Warum OT-Sicherheit essenziell ist, damit nicht plötzlich das Licht ausgeht

Wird das IT-System eines Unternehmens gehackt, drohen Produktionsausfälle, finanzielle Verluste sowie Reputationsschäden. Doch ist ein solcher Angriff auf eine Kritische Infrastruktur wie beispielsweise ein Kraftwerk erfolgreich, können davon weite Teile der Schweiz betroffen sein. Dies zu verhindern, ist die Aufgabe der Alsec Cyber Security Consulting AG.

Interview mit Reto Amsler und Markus Lenzin, Gründer der Alsec Cyber Security Consulting AG

Reto Amsler
Gründer Alsec Cyber Security Consulting AG

Markus Lenzin
Gründer Alsec Cyber Security Consulting AG

Reto Amsler, Markus Lenzin, was versteht man genau unter «Kritischen Infrastrukturen»?

Reto Amsler: In der Schweiz sind diese durch das Bundesamt für Bevölkerungsschutz genau definiert. Vereinfacht gesagt, handelt es sich bei Kritischen Infrastrukturen um Organisationen und Unternehmen verschiedener Sektoren, die zum Wohl der hiesigen Industrie oder der gesamten Schweizer Bevölkerung agieren. Konkret kann es sich dabei um Energieversorgungsunternehmen aller Art und Grösse handeln, welche Strom produzieren und diesen über die Netze bis an die Haushalte verteilen. Aber auch Spitäler gehören zu den Kritischen Infrastrukturen. Sie sind im Gegensatz zu anderen Unternehmen mit zusätzlichen Angriffsformen aus dem Cyberraum konfrontiert, zu denen auch Angriffe von staatlichen Akteuren zählen. Die Ausgangs- und Bedrohungslage ist also eine grundlegend andere. Dies war unter anderem in den Jahren 2015 und 2016 zu sehen, als erstmals durch ein Cyberangriff ein Blackout verursacht und somit aufgezeigt wurde, dass die Stromversorgung einer ganzen Region lahmgelegt werden kann.

Markus Lenzin: Wir sprechen in diesem Zusammenhang nicht von IT-, sondern von OT-Infrastrukturen. «OT» steht dabei als Kürzel für «Operational Technology», sprich für «Betriebstechnologie». Diese beschreibt die Verwendung von Hard- und Software zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen. Das Problem: OT-Infrastrukturen kann man nicht auf die gleiche Weise schützen wie IT-Systeme.

Warum ist das nicht möglich?

Markus Lenzin: Im OT-Bereich sprechen wir von sogenannten «SCADA-Systemen». Diese dienen der Überwachung und Steuerung von technischen Prozessen. Konkret kann es sich dabei um die Steuerung einer Industrieanlage handeln. Anders als IT-Softwares, die man alle drei bis fünf Jahre generalüberholt und auswechselt, haben OT-Systeme einen deutlich längeren Lebenszyklus. Wir sprechen schnell mal von zehn bis 15 Jahren Betriebsdauer. Diese Steuerungsanlagen sind oft stark an die jeweiligen Produktionsprozesse gekoppelt. Sie auszuwechseln, würde einen enormen Aufwand bedeuten und im schlimmsten Fall die Versorgungssicherheit einschränken. Darum werden sie heute oft so belassen und nur rudimentär gepatched. Natürlich akkumulieren sich dadurch mit der Zeit Schwachstellen. Glücklicherweise sind die meisten OT-Systeme, anders als IT-Systeme, nicht direkt mit dem Internet verbunden. Doch es gibt andere Mittel und Wege, wie Cyberangreifer ihren Weg in diese Kritischen Infrastrukturen finden können. Ist ein solcher Breach erst einmal erfolgt, ist das System oft veraltet und stellt den Angreifenden nur kleine Hürden in den Weg. Wenn wir uns nun die Relevanz von Kritischen Infrastrukturen vor Augen führen, wird klar, welch enormes Schadenspotenzial sich hier eröffnet.

Was wird also in diesem Bereich unternommen?

