. Dazu zählt nicht nur der Schutz gegen Hackerangriffe, sondern auch die Absicherung gegen Stromausfälle, Feuer oder Einbrüche", so das Resümee des Bereichsleiters, das zugleich als Empfehlung verstanden werden darf. ■