McAfee

Des menaces tapies dans l'ombre

Les infrastructures critiques face aux cyberattaques

Deuxième rapport annuel de McAfee sur la protection des infrastructures critiques

Des menaces tapies dans l'ombre

Auteurs :

Stewart Baker, membre invité du CSIS, associé du cabinet juridique Steptoe & Johnson

Natalia Filipiak, gestionnaire de projets et chercheuse associée auprès du CSIS

Katrina Timlin, assistante en recherche au CSIS

SOMMAIRE

Introduction et résumé

Il y a un an, le rapport de McAfee *Dans la ligne de mire : les infrastructures critiques à l'aube de la guerre numérique* montrait combien les infrastructures critiques du monde entier étaient vulnérables face aux cyberattaques. Depuis, Stuxnet a transformé le paysage des menaces. Cette arme sophistiquée et performante a été développée dans un seul but : saboter un système de contrôle industriel[1].

Le rapport de cette année se concentre sur les infrastructures civiles critiques les plus dépendantes des systèmes de contrôle industriels. A l'instar de la première édition, ce document se fonde sur des données, des recherches et des entretiens pour brosser un tableau très complet des cybermenaces propres à ces secteurs. Les secteurs d'activités que nous avons choisi d'étudier dans ce rapport, à savoir l'énergie, le pétrole, le gaz et l'eau, pourraient bien être les prochaines cibles d'une cyberattaque de grande ampleur.

Les informations recueillies montrent que ces secteurs ne sont pas prêts. Les professionnels chargés de la protection de ces systèmes révèlent que la menace s'est intensifiée alors que les moyens de réponse restent insuffisants. Les exploits et les attaques numériques se sont généralisés. Qu'il s'agisse de cybercriminels se livrant au vol ou à l'extorsion, ou d'Etats préparant des exploits sophistiqués tels que Stuxnet, les auteurs de cyberattaques ont visé des infrastructures critiques.

Bon nombre de ces menaces, d'un genre nouveau, posent un réel problème aux professionnels de l'informatique dans ces secteurs. Aujourd'hui, « si vous ne pouvez pas contrer une attaque de type "jour zéro" lancée à partir d'un lecteur USB », déclare l'ancien directeur de la CIA Jim Woolsey, « vous êtes sans défense ».

Les résultats de notre enquête montrent que les menaces et les vulnérabilités se multiplient à cadence accélérée. Pour la deuxième année consécutive, les responsables informatiques d'entreprises reposant sur des infrastructures critiques ont déclaré percevoir une cybermenace croissante et bien réelle. Les attaques par déni de service sur les réseaux de distribution d'énergie sont en hausse. Les tentatives d'extorsion sont également plus fréquentes dans les secteurs reposant sur des infrastructures critiques. Et les infiltrations hostiles de ces réseaux par certains Etats ont été fructueuses.

Des vulnérabilités continuent régulièrement d'apparaître. 40 % des cadres interrogés estiment que la vulnérabilité de leur secteur s'est intensifiée au cours de l'année écoulée ; un pourcentage près de deux fois supérieur à celui des répondants convaincus de sa diminution. Entre un cinquième et un tiers des personnes interrogées nous ont confié que leur société n'était pas du tout préparée, ou très mal, aux cyberattaques par des logiciels malveillants, déni de service ou autre, un chiffre qui ne s'est guère amélioré depuis l'année dernière.

En dépit de ces vulnérabilités et des dangers, de nombreuses compagnies d'électricité n'hésitent pas à prendre des risques en implémentant des réseaux de distribution « intelligents » qui donnent aux systèmes informatiques un contrôle accru sur la distribution d'électricité aux clients, et même aux appareils électriques individuels équipant les foyers. Sans un renforcement de la sécurité, ce contrôle accru peut tomber entre les mains de criminels ou de cyberactivistes et leur donner accès à des informations de facturation ou le contrôle sur la distribution d'électricité aux clients ou aux appareils électriques. Malheureusement, selon Jim Woosley qui présidait il y a deux ans un groupe de travail sur les vulnérabilités des réseaux de distribution électrique pour le ministère de la Défense, la sécurité n'est pas une priorité pour les concepteurs de tels réseaux. « 90 à 95 % du personnel participant au développement des réseaux de distribution intelligents ne se sentent pas concernés par la sécurité et ne considèrent celle-ci que comme un facteur accessoire. »

Des améliorations trop timides en matière de sécurité

L'année dernière, nous avons tenté d'évaluer objectivement la sécurité des entreprises en posant des questions spécifiques sur l'utilisation de 29 technologies de sécurisation spécifiques, du chiffrement à l'authentification. Nous avons utilisé leurs réponses pour créer une échelle objective du nombre exact de mesures de sécurité mises en place. Les données recueillies montrent que les dirigeants ont accompli des progrès modestes au cours de l'année écoulée en termes de sécurisation de leurs réseaux, en adoptant près de la moitié des technologies de sécurité identifiées. Le taux d'adoption des technologies de sécurité dans le secteur de l'énergie s'élève désormais à 51 %, ce qui représente une augmentation d'un seul petit point. Quant à celui des secteurs du gaz et du pétrole, il est en hausse de 3 % et atteint à présent 48 %. La seule augmentation notable (8 %) est à mettre au compte des sociétés de distribution d'eau et de traitement des eaux usées, un secteur à la traîne l'année dernière, avec un taux d'adoption de 46 %.

La tendance est pratiquement la même pour le taux d'adoption de mesures de sécurité relatives aux systèmes ICS (Industrial Control System) ou SCADA (Supervisory Control and Data Acquisitions) des répondants. Même si l'amélioration de la sécurité des réseaux ne revient pas simplement à multiplier les technologies, le taux d'adoption en hausse de certaines technologies spécifiques constitue une preuve objective que les entreprises ne restent pas inactives face aux problèmes de sécurité. Elles prennent des mesures pour la renforcer, mais les progrès par rapport à l'année dernière sont limités.

Il reste beaucoup à faire. 60 % des dirigeants informatiques interrogés déclarent exiger des jetons ou des cartes à puce pour la connexion des utilisateurs hors site à leurs systèmes critiques, au lieu de noms d'utilisateur et de mots de passe trop faciles à pirater. D'autres mesures plus sophistiquées, par exemple des outils visant à surveiller l'activité réseau ou à détecter des anomalies de comportement, ont été adoptées par une minorité des répondants (respectivement 25 et 36 %).

Perception des menaces et réaction variables selon les pays

En analysant les données par pays, les lacunes de sécurité mentionnées ci-dessus apparaissent encore plus clairement. Certains pays comme le Brésil, la France et le Mexique sont à la traîne et n'ont adopté que la moitié des mesures de sécurité par rapport aux pays en tête du classement tels que la Chine, l'Italie et le Japon.

Ces différences persistent également en termes de perception des menaces. Ainsi, 90 % des répondants australiens estiment que leur secteur spécifique est peu ou pas du tout préparé aux attaques par infiltration furtive. Dans la même optique, trois répondants brésiliens sur quatre et six répondants mexicains sur dix jugent que leur entreprise n'est pas préparée à une attaque par déni de service distribué de grande ampleur. L'Inde se singularise également dans le rapport dans la mesure où neuf dirigeants sur dix s'attendent à une cyberattaque majeure dans l'année à venir.

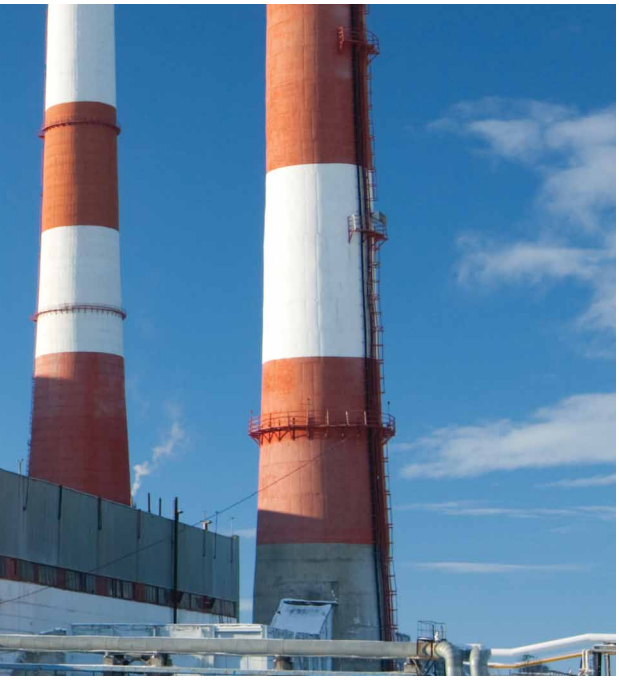
Le rôle encore flou des pouvoirs publics

Comment les pouvoirs publics réagissent-ils face à la vulnérabilité des infrastructures critiques civiles ? En général, ils continuent à jouer un rôle ambigu en matière de cybersécurité : parfois ils aident le secteur privé, parfois ils l'ignorent totalement.

Une fois encore, la Chine se démarque des autres pays. Le gouvernement chinois semble jouer un rôle très actif dans la sécurité qu'il exige pour ses infrastructures critiques. Ses exigences de sécurité, par exemple, sont respectées par les répondants chinois et la Chine présente le taux d'audits de sécurité officiels le plus élevé après le Japon. A l'inverse, les entreprises américaines et britanniques ne font presque jamais l'objet d'audits de sécurité par des organismes publics.

Cette tendance correspond également en partie aux niveaux de confiance témoignés par les répondants quant à la capacité des lois nationales en vigueur à prévenir et à décourager les attaques : les niveaux de confiance les plus élevés ont été observés au Japon (78 %), dans les Emirats arabes unis (67 %) et en Chine (56 %). Dans la course engagée par les autorités pour renforcer la protection de leurs infrastructures civiles contre les cyberattaques, ces réponses semblent suggérer que l'Europe et les Etats-Unis se laissent distancer par l'Asie.

En règle générale, les différents secteurs d'activités craignent les attaques lancées par des Etats et près de la moitié des répondants avouent avoir déjà été victimes de telles attaques. Le seul changement par rapport à l'année dernière est le pays considéré comme la plus grande menace à cet égard.



« 90 à 95 % du personnel participant au développement des réseaux de distribution intelligents ne se sentent pas concernés par la sécurité et ne considèrent celle-ci que comme un facteur accessoire ».

– Jim Woolsey, ancien directeur de la CIA

Le recul des Etats-Unis (12 % au lieu de 36 % l'année dernière) dans le classement des pays les plus « inquiétants » en matière de menaces et la progression relative des autres pays s'expliquent peut-être par le fait que les dirigeants informatiques du secteur commencent à prendre conscience de la prolifération des technologies d'attaques numériques.

