Investitionen in die Zukunft = Investir dans l'avenir

Autor(en): **Möll, Ralph**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **112 (2021)**

Heft 4

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-977541

dossier.

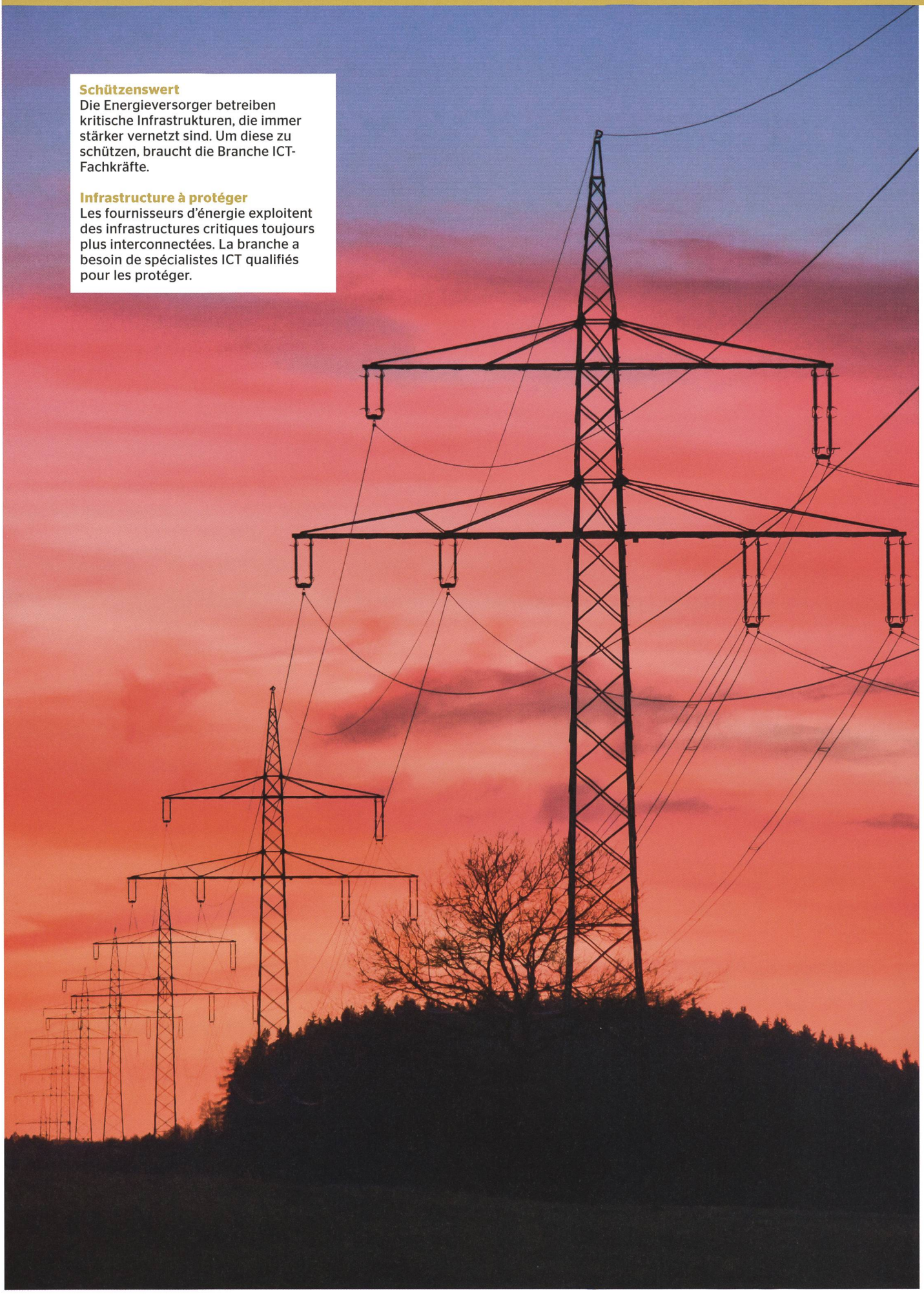
Investitionen in die Zukunft

ICT-Aus- und Weiterbildung | In der Energiebranche besteht nicht zuletzt aufgrund ihrer schützenswerten kritischen Infrastruktur grosser Bedarf nach ICT-Fachkräften. Verbände und Unternehmen kümmern sich aktiv um Nachwuchs.

