esolva
we make energy easy

news

Spielend einfach informiert.

Dezember 2021

Schütze deine Infrastruktur von A bis Z

Integrierte Sicherheit im Smart-Meter-Bereich: sicher – aber auch zukunftssicher?

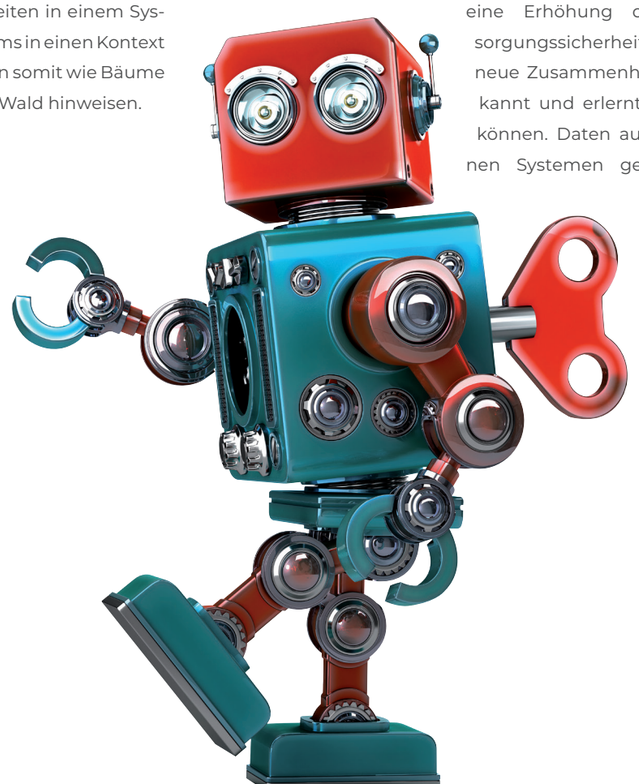
Cybersecurity ist in aller Munde, und spätestens seit dem BFE-Bericht zur Cybersicherheit in der Schweizer Stromversorgung ist gerade die Energiebranche unter Beobachtung. Gleichzeitig verändert die Energiewende zusehends die Situation in der Versorgungssicherheit. Gibt es einen Ansatz, um beiden Aspekten gleichzeitig entgegenzukommen?

Überall sind Bäume, nur wo ist der Wald?

In der heutigen Systemlandschaft sind Daten, die für den sicheren, leistungsfähigen und effizienten Netzbetrieb von Energieversorgungen notwendig sind, in vielen verschiedenen Systemen verteilt. Diese Systeme sind oftmals nicht miteinander verbunden und kommunizieren nicht miteinander. Der tägliche Betrieb ist gekennzeichnet von vielen manuellen Prozessen und uneinheitlichen Zugriffsrechten. Dies führt zu zwei Problemen: Zum einen sind manuelle Prozesse durch den Faktor Mensch immer fehlerbehaftet. Diese Prozesse stellen für Cyberangriffe ein erhöhtes Risiko dar. Zum anderen werden detektierte Angriffe, Fehlermeldungen und Unregelmässigkeiten in einem System nicht mit denen eines anderen Systems in einen Kontext gebracht. Hinweise eines Systems werden somit wie Bäume wahrgenommen, die aber nicht auf den Wald hinweisen.

Digitalisierung zu Ende denken

Das von der esolva eigens entwickelte Produkt «Secure Smart Metering» setzt genau hier an, um Smart Metering nicht nur sicher, sondern auch zukunftssicher zu machen. Durch den Aufbau einer Plattform, in welcher Logdaten aus allen möglichen Quellen zusammengeführt werden können, sehen wir Meldungen in einem erweiterten Kontext. Indem die Daten mit verschiedenen Systemen abgeglichen werden, können Ungereimtheiten im Netzwerk besser erkannt werden. Dies ist eine Massnahme zur Reduzierung der Risiken von Cyberangriffen. Gleichzeitig ergibt die Verbindung zwischen den Systemen eine Erhöhung der Versorgungssicherheit, da neue Zusammenhänge erkannt und erlernt werden können. Daten aus einzelnen Systemen generieren somit einen Mehrwert weit über ihr ursprüngliches System hinaus – ein Zeichen echter Digitalisierung.



