Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 115 (2024)
Heft: 3

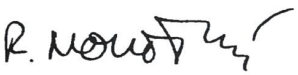
Vorwort: Versorgung und Sicherheit = Alimentation et sécurité
Autor: Novotný, Radomír

Radomír Novotný
Chefredaktor
Rédacteur en chef

Versorgung und Sicherheit

Vor einem Vierteljahrhundert hat sich die erste bekannte Malware automatisch per E-Mail verbreitet – ein Makrovirus namens Melissa. Er wurde in grosser Anzahl versandt und überlastete viele IT-Systeme. Glücklicherweise war er nicht mit schädlichem Code bestückt und verursachte keine beabsichtigten Datenverluste. Wenige Jahre später übertrafen Computerwürmer die Viren an «Leistungsfähigkeit». Neu war die Idee aber schon damals nicht: Bereits 1949 stellte John von Neumann die These auf, dass Computerprogramme möglich wären, die sich selbst reproduzieren können. Aber erst mit dem Aufkommen des Internets konnten sie ihre destruktive Wirkung global entfalten.

Wie sich die Situation bei den Cyberangriffen heute präsentiert, ist bekannt. Über Ransomware-Angriffe und ihre Folgen wurde bereits vielerorts berichtet, beispielsweise durch die NZZ, die im Februar ein detailliertes Protokoll veröffentlicht hat, wie ihre IT-Infrastruktur von kriminellen Hackern angegriffen wurde und wie sich dies auf die tägliche (und nächtliche) Arbeit ausgewirkt hat. Weil dieses Thema auch im Kontext der Versorgungssicherheit und der kritischen Infrastrukturen relevant ist, sind einige Beiträge dieser Ausgabe der Cybersicherheit gewidmet. Die Digitalisierung bietet aber sowohl im IT-Bereich als auch in der Leittechnik nicht nur Sicherheitslücken und Gefahren, sondern auch viele Chancen und Möglichkeiten, besonders im Hinblick auf die Energiewende. Die meisten Artikel der vorliegenden Ausgabe befassen sich deshalb mit dieser erfreulicheren Seite des vernetzten Rechnens.



Alimentation et sécurité

Il y a un quart de siècle, un macrovirus appelé Melissa – le premier malware connu – se propageait automatiquement par e-mail. Il avait été envoyé en grand nombre et avait surchargé de nombreux systèmes informatiques. Heureusement, il ne contenait pas de code malveillant et n'avait pas causé de pertes de données intentionnelles. Quelques années plus tard, les vers informatiques dépassaient les virus en termes de « performance ». Mais, à l'époque, l'idée n'avait déjà rien de neuf: dès 1949, John von Neumann avait en effet émis l'hypothèse qu'il était possible de concevoir des programmes informatiques capables de se reproduire eux-mêmes. Ce n'est toutefois qu'avec l'avènement d'Internet que les logiciels malveillants ont pu déployer leur effet destructeur à l'échelle mondiale.

La situation actuelle en matière de cyberattaques n'est pas un mystère... Des attaques par ransomware et leurs conséquences ont déjà été rapportées à maintes reprises, par exemple par la NZZ, qui a publié en février dernier un protocole détaillé relatant la manière dont son infrastructure informatique avait été hackée ainsi que les répercussions de cette attaque sur son travail au quotidien. Comme ce thème est également pertinent dans le contexte de la sécurité de l'approvisionnement et des infrastructures critiques, certains articles de ce numéro se consacrent à la cybersécurité. Cependant, tant dans le domaine de l'informatique que dans celui du contrôle-commande, la numérisation n'est pas seulement à l'origine de failles de sécurité et de dangers, mais offre aussi de nombreuses opportunités et possibilités, notamment dans la perspective de la transition énergétique. Raison pour laquelle la plupart des articles de ce numéro traitent de ce côté plus réjouissant de l'informatique en réseau.