Investir dans l'avenir

ICT formation et formation continue | La branche énergétique a un important besoin en spécialistes ICT, tout particulièrement en raison de son infrastructure sensible. Pour le couvrir, les associations et les entreprises s'engagent activement en faveur de la relève.

Bild | Figure: The Digital Artist/pixabay



Schützenswert
Die Energieversorger betreiben kritische Infrastrukturen, die immer stärker vernetzt sind. Um diese zu schützen, braucht die Branche ICT-Fachkräfte.

Infrastructure à protéger
Les fournisseurs d'énergie exploitent des infrastructures critiques toujours plus interconnectées. La branche a besoin de spécialistes ICT qualifiés pour les protéger.

Bild | Figure: hhach/pixabay

RALPH MÖLL

Was für eine schöne neue Welt: Die Energieversorgung der Weltgemeinschaft basiert vollständig auf Energieformen, welche als «erneuerbar» gelten. Autos, Lastwagen, Flugzeuge, Schiffe werden elektrisch angetrieben und stossen keine Treibhausgase mehr aus. Auch geheizt wird elektrisch und energieeffizient. Zur Produktion des dafür benötigten Stroms kommen weder fossile Rohstoffe wie Kohle oder Erdöl noch Kernenergie zum Einsatz. Im Gegensatz zur bisherigen zentralen Energieproduktion in grossen Kraftwerken werden vor allem Sonnen- und Windenergie stark dezentral gewonnen. Viele kleine Anlagen produzieren aus Sonnenlicht und Wind Strom und speisen diesen in das Netz. Typisch für diese dezentrale Stromproduktion sind nicht nur die höheren Anforderungen, welche das Netz dabei erfüllen muss, und die stark variierenden Stromflüsse, sondern auch eine riesige Menge Daten, welche Wasser-, Solar- und Windkraftanlagen produzieren. Diese Daten werden ausgetauscht, ausgewertet und abgelegt. Die Anlagen und Systemkomponenten kommunizieren dazu miteinander. Wo Systeme miteinander kommunizieren, bestehen Schnittstellen, welche – mögen sie noch so gut gesichert sein – angreifbar sind.

Einem breiten Publikum nach wie vor sehr gut in Erinnerung sind die Angriffe auf die Stromversorgung der Ukraine, welche 2015 und 2016 erfolgten. Die nachhaltige Prominenz dieser Angriffe dürfte zu einem grossen Teil in der Tatsache begründet sein, dass im Zuge der geopolitischen Entwicklungen (Annexion der zur Ukraine gehörenden Halbinsel Krim durch Russland) eine grosse Öffentlichkeit Notiz davon nahm. Und: Angriffe und Angriffsversuche auf die Stromversorgungen einer Nation hatte es zuvor gegeben und gab es auch danach. Nie war es Angreifern bislang jedoch gelungen, die Stromversorgung eines Landes tatsächlich zu unterbrechen. Die Folge: Hunderttausende ukrainische Haushalte waren stundenlang ohne Strom. Sogar der betroffene Stromversorger Kyivoblenergo hatte keinen Strom mehr, da die Angreifer auch die Notstromversorgung gekappt hatten.[1]

