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

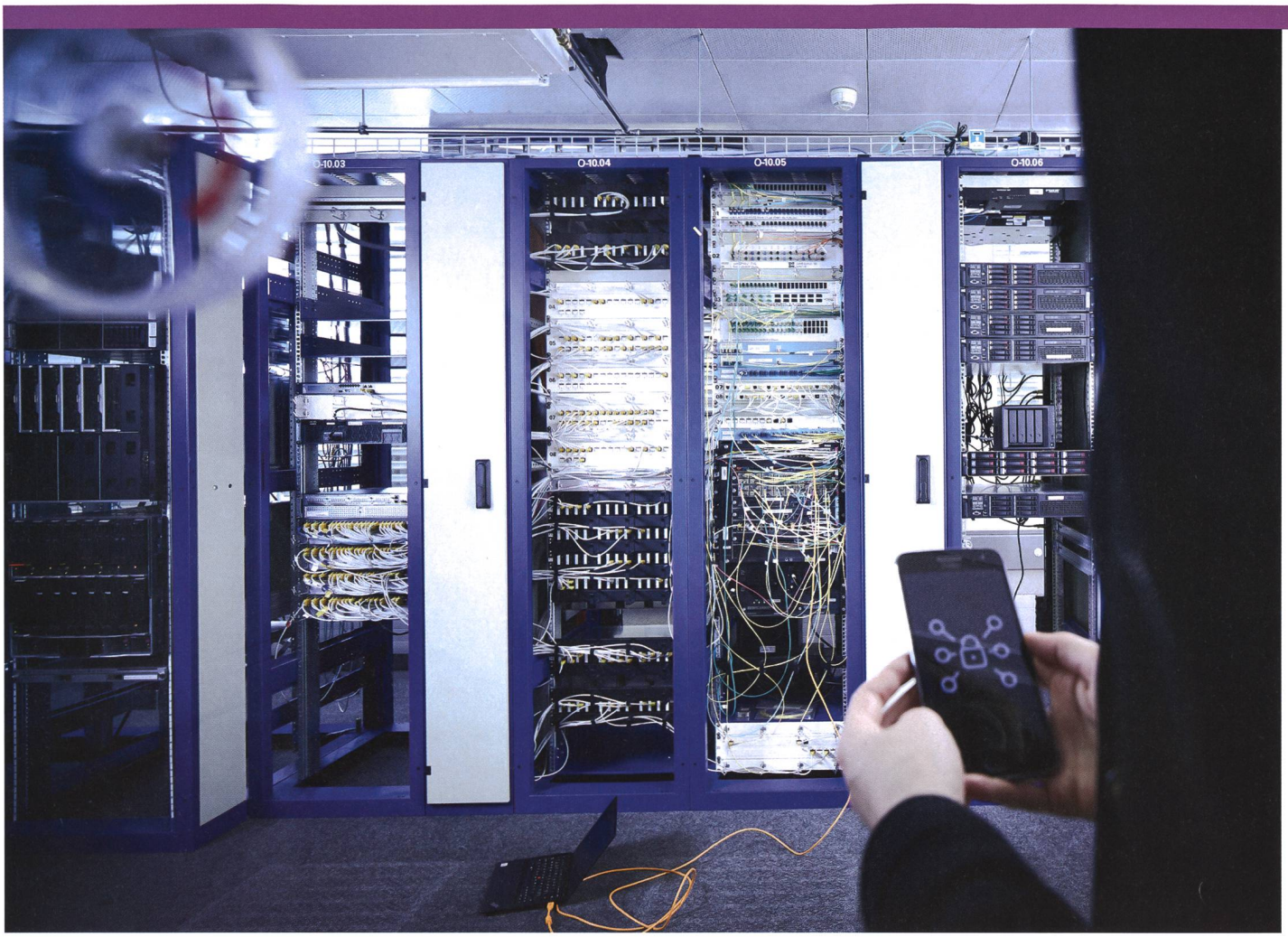
Band: 112 (2021)

Heft: 6

Artikel: Im Wettrüsten mithalten = Ne pas se laisser distancer!