Méthodologie

Nous avons interrogé plus de 200 cadres dirigeants de diverses entreprises gérant des infrastructures critiques dans 14 pays, qui ont répondu de façon anonyme à un questionnaire complet et détaillé sur leurs pratiques, attitudes et politiques en matière de sécurité. Les répondants étaient issus d'un panel de cadres informatiques dans les secteurs de l'énergie, du pétrole, du gaz et de l'eau. Leurs principaux domaines de compétences incluaient la sécurité des technologies de l'information, la sécurité générale et les systèmes de contrôle industriels. Ce rapport a été rédigé par une équipe du CSIS (Center for Strategic and International Studies) à Washington, après une analyse des données recueillies, complétée par des études et des entretiens complémentaires.

En règle générale, les différents secteurs d'activités craignent les attaques lancées par des Etats et près de la moitié des répondants avouent avoir déjà été victimes de telles attaques.

Il tente d'évaluer le point de vue des cadres dirigeants et d'offrir ainsi un aperçu des différents avis d'un groupe significatif de décideurs appartenant à plusieurs secteurs reposant sur des infrastructures critiques. En outre, les entretiens menés par l'équipe du CSIS lui ont permis d'établir le contexte de l'étude, de vérifier les données recueillies et de brosser un tableau très complet des réseaux de distribution électrique et des niveaux de menaces et de vulnérabilités de ce secteur, ainsi que des meilleures pratiques adoptées en matière de sécurité.

La montée en puissance des vulnérabilités et des menaces

Un répondant sur quatre a été victime d'extorsions à l'occasion ou sous la menace d'une cyberattaque.

L'un des résultats les plus saisissants de notre étude concerne la découverte des agressions et sondages continuels dont font l'objet ces réseaux de services publics cruciaux. Certaines compagnies d'électricité indiquent être victimes de milliers de sondages chaque mois. Les résultats de notre étude corroborent les récits d'opérations de reconnaissance et de planification menées par des militaires de différents pays en vue de cyberattaques contre des réseaux électriques d'autres nations ; ces opérations consistant à cartographier l'infrastructure réseau sous-jacente et à localiser ses vulnérabilités.

La cyberextorsion

La menace de cyberextorsion, dont l'existence est largement admise, pose un risque grandissant. En l'espace d'une année, le nombre d'entreprises victimes d'extorsion a augmenté de 25 %. Les affaires d'extorsion touchent de façon égale les différents secteurs exploitant des infrastructures critiques, ce qui signifie qu'aucun d'eux n'est à l'abri des cybercriminels. En Inde et au Mexique, le nombre de tentatives d'extorsion est élevé ; entre 60 et 80 % des cadres dirigeants interrogés de ces pays ont signalé avoir vécu ce type d'expérience.

L'intensification des attaques

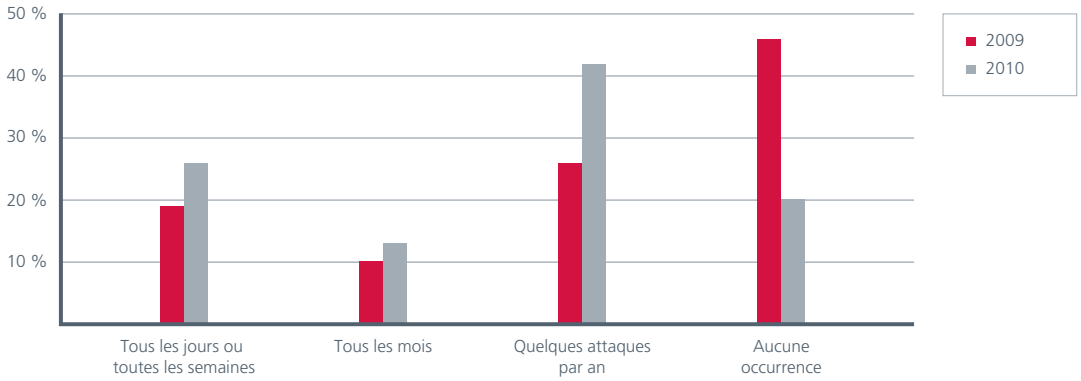
Pas plus tard que l'an dernier, près de la moitié des répondants déclaraient qu'ils n'avaient jamais été confrontés à des infiltrations réseau ni à des attaques par déni de service de grande envergure. Cette année toutefois, la situation a changé du tout au tout, puisque 80 % d'entre eux ont essuyé une attaque par déni de service à grande échelle et 85 % ont subi une infiltration réseau. Parallèlement, un quart a fait état d'attaques par déni de service à grande échelle quotidiennes ou hebdomadaires. Et la même proportion indique avoir été victime d'extorsion dans le cadre d'attaques réseau ou sous la menace de telles attaques. Fait inquiétant, près de deux tiers des personnes interrogées affirment découvrir fréquemment (au moins une fois par mois) sur leurs systèmes des logiciels malveillants conçus à des fins de sabotage.

L'extorsion, une pratique répandue

La cyberextorsion représente déjà une activité très rentable. Selon Allan Paller, directeur du SANS Institute, « plusieurs centaines de millions de dollars ont été extorqués [à diverses sociétés], peut-être même plus […]. Ce type d'extorsion est une réalité de la cybercriminalité le plus souvent passée sous silence[2] ». Un répondant sur quatre a déclaré avoir été victime d'extorsion à l'occasion ou sous la menace d'une attaque de réseau informatique au cours des deux dernières années, alors que seulement un sur cinq l'avait été il y a un an.

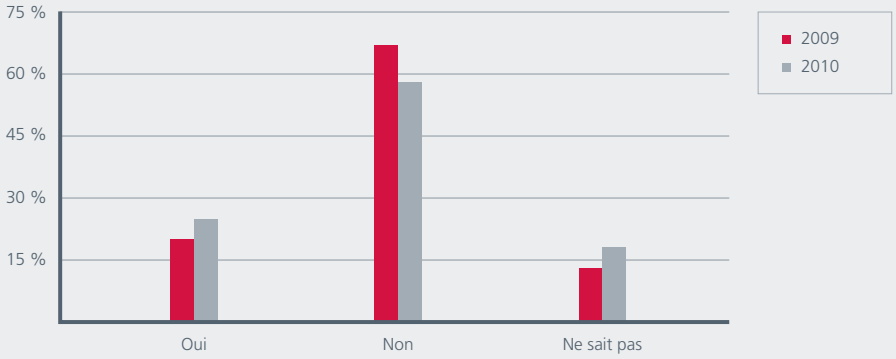
L'extorsion est un phénomène très répandu dans certains pays. Au Mexique et en Inde, respectivement 80 % et 60 % des personnes interrogées ont déclaré avoir été la cible de tentatives de cyberextorsion. Une hausse considérable par rapport à 2009, où seulement 17 % des répondants mexicains et 40 % des indiens dénonçaient de tels incidents.

Multiplication des menaces et des vulnérabilités



En 2010, 80 % des cadres dirigeants ont dû faire face à une attaque par déni de service à grande échelle et 85 % à une infiltration réseau.

Votre entreprise a-t-elle été victime de tentatives d'extorsion dans le cadre ou sous la menace d'une cyberattaque au cours des deux dernières années ?



Ces résultats confirment d'autres informations recueillies, suggérant que la cyberextorsion visant les réseaux électriques est une pratique qui s'étend. Pendant longtemps, des responsables de la cybersécurité de divers pays ont laissé entendre que des cyberexploits étaient à l'origine des pannes générales d'électricité qui ont frappé le Brésil, malgré les démentis opposés par les autorités brésiliennes[3]. Quoi qu'il en soit, la mésaventure brésilienne n'est pas un cas isolé : des déclarations d'agents du renseignement américain imputent à la cyberextorsion des coupures d'électricité survenues dans différents pays[4].

Stuxnet

Pour le commun des cybercriminels, la mise à l'arrêt d'un système électrique est davantage le signe d'un échec que d'une réussite. Après tout, l'objectif de la cyberextorsion est précisément d'obliger la victime à débourser de l'argent pour éviter toute interruption de service.

Les motivations des cyberguerriers sont d'une toute autre nature. Une attaque commanditée par un Etat aurait pour but de bloquer ou de porter atteinte à l'infrastructure qui dessert la population au quotidien, de détourner des ressources déjà insuffisantes, d'effriter le soutien des citoyens aux initiatives de guerre et de compliquer la mobilisation militaire qui repose sur l'infrastructure civile. Durant des années, les experts en technologies et porte-parole du secteur ont toutefois minimisé le risque de telles attaques, craignant qu'une reconnaissance officielle du risque se traduise par l'instauration de nouvelles réglementations en matière de sécurité. Même ceux qui étaient conscients des failles de sécurité des systèmes SCADA étaient enclins à nier le danger qu'elles posent, sous prétexte qu'il n'existait aucune preuve que d'autres nations étaient susceptibles de les exploiter à des fins de sabotage.

L'identification de Stuxnet, à l'été de 2010, a levé — ou aurait dû lever — toute équivoque. Ce logiciel malveillant d'une sophistication rare présentait deux caractéristiques qui prouvaient à quel point les cyberattaques constituaient une menace croissante.

Premièrement, Stuxnet ne semblait avoir aucune intention de lucre particulière ; il a été conçu exclusivement dans un but de sabotage. Stuxnet infecte les systèmes informatiques en exploitant diverses vulnérabilités de Microsoft Windows. Chargé sur l'ordinateur via des vecteurs tels qu'un lecteur USB, des fichiers réseau partagés ou des bases de données SQL, il cible un programme SCADA Siemens spécifique. Si ce logiciel est en cours d'exécution, Stuxnet recherche une configuration spécifique d'équipement industriel, puis lance une attaque visant à manipuler certains microcontrôleurs afin qu'ils se comportent de façon anarchique tout en signalant un fonctionnement normal aux opérateurs en charge du système.

Il s'agit là de sabotage pur et simple. Il est impossible d'utiliser facilement ce logiciel malveillant à des fins d'espionnage ou d'extorsion. Certains ont avancé l'hypothèse selon laquelle Stuxnet aurait pour but d'infiltrer les installations d'enrichissement d'uranium sous haute protection de Natanz, en Iran. Les centrifugeuses fragiles du site sont cruciales pour le programme d'armement nucléaire iranien et, depuis le lancement de Stuxnet, de nombreux dysfonctionnements inexpliqués y ont été constatés[5].

Stuxnet

Les données en notre possession indiquent clairement que le virus Stuxnet s'est propagé à l'échelle mondiale. Environ 40 % des répondants ont détecté la présence de Stuxnet sur leurs systèmes informatiques. Le logiciel malveillant était plus susceptible de prendre pour cible le secteur de l'électricité, avec 46 % des répondants de ce dernier ayant décelé sa présence.

Trois quarts des participants à l'étude ayant détecté Stuxnet étaient convaincus que le logiciel malveillant avait été supprimé de leurs systèmes. Les mesures prises pour neutraliser Stuxnet ont toutefois été très différentes selon les pays. Etonnamment, les niveaux de mise en œuvre de contre-mesures ont été relativement faibles dans certains pays où les taux d'infection étaient les plus élevés (comme l'Inde, la France ou l'Espagne).

57 % des répondants ont entrepris des audits de sécurité spéciaux en raison des inquiétudes suscitées par Stuxnet.

