Michael Paulus
Bereichsleiter Netze und Berufsbildung des VSE
michael.paulus@strom.ch

Responsable Réseaux et Formation professionnelle à l'AES
michael.paulus@electricite.ch

Eine Frage der Technologie?

Covid-19 hat viele von uns ins Homeoffice geschickt. Auch ich habe meinen Arbeitsplatz zu Hause für den täglichen Einsatz aufgerüstet und mein WLAN verstärkt. Ich war überrascht, wie schnell uns der Übergang in die Zusammenarbeit auf Distanz gelungen ist und wie effizient die elektronischen Werkzeuge eingesetzt werden konnten, nicht nur innerhalb des VSE, sondern auch mit anderen Unternehmen, Verbänden, Behörden.

Eine digitale Erfolgsgeschichte? Nun, der Newsticker von Melani, der Melde- und Analysestelle Informationssicherung des Bundes, berichtet zur gleichen Zeit: Zunahme von Phishing-Angriffen, grosse Welle von Erpresser-E-Mails, E-Mails mit angeblichen Steuerrückerstattungen. Offenbar nutzten kriminelle Absender die Gunst der Stunde vermehrt für Angriffe auf eine ausserhalb der Büroumgebung eingeschränkt geschützte IT-Infrastruktur. Klar, denkt man, die IT-Abteilungen sind gefordert, die Virenscanner und Firewalls auch für den Remote-Einsatz immer auf dem aktuellsten Stand zu halten oder ein geeignetes Sicherungskonzept für Dokumente einzusetzen.

Betrachtet man die erfolgreichen Angriffe genauer, dann ist jedoch nicht mangelhafte Technologie der Schlüsselfaktor, sondern der Mensch. Nach wie vor mit Abstand am häufigsten öffnen Mitarbeitende selbst die Einfallstore für Schadsoftware. Und tatsächlich, die Angriffe sind teilweise derart heimtückisch, dass sie auch auf den zweiten Blick mit «gesundem Menschenverstand» kaum zu erkennen sind. Die einzige Lösung dafür heisst Information und Sensibilisierung. Regelmässige Mitarbeiterschulungen und Kommunikationsmassnahmen sind unumgänglich. Welche Regeln sind am Arbeitsplatz, im Homeoffice einzuhalten? Was mache ich, wenn ich Verdacht schöpfe? Wie mache ich meine Kolleginnen, Kollegen, Vorgesetzten aufmerksam?

Unsere Branche trägt mit dem Betrieb kritischer Infrastrukturen zur Energieversorgung eine besondere Verantwortung für die Gesellschaft. Wir müssen die notwendigen Vorkehrungen für Cyber Security treffen. Doch Technologie alleine reicht dafür nicht aus. Es braucht vor allem geschulte und aufmerksame Mitarbeitende, die bei einer verdächtigen E-Mail lieber einmal zu oft persönlich nachfragen. Der VSE unterstützt Sie bei Ihrer Aufgabe mit seinen Ausbildungen und Produkten.

Une question de technologie ?

Le Covid-19 a envoyé nombre d'entre nous en télétravail. J'ai moi aussi aménagé mon bureau à la maison pour le travail quotidien et renforcé mon wifi. J'ai été surpris de voir à quelle vitesse nous sommes passés sans problème à la collaboration à distance et avec quelle efficacité les outils électroniques ont pu être employés, non seulement au sein de l'AES, mais aussi avec les autres entreprises, associations et autorités.

Un succès numérique ? Ne nous réjouissons pas trop vite : le fil d'actualité de Melani, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération, rapporte dans le même temps une hausse des attaques d'hameçonnage, une large vague d'e-mails de chantage, des e-mails contenant de prétendus remboursements d'impôt, etc. Manifestement, les expéditeurs criminels profitent de l'occasion pour attaquer davantage une infrastructure hors de l'environnement du bureau, dont la protection est plus limitée. Bien sûr, pense-t-on, les services IT sont tenus de mettre constamment à jour les scanners antivirus et les firewalls également pour l'utilisation à distance ou d'instaurer un concept de sécurité approprié pour les documents.

Si l'on considère de plus près les attaques réussies, le facteur-clé n'est toutefois pas une technologie déficiente, mais bien l'humain. Dans la grande majorité des cas, les collaborateurs ouvrent eux-mêmes les portes d'entrée aux logiciels malveillants. Et, effectivement, certaines attaques sont tellement perfides que, même en y regardant à deux fois, le « bon sens » ne permet pratiquement pas de les identifier. La seule solution à cela : information et sensibilisation. Formations régulières des collaborateurs et mesures de communication sont indispensables. Quelles sont les règles à respecter sur le lieu de travail ? Et en télétravail ? Que faire si j'ai des soupçons ? Comment puis-je attirer l'attention de mes collègues ou de mes supérieurs le cas échéant ?

En exploitant des infrastructures critiques pour l'approvisionnement en énergie, notre branche assume une responsabilité particulière envers la société. Nous devons prendre les dispositions nécessaires à la cybersécurité. Mais la technologie à elle seule ne suffit pas. Il faut surtout des collaboratrices et des collaborateurs formés et attentifs, qui vérifient personnellement, et plutôt deux fois qu'une, s'ils se trouvent ou non face à un e-mail douteux. L'AES vous soutient dans votre tâche grâce à ses formations et à ses produits.