Autor: Bangerter, Endre / Nikkel, Bruce

DOI: https://doi.org/10.5169/seals-977578



Im Wettrüsten mithalten

Strategien zur Abwehr von Cyberangriffen | Jeder und jede kann Ziel einer Cyberattacke werden. Da die Angreifer ihre Methoden ständig weiterentwickeln, sehen sich die potenziellen Opfer permanent mit neuen Bedrohungen konfrontiert. Doch auch die Möglichkeiten zur Abwehr werden immer besser.

ENDRE BANGERTER, BRUCE NIKKEL

Um gegen zukünftige Bedrohungen gewappnet zu sein, lohnt sich bisweilen ein Blick in die Vergangenheit. Das gilt auch beim Thema Cybercrime. Vor etwa 15 Jahren gehörten Bankkunden zu den ersten Opfern von Kriminellen, die versuchten, sich mit Trojaner-Programmen Zugriff auf das Internet-Banking zu verschaffen. Heute sind die Banken besser in der Lage, infizierte Kunden-Computer zu entdecken und Cyberangriffe rechtzeitig abzuwehren. Cyberkriminelle sind meistens Opportunisten. Wenn der Widerstand zu stark ist, suchen sie sich ein anderes Opfer oder ein neues Schlupfloch. So haben sie seit einigen Jahren vermehrt Firmen jeder Grösse und Branche mit Ransomware ins Visier genommen. Dabei ist häufig das gesamte IT-Netzwerk eines Unternehmens betroffen. Für die Freigabe der gehackten Daten versuchen die meistens aus dem Ausland operierenden Banden, ein Lösegeld in der Bitcoin-Währung zu erpressen. Die Fahndung nach den Tätern ist aufwendig und selten erfolgreich.

Menschen statt Maschinen hacken

Eine zunehmende Bedeutung hat Social Engineering, was sich mit «sozialer Manipulation» übersetzen lässt. Angreifer profitieren dabei von menschlichen Eigenschaften wie der Arglosigkeit. Es ist erstaunlich, wie viele Firmen ohne Not Informationen

Bild: BFH

preisgeben, die Eindringlingen Türen öffnen. Wenn etwa ein Job-Beschrieb auf der Firmenwebseite darüber Auskunft gibt, welche Software im Unternehmen im Einsatz ist, lässt sich das ausnützen – zum Beispiel indem sich ein Angreifer am Telefon als Mitarbeiter des Software-Herstellers ausgibt und ankündigt, er werde gleich ein Dokument mit wichtigen Update-Informationen schicken. Wird die Täuschung glaubhaft vorgebracht, öffnet der Empfänger möglicherweise das Dokument und gewährt einer Malware Zutritt ins Firmennetzwerk. Die Schwachstelle im System war dann nicht die Technik, sondern der Mensch. Ebenfalls zum Social Engineering gehören mit Methoden der künstlichen Intelligenz manipulierte Videos, in denen Gesichter verändert werden (Deepfakes). Damit kann man eine beliebige Person Dinge sagen lassen, welche diese Person in der Realität nie von sich gegeben hätte.

Vertrauen allein genügt nicht

Die Vernetzung in der digitalen Welt und die damit verbundenen gegenseitigen Abhängigkeiten eröffnen Hackern immer neue Möglichkeiten. Schlagzeilen machte der Fall des auf Netzwerkmanagement-Software spezialisierten US-Unternehmens Solarwinds. Wegen eines schwachen Passworts auf einem Updateserver konnten im Jahr 2019 Angreifer Schadprogramme in ein Softwareprodukt der Firma einschleusen und monatelang unentdeckt Kunden von Solarwinds ausforschen – eine klassische «supply chain attack». Eine einzige Sicherheitslücke am Ursprung der Lieferkette genügte in diesem Fall, um alle davon abhängigen Systeme zu infiltrieren. Die Erkenntnis aus diesem Vorfall lautet: Vertrauen ist gut, im Cyberspace aber nicht gut genug. Das gilt auch dann, wenn man Datenverarbeitung outsourct oder auf cloudbasierte Lösungen setzt. Dabei sollte gründlich geprüft werden, ob der externe Partner anerkannte Sicherheitsstandards erfüllt. Zudem sollten die gesetzlichen Bestimmungen des Landes beachtet werden, in denen der Partner seinen Geschäftssitz hat oder die anvertrauten Daten verarbeitet. Amerikanische IT-Dienstleister etwa sind von Gesetzes wegen verpflichtet, den US-Behörden Zugriff auf gespeicherte Daten zu gewähren («Cloud Act»), sogar wenn diese aus dem Ausland stammen.

