inciter l'ingénieur à télécharger le manuel piégé. Ce faisant, l'ingénieur ouvre involontairement les portes de sa centrale au cheval de Troie. Une fois que le fichier corrompu se trouve à l'intérieur, l'attaque proprement dite peut commencer.

Désynchroniser, surcharger, ralentir

Un programme malveillant qui a réussi à s'introduire dans un réseau de contrôle peut émettre des instructions aux conséquences dévastatrices. En 2007, le Département de la Sécurité intérieure des États-Unis a simulé une cyberattaque au Laboratoire national de l'Idaho. Au cours de cet exercice, nommé *Aurora*, un ingénieur jouant le rôle de pirate s'est frayé un chemin jusque dans un réseau connecté à un générateur de taille moyenne. Comme tous les générateurs, il produit du courant alternatif. L'attaquant a émis une rapide séquence d'instructions marche/arrêt aux disjoncteurs d'un générateur test du Laboratoire, qui ont eu pour effet de le désynchroniser par rapport au courant alternatif du réseau. À « contre-courant » du réseau, le générateur n'a pas résisté longtemps : une vidéo aujourd'hui déclassifiée montre l'énorme machine d'acier tremblant comme si un train l'avait heurtée. Quelques secondes plus tard, la pièce était envahie de fumée.

Les systèmes industriels peuvent aussi tomber en panne quand ils sont poussés au-delà de leurs limites. Des centrifugeuses qui tournent trop vite se désintègrent. Un attaquant pourrait faire en sorte qu'un générateur électrique produise une tension supérieure à ce que les lignes de transport peuvent supporter. La puissance excédentaire serait alors évacuée sous forme de chaleur, entraînant l'affaissement de la ligne, voire sa fusion. Si des lignes affaissées entrent en contact avec quoi que ce soit, cela peut créer un énorme court-circuit. Des relais de protection sont prévus pour empêcher de tels courts-circuits, mais une cyberattaque pourrait également modifier le fonctionnement de ces relais, de façon à infliger des dégâts. En outre, l'attaque pourrait aussi modifier l'information envoyée à la station de contrôle, empêchant les opérateurs de remarquer qu'il y a un problème, comme dans ces films où les cambrioleurs envoient au gardien des images de vidéosurveillance truquées.

Les stations de contrôle elles aussi sont vulnérables aux attaques. Les personnels en salle d'opérations suivent sur écran les données transmises par les postes électriques, puis émettent des instructions pour en modifier les paramètres de contrôle. Une station est souvent responsable du suivi de centaines de postes.

La communication entre les stations de contrôle et les postes électriques utilise des protocoles spécialisés qui peuvent eux-mêmes être vulnérables. Si un intrus parvient à lancer une attaque de l'homme du milieu, il peut insérer un message dans un échange ou corrompre un message existant, voire simplement injecter un message correctement formaté, mais hors contexte, pour induire une défaillance d'un ordinateur à l'une ou l'autre extrémité.

Une autre stratégie est de retarder les messages transitant entre les stations de contrôle et les postes électriques. D'ordinaire, le délai entre la mesure du courant dans un poste et la réaction par la station de contrôle est court (sinon, cela revient à conduire une voiture en regardant là où vous étiez il y a dix secondes !). Le manque de données sur la situation en temps réel du réseau était en partie responsable de l'immense panne de courant qui a frappé l'Amérique du Nord en 2003.

Pour la plupart de ces attaques, nul besoin de logiciel sophistiqué comme *Stuxnet* : la boîte à outils du pirate de base suffit. Par exemple, des pirates prennent fréquemment le contrôle de milliers d'ordinateurs de bureau auxquels ils font faire ce qu'ils veulent, formant un réseau de

Janvier 2003
Le virus informatique *Slammer* contourne de nombreux pare-feu pour infecter le centre de contrôle de la centrale nucléaire de Davis-Besse dans l'Ohio (États-Unis). Le virus se répand à partir de l'ordinateur d'un sous-traitant jusque dans le réseau commercial, d'où il gagne les ordinateurs contrôlant l'exploitation de la centrale, entraînant la panne de multiples systèmes de sécurité. La centrale était à l'époque hors réseau.

