Panne de courant via une cyberattaque : les spécialistes ne sont pas surpris

Le 23 décembre, quelque **80 000 foyers ukrainiens** ont été privés d'électricité pendant plusieurs heures, suite, semble-t-il, à une cyberattaque. Les premiers éléments publiés par l'éditeur d'antivirus Eset ou par la société de sécurité iSight indiquent en effet que la panne pourrait provenir de la diffusion d'un malware, BlackEnergy, reconfiguré pour aller perturber le fonctionnement de certains processus industriels.

Ce scénario, qui jusqu'à fin 2015 relevait de la science-fiction, a poussé une organisation américaine du secteur de l'électricité, le Electricity Information Sharing and Analysis Center (ou E-ISAC), à alerter les entreprises américaines assurant la distribution d'électricité dans le pays. L'E-ISAC presse ses membres de mettre à niveau leur sécurité pour se protéger des cyberattaques. Dans un document de 9 pages que s'est procuré Reuters, cette organisation proche du gouvernement américain explique que la panne dont a été victime la compagnie ukrainienne Prykarpattyaoblenergo semble bien résulter « *d'un effort coordonné d'un acteur malveillant* ». Le rapport n'identifie toutefois pas de faiblesses sur le réseau électrique américain pouvant aboutir à pareil incident. Détail intéressant, l'E-ISAC met au jour un point commun entre les trois opérateurs ciblés par la cyberattaque (Chernivtsioblenergo, Kyivoblenergo et Prykarpattyaoblenergo, seul le dernier ayant connu une défaillance physique sur son réseau de distribution) : un intégrateur, Galician Computer Co. Le vecteur de diffusion du malware ? Selon Eset toutefois, le malware BlackEnergy aurait été diffusé via une campagne d'e-mails ciblés et contrefaits contenant des macros Microsoft Office vérolées.

En France, comme le rappelle les experts interrogés ci-dessous, les pouvoirs publics ont lancé le chantier de sécurisation des infrastructures essentielles du pays, dont les réseaux d'électricité, dès la fin 2013, avec le vote de la Loi de programmation militaire. Un texte qui encadre la sécurité de ce que l'Etat a identifié comme des opérateurs d'importance vitale (OIV). Même si les arrêtés sectoriels transposant cette loi en dispositions pratiques dans chaque industrie (énergie, santé, télécoms, finance, transports…) ne sont encore sortis, la démarche a provoqué une prise de conscience dans les quelque 200 organisations concernées, expliquent nos interlocuteurs…

« Des systèmes très distribués, souvent fragiles »

Gérôme Billois, senior manager en gestion des risques et sécurité chez Solucom :

« D'abord, il faut rester prudent quant aux conclusions qu'on tire de l'affaire ukrainienne. On est ici dans un contexte où l'attribution est presque automatique (du fait du conflit entre l'Ukraine et la Russie, NDLR) et les informations disponibles émanent d'un nombre de sources limité. Si la panne de courant est toutefois bien due à une cyberattaque, cela ne constitue pas réellement une surprise. Les systèmes industriels restent trop peu sécurisés, en particulier les systèmes distribués, très souvent pilotés et supervisés à distance par des PC classiques. En plus de cette porosité entre les réseaux industriels et l'informatique classique, les systèmes industriels souffrent de leurs vulnérabilités propres. Certes, dans ce monde, la diversité des équipements est supérieure à celle rencontrée dans l'informatique traditionnelle, mais on ne parle *in fine* que d'une poignée de

constructeurs principaux. Ce n'est donc pas un monde hors de portée de cybercriminels motivés, d'autant que les Scada intègrent de plus en plus des briques provenant de l'informatique standard.

On assiste d'ailleurs à une montée en puissance des attaques ciblant les systèmes industriels. Fin 2014, le BSI, l'équivalent allemand de l'Anssi, mentionnait dans un rapport qu'un four d'une aciérie avait été endommagé suite à une cyberattaque.

Isoler des périmètres sensibles sur les réseaux industriels et sécuriser les composants peut être très couteux ; dans certains pays ou contextes, ce n'est pas forcément envisageable. Par ailleurs, on a souvent affaire à des systèmes très distribués, géographiquement mais également en termes d'organisation. Les SI industriels sont souvent déployés dans une usine via des décisions locales. Il faut donc convaincre et obtenir des budgets site par site. Par ailleurs, si cette stratégie d'isolation est efficace, elle se heurte à deux limites : elle peut créer des complexités pour les processus industriels eux-mêmes et elle doit s'accompagner d'une rigueur dans l'organisation. Rien ne sert d'isoler des équipements sensibles, si l'intégrateur assurant leur maintenance se connecte directement au cœur des réseaux protégés avec une machine elle-même infectée ou encore si les règles d'isolation ne sont jamais vérifiées ou contrôlées !