Resignation ist keine Option

Unternehmen und Institutionen haben in den vergangenen Jahren gelernt, mit der Cyberkriminalität umzugehen. Das Bewusstsein, dass man jederzeit Zielscheibe eines Angriffs werden kann, ist gestiegen. Bei der Planung von Vorsorgemassnahmen stellt sich dennoch die Frage nach dem richtigen Verhältnis zwischen Aufwand und Nutzen. Hochstehende Technologien bieten einen guten Schutz, kosten aber viel Geld. Und absolute Sicherheit können auch sie nicht bieten. Deswegen den Kopf in den Sand zu stecken, ist dennoch die schlechteste Option. Angreifer und Verteidiger liefern sich ein permanentes Wettrüsten mit wechselnden Vorteilen für die eine oder die andere Seite. Damit wird man weiterhin leben müssen. Der IKT-Minimalstandard des Bundes kann dabei helfen, den Handlungsbedarf im eigenen KMU zu ermitteln und Abwehrmassnahmen zu planen.

Herausforderung Datenanalyse

Wer immer noch glaubt, mit einer Firewall und einem Antivirenprogramm Angreifern den Zugang zum Firmennetzwerk zu verunmöglichen, muss jedenfalls umdenken. Wirksame Abwehrmassnahmen erfordern eine permanente Überwachung aller Systeme und Netzwerke. Die grosse Herausforderung besteht darin, die grossen Datenmengen rasch zu verarbeiten. Dies ist Voraussetzung, um Gegenmassnahmen einleiten zu können, bevor die Malware Schaden anrichtet. Ein innovativer Ansatz besteht darin, die Daten mit Methoden des «Machine Learning» zu analysieren. Die meisten Schadprogramme sind nicht vollständig neu entwickelt, sondern verwenden einzelne Komponenten aus bereits existierender Malware. Diese müssen allerdings erst aufgespürt werden, was mit einer manuellen Analyse sehr aufwendig und teuer ist. Mit einem vom BFH-Spin-off «Threatray» entwickelten Analysetool ist es nun möglich, automatisch und in kürzester Zeit Korrelationen von einer Vielzahl von Samples zu prüfen. Dazu muss es laufend mit allen verfügbaren Informationen über bereits bekannte Schadprogramme gefüttert werden.

Vom Wissen der anderen profitieren

Ein immer wichtigerer Faktor für die Abwehr von Cyberangriffen ist der Austausch von Wissen und Informationen auf nationaler und internationaler Ebene. Fast jede Branche bildet heute «Threat intelligence Communities» – Teams von Spezialisten der Mitglieder, die sich den gemeinsamen Herausforderungen stellen. Im Fall der Elektrizitätsversorger beispielsweise ist dies das EE-ISAC («European Energy – Information Sharing & Analysis Center»). Es stellt Basisinformationen und Handlungsempfehlungen auch Nichtmitgliedern zur Verfügung. Ausserdem sollten sich Unternehmen und Organisationen das Know-how der Schweizer Bildungsinstitutionen zunutze machen. Die technischen Hochschulen sowie verschiedene Universitäten und Fachhochschulen sind in den Bereichen Cyber-Security und digitale Forensik tätig. Laufend kommen neue Bildungsangebote dazu, 2020 etwa der Studiengang MAS Digital Forensics & Cyber Investigation der Berner Fachhochschule. Das dabei akkumulierte Know-how steht privaten Partnern für die Entwicklung von Praxisanwendungen zur Verfügung.

Autoren
Prof. Dr. **Endre Bangerter** ist Co-Leiter des Institute for Cybersecurity and Engineering (ICE).
→ BFH, 2501 Biel
→ endre.bangerter@bfh.ch

Prof. Dr. **Bruce Nikkel** ist Co-Leiter des Institute for Cybersecurity and Engineering (ICE).
→ bruce.nikkel@bfh.ch

Nur wer FL-Leuchten im Rückbau getrennt entsorgt, schaltet richtig.