Sicherheit in drei Aspekten

Unsere drei Aspekte lauten «Wir machen uns sicherer», «Wir machen euch sicherer» und «Wir machen das System sicherer». Während das neue Produkt «Secure Smart Metering» dem System ein höheres Sicherheitsniveau gibt, als in der Branche bisher üblich war, sind wir seit geraumer Zeit damit beschäftigt, unsere eigenen Prozesse und Systeme immer wieder Sicherheitstests zu unterziehen. Neben unserer ISO-27001-Zertifizierung wird das Bewusstsein der Mitarbeitenden bezüglich Cyberkriminalität immer wieder geschärft, sei es durch Phishingmailtests oder durch ein Audit von externen Experten. Wir garantieren so nicht nur die Sicherheit, sondern auch die stetige Integrität und Verfügbarkeit unserer Daten.

Der Aspekt «Wir machen euch sicherer» wird mit dem Security Assessment abgedeckt. Wir analysieren hierfür die Organisationsstruktur des Kunden, was implizit auch die Infrastruktur der IT (Information Technology) und der OT (Operational Technology) beinhaltet. So können kritische Gegebenheiten identifiziert und ein Bericht mit Handlungsempfehlungen verfasst werden. Die Empfehlungen können in Kooperation mit der esolva oder mit der Unterstützung anderer Unternehmen umgesetzt werden. Nach dem initialen Security Assessment steht es dem Kunden offen, weitere Assessments beizuziehen, beispielsweise ein technisches Audit, einen internen Pen-Test oder ein ICS-Audit.

Durch die Abdeckung aller drei Aspekte kann sichergestellt werden, dass das Gesamtsystem, mit all seinen Schnittstellen, eine hohe Grundsicherheit hat und damit einen Beitrag zu einer sicheren Energieversorgung leistet.

Im Gespräch

mit Jean-Marc Schreiber, CEO

Energieversorger gehören meist zur Unternehmenskategorie der KMU. Warum sind deiner Ansicht nach KMU eher von einem Cyberangriff bedroht als Grossunternehmen?
Ganz am Anfang standen die Grossunternehmen im Fokus der Angreifer. Grossunternehmen befassen sich jedoch seit Jahren mit der Thematik Cybersecurity und sind dementsprechend gut aufgestellt. Da ist ein Durchdringen für einen Angreifer sehr aufwendig. Das hat die Kriminellen bewogen, die Taktik zu ändern und Angriffe mittlerweile völlig willkürlich vorzunehmen. Ein Eindringen in die IT-/OT-Infrastruktur eines KMU ist wesentlich einfacher und somit lukrativer für die Angreifer.

Leistet die esolva einen aktiven Beitrag, um die Schweizer Energiebranche beim Thema IT-/OT-Security zu sensibilisieren und weiterzubringen?
Ja. Die esolva engagiert sich unter anderem aktiv beim Nationalen Zentrum für Cybersicherheit (NCSC). Die esolva gehört zum geschlossenen Kundenkreis des NCSC. Das bringt primär unseren Kunden grosse Vorteile. Einerseits wirken wir an vorderster Front mit, um neue Sicherheitsmassnahmen zu kreieren, und andererseits sind wir jeweils früher informiert als die breite Öffentlichkeit. So kann beispielsweise schneller auf grössere Cyberattacken reagiert werden, und die entsprechenden Massnahmen können getroffen werden.

Der Mensch ist und bleibt das schwächste Glied in der Kette. Wie kann diese Schwäche in eine Stärke transferiert werden?
Es ist ganz wichtig, dass neben den technischen Vorkehrungen unbedingt auch die Mitarbeitenden aktiv in den Sicherheitsprozess eingebunden werden. Seitens der esolva geschieht dies regelmässig mit Informationsveranstaltungen, internen Kommunikationen, Schulungen und Phishingtests. So wird das Bewusstsein geschärft, und jeder trägt zum Schutz für die Kunden und das Unternehmen bei.

Editorial

«Wir können den Wind nicht ändern, aber die Segel anders setzen» – nach diesem Grundsatz von Aristoteles richten wir unsere Dienstleistungen immer wieder neu aus. Dass sich der Energiemarkt im Wandel befindet, ist gewiss nichts Neues, aber nach wie vor aktuell.

