Cybersecurity made in Sachsen.

T-Systems-Tochter Multimedia Solutions überführt Cyber-Defense-Forschungslösung HoneySens des Freistaats Sachsen in den Produktivbetrieb und übernimmt die Vermarktung.

TEXT —— Thomas van Zütphen

Für eine funktionierende öffentliche Verwaltung sind Informationssicherheit und Datenschutz unabdingbar. Denn was immer Bürger und Unternehmen „aufs Amt" führt– von der simplen Adressänderung über die Gewerbeanmeldung, Fragen des Technologietransfers bis zum Schutz von Patenten –, könnte nicht nur die Aufmerksamkeit von Stadt, Land oder Bund auf sich ziehen. Mitunter auch die von Hackern.

Beispiel Sachsen: Mehr als 1400 direkte Angriffe auf sein Verwaltungsnetz (SVN) konnte allein der Freistaat im vergangenen Jahr detektieren und abwehren – eine Steigerung im Vergleich zu 2015 um 63 Prozent. In den 26 Millionen eingegangenen E-Mails der Landesverwaltung wurden 75 723 Schadprogramme gefunden, fast dreimal so viele wie im Jahr zuvor. „Unsere Netze können auch zum Ziel für Hacker werden, das können wir nicht verhindern", so Karl-Otto Feger, Beauftragter für Informationssicherheit des Landes. „Was wir aber verhindern können, ist, dass Cyberspione erfolgreich sind." Dabei sind die IT-Systeme der Sächsischen Landesverwaltung nicht nur Bedrohungen aus dem Internet ausgesetzt, sondern können ebenso Ziel von Angriffen aus dem internen Netzwerk werden. Ausgangspunkt sind typischerweise mit Schadsoftware befallene Rechner. Aber auch unbemerkt ins Netzwerk vorgedrungene Angreifer oder Mitarbeiter, die sich – oft irrtümlich – über Sicherheitsbestimmungen hinwegsetzen, stellen Gefahrenquellen dar. Klassische Sicherheitsmaßnahmen wie zentrale Firewalls und Anti-Virus-Systeme können diese Gefahrenquellen jedoch nicht oder nur ein wenig reduzieren.

Der Freistaat Sachsen initiierte daher 2014 das Forschungsprojekt HoneySens, um Hacker und Malware künftig schneller aufspüren zu können. Das im Ergebnis gemeinsam mit der TU Dresden entwickelte Softwaresystem lässt Sensoren im Netz verwundbare – für Angreifer attraktive – Schwachstellen simulieren. Die „Honigtöpfe" zeichneten zunächst in ausgewählten Teilnetzen des SVN alle verdächtigen Netzwerkaktivitäten oder Datenpakete auf und leiteten sie an einen Zentralserver zur Prüfung und Alarmierung weiter. „Durch die Sammlung und Auswertung wertvoller Informationen soll unser gesamtes IT-System mit insgesamt 28 Unternetzen und rund 40 000 PC-Arbeitsplätzen gegen unbefugte Zugriffe von außen gestärkt werden", erklärt Karl-Otto Feger.

Für den Sprung von einem reinen Entwicklungsprojekt zu einem dauerhaften, flächendeckenden Einsatz in der Landesverwaltung suchte der Freistaat Sachsen einen Industriepartner. Der sollte den Prototyp in den Produktivbetrieb des SVN überführen und das Softwaresystem zu einem eigenen, zugleich vermarktungsfähigen Produkt weiterentwickeln. Der Freistaat entschied sich aus mehreren Gründen für die T-Systems-Tochter Multimedia Solutions GmbH (MMS). Neben der jahrelangen Erfahrung von T-Systems in ihrer eigenen weltweiten Honeypot-Landschaft und deren Weiterentwicklung „werden wir laut Vertrag gewährleisten, dass die Softwareentwicklung auch für andere Nutzer günstig einsetzbar bleibt und es parallel zum angestrebten vereinbarten Produktivbetrieb auch eine dauerhaft frei nutzbare Open-Source-Version der Software geben wird", erklärt Marcel Wallbaum, der das Projekt aufseiten der MMS verantwortet.

In gewisser Weise jedoch, daraus macht Karl-Otto Feger kein Geheimnis, „kam bei der MMS auch der Standortvorteil Dresden zum Tragen. Mit der Wahl eines sächsischen Unternehmens haben wir bis zum vorgesehenen Launch des Produkts Ende 2017 kurze Wege und gewährleisten anschließend, dass die Vermarktung durch unseren Industriepartner wiederum auch dem Land Sachsen zugutekommt."

marcel.wallbaum@t-systems.com
https://www.egovernment.sachsen.de/1935.html
www.t-systems.com/solutions/cyber-security

Im Produktivbetrieb wird HoneySens das IT-System der Sächsischen Landesregierung mit 40 000 PC-Arbeitsplätzen flächendeckend gegen unbefugte Zugriffe von außen stärken.