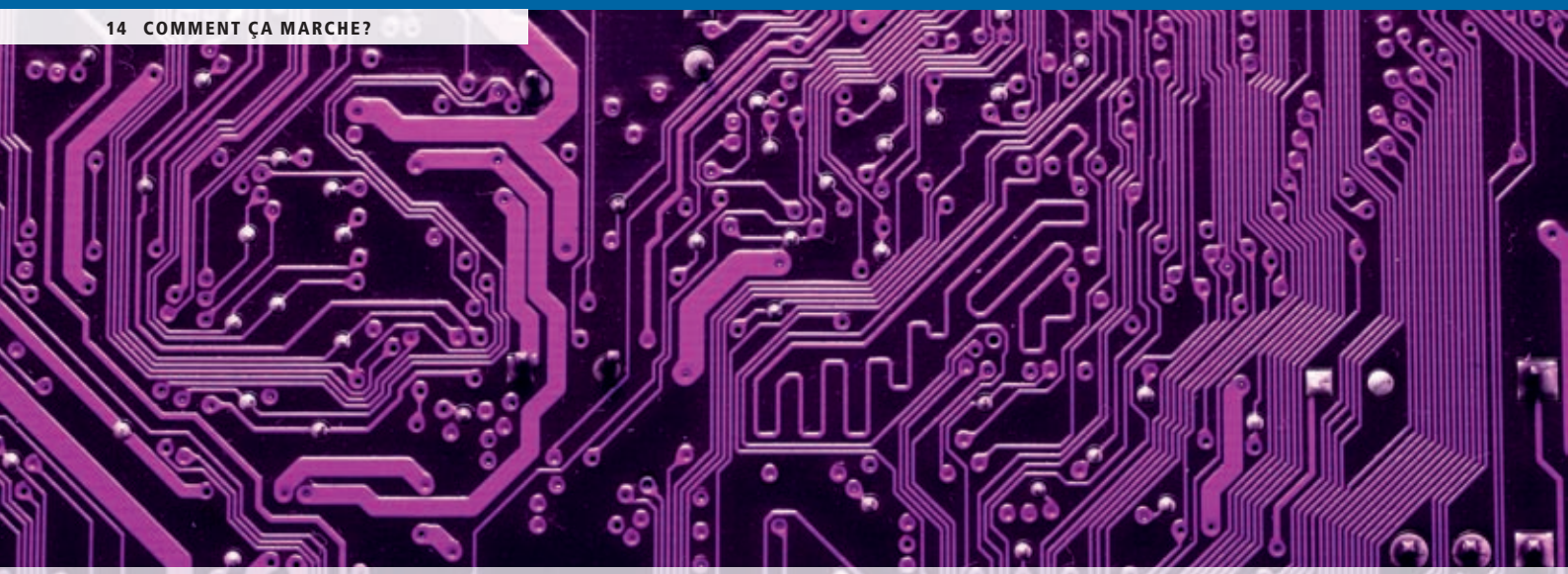

Stuxnet rappelle la vulnérabilité des systèmes énergétiques

Les attaques par le ver informatique Stuxnet, notamment contre la centrale nucléaire de Bushehr en Iran, ont montré la vulnérabilité des infrastructures informatiques modernes. Des réseaux électriques sophistiqués et des systèmes énergétiques entiers pourraient à l'avenir être la cible de pirates informatiques.

Stuxnet est un type tout à fait nouveau de ver informatique. Contrairement aux virus traditionnels, il ne s'attaque pas uniquement à des systèmes numériques, tels que des ordinateurs personnels ou des serveurs, mais vise finalement un système physique. «Ce ver informatique cible des infrastructures critiques en infiltrant des systèmes de surveillance et de pilotage de processus techniques», explique Srdjan Capkun, professeur d'informatique à l'EPFZ. Par conséquent, ce genre de piratage informatique peut non seulement endommager un logiciel mais aussi les installations qu'il pilote. «C'est le premier ver informatique susceptible d'avoir des effets dévastateurs sur le monde réel. Il est dangereux car il permet aux pirates de contrôler des fabriques et des centrales entières», écrit aussi la société de sécurité informatique Symantec sur son site Internet.

Prendre le contrôle sans être détecté

Stuxnet est la première cyber-attaque visant des systèmes de pilotage industriels. Selon Symantec, le ver Stuxnet cherche des systèmes de pilotage industriels et change leur code pour que les pirates puissent en prendre le contrôle sans être détectés par les exploitants. Le mode de fonctionnement ainsi que la conception de ce ver sont uniques. Selon le professeur Capkun, «la sophistication de Stuxnet est vraiment impressionnante». Ce ver a vraisemblablement été programmé par une équipe comprenant à la fois des cyber-experts et des spécialistes en exploitation de systèmes industriels. «En raison de sa complexité élevée et des coûts financiers, seuls quelques groupes sont en mesure de développer une telle menace», écrit Symantec. Ce ver se compose d'un code informatique très compliqué requérant de grandes connaissances techniques pour l'élaborer.

Danger momentanément écarté

Aujourd'hui, Stuxnet n'est plus dangereux. Toutes les sociétés d'anti-virus proposent les mises à jour nécessaires. Pour le professeur Capkun, les systèmes énergétiques et d'autres infrastructures, en particulier les centrales nucléaires suisses, sont actuellement protégés contre Stuxnet. «La sûreté des centrales nucléaires suisses et la protection des êtres humains et de l'environnement sont assurées», communique l'Inspection fédérale de la sécurité nucléaire (IFSN), qui connaît le ver informatique Stuxnet depuis plusieurs mois. Des spécialistes ont été en contact étroit avec les exploitants des centrales nucléaires suisses et avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI à Berne. L'IFSN précise: «Nos enquêtes ont montré que les systèmes nucléaires et les centrales de sécurité n'ont pas été contaminés par ce ver. Les autres systèmes, notamment les systèmes secondaires et auxiliaires, n'ont pas été attaqués et sont protégés».

Avertissement pour l'avenir

D'une manière générale, les risques d'infiltration augmenteront à l'avenir, met en garde le professeur Capkun. «Le fait que le ver se soit au début propagé au moyen d'une clé USB signifie qu'il peut même infiltrer des systèmes qui ne sont pas connectés à Internet.» Les compteurs dits intelligents installés dans les ménages, qui donnent en temps réel la consommation d'électricité et sont reliés entre eux et avec une centrale de communication et de pilotage, pourraient aussi être la cible d'attaques. «Lorsque tous les habitants ont, d'une manière ou d'une autre, une liaison de communication avec le réseau d'approvisionnement, cela ouvre de nouvelles voies aux pirates pour infiltrer ces systèmes et les détruire de l'intérieur». L'Office fédéral de l'énergie a aussi identifié ce problème. «Nous avons lancé un projet pour tester la dangerosité de cyber-attaques contre les futurs réseaux intelligents (Smart Grids)», explique Michael Moser, expert de l'OFEN chargé de cette question.

(klm)

Internet

Département d'informatique de l'EPFZ:
www.inf.ethz.ch

Fabricant d'anti-virus Symantec:
www.symantec.com/fr

Inspection fédérale de la sécurité nucléaire (IFSN):
www.ensi.ch

Programme de recherche Technologies et utilisations de l'électricité de l'OFEN:
www.bfe.admin.ch/recherche/electricite