Foto: WLV

Der Wasserleitungsverband Nördliches Burgenland stellt, mit über 2.900 km Leitungen, die Wasserversorgung in den Bezirken Eisenstadt, Mattersburg und Neusiedl sicher. Vor Kurzem wurde ein NIS-Audit durchgeführt.

Cybersecurity

NIS-Richtlinie: So läuft ein Audit ab

Mit der europäischen Cybersicherheitsrichtlinie NIS2 kommen ab Oktober 2024 Sicherheitsanforderungen auf viele Unternehmen zu, die bisher dem Bereich der kritischen Infrastrukturen vorbehalten waren. Bernhard Hanifl vom Wasserleitungsverband Nördliches Burgenland gewährt uns einen Blick hinter die Kulissen und erklärt im Interview, wie ein NIS-Audit abläuft.

AUTlook: Die Einhaltung der NIS-Richtlinie ist alle drei Jahre verpflichtend. Wie läuft ein Audit ab?

Bernhard Hanifl: Es gibt sogenannte qualifizierte Stellen, das sind IT-, EDV- oder Beratungsfirmen, die vom Ministerium geprüft werden und bestimmte Voraussetzungen erfüllen müssen. Man kann also nicht einfach irgendeine Firma beauftragen, sondern es gibt eine Liste von qualifizierten Stellen, die beim Ministerium zur Einsicht aufliegt. Natürlich wird man vorher informiert, wir haben zwei Jahre vorher mit den Vorbereitungen begonnen, mit einer GAP-Analyse, mit Vorbetrachtungen. Wir haben geschaut, wo wir stehen und was noch zu tun ist. Und dann wird ein Termin vereinbart.

Wie läuft der Besuch der Auditoren ab?

Hanifl: Während ihres dreitägigen Aufenthalts in unserem Haus haben sie zu dritt verschiedene Abteilungen und Teilbereiche überprüft. Es gibt mehrere Kapitel und Domänen, die untersucht werden müssen. Eine präzise Liste gibt vor, was zu erfüllen ist, und die wird sorgfältig durchgecheckt. Der konkrete Vorgang kann sich unterscheiden, ich habe Angebote von mehreren qualifizierten Stellen eingeholt.

Bedeutet das, dass es Unterschiede gibt, was geprüft wird?

Hanifl: Nein, es existieren standardisierte Berichte, die zu verfassen sind. Die Vorgehensweise ist klar definiert. Gewisse Abweichungen in der Ausführung sind jedoch möglich und verständlich.

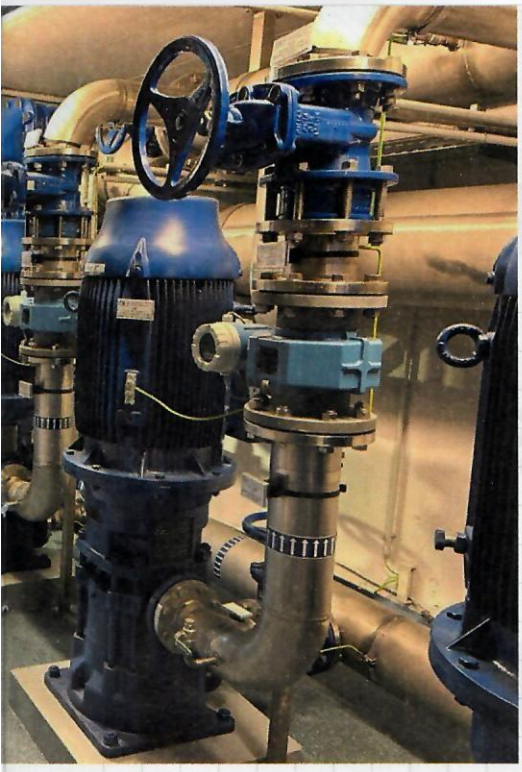
Wie ging es dann mit dem Prüfprogramm weiter?

Hanifl: Es existiert ein allgemeiner Leitfaden vom Ministerium, den wir für unseren Sektor angepasst haben. Die Vorgaben des Ministeriums können nicht abgeschwächt werden und müssen erfüllt werden, jedoch haben wir sie präzisiert. Zum Beispiel ist Trinkwasser als Medium nicht so zeitkritisch wie Strom oder Gas. In unserer Branche sprechen wir von anderen Reaktionszeiten. Diese Aspekte haben wir in diesem Leitfaden erörtert. Eine der Herausforderungen besteht darin, die OT klar von der IT abzugrenzen. Dieser Punkt wurde ausführlich geprüft und getestet. Im besten Fall hängt die OT nicht am Internet, und wenn das ordentlich nachgewiesen werden kann, dann hat man viele Sorgen weniger. Ein weiterer Aspekt betrifft das Thema Fernwartung. Vorab haben wir

Foto: Privat

„DAS AUDIT HAT UNS IN SICHERHEITSTECHNISCHER HINSICHT DEUTLICH WEITERGEBRACHT UND VIELE VERÄNDERUNGEN MÖGLICH GEMACHT."

Bernhard Hanifl,
Leiter der Elektroabteilung beim Wasserleitungsverband Nördliches Burgenland



eine Zwei-Faktor-Authentifizierung für jeden Fernzugriff eingeführt und die Zugriffe stark limitiert. Ganz wichtig war auch, dass wir ein IDS-System implementiert haben, das uns über Vorfälle informiert und kontinuierlich die OT überwacht.

Im Leitfaden steht, dass regelmäßige Überprüfungen des Informationssicherheitsmanagementsystems durchzuführen sind. Diese Empfehlung könnte allerdings spezifischer formuliert sein.

Hanifl: Wir lassen jedes Jahr einen externen Berater zwei Tage mit uns arbeiten. Er überprüft, ob alles in Ordnung ist. Zudem haben wir einen Informationssicherheitsbeauftragten (ISB), der sich um die Sicherheit kümmert und dafür sorgt, dass das NIS-Gesetz umgesetzt wird. Den ISB haben wir erst eingeführt, um uns auf das bevorstehende Audit vorzubereiten. Zuvor habe ich diese Aufgabe zusammen mit dem IT-Leiter wahrgenommen, aber das ist auf Dauer nicht machbar.

Es ist auch eine Risikoanalyse gefordert, in der das Funktionieren wesentlicher Dienste des Gemeinwesens bewertet wird. Was ist darunter zu verstehen?

Hanifl: Unser wesentlicher Dienst ist die Trinkwasserversorgung. Wir haben jede unserer Anlagen einer Risikoanalyse unterzogen. Das ist aus einer anderen Gesetzgebungsecke schon notwendig gewesen, deshalb haben wir es schon vorab gemacht. Das haben wir vorgelegt, haben dann die EDV-Komponenten dazu geliefert, die kritisch oder unkritisch sind.

Wenn Sie jetzt die ganze Erfahrung noch einmal Revue passieren lassen: Konnten Sie daraus einen Nutzen ziehen?

Hanifl: Ja, das Audit hat uns in sicherheitstechnischer Hinsicht deutlich weitergebracht und viele Veränderungen möglich gemacht. Durch die Umsetzung der 2-Faktoren-Authentifizierung laufen nun alle Zugriffe bei uns sicherer ab. Darüber hinaus haben wir diverse Anschaffungen wie zum Beispiel ein Intrusion Detection System getätigt. Ich muss sagen, dass mein Auditor vernünftig war. Ich habe schon oft von negativen Beispielen gehört. □