Interview

Schwachstellen aufspüren

[29.06.2021] Die Unternehmen cosymap und Trovent Security wollen auch kleineren Netzbetreibern eine rechtssichere Leitungsauskunft ermöglichen. Im Interview mit stadt+werk stellen cosymap-CTO Thomas Schamal und Alexander Caswell, Geschäftsführer der Trovent Security, ihre Lösung vor.

Herr Schamal, Herr Caswell, die GIS-Gesamtlösung von cosymap, die eine standardisierte Anwendung für die Leitungsauskunft beinhaltet, ist insbesondere für kleine und mittlere Stadtwerke geeignet. Gemeinsam mit der Trovent Security aus Bochum wird die Web-Applikation vor der Inbetriebnahme beim Kunden auf Sicherheitslücken geprüft. Warum legen Sie mit Ihrer Kooperation den Schwerpunkt gerade auf das Thema IT-Sicherheit?

Thomas Schamal: Das zentrale Thema unserer Kunden ist die Daseinsvorsorge und Versorgungssicherheit. Gerade für Netzbetreiber kritischer Infrastrukturen, wie Energie- und Wasserversorger, muss sichergestellt werden, dass diese jederzeit gewährleistet ist. Das heißt, die Leitungsnetze müssen vor Beschädigungen durch Fremdeinwirkung Dritter, etwa Bautätige, geschützt werden, zudem muss die dahinterliegende IT-Infrastruktur Angriffen von außen standhalten. Das betrifft auch das Ausspähen von geschützten Leitungsdaten.

Alexander Caswell: Aktuelle Statistiken zeigen, dass Cyber-Angriffe, insbesondere auf Unternehmen und öffentliche Einrichtungen, im vergangenen Jahr in Deutschland einen Höchststand erreicht haben. Auch aus diesem Grund hat das Bundeskabinett im Dezember 2020 die Novellierung des IT-Sicherheitsgesetzes 2.0 beschlossen. Es enthält für Betreiber kritischer Infrastrukturen deutliche Verschärfungen. Regelmäßig durchgeführte Penetrationstests tragen neben anderen technischen und organisatorischen Maßnahmen dazu bei, dass die erhöhten Anforderungen des Gesetzgebers erfüllt werden können.

„Unser Ziel ist es, Manipulationsmöglichkeiten präventiv zu verhindern.“
Worin unterscheidet sich die cosymap Lösung von herkömmlichen Applikationen zur Leitungsauskunft?

Schamal: Mit unserer Branchenlösung konzentrieren wir uns verstärkt auf kleinere und mittlere Versorgungsunternehmen. Gerade bei kleineren Stadtwerken sind die Ressourcen in der IT oftmals begrenzt. Die Vorgaben des Gesetzgebers und novellierte Regelwerke der Branchenverbände erzeugen einen hohen Modernisierungsdruck, dem die Unternehmen nur mit hohem Zeit- und Ressourcenaufwand nachkommen können. Die cosymap-Lösung als Standard-Software für Leitungsauskunft schlägt hier sozusagen zwei Fliegen mit einer Klappe: Zum einen basiert sie auf der aktuellen Rechtsprechung und ist somit rechts- und revisionssicher, zum anderen ermöglichen die kurze Implementierungsphase sowie der einfache und intuitive Umgang mit der Lösung einen schnellen Return-on-Investment. Die Option, die Software im Anwendungsumfeld mittels Penetrationstest zu überprüfen, ist für die Entscheider ein zusätzlicher und wichtiger Aspekt in puncto Betriebssicherheit.

An welchen Stellen sind die Systeme der Netzbetreiber besonders angreifbar und welche Szenarien werden mit dem Penetrationstest der cosymap-Applikation durchgespielt?

Schamal: Bei dem Test konzentrieren wir uns auf unsere Web-Applikation und deren Schnittstellen in der Anwendungsumgebung. Wir implementieren die bereits auf Sicherheit und Schwachstellen überprüfte cosymap-Software beim Kunden und überprüfen sie in der Betriebsumgebung dann nochmals auf einwandfreie und sichere Funktion. Dabei werden die Server- und Netzwerkinfrastruktur genau beleuchtet, um eventuell vorhandene Schwachstellen aufzudecken und zu beheben. Unser Ziel ist es, Manipulationsmöglichkeiten präventiv zu verhindern.

Caswell: Trovent Security arbeitet hierbei nach anerkannten Standards. Dazu zählen unter anderem der Penetration Testing Execution Standard (PTES), der OWASP Web Security Testing Guide sowie das Durchführungskonzept für Penetrationstests des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Wie läuft der Test im Stadtwerk konkret ab und mit welchem zeitlichen Rahmen muss der Kunde rechnen?

#bild2 Caswell: Zunächst werden gemeinsam mit dem Kunden Zielsetzung und Rahmenbedingungen für die Überprüfung festgelegt. Hierbei stehen Fragen im Vordergrund, welche die Art und die Vorgehensweise bei dem bevorstehenden Test betreffen. Dazu gehört beispielsweise, welche Informationen im Vorfeld über das Zielsystem zur Verfügung gestellt werden und wie aggressiv bei der Überprüfung vorgegangen werden soll und darf. Darüber hinaus werden die Zielsysteme für den Test festgelegt. Neben der cosymap-Leitungsauskunft können das auch die angeschlossenen Datenbank-Server sein. Unsere Tester führen danach die Überprüfung durch und greifen das Zielsystem mit den gleichen Mitteln an, die auch böswillige Angreifer anwenden, um mögliche IT-Sicherheitsrisiken aufzudecken. Werden im Zuge dessen Schwachstellen identifiziert, werden diese ausführlich dokumentiert und Verbesserungsvorschläge erarbeitet. Für einen vollständigen Penetrationstest ist mit etwa fünf Arbeitstagen zu rechnen.

Schamal: Natürlich werden die Ergebnisse der erfolgten Maßnahmen zur erhöhten IT-Sicherheit in Folgetests verifiziert und auch Releases der Software entsprechend überprüft.

Was bedeutet Ihr Vorstoß bei der Leitungsauskunft im Bereich der IT-Sicherheit für die Branche?

Schamal: In Gesprächen mit Unternehmen aus der Branche haben wir festgestellt, dass die eingesetzten Web-Applikationen oft nicht mehr den aktuellen IT-Sicherheitsanforderungen genügen. Die Kooperation mit Trovent Security ermöglicht es uns, unseren Kunden einen zuverlässigen Nachweis zu liefern, dass unsere Lösung zur Leitungsauskunft hinsichtlich der IT-Sicherheit dem aktuellen Stand der Technik entspricht. Der vergleichsweise überschaubare Aufwand für das Testverfahren im Zuge der Software-Implementierung zahlt maßgeblich in die Vertrauensbildung des Netzbetreibers ein. Vor allem aber dient er der Sicherheit der Netzinfrastruktur in Deutschland.

Caswell: Im Übrigen gilt das nicht nur für die Versorgungsbranche, wobei gerade die Betreiber kritischer Infrastrukturen eine hohe Verantwortung für das Gemeinwohl tragen.

()

Dieser Beitrag ist im Sonderheft Juni 2021 von stadt+werk zur Infrastruktur für die Smart City erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, cosymap, IT-Sicherheit, Penetrationstest, Trovent Security GmbH