Neue Dienstleistung für den Schutz der IT-/OT-Infrastruktur
Die Weiterentwicklung der Hardware- und Softwaresysteme bringt viele Vorteile für das Energieversorgungsunternehmen mit sich, aber auch Gefahren. Denn umso mehr Daten vorhanden sind, darauf zugegriffen werden kann und verarbeitet werden, umso interessanter sind diese für Hacker. Eine geschützte IT-/OT-Infrastruktur macht es den Hackern schwer, in dein Unternehmen einzudringen – wir zeigen dir auf, wie du dich schützt.

Eine Haustüre wird verriegelt – das gilt es auch bei der IT-/OT-Infrastruktur zu tun
Jeder von uns kennt es. Wenn wir nach Hause kommen, schliessen wir die Türe hinter uns ab. So muss das auch bei der IT-/OT-Infrastrukur unseres Unternehmens funktionieren. Wir müssen uns schützen, um ein Eindringen so schwierig wie möglich zu machen. Das Security Assessment der esolva hilft dir, ein funktionierendes Türschloss zu finden.

Im Namen des gesamten esolva-Teams wünsche ich dir eine schöne Adventszeit und einen erfolgreichen Jahresabschluss. Ich freue mich auf die persönlichen Begegnungen im Jahr 2022.

Marc Gerber
Leiter Marketing & Sales

IT-Sicherheit wird für KMU zum Grundbedürfnis der Zukunft

Mal ehrlich: Welcher Betrieb läuft heute noch ohne funktionierendes IT- und/oder OT-System? So ziemlich gar keiner. Klar, dass diese Systeme den grössten Schutzbedarf benötigen. Nur, schützen wir die Systeme wirklich – und wie?

Täglich werden auf Schweizer Unternehmen Cyberangriffe verübt. Zum grossen Entsetzen: meist erfolgreich für die Angreifer. Ein solcher Angriff kann ein Unternehmen die gesamte Existenz kosten. Denn kaum ein Unternehmen funktioniert noch komplett autonom, sprich, praktisch jeder ist für die Aufrechterhaltung des Betriebs auf die IT- und OT-Systeme angewiesen.

Klar definierte technische Massnahmen zur Vorbeugung von Cyberangriffen tätigen

Die technischen Massnahmen tragen schon einen wesentlichen Teil zum Schutz vor Angriffen bei. Hierzu zählen als Minimum ein funktionierender Virenschutz, regelmässig durchzuführende Updates, eine sauber eingerichtete Firewall sowie eine Zwei-Faktor-Authentifizierung. Backups mit Speicherung der Daten helfen, in einem Angriffsfall auf früher gespeicherte Daten zuzugreifen. Ein Datenverlust ist so zwar immer noch möglich, er fällt aber wesentlich geringer aus. Zudem trägt jeder einzelne User mit starken Passwörtern und deren regelmässiger Auswechslung ebenfalls zu einer hohen IT-Sicherheit bei.

Erst kürzlich war ein Unternehmen in der Energiebranche Opfer eines Angriffs

Die Wahrscheinlichkeit eines Hackerangriffs ist hoch. Ein aktuelles Beispiel zeigt es: Im November 2021 wurde ein KMU aus der Energiebranche gehackt. Nach über zwei Wochen waren die Systeme des betroffenen Unternehmens immer noch down. Das zeigt, wie wichtig die vorgängige Durchleuchtung der IT- und OT-Infrastruktur ist – das Security Assessment eruiert deinen aktuellen Stand und schlägt Massnahmen vor.

Gerätetest nach der Norm SNR 462638

Defekte Elektrogeräte verursachen in der Schweiz jedes Jahr zahlreiche Brände und Elektrounfälle mit Personenschaden. Das muss nicht sein! Wir helfen dir, diese Risiken zu vermeiden.

Als Arbeitgeber bist du gemäss Verordnung über die Verhütung von Unfällen (VUV) verpflichtet, dass die elektrischen Arbeitsmittel in deinem Betrieb sicher sind. Zur Erhaltung dieser Sicherheit müssen die Arbeitsmittel regelmässig geprüft und diese Prüfung dokumentiert werden. Vernachlässigst du diese Pflicht, kann dies bei einem Unfall zu hohen Schadenersatzforderungen führen.