Dans un second temps, Stuxnet représentait un progrès extraordinaire en termes de sophistication par rapport aux types de logiciels malveillants utilisés par les réseaux cybercriminels clandestins. La société de sécurité informatique biélorusse qui a été la première à repérer Stuxnet a tout d'abord pensé qu'il s'agissait d'une porte dérobée exploitée par des pirates. Une analyse plus approfondie a toutefois révélé la nature complexe du virus. Ce dernier contient plusieurs exploits auparavant inconnus, des modules de pilotes Microsoft Windows signés à l'aide de certificats de chiffrement authentiques, dérobés à des sociétés respectables, et environ 4 000 fonctions intégrées, en plus d'utiliser des techniques avancées de contournement d'analyse qui compliquent l'ingénierie inverse. Tout ceci donne à penser qu'il est très certainement l'œuvre d'un Etat et non d'un gang criminel.

En bref, Stuxnet est une arme. Il est la preuve concrète que des nations n'hésiteront pas à mettre au point des logiciels malveillants afin de saboter les systèmes informatiques et les infrastructures critiques de leurs ennemis ou rivaux. Et que des pouvoirs hostiles peuvent facilement cibler les systèmes SCADA sur lesquels reposent les systèmes vitaux des nations (approvisionnement en électricité, gaz, pétrole et eau, ou encore traitement des eaux usées), en anéantissant les mécanismes de défense mis en place dans la plupart des entreprises.

De l'avis d'un expert, la majorité des systèmes à infrastructures critiques n'ont pas été conçus en prenant suffisamment en compte la sécurité informatique. Ainsi, dans le secteur de l'électricité, la préoccupation majeure a toujours été d'assurer un approvisionnement électrique constant et un système efficace. Même aujourd'hui, nombreuses sont les compagnies qui continuent à utiliser les mots de passe par défaut du fournisseur car ceux-ci garantissent un accès aisé aux systèmes en cas de crise ou lors des interventions de maintenance et de réparation.

Les initiatives récentes de modernisation des réseaux électriques s'inscrivent dans cette même tendance. Elles ont certes accru l'efficacité, mais ont également introduit de nouvelles brèches de sécurité. Leurs conséquences ont été démontrées lors de tests menés à l'Idaho National Labs en 2007. Les chercheurs ont prouvé qu'il leur était possible d'accéder à distance aux systèmes de contrôle d'un générateur et de modifier, toujours à distance, son cycle de fonctionnement, jusqu'à le rendre incontrôlable. Une vidéo de l'incident montre le générateur cible qui vibre, se met à fumer puis arrête de fonctionner. Ce type de machine est onéreux, et sa réparation ou son remplacement peut prendre des semaines voire des mois.

Même s'il n'était pas dû à une cyberattaque, la panne générale d'électricité (*blackout*) qui a frappé le Nord-Est du continent américain en 2003 a révélé les effets en cascade que peut engendrer un dysfonctionnement d'une partie d'un réseau électrique, si petite soit-elle. Cette interruption massive a affecté 50 millions de personnes. Bien que dans la plupart des cas, le courant ait été rétabli dans les 48 heures, certaines régions sont restées sans électricité pendant une semaine[6]. Les défaillances se sont enchaînées trop rapidement pour une intervention manuelle : il n'a fallu que sept minutes pour que la panne s'étende à l'ensemble de la région[7].

L'incident démontre également l'efficacité potentielle de la fonction de blocage du signalement d'incidents mise en œuvre dans Stuxnet, qui, d'après un expert, permet de dissimuler toute activité au centre d'exploitation réseau lors d'une attaque ciblant le secteur de l'énergie ou d'autres secteurs. Selon un rapport de l'U.S.-Canada Power System Outage Task Force, qui a enquêté sur la panne de courant générale de 2003, des propriétaires de lignes individuelles avaient tenté de signaler les défaillances en cascade aux opérateurs de contrôle, mais ceux-ci ont mis du temps à réagir car les ordinateurs de contrôle affectés à la surveillance des

Les réseaux électriques dans la ligne de mire des terroristes ?

Si les Etats constituent une menace pour les services de fourniture d'électricité à la population et autres services similaires, qu'en est-il des terroristes ? Ces derniers peuvent-ils s'en prendre aux réseaux électriques et provoquer des pannes de courant à grande échelle ? Exception faite sans doute des groupes terroristes soutenus par des Etats, cette menace n'est pas considérée comme critique par les experts. « S'il est plus lucratif de s'en prendre à une infrastructure critique qu'à une base militaire, ce type d'attaque n'a pas même impact émotionnel que des images de carnage à la suite d'une explosion faisant des victimes civiles », affirme un expert. Il souligne toutefois que, maintenant qu'une jeune génération prend le pouvoir au sein des organisations terroristes, il y a fort à penser que les cyberattaques vont se multiplier.

systèmes SCADA ne révélaient aucun problème dans l'approvisionnement en électricité. Ce n'est que lorsque d'autres sociétés ont commencé à signaler l'incident que les opérateurs en ont réalisé toute l'ampleur[8].

« Les Etats demeurent la principale menace pour la sécurité des infrastructures critiques aux Etats-Unis », indique un expert du secteur. Le seul point positif à propos de ce constat, c'est que les attaques émanant de nations sont sans doute moins courantes que l'extorsion criminelle. L'expert ajoute : « Il est peu probable que les Etats effectuent des tirs d'essai. »

Lors d'un conflit toutefois, des attaques informatiques paraissent probables. Toutes les grandes puissances mondiales ont acquis ou sont sur le point d'acquérir des capacités de cyberattaques, et les infrastructures critiques demeurent une cible de choix.

Nous avons interrogé des responsables de secteurs d'activité dépendants des systèmes SCADA afin de savoir si Stuxnet avait affecté leurs opérations. Leurs réponses sont frappantes. 2/5ème des répondants, et près de la moitié de ceux appartenant au secteur de l'électricité, ont déclaré avoir détecté Stuxnet sur leurs systèmes. En fait, de tous les secteurs reposant sur des infrastructures critiques représentés dans l'étude, c'est celui de l'électricité où la présence de Stuxnet était la plus élevée. Plus de la moitié des personnes interrogées ont indiqué avoir dû prendre des mesures contre ce logiciel malveillant.

En raison de l'envergure mondiale de notre étude, ces résultats sont édifiants. Même sil est possible qu'il n'ait visé au départ qu'une seule installation, Stuxnet a choisi une voie détournée pour atteindre sa cible, infectant de fait tous les systèmes, puis restant inactif si le système infecté ne présentait pas la configuration spécifique qu'il recherchait. C'est peut-être pour cette raison que près de trois quarts des participants à l'étude qui avaient détecté Stuxnet étaient convaincus ou totalement convaincus que le logiciel malveillant avait été supprimé de leurs systèmes ou neutralisé.

Quelles conclusions le secteur a-t-il tirées de l'incident Stuxnet ?

Il ne fait aucun doute qu'il existe une prise de conscience généralisée de l'existence de menaces posées par d'autres nations. Plus de la moitié des cadres dirigeants sont convaincus de l'implication d'Etats étrangers dans des intrusions réseau perpétrés contre les infrastructures critiques de leur pays.

Néanmoins, la découverte de Stuxnet sur leurs systèmes ne semble pas avoir particulièrement motivé les entreprises à prendre des initiatives concrètes. Les niveaux les plus élevés de mesures de protection anti-Stuxnet ont été relevés aux Emirats arabes unis, en Italie et au Japon, des pays où paradoxalement, les taux d'infiltration de Stuxnet étaient comparativement faibles. A l'inverse, des pays tels que l'Inde, où l'infiltration est forte, ont affiché des niveaux de mise en œuvre de mesures comparativement faibles[9]. Comme l'explique un expert indien, Stuxnet et d'autres cyberincidents récents ont accru la sensibilisation à la cybersécurité, mais faute d'une politique claire des autorités publiques à cet égard, les entreprises et les ministères sont livrés à eux-mêmes et décident individuellement des actions à entreprendre. « Il n'existe aucune perspective au niveau national, [et les réseaux] deviennent toujours plus vulnérables », déclare l'expert indien.

De nombreux observateurs estiment que le déni est toujours l'une des réactions du secteur vis-à-vis du problème Stuxnet. D'après un expert, de nombreuses entreprises continuent de se focaliser sur leur résilience en cas d'attaque par déni de service, plutôt que d'envisager d'éventuelles attaques de pointe visant à saboter leur équipement — alors que ces dernières deviennent comme le principal danger posé au secteur de l'électricité et aux secteurs similaires. Selon une autre source, « Stuxnet a changé la donne, mais il ne modifiera en rien la direction que prend la législation américaine en matière de cybersécurité », dans la mesure où les décideurs politiques ont déjà pris conscience de la menace. La principale difficulté sera d'amener le secteur à en reconnaître la nature changeante.

« Nombreux sont ceux qui croient toujours [que le déni de service] est le principal problème et qu'ils sont capables de gérer une attaque par déni de service distribué, à moins que le système physique n'ait subi des dommages. Il est extrêmement difficile de leur faire comprendre que Stuxnet est une éventualité à envisager », déclare un expert consulté dans le cadre de cette étude. « Le problème n'est pas tant que l'on subtilise le matériel informatique ou qu'il tombe en panne, mais qu'une autre personne l'emploie pour exécuter illicitement des commandes. » La source cite l'exemple d'un piratage commis il y a quelques années aux Etats-Unis, au cours duquel un individu a pris le contrôle de feux de signalisation et les a manipulés à sa guise.

Plusieurs cadres dirigeants nous ont indiqué qu'ils étaient davantage préoccupés par les attaques par déni de service distribué que par des logiciels malveillants tel Stuxnet, ce qui confirme les dires de notre source. Un tiers des répondants ont en effet déclaré qu'ils n'avaient pas du tout ou pas très confiance dans la capacité de leur entreprise à contrer les attaques par déni de service distribué ou les infiltrations furtives. Interrogés au sujet des logiciels malveillants conçus à des fins de sabotage, les participants à l'étude ont exprimé le même sentiment dans environ 20 % des cas. Pourtant, comparées à Stuxnet, les attaques par déni de service distribué sont un jeu d'enfant à refouler. Un expert en cybersécurité basé aux Etats-Unis confirme : « Après les incidents Stuxnet, de nombreuses personnes ont dit : "Je n'ai pas de produits Siemens, je ne suis pas dans le nucléaire, donc je n'ai aucun souci à me faire". »

Vulnérabilités plus nombreuses et préparation aux attaques attendues

Plus de 40 % des cadres dirigeants interrogés s'attendent à être la cible d'une attaque informatique majeure au cours des 12 prochains mois ; on entend par là une attaque occasionnant par exemple une indisponibilité critique de services pendant au moins 24 heures, des blessures ou pertes en vies humaines ou la faillite d'une société. Ce pourcentage est étonnamment élevé dans certains pays, en particulier en Inde, où neuf cadres sur dix ont déclaré qu'ils pronostiquaient une telle attaque dans l'année, ainsi qu'au Mexique, où sept sur dix partageaient cet avis.