Alte FL-Leuchten müssen unbedingt getrennt entsorgt werden: Ihre Kondensatoren können PCB enthalten, eines der gefährlichsten Umweltgifte. Durch die lange Lebensdauer werden PCB-haltige Leuchten leider so schnell nicht aussterben und noch lange zum Rückbau-Alltag gehören. Da jedoch auch neuere Leuchten ohne Kondensatoren dem Elektro-Recycling zugeführt werden müssen, ist korrektes Handeln ganz einfach: Bestellen Sie die gewünschten Sammelgebinde konsequent auf jede Baustelle und instruieren Sie Ihr Personal zur Sortierung. Wir beraten Sie gerne.

Danke für die separate Entsorgung von Fluoreszenz-Leuchten, Sparlampen, LEDs, Dampflampen, allen anderen Leuchten und Elektrogeräten!

Die Gebinde werden kostenlos auf jede Baustelle geliefert und abgeholt.
Gebinde-Bestellungen und Abholaufträge per Tel. 043/255 20 00
oder auf www.slrs.ch > Entsorgung > **Abholaufträge** > Online-Abholauftrag.

SLRS

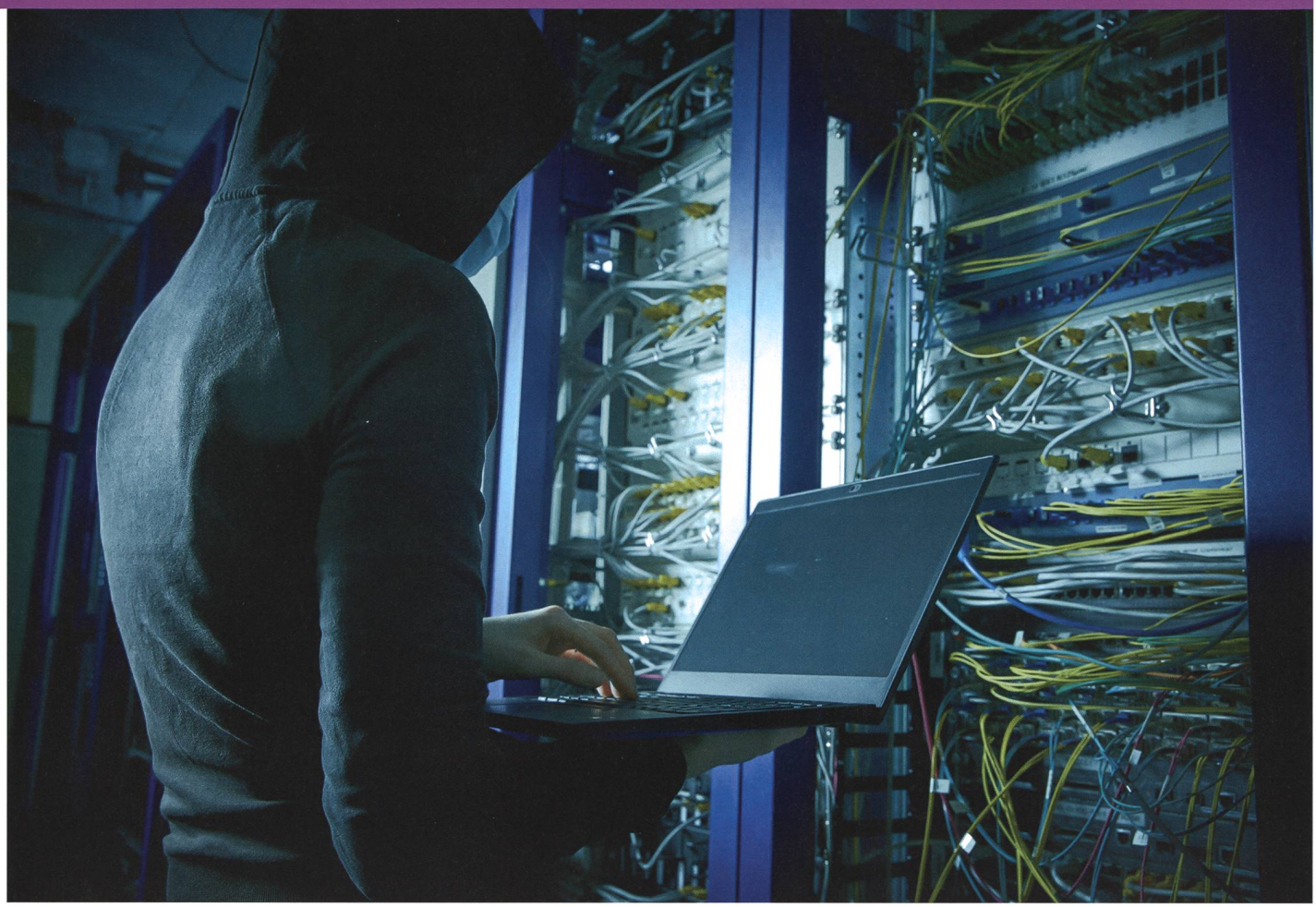


Figure: BFH

Ne pas se laisser distancer!