Diese Geräte müssen geprüft werden

- Elektrowerkzeuge
- Kabelrollen, Verlängerungs- und Geräteanschlussleitungen
- Laborgeräte
- Mess-, Steuer- und Regelgeräte
- Geräte zur Spannungsumformung und -erzeugung, die nicht Teil der Installation sind
- Geräte der Unterhaltungs-, Informations- und Kommunikationstechnik
- Leuchten, die nicht Teil der Installation sind
- Geräte für den Hausgebrauch und ähnliche Zwecke

Verschiedene Prüfintervalle für die Geräte

Die Prüfintervalle für die Wiederholungsprüfung werden vom Arbeitgeber aufgrund der Herstellerangaben festgelegt. Fehlen diese Herstellerangaben, muss eine Risikobeurteilung aufgrund der Empfehlungen der SNR 462638 vorgenommen werden. Je nach Einsatzort, Gebrauchshäufigkeit und Umgebungsbedingungen schwanken die Prüfungsintervalle zwischen sechs Monaten und fünf Jahren. Neben der Wiederholungsprüfung muss auch bei jeder Reparatur oder Instandhaltung eine Prüfung durchgeführt und dokumentiert werden.

Prüfbericht ist als Nachweis für den Kunden jederzeit abrufbar

Nach der Prüfung werden von den Spezialisten der esolva alle Messwerte pro Gerät in einem Prüfprotokoll festgehalten und in einer Datenbank abgelegt. Die Prüfberichte in der esolva-Datenbank sind für den Kunden jederzeit abrufbar. Damit hat der Kunde den Nachweis, dass die Geräte sicher sind und die empfohlenen Prüfungen durchgeführt wurden.

Ransomware-Attacken: Die Gefahr lauert überall

Ransomware, auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner genannt, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Manchmal fordern die Angreifer Lösegeld, manchmal aber auch nicht. Die Auswirkungen für ein Unternehmen können fatal sein und bis zum Konkurs führen.

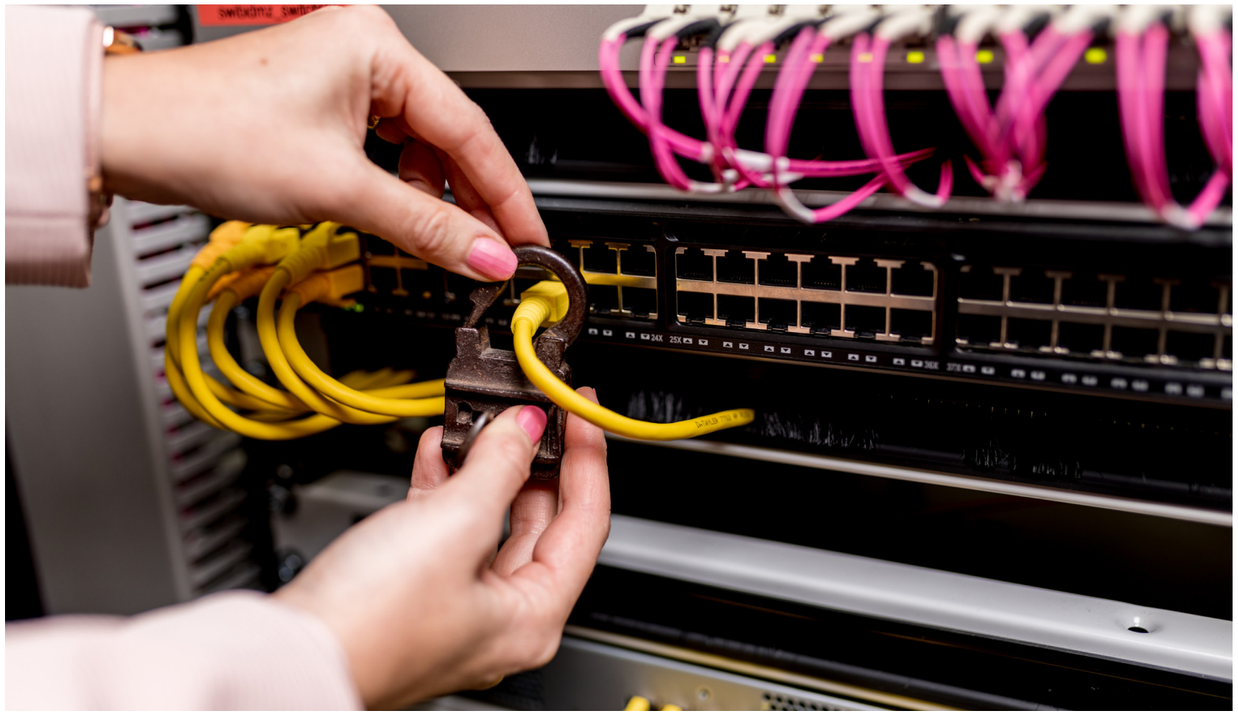
Bei einer Ransomware-Attacke werden die Daten verschlüsselt. Dies gilt es zu verhindern.