Will jemand rein, kommt er auch rein

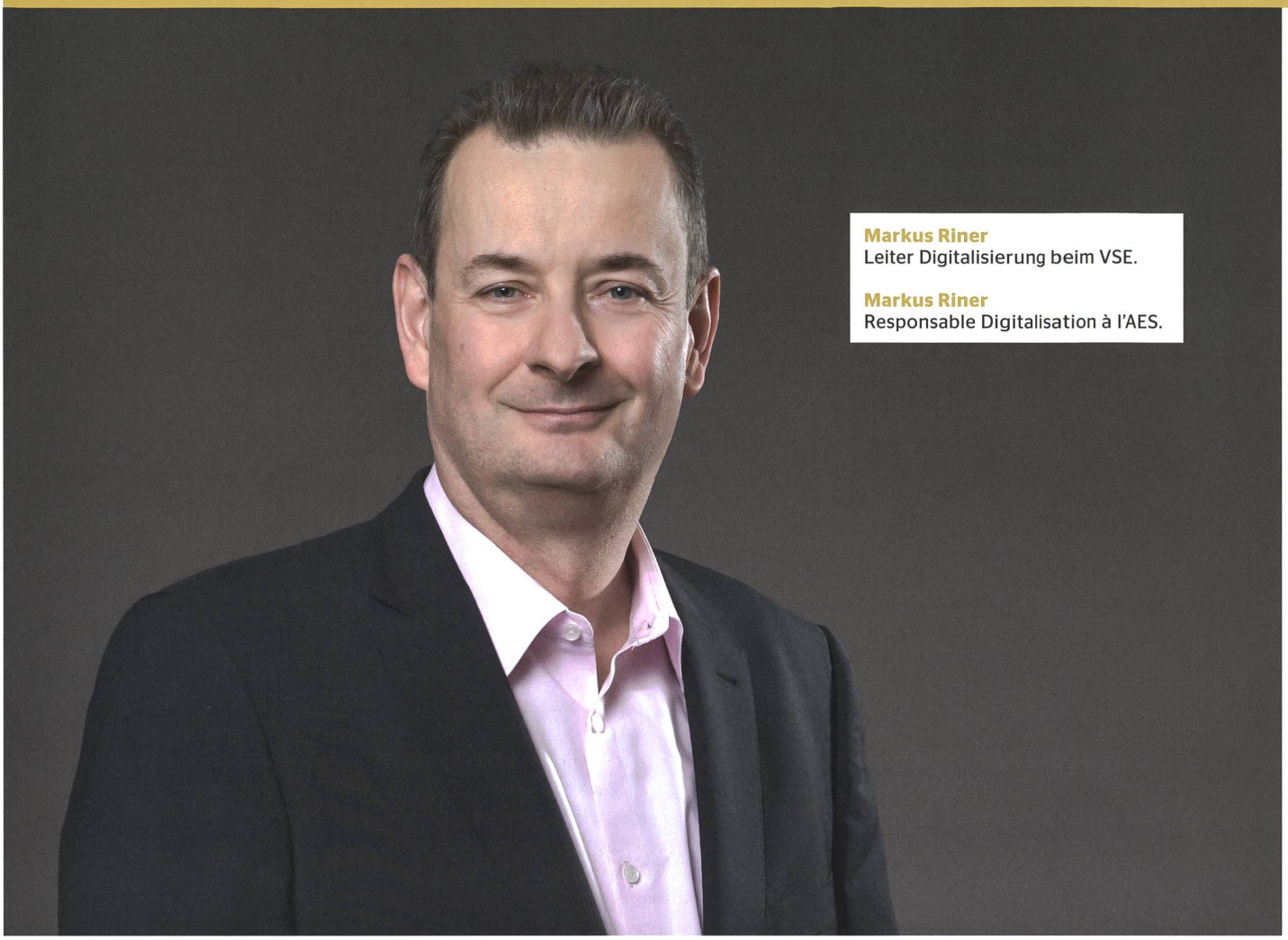
Das Beispiel zeigt: Ein Sicherheitssystem – selbst für kritische Infrastrukturen – kann noch so umsichtig konzipiert und aufgebaut sein, mit genügend krimineller Energie und Fachwissen ist es dennoch knackbar. Das Bewusstsein für Sicherheitsbelange hat in der Energiebranche in den letzten Jahren deutlich zugenommen. Das stellt auch Markus Riner, Leiter Digitalisierung beim Verband Schweizerischer Elektrizitätsunternehmen VSE, fest: «Die Vorfälle im Ausland haben dafür gesorgt, dass das Thema nicht mehr so stiefmütterlich behandelt wird wie früher.» Das habe sich auch in einer im vergangenen Jahr durchgeführten Branchenumfrage [2] gezeigt: «Gemeinsam mit dem Datenschutz wird die Cybersecurity als top Thema eingestuft.» Insgesamt sei der Branche klar, dass sie diesen Bereich im Auge haben und Mitarbeiterinnen und Mitarbeiter für diese Aufgaben weiterbilden und fit machen müsse.