Les craintes d'une attaque majeure sont également relativement élevées en Chine, où plus de la moitié des répondants prévoyaient une telle attaque en 2010 ou 2011.

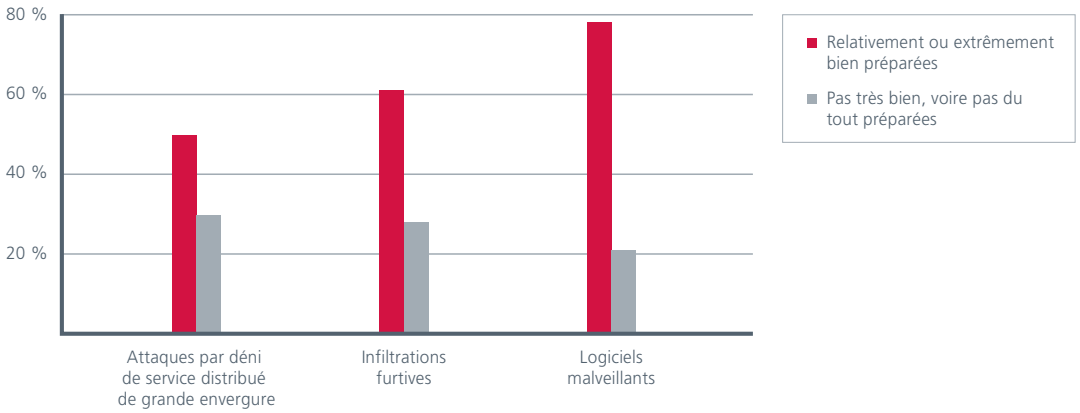
Dans certains pays, les résultats concernant les perceptions des vulnérabilités étaient encore plus alarmants. Ainsi, trois quarts des répondants brésiliens et 60 % des mexicains s'estimaient mal préparés à une attaque par déni de service à grande échelle contre leur entreprise. Et dans ces deux pays, ils étaient deux tiers à penser que leurs systèmes étaient vulnérables aux infiltrations furtives. Le niveau d'inquiétude élevé enregistré au Brésil peut être attribuable aux vagues de cyberattaques qu'a connues le pays et aux très nombreux pirates informatiques qui y sévissent (d'après une étude, un tiers des 50 principaux groupes actifs dans le détournement de sites web sont basés au Brésil[10]). Au vu des pannes d'électricité massives qui ont frappé les principales métropoles brésiliennes en 2005 et 2007, il n'est pas surprenant de constater que 91 % des répondants de ce pays estimaient leur secteur mal préparé aux attaques par logiciels malveillants.

Les répondants australiens sont eux aussi étonnamment inquiets de la vulnérabilité de leur secteur. Neuf sur dix estimaient que leur secteur n'était pas du tout ou peu préparé à une infiltration furtive de leur réseau. « En Australie, le gouvernement a lancé une série de programmes et d'initiatives de grande envergure, destinés à promouvoir la protection des infrastructures critiques. Le sentiment d'un manque de préparation naît d'une conscience plus aigue [de l'existence de la menace] chez les dirigeants d'entreprise, en raison des efforts importants de sensibilisation de la part des pouvoirs publics », explique Ajoy Ghosh, directeur de la sécurité informatique chez Logica Australia.

Interconnectivité croissante et réseaux de distribution intelligents

En dépit du malaise profond qui règne concernant la vulnérabilité toujours plus grande des réseaux électriques et la préparation insuffisante pour parer à une attaque réseau, les compagnies d'électricité et les pouvoirs publics s'orientent au contraire vers une stratégie comportant encore plus de risques.

Dans quelles mesures les entreprises sont-elles préparées à contrer des attaques ?



Aujourd'hui, l'initiative majeure en matière de réseaux électriques n'est pas centrée sur une dynamique d'amélioration de la sécurité, mais concerne la création de « réseaux de distribution intelligents ». Ces derniers utilisent un flux d'informations bidirectionnel qui permet au fournisseur d'électricité de surveiller et de contrôler le flux d'électricité à destination et parfois au sein de l'habitation du client. Ils ont pour objectif de mieux corréler l'offre et la demande par une modification des prix et même une coupure de l'électricité pour des usagers ou appareils particuliers en cas de pics de demande, par exemple les soirs d'hiver. La réduction des pointes de consommation permet de limiter le nombre de centrales électriques. Des projets visant à exercer un contrôle nettement plus précis sur l'utilisation de l'électricité par les consommateurs a suscité un grand enthousiasme des dirigeants politiques, en particulier en Chine et aux Etats-Unis.

A l'horizon 2015, les dépenses en réseaux de distribution intelligents dépasseront les 45 milliards de dollars à l'échelon mondial[11]. Parallèlement, les consommateurs et groupes de consommateurs ont manifesté leurs inquiétudes quant aux répercussions de ces réseaux sur les prix énergétiques et en termes de respect de la vie privée[12]. Lew Owens, PDG d'ETSA, distributeur d'électricité privé basé en Australie, s'est exprimé dans le même sens auprès de l'Australian Broadcasting Corporation : « Parler de "compteurs intelligents" paraît fantastique […], mais en réalité, les usagers se verront forcés de réduire leur consommation parce que les prix grimperont à un point tel qu'ils devront couper l'électricité […][13]. »

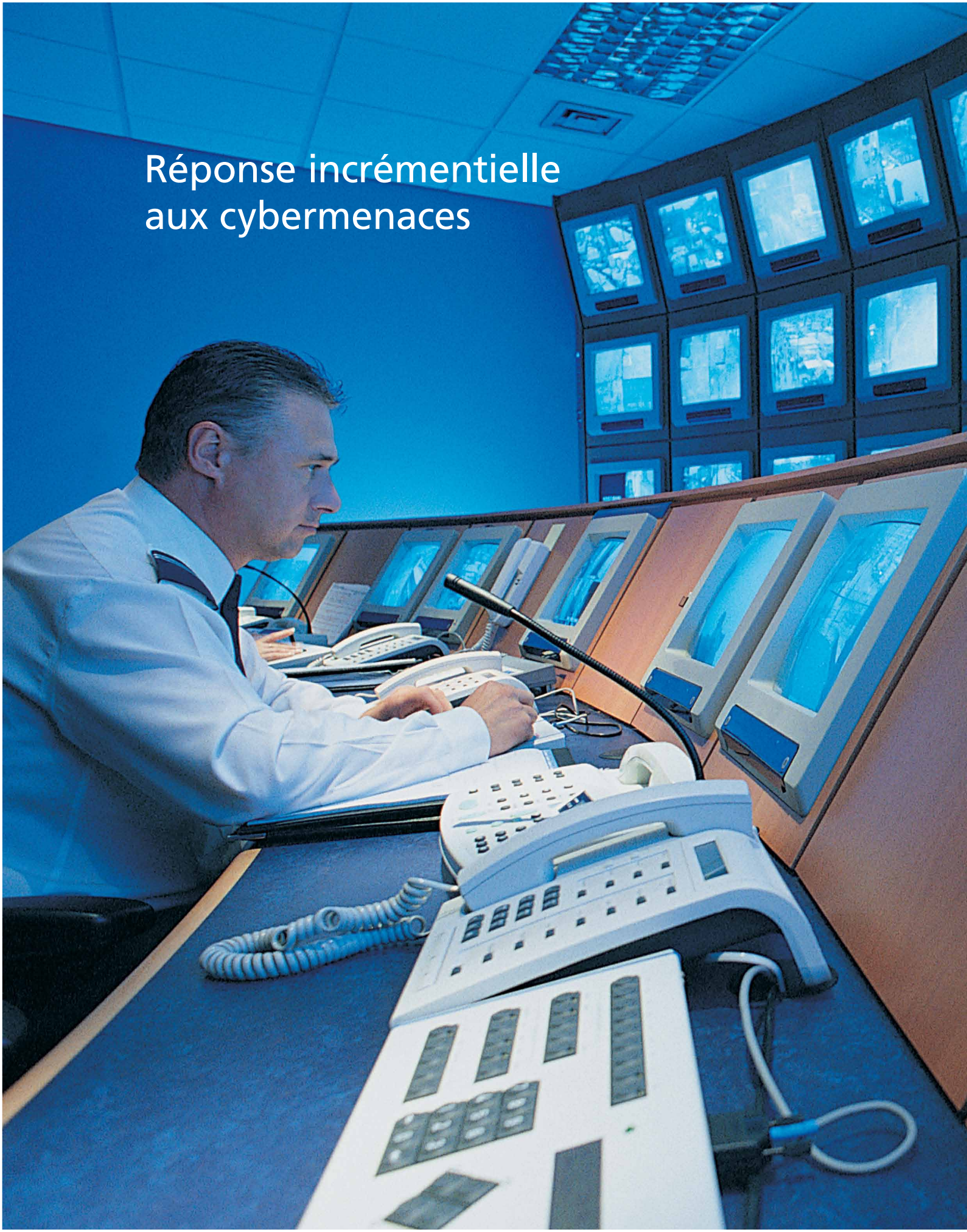
Nos résultats révèlent toutefois que le secteur se lance tête baissée dans la mise en œuvre de ces réseaux de nouvelle génération. Quatre cadres dirigeants sur cinq ont déclaré que leur entreprise avait l'intention d'implémenter des contrôles de réseaux de distribution intelligents, tels que la différenciation des tarifs en fonction des plages horaires, les coupures de l'alimentation électrique et les limitations de puissance.

Toutefois, l'extension du contrôle du réseau au niveau du ménage voire de l'appareil électrique créera de nouveaux dangers si le réseau lui-même n'est pas sécurisé. Si les auteurs d'attaques peuvent prendre les commandes des nouveaux compteurs intelligents ou de leur réseau sous-jacent, ils s'en serviront pour perturber l'approvisionnement en électricité de façon extrêmement précise, en privant de courant une habitation ou un appareil spécifique ou peut-être en y générant des surtensions. Comme l'explique un expert en sécurité, « l'automatisation des systèmes et la possibilité d'y accéder à distance les ont rendus de plus en plus vulnérables, étant donné la multiplication des points d'accès à partir desquels il est possible de lancer des attaques. De plus, nous nous adaptons mal et lentement, de sorte que nous restons vulnérables plus longtemps. »

La plupart des cadres dirigeants et des observateurs ne pensent pas que les réseaux contrôlant les systèmes électriques soient sécurisés à l'heure actuelle, en particulier contre les attaques perpétrées sous l'égide d'une nation. Au moins un des dirigeants interrogés a dénoncé « la stupidité d'une approche qui consisterait à mettre sur Internet les systèmes d'approvisionnement en électricité de l'ensemble des foyers—et comble de l'ironie, on appelle ça des réseaux "intelligents" ».

