du réseau ne peuvent pas être arrêtés pour maintenance ne serait-ce que quelques heures par semaine : ils doivent fonctionner en permanence. Les opérateurs sont aussi assez conservateurs. Les réseaux de contrôle sont en place depuis longtemps, et les opérateurs ont leurs routines qui ont fait leurs preuves. Ils se méfient de tout ce qui risquerait de menacer la disponibilité ou d'interférer avec l'exploitation normale.

Sécuriser le réseau d'ici 2020

Le NERC *(North American Electric Reliability Corporation)*, un organisme de tutelle des opérateurs du réseau américain, a édicté un ensemble de normes destinées à protéger l'infrastructure face à un danger clair et immédiat. Les entreprises de service public doivent maintenant identifier leurs dispositifs critiques et faire la preuve auprès d'auditeurs nommés par le NERC qu'ils sont capables de les protéger des intrusions.

Mais les audits de sécurité, comme les audits financiers, ne sont jamais exhaustifs. Les détails techniques audités ne sont qu'une sélection de points, et la conformité se limite à ce que l'auditeur voit.

La stratégie de protection la plus courante consiste à dresser une sorte de ligne Maginot électronique. La première ligne de défense est un « pare-feu », un dispositif à travers lequel passent tous les messages électroniques. Chaque message possède un en-tête indiquant d'où il vient, où il va, et le protocole utilisé pour l'interpréter. Sur la base de ces informations, le pare-feu laisse passer certains messages et en bloque d'autres. Les agences de certification doivent s'assurer que les centaines ou les milliers de pare-feu d'un site sensible sont correctement configurés. Pour ce faire, ils identifient quelques éléments critiques, se procurent les fichiers de configuration du pare-feu et essayent de déterminer manuellement comment un pirate traverserait le pare-feu.

Mais les pare-feu sont tellement complexes qu'il est difficile d'examiner la multitude de possibilités. Des outils automatisés seraient utiles. Notre équipe de l'Université de l'Illinois à Urbana-Champaign a développé le *Network Access Policy Tool*, aujourd'hui utilisé par des entreprises de service public et des équipes d'évaluation. Ce logiciel libre n'a besoin que des fichiers de configuration des pare-feu d'une entreprise. Il a d'ores et déjà permis d'identifier un certain nombre de chemins d'accès inconnus ou tombés dans l'oubli, que des attaquants auraient pu exploiter.

Le Département américain de l'Énergie a établi une feuille de route pour renforcer la sécurité du réseau d'ici à 2020. L'un des buts est de mettre au point un système qui reconnaît une tentative d'intrusion et qui y réagit automatiquement. Cela bloquerait un virus de type *Stuxnet* dès sa sortie de la clef USB. Mais comment un système d'exploitation peut-il savoir à quels programmes faire confiance ?

Une solution serait d'utiliser une technique cryptographique appelée fonction de hachage à sens unique. Une fonction de hachage prend un nombre immensément grand, par exemple le nombre de 0 et de 1 d'un fichier informatique, et le convertit en un nombre beaucoup plus petit, qui joue le rôle de signature. Il est très improbable que deux programmes différents et assez longs aient la même signature. Imaginez que chaque programme qui veut s'exécuter sur un système doive d'abord passer par la fonction de hachage. Sa signature est alors vérifiée par comparaison avec une liste de référence. Si elle ne correspond pas, l'attaque s'arrête là.

Le Département de l'Énergie recommande également d'autres mesures de sécurité, comme des vérifications de sécurité physiques aux postes de travail des opérateurs (des puces radio dans les badges d'identification, par exemple). Il souligne également le besoin d'exercer un contrôle plus strict sur les communications entre les dispositifs à l'intérieur du réseau électrique. La démonstration *Aurora* impliquait un programme malveillant qui faisait croire au dispositif de contrôle du générateur qu'il envoyait des instructions fiables...

Ces mesures nécessiteront du temps, de l'argent et des efforts, mais elles en valent la peine. Si nous voulons sécuriser le réseau électrique d'ici 2020, il va falloir accélérer le rythme. En espérant que d'ici là, il n'arrive rien de fâcheux. ■

LA MISE HORS SERVICE DE 200 POSTES DE TRANSMISSION bien choisis, soit deux pour cent du total, mettrait à genoux 60 pour cent du réseau électrique américain.

L'AUTEUR

David NICOL est professeur au Département de génie électrique et informatique de l'Université de l'Illinois à Urbana-Champaign, aux États-Unis. Il est aussi directeur de l'*Information Trust Institute* de cette université.

✔ BIBLIOGRAPHIE

J.-Y. Marion et M. Kaczmarek, **Boulevard du cybercrime**, *Dossier Pour la Science* n °66, janvier-mars 2010, www.pourlascience.fr/u.php?s=cybercrime

J. Eisenhauer et *al*., **Roadmap to secure control systems in the energy sector**, *Energetics Incorporated*, janvier 2006. www.oe.energy.gov/csroadmap.htm

D. Geer, **Security of critical control systems sparks concern**, *IEEE Computer*, vol. 39, n°1, pp. 20-23, janvier 2006.

Trustworthy Cyber Infrastructure for the Power Grid, projet interuniversitaire financé par le Département américain de l'Énergie : www.tcipg.org

What Is the Electric Grid, and What Are Some Challenges It Faces?, Département américain de l'Énergie, www.eia.doe.gov/energy_in_brief/power_grid.cfm

✔ SUR LE WEB

Le portail gouvernemental français sur la sécurité informatique : http://www.ssi.gouv.fr/

La vidéo de l'exercice *Aurora* : http://bit.ly/pls407-video-aurora