Sustainable Cyber Resilience im Wassersektor:

Öffentliche Wassserversorgung und Abwasserbeseitigung

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Die öffentliche Wasserversorgung und Abwasserbeseitigung zählt zu den kritischen Infrastrukturen und ist ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Wassersektor so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyber-Angriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetzt (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist Wasser mit den Sparten öffentliche Wasserversorgung und Abwasserbeseitigung. Er umfasst zum Beispiel Wasserwerke, Pumpanlagen, Wasserleitungen und -netze, Kläranlagen, die Kanalisation sowie Stau- und Hochwasserschutzanlagen. Sie alle spielen eine entscheidende Rolle für unsere Gesellschaft. Ohne ausreichend sauberes Trinkwasser könnten wir Menschen nicht leben. Doch Wasser ist nicht nur unser wichtigstes Nahrungsmittel – wir brauchen es auch für die Körperhygiene, zum Wäschewaschen, Putzen und Kochen. Die Nahrungsmittelindustrie benötigt Wasser als Rohstoff für die Produktion, und auch andere Industriezweige wären ohne das wertvolle Nass nicht funktionsfähig. Angriffe auf die Wasserversorgung könnten eine Gesellschaft daher bis ins Mark treffen und im schlimmsten Fall Menschenleben bedrohen. Ebenso gefährlich sind Attacken auf die Abwasserentsorgung. Funktioniert sie nicht mehr, würde das zu erheblichen hygienischen und gesundheitlichen Problemen führen. Da in der Wasserinfrastruktur heute eine Vielzahl von IT-Systemen und elektronischen Steuerungssystemen (ICS) zum Einsatz kommt, wird sie zum attraktiven Ziel für Hacker.

Beispiele für Cyber-Attacken auf Wasser-Infrastrukturen

In den vergangenen Jahren gab es weltweit bereits zahlreiche Angriffe auf Wasser-Infrastrukturen. Gravierende Folgen blieben dabei bisher zum Glück aus. Die Attacken zeigen jedoch, dass Hacker ausloten, wie sie die Kontrolle über Steuerungssysteme übernehmen und weitere Angriffe vorbereiten können. So versuchten 2013 iranische Hacker in die Systeme des Bowman Avenue Damms in der Nähe des Ortes Rye Brooke bei New York einzudringen. Der Damm dient dazu, den Wasserfluss nach starken Regenfällen zu kontrollieren und eine Überflutung des Orts zu vermeiden. Den Hackern gelang es, Kontrolle über die Steuerung der Fluttore zu erlangen. Da diese aber gerade wegen einer Wartung nicht am Netz waren, konnten die Cyber-Kriminellen keinen Schaden anrichten.

Im März 2016 berichtete der Sicherheitsspezialist Verizon in seinem monatlichen Security Breach Report von einem Cyber-Angriff auf einen amerikanischen Wasserversorger, der unter dem Pseudonym Kemuri Water Company genannt wird. Hacker waren in die SCADA-Plattform, das übergeordnete Steuerungssystem des Unternehmens, eingedrungen. Dadurch konnten sie programmierbare Logik-Controller (PLCs) manipulieren. Sie änderten Einstellungen am Wasserfluss und an der Menge der Chemikalien, die für die Wasseraufbereitung zugesetzt wurden. Glücklicherweise entdeckte der Wasserversorger den Vorfall schnell und konnte die Einstellungen wieder korrigieren, ohne dass größerer Schaden entstand. Für ihren Angriff nutzten die Hacker eine ungepatchte Schwachstelle im Kunden-Zahlungs-Portal aus.

Zwischen November 2016 und Januar 2017 hackten Cyber-Kriminelle mehrere Mobilfunk-Router einer US-Wasserbehörde. Die Router dienten dazu, sicheren kabellosen Zugang für das Monitoring der Pumpstationen zur Verfügung zu stellen. Zum Glück waren die Angreifer jedoch nicht auf Sabotage aus, sondern hatten es auf die Internetressourcen der Behörde abgesehen. Deren Rechnung stieg von durchschnittlich 300 US-Dollar pro Monat auf satte 45.000 Dollar im Dezember und 53.000 Dollar im Januar an. Für ihre Attacke nutzen die Hacker eine Schwachstelle in den Routern des Herstellers Sixnet aus. Dieser hatte nach eigenen Angaben bereits im Mai einen Patch zur Verfügung gestellt, den die Behörde jedoch nicht installiert hatte.