Il y a certainement lieu de s'interroger sur le niveau de sécurité dont bénéficieront les nouveaux systèmes. Plus de la moitié (56 %) des cadres dirigeants dont les entreprises projettent de mettre en œuvre des systèmes de réseaux de distribution intelligents ont également l'intention de les connecter à l'usager via Internet. La plupart ont pris conscience du fait que ces nouveaux systèmes introduiront des vulnérabilités très complexes au sein d'un réseau électrique déjà en proie aux menaces, mais seulement deux tiers ont adopté des mesures de sécurité spécifiques pour les contrôles de ces nouveaux réseaux. Selon Jim Woolsey, ancien directeur de la CIA, « 90 à 95 % du personnel participant au développement des réseaux de distribution intelligents ne se sentent pas concernés par la sécurité et ne considèrent celle-ci que comme un facteur accessoire ».

Réponse incrémentielle aux cybermenaces



De nouvelles mesures de sécurité continuent d'être adoptées, et c'est là une bonne nouvelle. En revanche, à la différence des menaces et des vulnérabilités, l'adoption de ces mesures progresse avec une extrême lenteur.

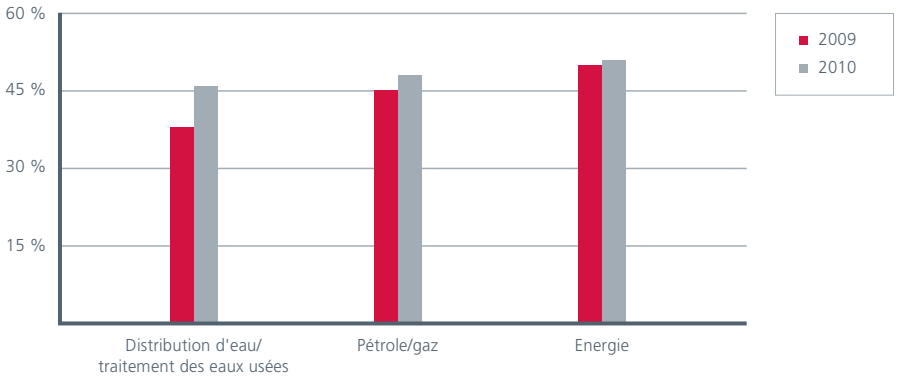
Les menaces et les vulnérabilités se multiplient, mais qu'en est-il des mesures de sécurité ? Notre étude suggère que les investissements en sécurité peinent à démarrer.

Nous avons interrogé les cadres dirigeants du secteur sur les mesures de sécurité implémentées pour contrer les vulnérabilités et menaces dont la plupart d'entre eux reconnaissent l'existence. De nouvelles mesures de sécurité continuent d'être adoptées, et c'est là une bonne nouvelle. En revanche, à la différence des menaces et des vulnérabilités, l'adoption de ces mesures progresse avec une extrême lenteur.

Cette conclusion n'est pas fondée sur l'évaluation subjective donnée par les cadres quant aux niveaux de protection mis en place. En effet, les jugements subjectifs ne sont pas fiables dans ce contexte. Pour bénéficier d'une mesure de référence plus objective, nous leur avons posé des questions précises et détaillées concernant 29 mesures de sécurité différentes que les sociétés peuvent mettre en œuvre pour défendre leurs réseaux. Ces questions sont similaires à celles du précédent rapport, mais le questionnaire de cette année inclut également plusieurs questions sur les défis de sécurité posés par les nouveaux projets technologiques, dont l'accès au réseau via les téléphones mobiles et les connexions IP.

Ces mesures de sécurité comprennent les technologies de sécurisation, les stratégies de sécurité, le chiffrement, l'authentification et la connectivité réseau. Etant donné que la liste des mesures de sécurité possibles de cette année est comparable à de nombreux égards à celle de l'année précédente, nous avons pu constituer une ébauche de guide récapitulant les progrès accomplis par les sociétés dans le renforcement de leur sécurité. Ce « taux d'adoption des mesures de sécurité » reste naturellement approximatif puisque la sécurité des réseaux ne consiste pas simplement à accumuler des technologies de sécurité et que toutes ces technologies ne présentent pas la même efficacité. Néanmoins, ce taux donne une idée assez précise de la situation, à savoir si le secteur ajoute réellement de nouvelles mesures de sécurité en réponse aux nouvelles menaces et vulnérabilités[14].

Evaluation des améliorations : taux d'adoption des mesures de sécurité



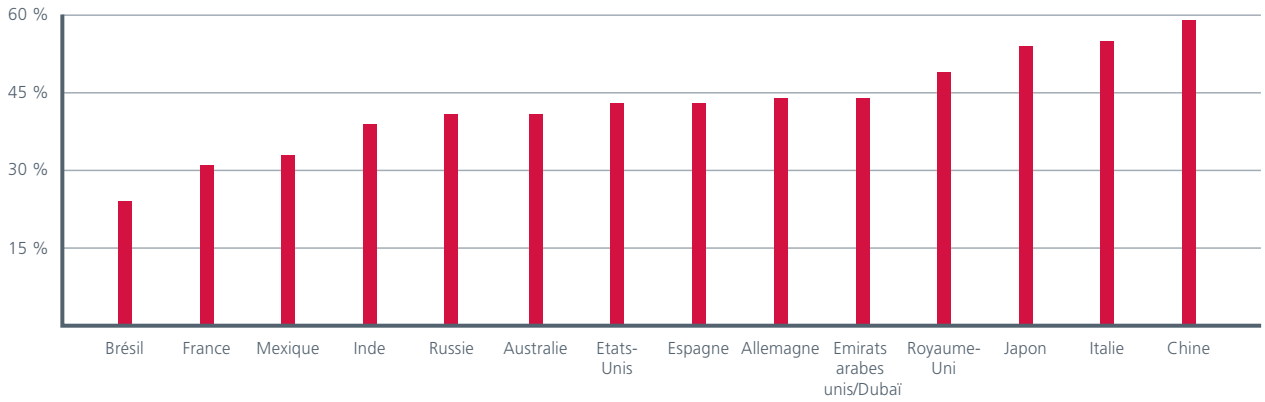
C'est effectivement le cas, même si les progrès sont très lents. Dans chacun des secteurs analysés, les cadres dirigeants déclarent avoir adopté cette année un nombre plus important de technologies de sécurité que l'année précédente. Le secteur de la distribution d'eau et du traitement des eaux usées, qui affichait en 2009 un taux d'adoption de mesures bien inférieur à la moyenne, s'est considérablement amélioré puisque son taux a progressé de 38 % à 46 %. Les dirigeants des compagnies pétrolières et gazières présentent un taux d'adoption de 48 % par rapport aux 45 % de l'année précédente. Quant au secteur de l'énergie, en tête du classement l'année dernière, il s'est visiblement reposé sur ses lauriers puisque le déploiement des mesures de sécurité n'a progressé que d'un seul point, de 50 à 51 %.

En dépit de ces augmentations, force est de constater que la plupart des sociétés n'ont pas adopté les nombreuses mesures de sécurité qu'ils ont à leur disposition. En d'autres termes, la sécurité reste pour beaucoup rudimentaire. Ainsi, 44 % des responsables interrogés ont déclaré utiliser une authentification uniquement basée sur le nom d'utilisateur et le mot de passe (« secret partagé ») pour l'accès au réseau sur site. En revanche, moins d'une entreprise sur cinq utilise des jetons et 3 % seulement ont recours aux mesures biométriques. Moins d'une société sur dix déclare utiliser les trois méthodes pour l'accès au réseau sur site.

Mesures de sécurité prises en compte :

- Correctifs de sécurité et maintenance logicielle
- Configuration normalisée des postes de travail
- Partage des informations avec des partenaires publics/du secteur
- Abonnement à un service de surveillance des menaces
- Interdiction ou restriction de l'utilisation de périphériques USB ou d'autres supports amovibles
- Authentification sur le réseau informatique à l'aide par exemple de jetons ou d'identifiants biométriques
- Authentification sur le réseau informatique hors site à l'aide par exemple de jetons ou d'identifiants biométriques
- Installation de pare-feux vers les réseaux publics
- Mesures de contrôle de l'accès au réseau
- Contrôles d'accès et de sécurité propres aux bases de données
- Systèmes de prévention des intrusions
- Systèmes de détection des intrusions
- Pare-feux entre systèmes d'entreprise
- Outils de gestion des informations de sécurité
- Outils de prévention des fuites de données
- Détection des anomalies au niveau des activités et des rôles
- Listes d'autorisation d'applications
- Outils de surveillance de l'activité réseau
- Utilisation du chiffrement (pour les transmissions en ligne, les données stockées sur le réseau, les disques durs des ordinateurs portables, les bases de données, le courrier électronique et les supports amovibles)
- Utilisation réglementée des équipements mobiles (logiciels antivirus, reprogrammation du microcode, restriction de la connexion au réseau)
- Surveillance des nouvelles connexions du réseau informatique à l'aide d'audits ou d'outils d'analyse des comportements sur le réseau

Taux d'adoption des mesures de sécurité par pays



L'accès hors site est à peine plus sécurisé : 26 % des répondants utilisent uniquement des mots de passe, un cinquième uniquement des jetons et 3 % seulement l'authentification biométrique. Seul un répondant sur dix déclare avoir interdit complètement tout accès au réseau hors site.

D'autres mesures de sécurité plus sophistiquées, notamment des outils destinés à surveiller l'activité réseau ou à détecter des anomalies de comportement, ont été adoptées par une minorité des répondants (respectivement 25 et 36 %). Pourtant, comme le confirme un expert en sécurité, ces mesures s'avèrent les plus efficaces et nécessaires pour la sécurité réseau. « La priorité est à présent aux audits, aux outils de suivi des activités pour détecter les anomalies et au développement de composants plus intelligents et plus résilients », a-t-il déclaré. Certains pays sont incontestablement plus attentifs que d'autres à la sécurité. L'année dernière, la Chine se démarquait en devançant nettement tous les autres pays en matière d'adoption de mesures de sécurité. Cette année, les chiffres montrent que la situation n'a guère changé. La Chine conserve sa première place en termes d'adoption des mesures de sécurité avec un taux global de 59 %, suivie par l'Italie et le Japon, avec respectivement 55 % et 54 %. En revanche, le Brésil, la France et le Mexique sont franchement à la traîne, avec des taux d'adoption presque deux fois inférieurs aux premiers du classement. Tous les autres pays forment un groupe dont les taux d'adoption sont très proches du taux moyen de 43 %.

32 % des sociétés interrogées n'ont pas adopté des mesures de sécurité spécifiques pour les contrôles des réseaux de distribution électrique intelligents.

Deux extrêmes au sein du BRIC

En dépit de leur statut commun de superpuissance émergente, le Brésil et la Chine ont des stratégies radicalement différentes en matière de cybersécurité. D'un côté, le Brésil présente de nombreuses contradictions entre la perception des menaces et les réponses à celles-ci. Le pays arrive systématiquement en dernière place en termes d'adoption de mesures de sécurité alors qu'il est le premier à avoir conscience des vulnérabilités existantes parmi tous les pays interrogés. Le niveau de confiance accordé aux pouvoirs publics brésiliens est également l'un des plus faibles observés. Pourtant le Brésil, qui a été confronté à des cas avérés de cyberextorsion, présente l'un des taux d'anticipation des attaques les plus faibles : seul un petit tiers des répondants redoute une cybermenace majeure au cours des douze prochains mois.

