IKT Minimalstandard Abwasser

Risikoexposition nimmt mit steigender Vernetzung und Nutzerzahl zu

Eine Kläranlage ist heute in der Regel eine hochautomatisierte Anlage mit zunehmender Vernetzung innerhalb von Systemen (ARA, Aussenbauwerke) und auch der steigenden Anzahl von Benutzern (Pikettdienst, Dritte). Durch die damit verbundenen zunehmenden Angriffsmöglichkeiten wächst die Gefahr eines Cybervorfalles (Notfall).

Die durch den ARA Betreiber vorzukehrenden Massnahmen sind bei steigender Vernetzung umfassender zu gestalten und betreffen nicht nur die technischen Einrichtungen, sondern auch die Benutzer, deren Rechte einzuschränken sind. Dies hat zur Folge, dass das Login mehr Zeit beansprucht, bisherige Möglichkeiten gesperrt werden müssen. Sind diese Massnahmen vom ARA Betreiber definiert, gilt es sicherzustellen, dass alle Betroffenen (Mitarbeiter, Systemlieferanten, Partner) diese kennen und sich ihrer Verantwortung diesen gegenüber bewusst sind und die Cybersicherheit leben.

Möglichen Gefahren kann angemessen begegnet werden.

Vernetzung	Durch die Vernetzung der Systeme mit dem Internet wird die Angriffsfläche drastisch erhöht. Zusätzlich möchte jeder Akteur von der Vernetzung profitieren und Zugriff auf die Anlage haben.
Schnittstellen	Da die Leitsystemebene (OT) andere Vorgaben bezüglich Sicherheit und Verfügbarkeit als die Büronetzumgebung (IT) hat, muss den Schnittstellen dieser beiden Umgebungen besondere Aufmerksamkeit gewidmet werden. Es gilt die beiden Netze klar voneinander zu trennen. Innerhalb vom OT-Netz nur die Datenflüsse zu erlauben, die für die Bedienung des PLS (ARA oder Aussenbauwerke) notwendig sind.
Verantwortungsbewusstsein	Je mehr Akteure auf das System Zugriff haben, konzentriert sich das Verantwortungsbewusstsein des Einzelnen vermehrt auf seinen Bereich und der Blick für das grosse Ganze gerät in den Hintergrund. Es dauert länger bis alle Beteiligten die Cybersicherheitsvorgaben und -massnahmen akzeptieren, diese als sinnvoll erachten und die Direktiven mittragen.
Akzeptanz	Die Benutzer tragen wesentlich zur Cybersicherheit bei, wenn sie verstehen, dass Cybersicherheit Vorrang vor den eigenen persönlichen Bedürfnissen in der Bedienung des Systems hat. Dieser Lernprozess findet an vielen Orten erst noch statt. So dürfen beispielsweise nur jene Aufgaben im Leitsystem (OT-System) durchgeführt werden, für die es vorgesehen ist. Andere Verwendungen der Computer des Leitsystems sind nicht gestattet. Beispielsweise sind die Daten für eine Auswertung zentral anzufragen und auf einen geeigneten Computer zu transferieren. Dies kann den Benutzern mühsam erscheinen, ist jedoch der sichere Weg in Bezug auf Cyberrisiken.
Reduktion der Risiken	Eine Reduktion der Benutzeranzahl und die strikte Trennung von Leitsystemebene (OT) mit der Büronetzumgebung (IT) reduziert das Cyberrisiko deutlich. Ebenso verhält es sich, wenn das OT-System keine IT-Anwendungen zulässt.
Erkennbarkeit von Risiken	Je verantwortungsbewusster die Benutzer der Systeme sind können Risiken reduziert werden. Je komplexer die Umgebungen sind, desto schwieriger ist es, Risiken zu erkennen und nachhaltig zu beheben.

Herausgeber: step by STEP | VSA
www.step-ara.ch | www.vsa.ch