Stratégies de défense contre les cyberattaques | Personne n'est à l'abri d'une cyberattaque. Les assaillants ne cessent de faire évoluer leurs méthodes. Les victimes potentielles sont donc constamment confrontées à de nouvelles menaces. Mais les techniques de défense progressent, elles aussi.

ENDRE BANGERTER, BRUCE NIKKEL

Afin d'anticiper les menaces futures, il est parfois utile de regarder en arrière. Ce précepte vaut également dans le domaine de la cybercriminalité. Il y a une quinzaine d'années, les clients bancaires figuraient parmi les premières victimes des criminels, qui cherchaient à pénétrer les services d'e-banking en utilisant des « chevaux de Troie ». Grâce aux progrès réalisés, les banques sont aujourd'hui mieux en mesure de détecter si l'ordinateur d'un client est infecté et de parer l'attaque.

Les cybercriminels sont avant tout des opportunistes: s'ils rencontrent une résistance trop forte, ils cherchent une autre victime ou une autre faille. C'est la raison pour laquelle de plus en plus d'entreprises de toutes tailles et de toutes branches sont ciblées avec des ransomwares. Lorsque l'attaque réussit, c'est en général l'ensemble du réseau informatique de l'entreprise qui est touché. En échange de la clé de chiffrement des données prises en otage, les bandes, qui opèrent le plus souvent depuis l'étranger, tentent d'extorquer une rançon à payer en bitcoin. La recherche des auteurs de ces méfaits est coûteuse et n'aboutit que rarement.

« Piratage » des humains plutôt que des machines

Le phénomène de « social engineering » ou « ingénierie sociale », que l'on peut aussi traduire par « manipulation psychologique », gagne en importance. Il consiste, pour les assaillants, à exploiter des traits de personnalité tels que la candeur. Le nombre d'entreprises qui livrent spontanément des informations

– susceptibles portes d'entrée pour les intrus – est impressionnant. Une description de poste publiée sur le site Internet de l'entreprise, qui mentionne les logiciels utilisés, peut déjà constituer une faille exploitable : un assaillant peut, par exemple, se faire passer au téléphone pour un employé du développeur de logiciels et annoncer qu'il ou elle enverra un document contenant d'importantes informations de mise à jour. Si la tromperie est présentée de façon plausible, il est probable que le destinataire ouvre le document, permettant dès lors à un logiciel malveillant de faire son nid sur le réseau de l'entreprise. Dans ce cas, le talon d'Achille du système n'était pas la technologie, mais l'humain.

L'ingénierie sociale revêt également d'autres formes, notamment la manipulation de vidéos au moyen de l'intelligence artificielle pour modifier les visages (deepfakes). Cette technique permet de faire tenir à une personne des propos qu'elle n'aurait jamais tenus dans la réalité.

La confiance seule ne suffit pas

L'interconnexion du monde numérique et les interdépendances qu'elle crée offrent constamment de nouvelles opportunités aux pirates informatiques. Le cas de l'entreprise américaine Solarwinds, spécialisée dans les logiciels de gestion de réseau, avait fait la une des journaux. En 2019, un serveur insuffisamment protégé – le mot de passe était trop faible – a permis à des agresseurs d'infecter la mise à jour d'une des applications de l'entreprise avec un code malveillant, et ainsi de surveiller pendant plusieurs mois les clients de Solarwinds sans être détectés. Une technique classique d'« attaque de la chaîne d'approvisionnement ». Cet exemple met en évidence qu'une seule faille de sécurité au sommet de la chaîne d'approvisionnement suffit pour infiltrer tous les systèmes qui en dépendent. La leçon à tirer de cet incident : la confiance est une bonne chose, mais elle ne garantit pas, à elle seule, la sécurité dans le cyberespace.