Ça y est, nous y sommes parvenus ! L'approvisionnement énergétique mondial repose entièrement sur des formes d'énergie dites « renouvelables ». Voitures, camions, avions, bateaux : tous fonctionnent à l'électricité et n'émettent plus de gaz à effet de serre. Il en va de même des systèmes de chauffage, qui affichent par ailleurs une efficacité énergétique élevée. L'électricité nécessaire à leur utilisation ne provient ni de matières premières fossiles, telles que le charbon ou le pétrole, ni de l'énergie nucléaire. Contrairement à l'ancien mode de production – centralisé dans de grandes usines électriques – les énergies solaire et éolienne, notamment, s'inscrivent dans un schéma décentralisé : de nombreuses petites installations créent du courant à partir de la lumière du soleil et du vent, puis l'injectent dans le réseau. Ce type de production se caractérise non seulement par des exigences élevées pour le réseau et une forte fluctuation des flux, mais également par un énorme volume de données générées par les installations hydroélectriques, solaires et éoliennes, qui doivent être échangées, évaluées et archivées. Pour ce faire, les installations et composants du système communiquent entre eux. Or toute transmission entre systèmes suppose l'existence d'interfaces qui, même extrêmement sécurisées, peuvent être la cible d'attaques.

Nombre d'entre nous se souviennent de celles qui ont frappé le réseau électrique ukrainien en 2015 et 2016. Leur retentissement sur le long terme est probablement dû en grande partie au fait qu'en raison du contexte géopolitique de l'époque (annexion par la Russie de la péninsule de Crimée appartenant à l'Ukraine), un large public en a eu connaissance. Bien sûr, ce n'étaient pas les premières attaques ou tentatives d'attaques perpétrées contre le réseau électrique d'une nation, et il y en a eu d'autres par la suite, mais les auteurs de ces faits n'avaient encore jamais réussi à couper le courant d'un pays. Conséquence : des centaines de milliers de foyers ukrainiens ont été privés d'électricité pendant des heures. La compagnie d'électricité visée, Kyivoblenergo, n'a pas non plus été épargnée, les attaquants ayant également saboté l'alimentation de secours.[1]

Nul n'est jamais à l'abri

Comme le montre cet exemple, tout système de sécurité, aussi savamment conçu soit-il, peut être piraté par des personnes dotées des intentions criminelles et connaissances spécifiques suffisantes, et les systèmes d'infrastructures sensibles ne font pas exception. Ces dernières années, la branche énergétique a pris davantage conscience de l'importance de la sécurité. Markus Riner, responsable Digitalisation au sein de l'Association des entreprises électriques suisses (AES), dresse le même constat : « Les incidents survenus à l'étranger ont conduit à ne plus traiter la problématique avec la même légèreté qu'auparavant. » C'est également ce que montre une enquête de branche [2] menée l'an passé : « Avec la protection des données, la cybersécurité est devenue l'un des



Markus Riner
Leiter Digitalisierung beim VSE.

Markus Riner
Responsable Digitalisation à l'AES.

Vielfach hapert es jedoch gerade in diesem Bereich: dem Weiterbilden und Fitmachen der Mitarbeiterinnen und Mitarbeiter. «Vor allem die kleineren EVUs stossen bei Cybersecurity-Fragen aus Kapazitätsgründen schnell einmal an Grenzen. Als Branchendachverband wollen wir unsere Mitglieder daher unterstützen.» Konkret geschehe dies beispielsweise mit dem Aufbau eines VSE-Forums für Digitalisierung, das im zweiten Quartal dieses Jahres online gehen soll. Im Unterforum «Digital Upskilling» würden Fähigkeiten gesammelt und besprochen, welche nötig seien, um die Digitalisierung in der Branche erfolgreich umzusetzen. Weiter unterstützt der Verband seine Mitglieder mit spezifischen Weiterbildungsangeboten [3], mit Branchenempfehlungen und ganz generell mit der Förderung des Bewusstseins, dass Sicherheitsaspekte auf jeder Ebene wichtig sind.

E-Learning, Fake-Attacken und neue Kurse

Ein solches Angebot ist beispielsweise ein E-Learning-Kurs, mit dem Unternehmen ihre Mitarbeiterinnen und Mitarbeiter online testen können. Obwohl viele der dabei vermittelten Inhalte bekannt sein sollten, sind solche Kurse wichtig. Denn trotz der medialen Omnipräsenz des Themas Cybersecurity und der bekannten Gefahren, welche als harmloser Anhang verkleidet in der Mailbox landen

grands enjeux. » D'une manière générale, la branche sait qu'il faut faire preuve de vigilance et qu'elle doit former et préparer ses collaboratrices et collaborateurs en conséquence.