In den Medien ist immer öfters zu erfahren, dass Unternehmen von einer sogenannten Ransomware-Attacke betroffen sind. Bei einer solchen Attacke wird z. B. über eine Phishingmail eine Schadsoftware eingeschleust, welche dann Daten oder die gesamte Client- und Serverinfrastruktur verschlüsselt, sodass nicht mehr darauf zugegriffen werden kann. Die Angreifer stehlen vorgängig die Daten und verschlüsseln sie anschliessend, um ein Lösegeld zu erpressen. Wenn nicht bezahlt wird, können die Angreifer die Daten im Darknet weiterverkaufen – oder das Unternehmen erneut erpressen. Nach Zahlung des Lösegeldes werden die Daten wieder entschlüsselt – oder auch nicht. Es ist bereits vorgekommen, dass Unternehmen, welche von einer solchen Attacke betroffen waren, Konkurs anmelden mussten, weil sie nicht mehr auf ihre Daten zugreifen konnten.

Digitalisierung zu Ende denken

Solche Ransomware-Attacken sind schwierig zu erkennen. Sehr oft tummeln sich die Angreifer monatelang im Netzwerk herum und schlagen dann plötzlich zu. Die entsprechende Sensibilisierung der Mitarbeitenden auf solche Themen ist sicher hilfreich – dennoch empfiehlt die esolva, auch eine Software einzusetzen, welche Ransomware erkennt. So können betroffene Netzwerksegmente schon frühzeitig isoliert und ein grösserer Schaden vom Unternehmen abgewendet werden. Ebenso wichtig sind Offline-Backups. Diese sind eine Art Lebensversicherung, denn es gilt zu verhindern, dass die eigenen Backups verschlüsselt werden können. So hat das Unternehmen im Angriffsfall die Chance, die bestehenden Daten wieder herzustellen und den Betrieb innert nützlicher Frist wieder aufzunehmen.

Wichtig ist, sich bewusst zu sein: Es stellt sich nicht die Frage, «ob» du angegriffen wirst, sondern «wann».



Elektrokontrollen in der Migros-Betriebszentrale Gossau

Die Migros trägt einen wichtigen Teil zur Lebensmittel-Grundversorgung der Schweizer Bevölkerung bei. Somit ist es selbsterklärend, wie wichtig eine funktionierende und sichere Stromversorgung ist. Nur wenn alle Geräte einsatzfähig sind, funktioniert die Nahrungsmittelkette zur richtigen Zeit am richtigen Ort.

Die Betriebszentrale in Gossau ist das bedeutendste Verteilzentrum für das Filialnetz der Genossenschaft Migros Ostschweiz. In riesigen Kühlhallen werden beispielsweise die Frischprodukte gelagert, bevor sie an die entsprechenden Filialen ausgeliefert werden. Eine funktionierende Stromversorgung ist hier unerlässlich. Der Schaden wäre bei einem Ausfall immens. Deshalb setzt die Migros-Betriebszentrale Gossau auf die regelmässigen periodischen Elektrokontrollen durch die esolva und lässt zudem das betriebseigene Personal durch die Spezialisten der esolva ausbilden.