Tout à fait à l'opposé du spectre, la Chine conserve sa première place en termes d'adoption de mesures de sécurité ainsi qu'un niveau de confiance élevé dans la capacité des autorités chinoises à prévenir et à décourager les cyberattaques. Le gouvernement a participé activement à relever le défi de la cybersécurité, ce qui a permis à la Chine de devancer tous les autres pays en développement en matière de sécurisation des réseaux et de réduire l'écart qui la sépare des pays développés les plus performants en matière de sécurité. Ces observations suggèrent qu'en dépit de certaines lacunes, la Chine possède clairement un plan d'action concernant la cybersécurité.

Réaction des pouvoirs publics

Les pouvoirs publics peuvent encourager la sécurité en collaborant avec le secteur et en adoptant des réglementations plus exigeantes que celles préconisées par le marché.

De nombreuses raisons expliquent les écarts constatés entre les pays en matière de sécurité. L'une d'elles est incontestablement liée au rôle joué par les pouvoirs publics. Ces derniers peuvent encourager la sécurité en collaborant avec le secteur et en adoptant des réglementations plus exigeantes que celles préconisées par le marché. Certains pouvoirs publics participent activement tandis que d'autres sont plus réticents à intervenir. Au bout du compte, et sans doute étonnamment, ce sont les pays les plus activement réglementés qui bénéficient du plus grand respect et niveau de confiance de la part du secteur privé.

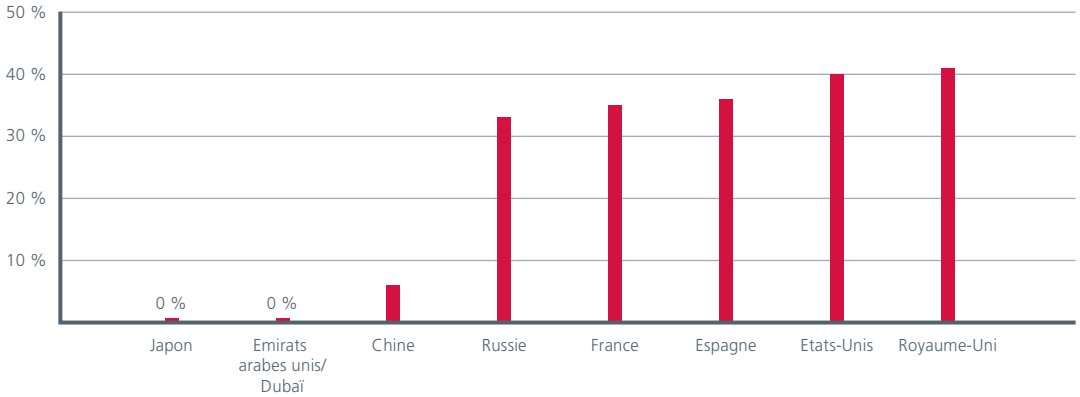
Rôle des pouvoirs publics

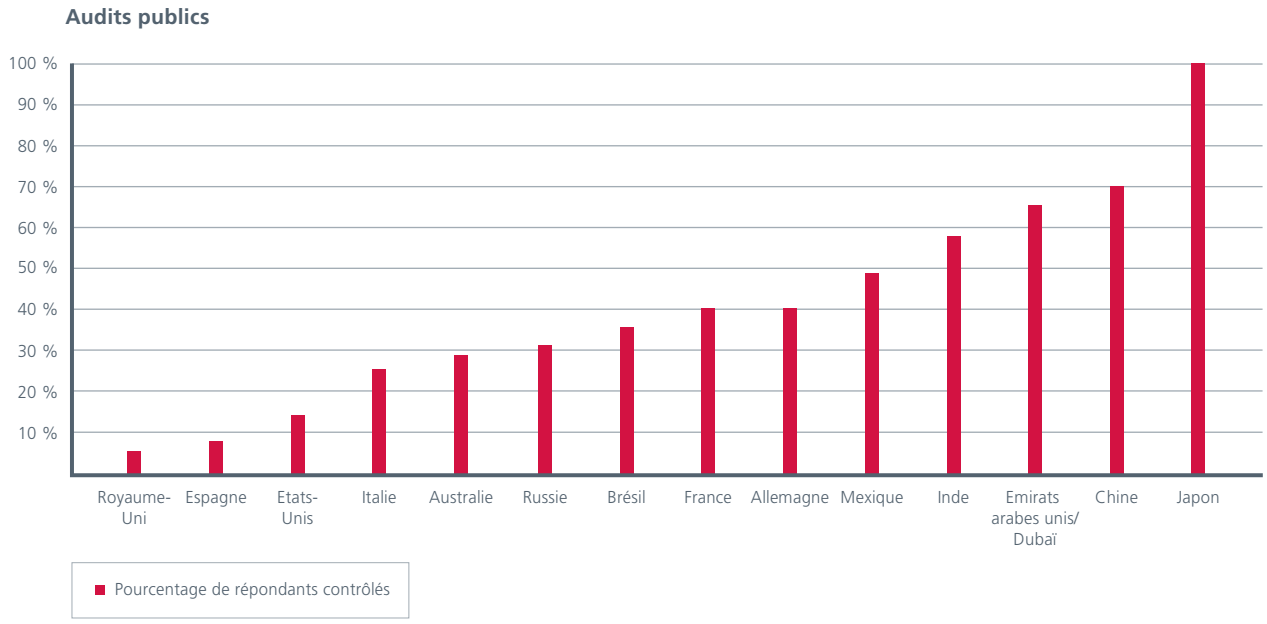
Pour évaluer la relation entre le secteur public et privé, nous avons demandé aux dirigeants informatiques de définir leurs interactions avec leur gouvernement en suggérant plusieurs possibilités (aucune interaction, partage informel d'informations et supervision réglementaire).

La Chine arrive en tête avec un nombre important de répondants indiquant un niveau élevé d'interactions formelles et informelles avec leurs dirigeants politiques sur le thème de la sécurité[15]—l'un des taux de non-intervention les plus faibles parmi tous les pays interrogés.

L'autre pays présentant une interaction élevée entre le public et le privé est le Japon où la supervision de la cybersécurité semble avoir considérablement augmenté au cours de l'année écoulée. Près de la moitié (44 %) des répondants japonais déclarent que les organismes publics ont exercé un pouvoir réglementaire général ou précis sur leurs mesures de protection réseau. Cette pression réglementaire est encore plus importante qu'en Chine où 28 % déclarent avoir été soumis à des réglementations détaillées. Autre observation surprenante, environ neuf Japonais sur dix indiquent coopérer avec les pouvoirs publics et les consulter par l'intermédiaire de partenariats public-privé, bien plus que n'importe quel autre Etat. Un expert en sécurité japonais attribue ce niveau de collaboration élevé à la nature particulière de la collaboration entre le secteur public et privé japonais en matière de cybersécurité : « La relation entre le public et le

Pourcentage de répondants à n'avoir aucune interaction avec leurs pouvoirs publics en matière de cybersécurité ou de protection des réseaux





privé est caractéristique en cela que les pouvoirs publics encouragent l'autonomie des propriétaires et opérateurs d'infrastructures critiques [et] soutiennent leurs initiatives privées au lieu de les réglementer. »

A l'inverse, dans des pays comme l'Espagne, les Etats-Unis et le Royaume-Uni, plus d'un tiers des répondants déclarent n'avoir aucun contact avec les autorités publiques concernant la cybersécurité tandis que le reste indique qu'il s'agit d'échanges essentiellement informels.

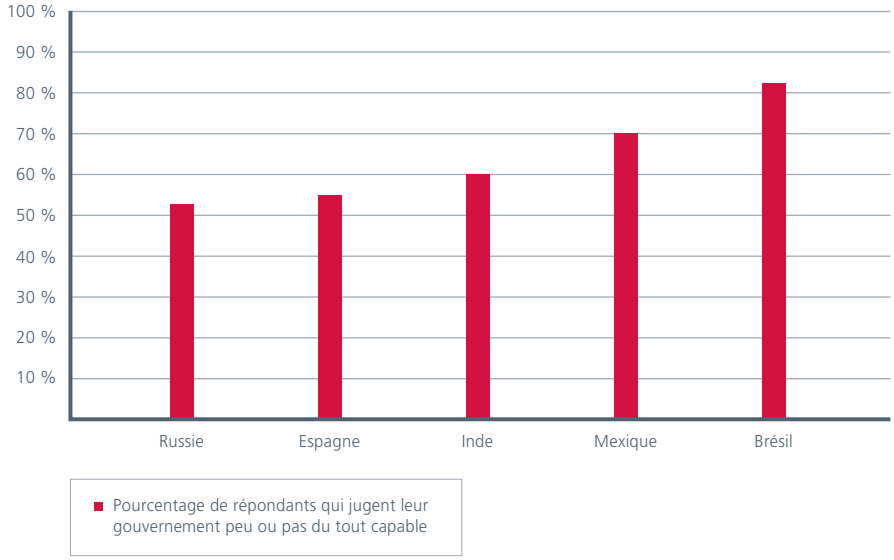
La tendance est pratiquement identique lorsque nous avons demandé aux dirigeants informatiques si leurs plans de sécurité étaient audités par les pouvoirs publics. Pratiquement tous les répondants japonais ont déclaré avoir été soumis à de tels audits. Il s'agit d'une augmentation sensible pour le Japon par rapport à l'année dernière, qui voyait la Chine se classer en première place des audits de sécurité. Cette année, la Chine arrive deuxième avec sept répondants sur dix déclarant être soumis à des audits. Les taux d'audit les plus faibles sont observés au Royaume-Uni, en Espagne et aux Etats-Unis, tous sous la barre des 20 %.

Au cours de l'année écoulée, certains pays semblent avoir considérablement étendu la portée de leurs audits de sécurité alors que d'autres les ont réduits. En 2009, l'écart entre les pays présentant le nombre d'audits officiels le plus élevé et le plus faible s'élevait à 50 %. Bien qu'il s'agisse d'une marge considérable, en 2010, celle-ci a grimpé à 94 %, ce qui représente la différence entre les 100 % d'audits du Japon et les 6 % d'audits du Royaume-Uni.

Si l'on s'en réfère à ces chiffres, il semble que l'Europe et les Etats-Unis se laissent distancer par l'Asie dans la course engagée par les autorités pour renforcer la protection de leurs infrastructures civiles contre les cyberattaques.

25 % des entreprises d'infrastructures critiques n'ont pas d'interaction avec les autorités en matière de cybersécurité ou de protection des réseaux.

Répondants considérant que leurs pouvoirs publics sont *incapables* de prévenir ou de décourager des cyberattaques



Niveau de confiance global envers les autorités

Nous avons également évalué la confiance des dirigeants informatiques dans la capacité des pouvoirs publics à prévenir et à décourager les attaques informatiques potentielles. Leurs réponses restent pratiquement inchangées par rapport aux résultats de 2009. Cette année, 54 % des répondants estiment les autorités relativement capables, capables et tout à fait capables de prévenir ou de décourager les attaques, un pourcentage similaire aux 55 % observés en 2009.