C'est toutefois à ce niveau que le bât blesse. « Par manque de ressources, les petites EAE en particulier se heurtent rapidement à leurs limites lorsqu'il s'agit de cybersécurité. En tant qu'association faîtière, nous voulons donc soutenir nos membres. » Concrètement, cette volonté passe par exemple par la création d'un forum AES dédié à la digitalisation dont la mise en ligne est prévue au cours du deuxième trimestre 2021. Le sous-forum « digital upskilling » devrait permettre de répertorier les compétences et d'évaluer celles qui sont nécessaires à la mise en œuvre réussie de la digitalisation au sein de la branche. En outre, l'association s'engage aux côtés de ses membres de diverses façons : formations continues spécifiques [3], recommandations de la branche et, de manière générale, actions de sensibilisation soulignant l'importance des questions de sécurité à tous les niveaux.

E-learning, simulations d'attaques et nouveaux cours

L'offre de formation propose notamment un cours d'e-learning que les entreprises peuvent tester en ligne

Bild | Figure: VSE | AES

können, sind die Mitarbeiterinnen und Mitarbeiter nämlich noch immer der Risikofaktor Nummer eins. «Das ist leider so», bestätigt Markus Riner. Nach wie vor seien Menschen, die unbedacht einen Link klickten oder einen Anhang öffneten, die grösste Gefahr für IT-Systeme. «Die Methoden der Angreifer werden aber auch immer raffinierter. Deshalb müssen wir die Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter auf dieses Thema lenken – immer und immer wieder.» Eine weitere Möglichkeit, um die digitale Fitness von Mitarbeiterinnen und Mitarbeitern zu testen, sind Fake-Attacken. Dabei werden im Unternehmen E-Mails mit einem verdächtigen, aber selbstverständlich ungefährlichen Anhang verschickt. Die Öffnungsrate gibt dann Aufschluss darüber, ob das Unternehmen zusätzliche Weiterbildungsmassnahmen ergreifen sollte oder nicht.

«Wir entwickeln laufend solche Schulungs- und Weiterbildungsangebote, um die Branche zu unterstützen», erklärt Markus Riner. «IT-/OT-Grundschutz für IT-/OT-System-Engineers» sei beispielsweise ein solcher Kurs, der dem Umstand Rechnung trage, dass OT-Infrastrukturen (Operational Technology) schon lange nicht mehr als Inselbetriebe funktionierten und folglich entsprechenden Risiken ausgesetzt seien. In besagtem Kurs wird nicht nur die aktuelle Cyber-Bedrohungslage vorgestellt, sondern auf Basis eines Branchendokuments auch gezeigt, welche präventiven Massnahmen EVUs gegen diese Bedrohung ergreifen können. «Cybersecurity ist – vor allem bei unseren kritischen Infrastrukturen – auf allen Ebenen wichtig und muss integrativ betrieben werden.» Aus diesem Grund hat der VSE gemeinsam mit der Branche eine entsprechende Task Force «Cyber Security IT-/OT-Systems and Clouds» gegründet, welche sich des Themas annimmt.

Gibt es bald eine Ausbildung mit Zertifikat?

Einen weiteren Ansatz bringt Thomas Mettler, Stabstellenleiter IT bei der Arbon Energie AG, ins Spiel: «Wünschenswert wäre ein Zertifikatslehrgang für IT-/OT-Security, beispielsweise ein CAS Energiewesen in Zusammenarbeit mit einer Hochschule. Das verleiht nicht nur der Ausbildung mehr Gewicht, sondern würde auch das Bewusstsein für Sicherheitsbelange in der Branche erhöhen.» In einer vom VSE und den Mitgliedunternehmen initiierten Koordinationsgruppe Digitalisierung, in welcher Thomas Mettler Einsitz nimmt, werden solche Themen diskutiert. «Dabei dürfen wir nicht ausser Acht lassen, dass IT nicht das Kerngeschäft unserer Branche ist und dass gerade kleinere Unternehmen schlicht nicht über die nötigen Ressourcen verfügen, um sich eigene IT-Abteilungen leisten zu können. So sei er selbst bei seiner Arbeitgeberin auch der einzige Informatiker. «Wenn man diese Arbeiten an einen externen Anbieter auslagert oder die Stellvertreterlösung mit externen Spezialisten regelt, kann dies genauso gut ein Lösungsansatz sein. Wichtig ist, dass sich das Management der Bedeutung bewusst ist und dass es die Aufgaben an die korrekte Stelle adressiert sowie die notwendigen finanziellen Mittel zur Verfügung stellt.»