Periodische Elektrokontrolle vom Bürobetrieb bis zur Recyclinganlage

Die Migros-Betriebszentrale in Gossau ist auf verschiedene Gebäudekomplexe aufgeteilt und mit ganz unterschiedlichen Maschinen und Anlagen ausgestattet – vom Bürobetrieb bis zur Recyclinganlage. Die Elektroinstallationen sind nicht nur als Teil der Liegenschaft zu betrachten, sondern sie sind vielmehr das Herzstück aller elektrischen Anlagen und daher sehr schützenswert.

Nachteinsätze für eine unterbruchsfreie Stromversorgung der Migros-Betriebszentrale

In der Verordnung über elektrische Niederspannungsinstallationen (NIV) ist festgehalten, in welchem Intervall die periodischen Kontrollen durchgeführt werden müssen. Die Verantwortung zur Einhaltung dieser Fristen liegt beim Eigentümer. Deshalb ist ein verlässlicher Partner für die termingerechte Ausführung sehr wichtig. Für eine nahtlos funktionierende Lieferkette sind Stromunterbrüche während des Tagesbetriebs möglichst zu vermeiden. Es ist für die esolva-Spezialisten selbstverständlich, diese Kontrollen teilweise während der Nacht durchzuführen, um dadurch den Tagesbetrieb nicht zu stören. Weiter gehört es auch dazu, dass mal mehrere Kontrolleure gleichzeitig für eine grosse Kontrolle aufgeboten werden.

Wissensvermittlung und -überprüfung vom Profi für den Profi

Der sichere Umgang mit Strom will gelernt, laufend repetiert und überprüft sein. Deshalb werden die Migros-eigenen Betriebselektriker jährlich von einem Spezialisten der esolva überprüft. Des Weiteren bilden sich die Migros-Betriebselektriker intern wie extern weiter. Der Wissenstransfer steht ganz unter dem Motto: vom Profi für den Profi. So sind die Migros-Betriebselektriker befugt, den 24-Stunden-Betrieb unter den aktuell geltenden Normen und Richtlinien sicherzustellen.

Herzlichen Dank an das ganze Team der Migros-Betriebszentrale Gossau für die vertrauensvolle und partnerschaftliche Zusammenarbeit.

Peter Gallego
LEITER GEBÄUDETECHNIK,
GENOSSENSCHAFT MIGROS OSTSCHWEIZ

Durch das umfassende Fachwissen und die unkomplizierte Zusammenarbeit mit der esolva können unsere periodischen Kontrollen sauber abgewickelt werden. Dies schont unsere Ressourcen und hilft mit, bestehende Prozesse zu vereinfachen.

Kurzmeldungen

Mehr auf **esolva.ch**

Die beliebte Branchenmesse findet wieder statt: Powertage vom 17. bis 19. Mai 2022 in der Messe Zürich

Endlich ist es wieder so weit: Die Branchenmesse Powertage findet wieder in der Messe Zürich statt. Nach dieser aussergewöhnlichen Zeit stehen die Powertage ganz besonders im Zeichen persönlicher Begegnungen. Denn nur ein Live-Event bietet die Möglichkeit für spontane Gespräche und das richtige Erleben der vielen Branchenneuheiten.
Unter www.esolva.ch/powertage findest du laufend die neusten Informationen. Wir freuen uns auf viele interessierte Messebesucher.

Mit Blitzschutzkontrollen Menschen, Installationen und Geräte schützen

Um nach einem Blitzeinschlag gefährliche Überspannungen mit Gefährdungspotenzial für den Menschen und das Risiko von Schäden an baulichen Anlagen zu verhindern, müssen Blitzschutzanlagen einwandfrei funktionieren. Fangeinrichtung, Ableitungseinrichtung sowie Erdungsanlage müssen korrekt dimensioniert sein. Dann kann die Anlage Blitze ableiten und den Blitzstrom in der Erde verteilen. Mehr zu den Blitzschutzkontrollen unter www.esolva.ch/angebot/sicherheit.

Agenda

Schaltkurse – Grundkurs und Refresher
8. und 10. Februar 2022, esolva Weinfelden
www.esolva.ch/schaltkurs

NIN-Weiterbildungskurs
23. März 2022, Pfarreizentrum Weinfelden
www.esolva.ch/nin-kurs