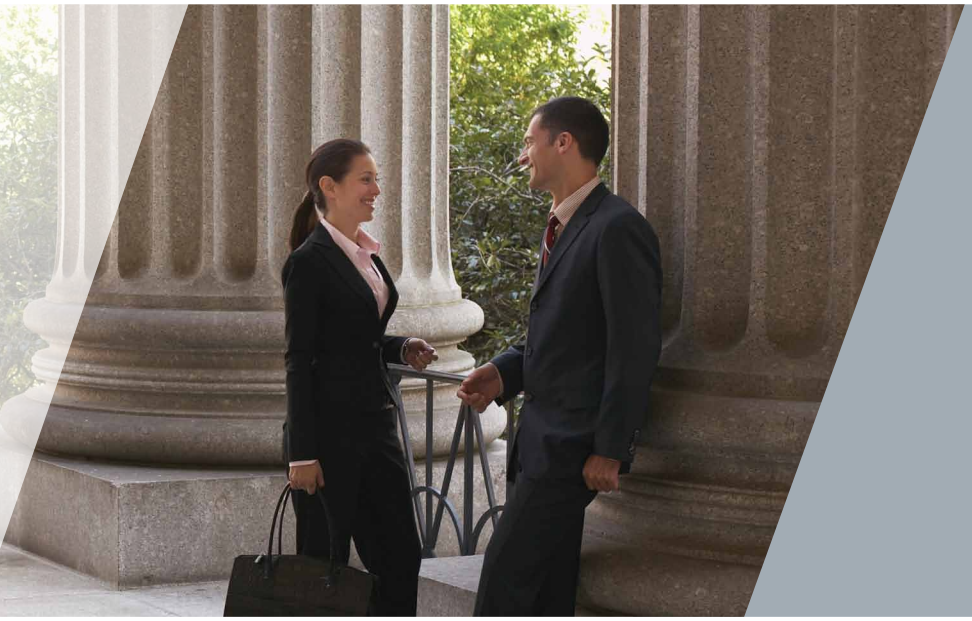
Les évaluations de la capacité propre à chaque pays varient considérablement, comme l'année dernière. L'attention accrue accordée par le Japon aux réglementations et aux audits pourrait bien avoir modifié l'avis des répondants japonais quant à la capacité de leur gouvernement, puisque le niveau de confiance s'élève à 83 % cette année au lieu de 56 % en 2009.

Les « votes de défiance » les plus élevés reviennent au Brésil, au Mexique et à l'Inde, qui ont moins confiance en leurs pouvoirs publics qu'en 2009. Cette situation peut s'expliquer en partie par le nombre limité d'audits officiels. Selon un expert, la nature sporadique des audits de sécurité en Inde induit souvent un sentiment de sécurité trompeur. « Il s'agit d'un secteur si dynamique que les audits effectués six ou huit mois plus tôt ne sont plus valables. Il est nécessaire de mettre en place un cycle d'audits trimestriel et un système de contrôles inopinés », a déclaré un expert indien.

Une tendance similaire émerge dans les réponses des responsables interrogés lorsque nous leur avons demandé s'ils pensaient que les législations actuelles étaient suffisantes pour prévenir ou décourager les attaques. Les niveaux de confiance les plus élevés ont été observés au Japon (78 %), dans les Emirats arabes unis (67 %) et en Chine (56 %). Le Brésil, où moins d'un répondant sur cinq fait confiance aux autorités, se classe en dernière position. L'Italie, le Mexique et l'Australie accordent également une confiance très limitée dans la capacité de leur législation à résoudre les incidents de sécurité informatique. La surprise vient de l'Inde qui est très confiante (90 %) dans la capacité de sa législation à décourager les cyberattaques, en dépit de la méfiance témoignée envers les institutions gouvernementales.

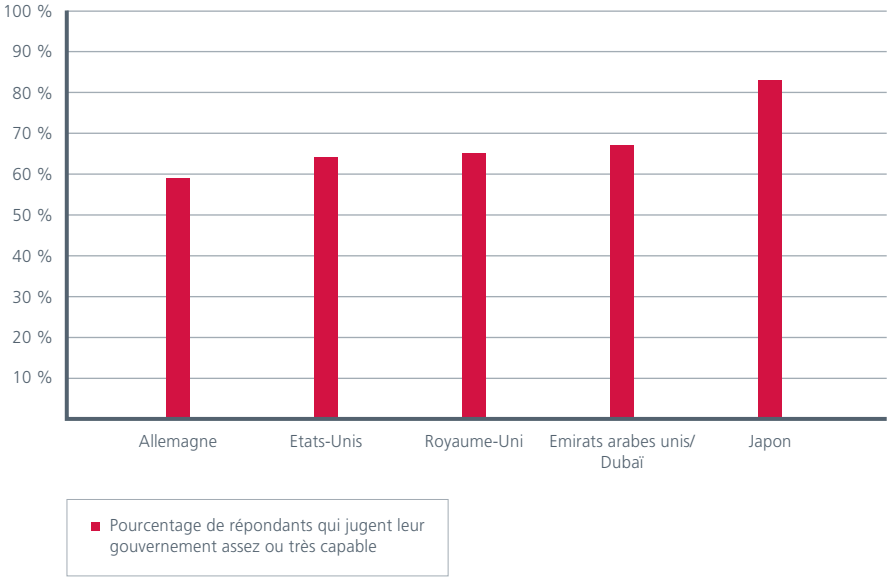
Des pouvoirs publics considérés comme des menaces

Les pouvoirs publics jouent également un autre rôle, plus médiatisé, en matière de sécurité informatique. Leurs armées et services de renseignements infiltrent et préparent des attaques contre les réseaux d'autres pays. Au cours des entretiens menés dans le cadre de cette étude, la cybermenace la plus souvent citée était l'espionnage et les actes de sabotage commandités par des Etats.



Au cours des entretiens menés dans le cadre de cette étude, la cybermenace la plus souvent citée était l'espionnage et les actes de sabotage commandités par des Etats.

Répondants considérant que leurs pouvoirs publics sont *capables* de prévenir ou de décourager des cyberattaques



« Aujourd'hui, la résilience est la priorité numéro un, mais qu'en est-il de l'espionnage ? », se demande l'adjoint d'un sénateur américain. « Il s'agit d'un problème essentiel que nous devons résoudre ; une attaque par déni de service n'est pas le souci majeur. » De nombreux experts en cybersécurité s'inquiètent de la surveillance du réseau de distribution électrique américain par d'autres nations. Un rapport confidentiel publié en 2008 par le DSB (Defense Science Board) avait également mis au jour la vulnérabilité du réseau de distribution d'électricité américain aux cyberattaques. Par ailleurs, des hauts responsables militaires ont déclaré publiquement que des opposants potentiels se livraient à une cyber-reconnaissance des compagnies électriques reposant sur des infrastructures critiques en vue de planifier une attaque.

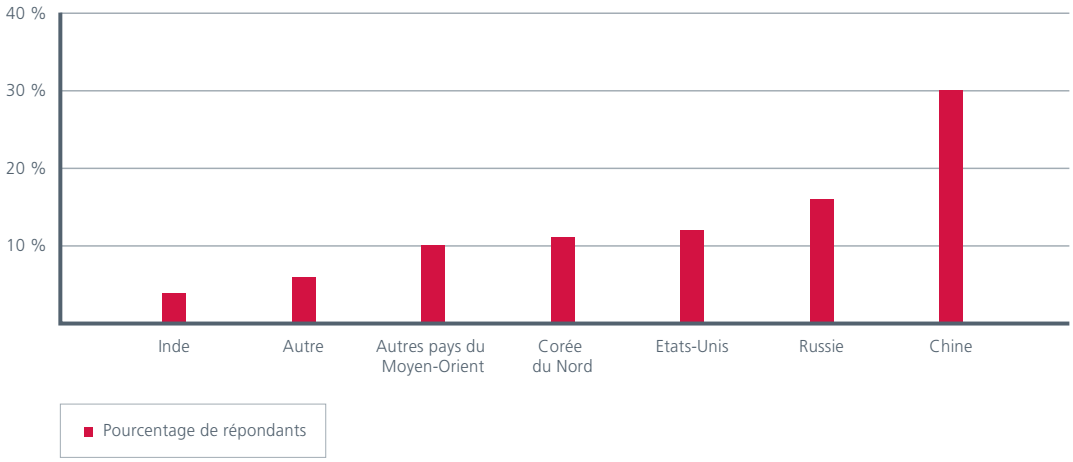
L'année dernière et cette année encore, nous avons demandé aux dirigeants informatiques des secteurs d'infrastructures critiques s'ils pensaient avoir été infiltrés ou attaqués par des Etats et, si c'était le cas, quels pays représentaient la plus grande menace à cet égard. En 2009 et en 2010, le nombre d'attaques perçues comme étant instiguées par des nations est resté stable et élevé, trois cinquièmes des cadres dirigeants déclarant que des pays étrangers avaient été impliqués dans des attaques réseau contre leur infrastructure critique nationale.

Le seul changement par rapport à l'année dernière est le pays considéré comme la plus grande menace. En 2009, les Etats-Unis venaient en tête, suivis de près par la Chine. Tous deux étaient considérés comme une menace par un tiers des dirigeants convaincus que leur secteur avait été victime d'une attaque.

En revanche, le pourcentage de répondants considérant les Etats-Unis comme une menace a fortement baissé, de 36 à 12 %. La Russie (16 %), la Corée du Nord (11 %) et l'Inde (4 %) occupent un rang assez élevé dans ce classement, dans la mesure où les responsables informatiques du secteur commencent à réaliser l'ampleur de la prolifération des technologies d'attaque numérique.

Les variations constatées dans les sources de menaces restent assez homogènes au sein d'une région géographique donnée. Assez logiquement, les répondants de la région Asie-Pacifique considèrent la Russie, la Corée du Nord et les Etats-Unis comme les principales sources de menaces. Au sein de ce groupe, près de deux tiers des répondants japonais citent la Corée du Nord comme principale source de cybermenaces.

Quel pays considérez-vous comme la plus grande menace en termes d'attaques réseau lancées contre votre pays ou secteur ?



Les variations constatées dans les sources de menaces restent assez homogènes au sein d'une région géographique donnée.

Dans le cas de l'Australie, 40 % des répondants s'inquiètent principalement de la menace posée par la Russie. Le seul pays à diverger de cette perception à caractère régional est naturellement la Chine, dont les trois quarts des répondants craignent surtout les Etats-Unis.

Les résultats des autres régions sont également liés aux points de vue régionaux. Deux tiers des personnes interrogées dans les Emirats arabes unis craignent surtout les autres pays du Moyen-Orient. Les répondants européens s'inquiètent principalement de la Chine, de la Russie, de la Corée du Nord et des Etats-Unis tandis que l'Inde perçoit la Russie comme la plus grande menace. Il est intéressant de noter que seuls 14 % des répondants indiens considèrent la Chine comme une menace alors qu'un tiers craint le Royaume-Uni.