avec leurs équipes. Bien qu'une grande partie des contenus abordés ne soient pas nouveaux, de tels cours sont importants. En effet, malgré l'omniprésence de la cybersécurité dans les médias et la connaissance des dangers que peuvent représenter, dans une messagerie, des pièces jointes semblant inoffensives, le facteur de risque numéro un demeure le personnel. « C'est la triste vérité », confirme Markus Riner. Celles et ceux qui, machinalement, cliquent sur un lien ou ouvrent une pièce jointe représentent aujourd'hui encore la plus grande menace pour les systèmes informatiques. « Mais les méthodes utilisées par les pirates sont également de plus en plus élaborées. Il est donc de notre devoir d'attirer sans cesse l'attention de nos équipes sur le sujet. » Les simulations d'attaques permettent aussi de tester l'agilité digitale de tous. Elles consistent à envoyer dans l'entreprise des e-mails contenant une pièce jointe douteuse – mais bien évidemment sans danger. En analysant le taux d'ouverture, il est ensuite possible de déterminer si l'entreprise doit ou non organiser des formations continues supplémentaires.

« Nous développons en permanence des offres de formation et de formation continue en vue de soutenir la branche », explique Markus Riner. Le cours « IT-/OT-Grundschutz für IT-/OT-System-Engineers » (protection de base IT/OT pour les ingénieurs système IT/OT) tient par exemple compte du fait que les infrastructures OT (Operational Technology) ne fonctionnent plus depuis longtemps de manière isolée et sont donc exposées aux risques associés. Il présente non seulement la situation actuelle en matière de cybermenaces, mais montre également, sur la base d'un document de la branche, les mesures préventives que peuvent prendre les EAE pour lutter contre celles-ci. « La cybersécurité est essentielle à tous les niveaux – d'autant plus pour nos infrastructures sensibles – et doit être intégrée dans le fonctionnement des entreprises. » En collaboration avec la branche, l'AES a donc constitué le groupe de travail « Cyber Security IT/OT Systems and Clouds ».

Une formation avec certificat : la solution ?

Thomas Mettler, responsable de l'état-major IT chez Arbon Energie AG, réfléchit à une autre approche : « Il serait souhaitable de mettre en place une formation avec certificat de capacité en matière de sécurité IT/OT, par exemple un CAS Énergie en collaboration avec une haute école. Cette solution conférerait non seulement plus de poids à la formation, mais permettrait également de sensibiliser davantage la branche aux questions de sécurité. » Ces sujets sont discutés au sein d'un groupe de coordination dédié à la digitalisation dont Thomas Mettler fait partie. Celui-ci a été créé par l'AES et les entreprises membres. « Nous ne devons pas oublier que l'informatique n'est pas notre cœur de métier et que les petites entreprises n'ont tout simplement pas les ressources nécessaires pour se doter de leurs propres services informatiques. » Il est d'ailleurs lui-même le seul informaticien au sein de son entreprise. « Confier ces tâches à un prestataire externe, ou régler la suppléance avec des spécialistes externes peut

Massiver Digitalisierungsschub

Ob mit einer eigenen Abteilung oder durch einen externen Dienstleister: Damit der Schutz der Systeme von EVUs überhaupt gewährt werden kann, braucht es zuerst einmal ausgebildete IT-Fachkräfte. Genau an diesen Fachpersonen besteht in der Schweiz aber ein eklatanter Mangel. So schlug beispielsweise ICT-Berufsbildung Schweiz – der Verband vertritt branchenübergreifend das Thema ICT-Kompetenzen in der Berufsbildung – im vergangenen Herbst Alarm und prognostizierte, dass bis 2028 rund 36 000 ICT-Fachkräfte fehlen würden.[4] Die Pandemie habe viele Unternehmen gezwungen, Kommunikationswege und Prozesse zu digitalisieren. Gleichzeitig erfolgten Strukturwandel und Wirtschaftsentwicklung aber noch schneller als prognostiziert. Dies führe zu einem exponentiellen Anstieg des Fachkräfte-Bedarfs, erklärt Serge Frech, Geschäftsführer von ICT-Berufsbildung Schweiz. Und: «Ist die Pandemie einmal ausgestanden, werden wir feststellen, dass Unternehmen mit digitalisierten Prozessen einen grossen Wettbewerbsvorteil haben. Dann werden ihre Mitbewerber nachziehen, und der Bedarf wird noch weiter steigen.»