Ce principe vaut également lorsque l'on externalise le traitement des données ou que l'on utilise des solutions informatiques dématérialisées (cloud). Des vérifications approfondies s'imposent pour s'assurer que le partenaire externe applique bien les normes de sécurité reconnues et certifiées. En outre, il convient de s'informer sur les dispositions légales du pays dans lequel le partenaire a son siège ou traite les données qui lui sont confiées. Les fournisseurs de services informatiques américains, par exemple, sont tenus par la loi – le « Cloud Act » – d'accorder aux autorités américaines l'accès aux données stockées, même si ces données proviennent de l'étranger.

Se résigner n'est pas une option

Ces dernières années, les entreprises et les institutions ont appris à faire face à la cybercriminalité. Elles ont davantage pris conscience qu'elles pouvaient se retrouver à tout moment dans le viseur de pirates informatiques. Néanmoins, la question du rapport coût-utilité continue de se poser lors de la planification de mesures préventives. Les technologies de pointe offrent une bonne protection, mais elles sont onéreuses. Et il faut garder à l'esprit que la sécurité absolue n'existe pas. Sachant cela, la pire option serait cependant de faire l'autruche. Les assaillants et les défenseurs se rendent coup pour coup, l'avantage changeant sans cesse de camp. C'est une situation avec laquelle nous devons apprendre à vivre. À cet égard, la Confédération a défini une norme minimale pour les TIC (technologies de l'information et de la communication) ; cet instrument peut faciliter l'identification des besoins au sein de sa PME et permettre de planifier les mesures défensives appropriées.

L'analyse des données : un défi à relever

Toute personne qui croit encore qu'un pare-feu et un programme antivirus peuvent empêcher l'accès à son réseau d'entreprise doit se remettre en question. Pour être efficaces, les mesures de défense requièrent la surveillance permanente de tous les systèmes et réseaux, ce qui pose un défi majeur : comment traiter rapidement les quantités de données que cela représente ? Il s'agit en effet d'une condition essentielle pour que des contremesures puissent être déclenchées avant que le logiciel malveillant ne cause des dommages.

Une approche innovante consiste à analyser les données à l'aide de méthodes reposant sur des algorithmes d'apprentissage automatique. La majorité des logiciels malveillants ne sont en effet pas entièrement nouveaux, et utilisent certains éléments issus de malwares existants. Mais avant de les neutraliser, il faut les repérer, un procédé très long et onéreux dans le cadre d'une analyse manuelle. Grâce à une technologie d'analyse développée par Threatray, un spin-off de la BFH, il est désormais possible de mettre très rapidement en évidence les similarités entre les données traitées et les menaces connues. Pour y parvenir, l'outil doit être alimenté en permanence avec toutes les informations disponibles sur les logiciels malveillants déjà connus.

Tirer profit du partage des connaissances

L'échange de connaissances et d'informations sur le plan national et international constitue un facteur de plus en plus important dans la défense contre les cyberattaques. Il existe aujourd'hui dans presque tous les secteurs d'activité des communautés de renseignement sur les menaces (Threat intelligence Communities), dans le cadre desquelles des spécialistes dépêchés par les différents membres relèvent ensemble des défis communs. Dans le cas des fournisseurs d'électricité, par exemple, il s'agit du centre sectoriel d'échange et d'analyse d'informations EE-ISAC (European Energy – Information Sharing & Analysis Center). Il met à disposition des informations de base et recommande des actions à entreprendre, et ce, également aux non-membres.

En outre, les entreprises et les organisations devraient tirer parti du savoir-faire des établissements d'enseignement suisses. Les écoles polytechniques ainsi que diverses universités et hautes écoles spécialisées effectuent des recherches dans les domaines de la cybersécurité et de la criminalistique numérique. De nouvelles formations sont continuellement ajoutées, telles que la filière MAS Digital Forensics & Cyber Investigation à la Haute école spécialisée bernoise en 2020. Le savoir-faire acquis est mis à disposition de partenaires privés pour le développement d'applications pratiques.

Auteurs

Prof. Dr **Endre Bangerter** est coresponsable de l'Institute for Cybersecurity and Engineering (ICE).
→ BFH, 2501 Bienne
→ endre.bangerter@bfh.ch

Prof. Dr **Bruce Nikkel** est coresponsable de l'Institute for Cybersecurity and Engineering (ICE).
→ bruce.nikkel@bfh.ch