In Deutschland gab es zwar noch keinen vergleichbaren Vorfall, das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet in seiner aktuellen Studie zur Lage der IT-Sicherheit in Deutschland jedoch von Sicherheitslücken bei mehreren Wasserwerken. Ihre Steuerungssysteme waren vom Internet aus öffentlich einsehbar. Dadurch konnte auch eine mögliche Manipulation nicht ausgeschlossen werden. Das BSI hat die Betreiber der Wasserwerke unmittelbar kontaktiert und die Sicherheitslücken wurden geschlossen.

IT-Systeme und Prozesse im Wassersektor

IT- und OT-Systeme (Operational Technology) unterstützen den Wasserkreislauf wie in der Grafik unten dargestellt. In der Wassererzeugung (1) werden Systeme zur Qualitätskontrolle (automatische Entnahme und Prüfung) und digitale Pumpensteuerung genutzt, um den Wasserzufluss aus verschiedenen Quellen hin zur Wasserverteilung (2) zu steuern. Digitale Mess- und Steuerungsverfahren kontrollieren Wasserdruck und -qualität im Wassernetz und sind somit Teil der gesamten IT-Angriffsfläche. In der Entwässerung (3) sind Abwasserpumpen und Vorreinigung durch Siebe (überwacht an zentralen Stellen) eingesetzt. Die Aufbereitung (4) ist gerade durch die notwendige digitalisierte Steuerung von physikalischen, chemischen und biologischen Prozessen eine kritische Komponente.

In der Trinkwasserversorgung und Abwasserentsorgung kommen daher eine Vielzahl von vernetzten IT-Systemen und industriellen Steuerungssystemen (ICS) zum Einsatz, die weitgehend automatisierte Prozesse ermöglichen. An den Pumpen, Ventilen, Wassertanks und anderen Geräten befinden sich Sensoren, die zum Beispiel Werte wie die Temperatur, Durchflussgeschwindigkeit oder den Chlorgehalt messen. Sie geben ihre Daten an die Steuerungssysteme weiter, die dann automatisiert reagieren. ICS dienen beispielsweise zum Monitoring des Quellwassers und der kontinuierlichen Kontrolle der Wasseraufbereitung. Sie überwachen und managen den Druck und den Wasserfluss in den Rohren. Außerdem loggen sie Daten mit und übernehmen Diagnose- und Alarm-Funktionen. So können die intelligenten Systeme zum Beispiel in Echtzeit einen Druckabfall und mögliche Lecks erkennen und den Netzbetreiber informieren. Bei Verbrauchern kommen zunehmend smarte, fernauslesbare Zähler zum Einsatz, die es ermöglichen, Verbrauchsdaten in Echtzeit zu erheben und Geschäftsmodelle darauf abzustim-

IT-gestützte Kontrollsysteme im Wasserkreislauf

men. Auch sie sind potenzielle Einfallstore für Hacker. Darüber hinaus findet die Kommunikation mit Kunden häufig über Webportale oder mobile Apps statt. Um einen Zustand der Sustainable Cyber Resilience zu erreichen, müssen Unternehmen aus dem Wasser-Sektor das gesamte Spektrum der vernetzten Systeme, Geräte und Applikationen berücksichtigen.

Besondere Herausforderungen für Resilience im Wassersektor

Die hochgradige Automatisierung und Abhängigkeit von Industriesteuerungen macht die Wasserinfrastruktur besonders angreifbar. Außerdem werden die eingesetzten IT-Systeme immer komplexer. Dadurch haben es Unternehmen schwer, ein ausreichendes Schutzniveau zu erreichen. Die zunehmende Vernetzung von Komponenten innerhalb der Feld- und Steuerungsebene sowie der Steuerungs- und Prozessleittechnik erhöht die Komplexität noch weiter. Gleichzeitig vergrößert sich damit die Angriffsfläche für Hacker. Sie haben immer mehr Möglichkeiten, in Netzwerke einzudringen, Daten zu stehlen oder Industrie-Steuerungen zu manipulieren. Erschwerend kommt hinzu, dass die ICS, die in der Wasserinfrastruktur im Einsatz sind, aus unterschiedlichen Generationen stammen. Viele der älteren Steuerungssysteme wurden in einer Zeit designt, in der Cyber Security noch kaum oder gar nicht berücksichtigt wurde. Das führt zu einer heterogenen, verwundbaren IT-Landschaft.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeiten eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffes zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

Greenbones Schwachstellenmanagement funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden. Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hackerangriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**