être une approche de solution. Il faut surtout que le management ait conscience que cela est important, qu'il transfère les tâches au bon service et qu'il mette à disposition les moyens financiers nécessaires.»

Poussée massive de la digitalisation

Qu'une EAE dispose de son propre service ou fasse appel à un prestataire pour la protection de ses systèmes, l'important est de pouvoir compter sur des spécialistes informatiques qualifiés. Or la Suisse souffre d'un manque criant d'experts. L'automne dernier, ICT-Formation professionnelle Suisse – une association représentant les compétences ICT de toute la branche dans la formation professionnelle – tirait la sonnette d'alarme en annonçant que d'ici 2028, quelque 36 000 spécialistes ICT feraient défaut.[4] La pandémie a en effet contraint nombre d'entreprises à digitaliser leur communication et leurs processus. Mais, parallèlement, les mutations structurelles et les évolutions économiques se sont produites encore plus rapidement que prévu. L'ensemble va conduire à une augmentation exponentielle de la demande en spécialistes, analyse Serge Frech, direc-

Thomas Mettler
Stabstellenleiter IT bei Arbon Energie AG.

Thomas Mettler
Responsable de l'état-major IT chez Arbon Energie AG.

Bild | Figure: Arbon Energie AG

Serge Frech
Geschäftsführer ICT-Berufsbildung Schweiz.

Serge Frech
Directeur d'ICT-Formation professionnelle Suisse.

Zwar fehlen ICT-Fachkräfte in allen Bereichen, doch vor allem auf dem Gebiet ICT-Security ortet Serge Frech erheblichen Bedarf: «In diesem Bereich ist der Mangel massiv. Daher gehen wir auch davon aus, dass hier das grösste Wachstum zu erwarten ist.» Gerade in der Energiebranche mit ihren besonders schützenswerten kritischen Infrastrukturen seien gut ausgebildete ICT-Security-Fachleute extrem wichtig. Ein Aufruf an die Unternehmen, mehr Ausbildungsplätze zu schaffen, also? «Natürlich! ICT-Security umfasst ja nicht nur den Schutz von IT- und OT-Systemen, sondern es geht auch um Themen wie Datenhaltung und vor allem Datenschutz. Das betrifft jedes einzelne EVU.» Es sei ein Aufwand, Lernende auszubilden, aber diese Investition lohne sich. Lernende auf den eigenen Systemen auszubilden, zahle sich schon während der Ausbildung aus: «Mitarbeiterinnen und Mitarbeiter, welche im Betrieb ausgebildet worden sind, kennen und leben die Unternehmenskultur, sie sprechen die Unternehmenssprache und kennen die Prozesse in- und auswendig. Das sind quasi die perfekten Mitarbeiterinnen und Mitarbeiter.» Nun gibt es in der Energiebranche das geflügelte Wort, dass kein Kraftwerk wie das andere ist. Ausbildungen auf IT- und OT-Systemen können je nach Werk ganz andere Anforderungen an die Lernenden stellen. ICT Berufsbildung gestaltet daher die Ausbildungspläne so, dass Unternehmen sehr viel Spielraum

teur d'ICT-Formation professionnelle Suisse. « Une fois la pandémie derrière nous, nous constaterons que les entreprises appliquant des processus digitalisés auront un avantage concurrentiel considérable. La concurrence fera de même et le besoin en personnes qualifiées ira en s'amplifiant. »

Si la pénurie de spécialistes ICT est à déplorer dans tous les secteurs, elle concerne avant tout le domaine de la sécurité des ICT, comme l'explique Serge Frech : « Elle est colossale. Nous partons donc du principe que c'est ici que nous observerons la plus forte croissance. Dans la branche énergétique, qui se caractérise par des infrastructures particulièrement sensibles, il est crucial de pouvoir compter sur des spécialistes en sécurité des ICT qualifiés. » Est-ce donc un appel aux entreprises à créer plus de postes de formation ? « Bien évidemment ! La sécurité des ICT ne se résume pas à la protection des systèmes IT et OT ; elle englobe également des sujets comme la gestion et, surtout, la protection des données. C'est un point essentiel pour toutes les EAE. » Si former des apprentis est un investissement, celui-ci s'avère payant, et ce pendant l'apprentissage déjà : « Les collaboratrices et collaborateurs ayant été formés au sein de l'entreprise connaissent et incarnent la culture de cette dernière, et parlent le langage interne. Les processus n'ont aucun secret pour eux. Ce sont en quelque sorte les profils idéaux. » Dans la branche énergé-

Bild | Figure: ICT-Berufsbildung Schweiz | ICT-Formation professionnelle Suisse

erhalten, um ihren Nachwuchs auf eigenen Systemen auszubilden. «Sie sollen die Technologien und Systeme ihres Unternehmens so gut wie möglich kennenlernen.»