Mars 2007
Des agents du gouvernement américain simulent une cyberattaque, nommée *Aurora*, sur un générateur électrique au Laboratoire national de l'Idaho. Le générateur est détruit.

Janvier 2008
Un responsable de la CIA révèle que des pirates informatiques auraient souvent infiltré les services d'électricité hors des États-Unis, avec des tentatives d'extorsion. Dans au moins un cas, les pirates auraient réussi à couper l'alimentation électrique de plusieurs villes, non nommées.

Avril 2009
Selon le *Wall Street Journal*, des cyberespions de Chine, Russie et d'autres pays auraient pénétré le réseau électrique américain et y auraient laissé des logiciels pouvant être utilisés pour le mettre hors service.

Octobre 2010
Des responsables de la sécurité en Iran, en Indonésie et ailleurs signalent la découverte de *Stuxnet*, un virus conçu pour attaquer des systèmes de contrôle industriels fabriqués par *Siemens*, qui commandent les centrifugeuses iraniennes.

2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

Mark Duncan AP Photo, Mark Peterson Redux Pictures, Ebrahim Norouzi AP Photo

« machines zombies », ou botnet. Le type le plus simple d'attaque par botnet consiste à inonder un site Internet de messages quelconques pour ralentir ou bloquer la circulation de l'information. Ces attaques par « déni de service » pourraient être utilisées pour ralentir le trafic entre les postes électriques et les stations de contrôle.

Des botnets pourraient également s'implanter au sein même des ordinateurs du réseau de postes électriques. En 2009, le botnet *Conficker* avait investi dix millions d'ordinateurs. Un tel botnet pourrait intégrer des ordinateurs des postes électriques, et son contrôleur pourrait alors leur faire exécuter simultanément telle ou telle instruction. D'après le Département de l'Énergie des États-Unis, la mise hors service de 200 postes de transmission soigneusement choisis, soit deux pour cent du total, mettrait à genoux 60 pour cent du réseau électrique.

Quand une entreprise comme *Microsoft* a connaissance d'une faille de sécurité de ses logiciels, elle fournit un correctif. Les utilisateurs du monde entier téléchargent ce correctif, mettent à jour leur logiciel et se protègent ainsi de la menace. Malheureusement, les choses ne sont pas aussi simples sur le réseau électrique.

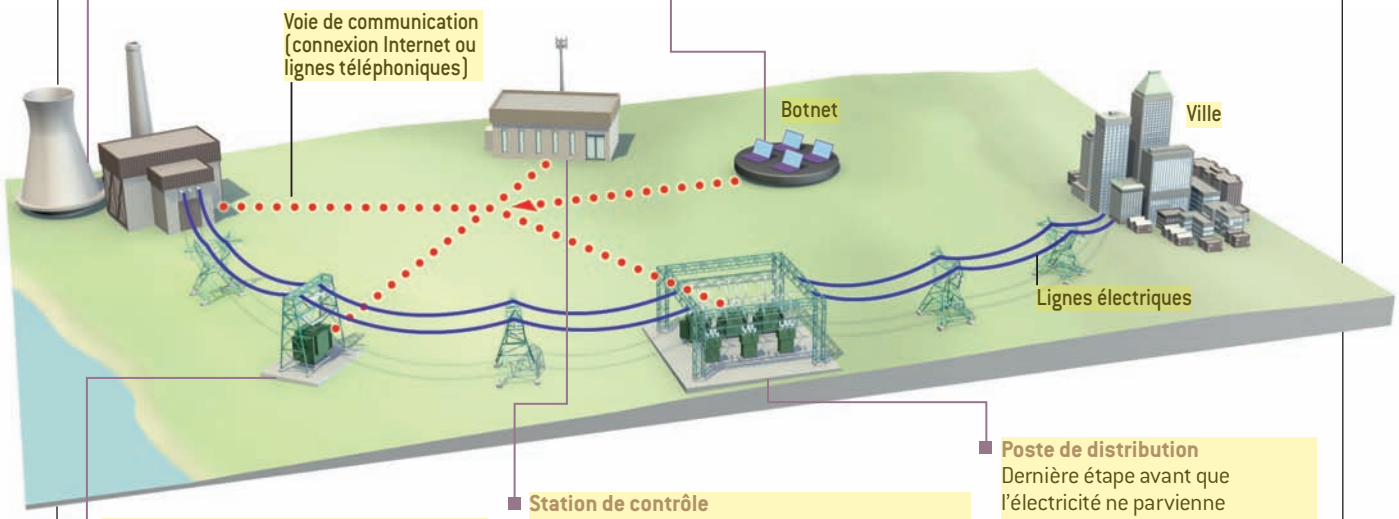
Même si le réseau électrique utilise du matériel et des logiciels grand public, les responsables informatiques des centrales électriques ne peuvent pas simplement corriger les logiciels défectueux quand des failles se révèlent. Les systèmes de contrôle