Markus Lenzin: Der VSE (Verband Schweizerischer Elektrizitätsunternehmen) hat eine Branchenempfehlung zur OT-Sicherheit in der Strombranche herausgegeben. Wir von ALSEC sind primär in diesem Sektor tätig und wissen daher, dass die Umsetzung dieser Empfehlungen noch vielerorts am Anfang steht. Das hat auch damit zu tun, dass die Projekte zum einen sehr aufwendig sind und zum anderen die notwendigen Fachleute fehlen, um eine durchgehende Cybersicherheit zu gewährleisten.

Gibt es denn konkrete regulatorische Anforderungen im Bereich OT-Security?

Reto Amsler: Aktuell muss man das leider verneinen, zumindest für die Schweiz. In Deutschland beispielsweise existieren mit der KRITIS-Rechtsverordnung und dem IT-Sicherheitsgesetz Vorgaben für die Betreibenden von Kritischen Infrastrukturen. Hierzulande gibt es mittlerweile für den Energiesektor die besagte Branchenempfehlung, welche auf der Basis von bestehenden Standards, Best Practices sowie dem aktuellen Stand der Technik beruht, die letztlich aber nur das ist: eine Empfehlung. Das ist problematisch, da SCADA-Systeme oft schlüsselfertig von den Anbietern übernommen werden. Die Hauptanforderung von Kundenseite lautet: Das System muss primär verlässlich funktionieren. Auf das Thema «Security» legte man hingegen bisher viel zu wenig Wert, auch vonseiten der Hersteller, da der Kundendruck in den Ausschreibungen fehlte. Die Quintessenz lautet dementsprechend: Die Betreibenden von Kritischen Infrastrukturen müssen künftig höhere Anforderungen hinsichtlich Sicherheit stellen. «Security by Design» wäre hier anzustreben.

Gibt es ausreichend Know-how im Bereich OT-Security, um «Security by Design» zu etablieren?

Reto Amsler: Auch diese Frage muss man aktuell bedauerlicherweise verneinen. Das Grundproblem liegt darin, dass OT-Security nicht attraktiv scheint im Vergleich zu anderen Cybersecurity-Disziplinen. So wird zwar an den Fachhochschulen viel Know-how hinsichtlich Cybersecurity geschaffen, doch diese Expertise konzentriert sich vornehmlich auf den IT-Bereich. Industrielle Umgebungen hingegen sind weniger gefragt. Der Bereich OT- oder SCADA-Security kommt heute noch viel zu kurz. Das ist eine bedauerliche Entwicklung, denn der Bedarf an sicheren OT-Lösungen wird mit den ganzen Industrie-4.0-Themen noch zunehmen. Wie bereits angetönt, haben die ersten Blackouts in der Ukraine 2015 und 2016 klargemacht, wie gefährlich ein Cyberangriff auf Kritische Infrastrukturen sein kann.

Sind die Schweizer Stromnetze geschützt vor Cyberangriffen?

Markus Lenzin: Jein, weil sie derzeit mehrheitlich noch vom Internet abgekoppelt funktionieren. Doch es gibt andere Möglichkeiten, um in diese Systeme zu gelangen. Schadsoftware kann zum Beispiel durch USB-Sticks eingeschleppt werden. Oder wenn eine Person in den Ferien ihren Laptop im Internet verwendet und nach ihrer Rückkehr wieder ans System der Firma anhängt. Auf diese Weise finden Cyberkriminelle ihren Weg in die Anlagen von Kritischen Infrastrukturen. Das lässt sich also meistens auf menschliches Fehlverhalten sowie fehlende Awareness zurückführen. Hinzu kommt die Tatsache, dass unser Stromnetz mittel- bis langfristig noch mehr vernetzt sein wird. Smart Grids uns Smart Meters sollen ein «intelligentes Stromnetz» schaffen, das unter anderem Energieschwankungen ausgleichen kann und so die Versorgungssicherheit erhöht. Durch diese Vernetzung nimmt aber auch der Gefährdungsgrad sprunghaft zu. Darum sollte man mit externen Fachleuten zusammenarbeiten und bereits jetzt die notwendigen Schritte einleiten, die zu einer erhöhten OT-Sicherheit beitragen.