Die Interessenten wären da

Neben den Unternehmen sieht Serge Frech auch die Verbände in der Pflicht, sich für die ICT-Ausbildung einzusetzen. «Typische Branchenverbände wie der VSE oder Swissmem sind in kritischem Masse abhängig von einer funktionierenden IT. Mit ihrer Mitgliedschaft helfen sie nicht nur, die Zahl der Ausbildungsplätze zu erhöhen, sondern auch, ICT-Fachkräfte mit jenen Fähigkeiten auszustatten, die der jeweiligen Branche zugutekommen. Das ist vorbildlich.» So war beispielsweise der VSE, seit 2017 Mitglied bei ICT-Berufsbildung Schweiz, stark in die Entwicklung des eidgenössischen Diploms ICT Security Expert eingebunden. «An erster Stelle stehen aber die Unternehmen», sagt Serge Frech. «Es gibt mehr junge Menschen, die sich für eine ICT-Ausbildung interessieren, als entsprechende Lehrstellen. Dagegen können Unternehmen etwas tun, indem sie Ausbildungsplätze schaffen.»

Referenzen
[1] www.it-daily.net/it-sicherheit/cybercrime/26285-der-angriff-auf-das-ukrainische-stromnetz-schreibt-geschichte
[2] www.strom.ch/system/files/media/documents/202009_Paper%20Digital%20%40%20EVU_14.pdf
[3] www.strom.ch/de/veranstaltung/it-ot-grundschutz-fuer-it-ot-system-engineers-vertiefungsmodul-1-0
[4] www.ict-berufsbildung.ch/themen/news/detail/n-n/589/

Autor | Auteur
Ralph Möll ist Chefredaktor VSE.
Ralph Möll est rédacteur en chef AES.
→ VSE, 5000 Aarau
→ ralph.moell@strom.ch

tique, il est coutume de dire qu'aucune centrale ne se ressemble. Les formations aux systèmes IT et OT peuvent poser des exigences totalement différentes aux apprentis selon les structures. ICT-Formation professionnelle Suisse organise donc des plans de formation de manière à ce que les entreprises disposent de la marge de manœuvre nécessaire pour former la relève à leurs propres systèmes. « Celle-ci doit connaître les technologies et les systèmes de l'entreprise le mieux possible. »

La demande est là

Pour Serge Frech, outre les entreprises, les associations sont elles aussi tenues de s'engager en faveur de la formation ICT. « Les grandes associations de branche comme l'AES ou Swissmem dépendent de façon critique d'une structure informatique efficace. En adhérant, elles permettent non seulement d'augmenter le nombre de places de formation, mais également de fournir aux spécialistes ICT les compétences utiles à la branche. Elles montrent l'exemple. » Membre de l'ICT-Formation professionnelle Suisse depuis 2017, l'AES est par exemple fortement impliquée dans le développement du diplôme fédéral d'expert en sécurité des ICT. « Mais pour que les lignes bougent, il faut que les entreprises agissent », déclare Serge Frech. « Le nombre de jeunes intéressés par une formation ICT dépasse celui de postes d'apprentissage disponibles. Ce sont les entreprises qui ont la solution entre les mains: elles doivent créer des places de formation. »

Références
[1] www.it-daily.net/it-sicherheit/cybercrime/26285-der-angriff-auf-das-ukrainische-stromnetz-schreibt-geschichte (en allemand)
[2] www.strom.ch/system/files/media/documents/202009_Paper%20Digital%20%40%20EVU_14.pdf (en allemand)
[3] www.strom.ch/de/veranstaltung/it-ot-grundschutz-fuer-it-ot-system-engineers-vertiefungsmodul-1-0 (en allemand)
[4] www.ict-berufsbildung.ch/fr/themes/news/details/n-n/589/