DES FAILLES DANS LE RÉSEAU

Le réseau électrique repose sur un équilibre complexe entre la quantité d'énergie dont les usagers ont besoin et la quantité produite par les centrales. Des dizaines de composants orchestrent la circulation de l'électricité sur des distances de centaines de kilomètres. Chacun de ces composants peut être mis à mal par des cyberattaquants. Voici quelques-uns des points les plus sensibles et comment ils pourraient être attaqués.

Centrale électrique
Que la centrale utilise du charbon, de l'uranium ou même l'énergie solaire, l'électricité injectée dans le réseau doit être un courant alternatif synchronisé avec le reste du réseau. Un attaquant pourrait envoyer des instructions à un générateur pour lui faire fournir un courant déphasé. Cela équivaut à passer la marche arrière alors que vous roulez sur une route à 80 kilomètres par heure : le générateur, opposé à l'inertie du réseau, va griller.

Transmission de l'information
La station de contrôle doit savoir à la seconde près ce qui se passe à chaque étape du transport pour que les techniciens puissent réagir et adapter les différents paramètres du réseau. Des pirates contrôlant des milliers d'ordinateurs (un botnet) pourraient ralentir les communications en inondant la station de contrôle de messages inutiles (attaque par déni de service). Les opérateurs prendraient des décisions en s'appuyant sur des informations anciennes, ce qui peut être inadapté à la situation réelle.



Poste de transmission
Le courant livré par les centrales électriques est à très haute tension, afin de limiter les pertes d'énergie durant le transport, dues à la résistance électrique. Les postes de transmission sont la première étape pour abaisser cette tension. De nombreux postes parmi les plus anciens sont équipés de modems auxquels les techniciens se connectent pour effectuer la maintenance. Des pirates peuvent les utiliser pour accéder aux réglages sensibles et les modifier.

Station de contrôle
Centres névralgiques du réseau électrique, les stations de contrôle surveillent l'ensemble des conditions de fonctionnement. C'est également là qu'est gérée l'adéquation entre l'offre et la demande. Quand la demande augmente, une entreprise mobilise plus de capacité de production pour répondre aux besoins. Bien que la salle d'opérations d'une station de contrôle ne soit pas censée être raccordée à Internet, la branche commerciale de la compagnie l'est. Un pirate peut s'infiltrer dans le réseau commercial et passer dans le réseau d'exploitation pour attaquer des systèmes de contrôle critiques.

Poste de distribution
Dernière étape avant que l'électricité ne parvienne aux particuliers et aux entreprises, ces postes peuvent combiner le courant provenant de plusieurs centrales différentes et l'envoyer sur des centaines de lignes plus petites. Les stations les plus récentes sont parfois équipées de dispositifs de communication radio ou Wi-Fi. Un intrus qui se cache à proximité du poste pourrait intercepter les échanges et leur substituer des instructions illégitimes.

George Retseck

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