Wie unterstützen Sie bei Alsec Cyber Security Ihre Kundschaft dabei?

Reto Amsler: Es gibt verschiedene Andockstellen, über die wir die Betreibenden von Kritischen Infrastrukturen mit unserer Erfahrung, unserem Fachwissen sowie unserem Technologieverständnis unterstützen. Eine essenzielle Aufgabe von uns besteht in der Schaffung von Awareness, Transparenz sowie klaren Zuständigkeiten. Denn oft ist im Unternehmen nicht festgelegt, wer für welche Aspekte von OT-Sicherheit verantwortlich ist. In den meisten «gewöhnlichen» Firmen liegt diese Kompetenz beim CISO, doch in Energieversorgungsunternehmen sind es meist die Expertinnen und Experten der Energietechnik, die den technischen Takt vorgeben. Und diesen geht es vor allem um die Aufrechterhaltung der Versorgungssicherheit. Der CISO hat darauf keinen oder wenig Einfluss. Solche organisatorischen Stolpersteine entfernen wir, indem wir Assessments durchführen und uns so einen Einblick in die Wirkmechanismen des Unternehmens verschaffen. Basierend auf diesen Learnings erstellen wir gemeinsam mit dem Kunden eine Strategie mit einem Massnahmenplan, welcher hilft, Bedrohungen frühzeitig zu erkennen – und entsprechende Massnahmen rechtzeitig zu implementieren.

Markus Lenzin: Nebst diesen präventiven Massnahmen stehen wir unserer Kundschaft auch zur Seite, wenn es darum geht, auf Angriffe zu reagieren. Das Incident Management stellt sicher, dass Attacken sofort erkannt und schnellstmöglich unschädlich gemacht werden. Ziel dabei ist immer das Aufrechterhalten des sicheren Betriebs einer Kritischen Infrastruktur. Dazu gehören auch flankierende Massnahmen wie die Netzwerksegmentierung: Auf diese Weise können die Anlagen weiterlaufen, während man andernorts die Gefährder unschädlich macht.

Was hat es mit Ihrem IT-/OT-Cyberlabor auf sich?

Reto Amsler: Dieses ist enorm wichtig, um den Akteuren der Energiebranche die Relevanz von OT-Sicherheit aufzuzeigen. Wir bieten ihnen in Zusammenarbeit mit der HSLU ein Praxislabor an, welches den aktuellen Cyber-Security-Vorgaben der Branche entspricht und alle aktuellen Technologien umfasst. Das Labor beinhaltet sechs Unterwerke mit Anbindung an ein zentrales Leitsystem, dem SCADA. Wir stellen dieses praxisorientierte Labor einem breiten Publikum für praktische Lösungen, Integration und Weiterbildung zur Verfügung und können es ebenfalls gut an andere Branchen adaptieren. So wird das relativ abstrakte Thema OT-Security im wahrsten Sinne des Wortes erfassbar und greifbar. Dieses wichtige Fachwissen weiterzugeben, ist eines unserer zentralen Anliegen. Aus diesem Grund bieten wir auch eigene oder gemeinsam mit dem VSE OT-Security-Kursreihen für technisches Personal und Führungskräfte mit einer anschliessenden Zertifizierung an.

Über die Alsec Cyber Security Consulting AG

Gegründet am 1. März 2019 von Markus Lenzin und Reto Amsler, fokussiert sich die Alsec Cyber Security Consulting AG auf die Erbringung von Cyber-Security-Dienstleistungen im Operational Technology (OT) Umfeld nach höchsten Standards. Die Kundschaft umfasst Organisationen und Unternehmen, die Kritische Infrastrukturen betreiben, deren Sicherheit integral unter den Aspekten Organisation, Technologie, Prozesse und Ausbildung betrachtet werden muss.

Weitere Informationen finden Sie unter **www.alsec.ch**

ALSEC protect critical infrastructure