En France, grâce à la législation sur les OIV, les choses progressent, avec des budgets mobilisés sur ces sujets. Même si les arrêtés mettent plus de temps à sortir que prévu initialement, les actions devraient s'étaler entre 2016 et 2018 environ. A l'issue de cette phase, on pourra jauger l'efficacité de ces mesures. Il faut avoir conscience qu'il s'agit là d'une grosse machinerie : 13 secteurs d'activité – certains sous-découpés en plusieurs sous-groupes – sont concernés et les acteurs visés sont loin d'être tous au même niveau de maturité sur le sujet. »

« La porosité avec les systèmes bureautiques »

Wilfrid Blanc et Simon Deterre, consultants en sécurité chez Lexsi :

« A la lecture des informations disponibles, on ne peut pas avoir de certitude absolue quant à l'origine de la panne d'électricité en Ukraine. Mais de nombreux éléments concordants, notamment publiés par l'éditeur Eset, plaident pour la thèse de la cyberattaque. A la lumière de notre retour d'expérience chez nos clients industriels, ce n'est pas forcément une surprise. Une fois passé la barrière périmétrique, nous constatons que le niveau de sécurité est souvent bien moindre. Il faut garder à l'esprit que les questions de cybersécurité des systèmes industriels n'ont pris leur essor qu'en 2010, avec la découverte de Stuxnet. Depuis, les chercheurs et les cybercriminels – avec des profils d'hacktivistes ou de hackers sponsorisés par des Etats – s'y intéressent de plus en plus. La vulnérabilité des systèmes industriels est accentuée par la porosité croissante entre les systèmes bureautiques et les Scada, une interconnexion mise en place afin de descendre des ordres de production, de remonter les données de la production ou de piloter les systèmes à distance. Si on se fie aux informations d'Eset, ce danger est bien illustré par le cas ukrainien, où le malware BlackEnergy a été déployé via spearphishing (un mail contrefait contenant une pièce jointe infectée et envoyé à des personnes précises dans l'organisation, NDLR). En théorie, ces deux mondes-là ne devraient jamais être interconnectés simplement. Sur le terrain, dans le meilleur des cas, ils ne sont isolés l'un de l'autre que par un firewall. Et il suffit que les règles de filtrage de cet équipement ne soient pas suffisamment robustes pour que les assaillants conservent une possibilité de rebondir

d'un monde à l'autre.

En France, via la législation sur les OIV, l'Anssi a fait un gros travail de sensibilisation. L'Hexagone est certainement l'un des pays du monde, avec les États-Unis et Israël, où la question de la sécurisation des systèmes industriels est la mieux prise en compte par les pouvoirs publics. Les OIV savent qu'ils vont devoir rendre des comptes et les futurs arrêtés leur apparaissent comme une épée de Damoclès les poussant à investir. D'ores et déjà, l'Anssi a publié des guides de bonnes pratiques, renfermant 279 mesures. C'est ce canevas découpé en deux parties – mesures techniques d'un côté, organisationnelles de l'autre – qui doit être adapté à chacun des 13 secteurs d'activité identifiés. Hors OIV, la situation est bien sûr plus contrastée. En général, c'est la sensibilité du dirigeant sur ces sujets qui prime. »

« La fraude depuis les postes des opérateurs Scada »

Tewfik Megherbi, consultant avant-vente de F5 Networks :

« La Loi de programmation militaire (LPM) aborde les aspects de protection contre les cybermenaces et liste les mesures de sécurité à mettre en œuvre en vue de protéger les infrastructures vitales. Afin de se préparer au mieux contre des attaques visant des OIV, il faut effectivement mettre en place des mécanismes de protection et de cloisonnement entre les réseaux Scada et les autres réseaux ; mais encore faut-il avoir la visibilité et l'intelligence pour détecter les intrusions au niveau applicatif. La solution pourrait venir de l'analyse comportementale ou des "analytics" qui consistent à agréger, corréler et interpréter des informations issues des infrastructures réseaux et applicatives.

Dans le cas des centrales électriques ukrainiennes, le cheval de Troie BlackEnergy a ciblé et exploité des postes de travail des opérateurs, donc « légitimes », en utilisant des vulnérabilités connues comme vecteurs d'attaques. Une fois installé sur le poste de l'opérateur, BlackEnergy a eu le champ libre pour intercepter les crédentiels (couples noms d'utilisateurs / mots de passes) utilisés par les opérateurs en charge des systèmes Scada.

Face à ce mode opératoire, la solution consiste à mettre en place des technologies de protection contre la fraude qui permettent d'avoir une visibilité sur les activités frauduleuses initiées depuis le poste de l'opérateur d'un système Scada. L'objectif étant de détecter les comportements identifiables d'un malware et de brouiller, par exemple, les crédentiels collectés lors de l'utilisation d'un navigateur Web. »

A lire aussi :

Scada : quand une cyberattaque provoque une panne de courant

L’Anssi met son nez dans la sécurité des grandes entreprises

Sécurité des Scada : pourquoi la côte d’alerte est atteinte

Crédit photo : chungking / Shutterstock