Dans l'hémisphère ouest, les Etats-Unis s'inquiètent principalement de la Chine. Les répondants latino-américains avancent la liste la plus variée de sources de menaces, même si trois quarts des personnes interrogées au Brésil et près de la moitié au Mexique voient la Chine ou la Russie comme les principaux fauteurs de troubles. Cette opinion correspond à l'un des taux les plus élevés d'incidents d'intrusion réseau déclarés. Dans l'ensemble, le Mexique et le Brésil représentent deux des pays les plus vulnérables de l'enquête et expriment de sérieux doutes quant à la capacité de leur pays à réagir face à tous les types d'incidents informatiques, tout particulièrement les infiltrations furtives et les attaques par déni de service distribué.

Recommandations

L'apparition de Stuxnet contraint les entreprises reposant sur des infrastructures critiques à prendre conscience des changements intervenus dans le paysage des menaces. Elles doivent focaliser leur attention non seulement sur les risques que posent les attaques par déni de service, mais aussi sur des menaces plus sophistiquées, notamment les infiltrations furtives de pirates commanditées par des Etats ou perpétrées par des cyberextorqueurs. Comme le montrent nos recherches, le secteur des infrastructures critiques met du temps à réagir face à cette évolution. Pour relever les défis posés par ces nouvelles menaces, les stratégies de protection des infrastructures critiques doivent actualiser les mesures de réponses aux menaces et inclure notamment les éléments suivants :

- Amélioration des mesures d'authentification en abandonnant les mots de passe au profit des jetons et des identifiants biométriques
- Meilleure protection des systèmes réseau, qui doit inclure des technologies de chiffrement et la surveillance des activités réseau afin de détecter les anomalies au niveau des activités et des rôles
- Supervision accrue de l'accès aux systèmes de contrôle industriels, y compris leur mode d'accès à Internet, par une surveillance et une gestion active des connexions Internet, des équipements mobiles et des supports amovibles
- Collaboration étroite avec les pouvoirs publics (Le type de partenariat variera selon les pays et pourra aller du simple encouragement aux mesures obligatoires, mais la nature des nouvelles menaces encourues par le secteur exige une participation des autorités.)

Conclusion

En ce qui concerne la cybersécurité des réseaux de distribution électrique et autres services publics essentiels qui dépendent des technologies de l'information et des systèmes de contrôle industriels, les nouvelles ne sont globalement pas réjouissantes. Les améliorations restent modestes et ne font pas le poids face à la menace. Ces secteurs ont beau être victimes d'attaques par déni de service distribué, ils souffrent encore plus de ce que l'on pourrait qualifier d'un « déni d'attaques » généralisé. Très peu de sociétés relèvent le défi posé par les attaques potentielles et les infiltrations commanditées par des Etats. C'est tout particulièrement le cas de l'hémisphère ouest, de l'Inde et de l'Europe. En Asie de l'Est, les organismes de réglementation publics semblent mener une campagne plus concertée pour améliorer sensiblement la sécurité.

Le déni est une stratégie inconcevable à long terme. Certes, l'efficacité des audits et réglementations similaires dans l'amélioration de la sécurité reste à prouver, mais nous ne pouvons plus prétendre que rien n'a changé dans le monde de la cybersécurité.

D'autres observateurs estiment même qu'une action plus décisive s'impose. « L'application réglementée des outils de sécurité existants ne résoudra vraisemblablement pas le problème », a déclaré Jim Woolsey. « La vraie réponse se trouve dans les nouvelles technologies et la production distribuée. Toutes les initiatives prises pour encourager l'innovation et la production distribuée constituent un pas dans la bonne direction. » Bien qu'il soit difficile de savoir si Jim Woolsey a raison de croire que la résolution du problème passe par l'adoption de nouvelles technologies, ou si une réglementation plus adaptée permettra d'améliorer la sécurité, cette étude montre qu'il faudra encore du temps avant que la sécurité s'améliore. Le temps sans doute qu'une population mal préparée subisse une cyberattaque contre ses secteurs de l'énergie, du pétrole et du gaz ou de l'eau.

Remerciements

L'enquête a été réalisée en novembre 2010 par Vanson Bourne. Le bureau d'études a interrogé des répondants de 14 pays : l'Allemagne, l'Australie, le Brésil, la Chine, les Emirats arabes unis, l'Espagne, les Etats-Unis, la France, l'Inde, l'Italie, le Japon, le Mexique, le Royaume-Uni et la Russie.

Les auteurs remercient toutes les personnes qui ont contribué à la réalisation de ce rapport pour leurs avis éclairés.

Notes

1 Il s'agit des systèmes qui contrôlent les réseaux de distribution d'électricité, les raffineries, les réseaux de distribution d'eau, les stations d'épuration et autres processus industriels.

2 Duclos, Susan. « Cyber Attacks Black Out Cities Outside the U.S. — Cyber Terrorism » (Des cyberattaques plongent des villes dans le noir — Cyberterrorisme), *Digital Journal*, 19 janvier 2008. *http://www.digitaljournal.com/article/249107?tp=1*

3 *Cyber War: Sabotaging the System (Cyberguerre : sabotage du système).* Prod. Graham Messick. CBS : 60 Minutes, 2009. 8 novembre 2009. Web. 3 janvier 2011. *http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml*. Harris, Shane. « Brazil to "60 Minutes": It Wasn't A Hacker » (Le Brésil répond à l'émission 60 Minutes : ce n'était pas un acte de piratage informatique). *The Atlantic*. 10 novembre 2009. Web. 3 janvier 2011. *http://www.theatlantic.com/politics/archive/2009/11/brazil-to-60-minutes-it-wasnt-a-hacker/29934/*

4 SANS NewsBites, Volume X, numéro 5, 18 janvier 2008. *http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5&rss=Y*

5 William J. Broad, John Markoff et David E. Sanger. « Israeli Test on Worm Called Crucial in Iran Nuclear Delay » (Tests israéliens sur un ver jugés essentiels pour retarder le programme nucléaire iranien), *The New York Times*, 15 janvier 2011. *http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html*

6 Kaplan, Stan Mark. *Electric Power Transmission: Background and Policy Issues (Distribution d'électricité : contexte et problèmes liés à la politique),* Congressional Research Service (CRS) Reports and Issue Briefs, Washington, Congressional Research Service, 2009.

7 Michael Giberson, Lynne Kiesling. « Analyzing the Blackout Report's Recommendations: Alternatives for a Flexible, Dynamic Grid » (Analyse des recommandations du rapport sur la panne générale d'électricité : solutions alternatives pour un réseau de distribution souple et dynamique), *Electricity Journal* 17.6 (2004) : 51–59.

8 U.S.-Canada Power System Outage Task Force, « Context and Preconditions for the Blackout: The Northeastern Power Grid Before the Blackout Began » (Contexte et conditions préalables à la panne généralisée : réseau de distribution du Nord-Est avant le début du *blackout*), *August 14th Blackout: Causes and Recommendations* (Panne d'électricité du 14 août : causes et recommandations), p. 53. *https://reports.energy.gov/B-F-Web-Part2.pdf*

9 L'Australie et l'Italie se partagent la cinquième place avec 40 % de répondants admettant des incidents liés à Stuxnet. En comparaison, 100 % des répondants indiens, 59 % des répondants allemands et français, 45 % de répondants espagnols et 44 % de répondants chinois ont déclaré avoir été confrontés à une infiltration de réseau par le ver Stuxnet.

10 Mylrea, Michael. « Brazil's Next Battlefield: Cyberspace » (Le cyberespace, prochain champ de bataille du Brésil), The Fletcher School, 15 novembre 2009. *http://fletcher.tufts.edu/news/2009/11/opeds/Mylrea-Nov15.shtml*

11 ABI Research : *http://www.abiresearch.com/research/1005219.* Cité ici : *http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100708005824&newsLang=en*

12 Peeples, Doug. « Anti-Meter Fever Strikes Australia Too » (Le mouvement de protestation contre le déploiement de compteurs intelligents s'étend à l'Australie), *Smart Grid News.com*, 24 février 2010. *http://www.smartgridnews.com/artman/publish/Technologies_Metering_News/Anti-Meter-Fever-Strikes-Australia-Too-1926.html*

13 ABC Radio National, « Electric shocks » (Electrochocs), 5 novembre 2006. *http://www.abc.net.au/rn/backgroundbriefing/stories/2006/1777438.htm*

14 Nous avons posé deux questions distinctes sur l'adoption de mesures de sécurité pour les réseaux informatiques critiques et pour les systèmes de contrôle industriels/SCADA, mais les tendances présentaient une telle similitude que nous n'avons abordé ici que les mesures de sécurité des réseaux critiques.

15 Catégories mentionnées : « par une participation à des associations de partage d'informations sectorielles» ; « par des commentaires publics sur les modifications apportées aux réglementations/législations » ; « par un lobbying actif au sein de groupes de l'industrie concernant les réglementations/législations » ; « par une consultation via des organisations de partenariat entre le secteur public et privé ».

Les auteurs

Stewart Baker est membre invité du CSIS (Center for Strategic and International Studies) et associé au sein du cabinet d'avocats Steptoe & Johnson de Washington. De 2005 à 2009, il a été sous-secrétaire aux affaires politiques au sein du ministère américain de la Sécurité intérieure. Avant cela, il a été avocat-conseil de la commission Silverman-Robb, chargée d'enquêter sur les manquements des services de renseignements américains concernant les armes de destruction massive irakiennes. De 1992 à 1994, il a été avocat-conseil pour la NSA (National Security Agency).

Natalia Filipiak est gestionnaire de projets et chercheuse associée pour le programme Technology and Public Policy du CSI (Center for Strategic and International Studies). Elle est titulaire d'une maîtrise en relations internationales de la Johns Hopkins University School of Advanced International Studies.

Katrina Timlin est assistante en recherche pour le programme Technology and Public Policy du CSI (Center for Strategic and International Studies). Elle est titulaire d'une licence en affaires internationales de la George Washington University.

Le CSIS (Center for Strategic and International Studies) est un groupe de réflexion qui fournit des analyses stratégiques et des solutions politiques aux décideurs appartenant aux pouvoirs publics, aux institutions internationales, au secteur privé et à la société civile. Organisation bipartite sans but lucratif basée à Washington, le CSIS réalise des recherches, des analyses et élabore des stratégies sur l'évolution future et l'anticipation des changements.

Pour plus d'informations sur le CSIS, visitez son site à l'adresse : www.csis.org.

McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC) est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. Elle fournit dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes, des réseaux et des équipements mobiles et permettent aux utilisateurs de se connecter à Internet, de surfer ou d'effectuer leurs achats en ligne en toute sécurité. Grâce au soutien de son système hors pair de renseignements sur les menaces, Global Threat Intelligence, McAfee crée des produits innovants au service des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable.

Pour plus d'informations, visitez notre site à l'adresse : www.mcafee.com/fr.

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

21900rpt_cip_0311