

**Dr Jacques Supcik**

Professeur à la Haute école
d'ingénierie et d'architecture
de Fribourg

Professor an der Hochschule
für Technik und Architektur
Freiburg

Sommes-nous à l'abri d'un ransomware?

En juin dernier, Jennifer Granholm, secrétaire à l'Énergie des États-Unis, affirmait sur CNN que les adversaires de l'Amérique ont la capacité de mettre son réseau électrique hors service. Cette déclaration peu rassurante faisait suite à une série d'attaques informatiques contre les infrastructures sensibles des États-Unis, notamment celle perpétrée sous forme de « ransomware » contre le plus grand pipeline alimentant la côte Est. Cette attaque a contraint Colonial Pipeline à fermer l'oléoduc pendant cinq jours, créant ainsi un vent de panique sur les automobilistes de Floride, qui se sont rués sur les stations-service.

Un ransomware (ou rançongiciel) est un logiciel malveillant qui « vole » les données, souvent en les chiffrant, et demande à la victime de payer une rançon pour pouvoir les récupérer. Quand un ransomware s'attaque à un particulier, la rançon est souvent de quelques centaines de francs, mais pour Colonial Pipeline, elle s'élevait à 4,4 millions de dollars... et la compagnie a payé! Les experts recommandent de ne pas le faire, car cela montre aux malfaiteurs que ces pratiques rapportent gros et les encourage à continuer. En juillet 2020, des pirates auraient même obtenu 10 millions de dollars, payés par Garmin, pour une attaque du même genre.

En Suisse, aucun cas de ransomware envers une infrastructure sensible ne semble avoir été publié, mais dans son rapport de situation 2021, le service de renseignement de la Confédération écrit que dans un contexte d'attaques informatiques, «... les entreprises fournissant des équipements et prestations spécialisées destinés aux exploitants d'infrastructures critiques deviennent des cibles privilégiées».

Ces attaques ont beau avoir lieu dans le monde virtuel, les conséquences se font bien sentir dans le monde réel et peuvent provoquer d'énormes dégâts. Nos maisons et notre réseau électrique sont de plus en plus « smart », de plus en plus connectés, et donc de plus en plus vulnérables. Nous avons tous un rôle à jouer pour ne pas être le maillon faible: sauvegarder régulièrement ses données, ne pas payer de rançon en cas d'attaque via un ransomware, choisir des mots de passe uniques et forts, opter pour la double authentification partout où c'est possible, et s'informer sur les bonnes pratiques en matière de sécurité informatique.

Sind wir vor Ransomware sicher?

Im Juni sagte die US-Energieministerin Jennifer Granholm auf CNN, dass Amerikas Gegner in der Lage sind, das US-Stromnetz ausser Betrieb zu setzen. Diese wenig beruhigende Aussage folgte auf eine Reihe von Computerangriffen auf sensible US-Infrastrukturen, unter denen sich der « Ransomware »-Angriff auf die grösste Pipeline, die die Ostküste versorgt, befand. Dieser Angriff zwang Colonial Pipeline, die Pipeline für fünf Tage abzustellen, was zu einer Panik unter den Autofahrern in Florida führte. Sie standen Schlange, um ihre Benzinkanister an den Tankstellen zu füllen.

Eine Ransomware ist eine bösartige Software, die Daten « stiehlt », oft durch Verschlüsselung, und das Opfer auffordert, ein Lösegeld zu zahlen, um sie zurückzubekommen. Wenn Ransomware eine Einzelperson angreift, beträgt das Lösegeld oft ein paar Hundert Franken, aber bei Colonial Pipeline waren es 4,4 Millionen Dollar... und Colonial Pipeline hat bezahlt! Experten raten davon aber ab, da es Kriminellen signalisiert, dass sich diese Praktiken lohnen und sie ermutigt, weiterzumachen. Im Juli 2020 hätten Hacker für einen ähnlichen Angriff sogar 10 Millionen Dollar erhalten, die von Garmin bezahlt wurden.

In der Schweiz scheinen keine Fälle von Ransomware gegen sensible Infrastrukturen veröffentlicht worden zu sein, aber der Nachrichtendienst des Bundes schreibt in seinem Lagebericht 2021, dass im Zusammenhang mit Cyberangriffen «... die Unternehmen, die Ausrüstung und spezialisierte Dienstleistungen für Betreiber kritischer Infrastrukturen anbieten, zum bevorzugten Ziel der Angreifer [werden] ».

Obwohl diese Angriffe in der virtuellen Welt stattfinden, sind die Folgen in der realen Welt zu spüren und können enormen Schaden anrichten. Unsere Häuser und Stromnetze werden immer smarter, vernetzter und damit auch anfälliger. Wir alle müssen unseren Teil dazu beitragen, um nicht das schwächste Glied zu sein: Daten regelmässig sichern, im Falle eines Ransomware-Angriffs kein Lösegeld zahlen, einmalige und starke Passwörter wählen, sich für eine doppelte Authentifizierung entscheiden, wo immer dies möglich ist, und sich über gute IT-Sicherheitspraktiken informieren.