La convergence, moteur d'occasions et de risques

Protéger les technologies opérationnelles contre les cyberattaques

CGI

La force de l'engagement[MD]

Les sociétés de services publics subissent des pressions inégalées les incitant à protéger leurs technologies opérationnelles (TO) et leurs technologies de l'information (TI). Ces deux types de systèmes appellent toutefois des mesures de sécurité considérablement différentes. Le transfert des processus et des outils de cybersécurité d'un environnement à l'autre n'est donc pas viable. La présente étude technique examine les facteurs récents ayant une incidence sur la sécurité des services publics tout en offrant une approche ciblée pour gérer les réseaux et les établissements de TO.

Introduction

Les systèmes de contrôle industriels qui assurent l'alimentation continue en électricité, en eau et en gaz, appelés technologies opérationnelles (TO), sont de plus en plus exposés aux cyberattaques. Puisque l'énergie et l'eau sont indispensables à la société, les risques potentiels pour cette infrastructure essentielle représentent également un risque pour la collectivité en général.

Dans leurs efforts continus pour obtenir une efficience et une efficacité accrues, les fournisseurs de services publics ajoutent sans cesse de nouvelles connexions Internet à leurs réseaux de TO. Cette convergence positive entraîne une hausse de performance et une rationalisation des méthodes de travail en fournissant des capacités comme la surveillance hors site et la maintenance à distance. Une grande partie de l'équipement de TO remonte cependant aux années 1980 et 1990, ce qui signifie qu'il n'a pas été conçu pour une société connectée et, par conséquent, qu'il dispose de peu de mesures de sécurité.

En l'absence d'une planification rigoureuse et d'une surveillance efficace, des milliers d'établissements de TO physiques sont exposés aux réseaux de TI, ce qui pose un défi de taille en matière de sécurité pour les sociétés de services publics. À ces difficultés s'ajoute le nombre croissant de parties malveillantes prêtes à exploiter les vulnérabilités dans le but de perturber la vie des citoyens. Par exemple, le vol de renseignements et de plans de centrales nucléaires et de sociétés de distribution d'eau peut mettre en péril des collectivités entières en causant une panne de courant à grande échelle, une altération du réseau ou la contamination de l'eau.

On observe en outre une structure réglementaire de plus en plus stricte en matière de signalement des atteintes à la sécurité, une évolution de l'Internet des objets (IoT) et des citoyens qui se font entendre et qui sont prêts à réagir à une situation problématique.

Ainsi, les exploitants de sociétés de services publics subissent des pressions inégalées les incitant à protéger leurs systèmes de TO et de TI. Ces deux types de systèmes exigent cependant des mesures de sécurité considérablement différentes. Le transfert des processus et des outils de cybersécurité directement des TI vers les TO n'est donc pas viable.

Dans un contexte où de nouveaux adversaires mènent des cyberattaques de plus en plus importantes et complexes, les fournisseurs de services publics doivent bien comprendre les risques qui pèsent sur eux. Comme il est pratiquement impossible de corriger toutes les vulnérabilités potentielles en même temps, les mesures d'atténuation doivent être classées en ordre de priorité en fonction des répercussions possibles.

Cette étude technique examinera les changements énoncés et proposera un processus que les hauts dirigeants peuvent suivre pour sécuriser les flux de services aux clients essentiels et protéger à la fois leurs employés et les citoyens en général.

Le portrait actuel

DES ATTAQUES SUR LES RÉSEAUX ET DES COLLECTIVITÉS EXPOSÉES À DES RISQUES

L'interconnectivité crée un monde extrêmement vulnérable, particulièrement sur le plan des TO. Par conséquent, les fournisseurs de services publics commencent à diriger leur attention et leurs ressources vers la sécurité de ces systèmes.

Actuellement, les menaces informatiques proviennent de plusieurs sources : la communauté de pirates informatiques, les membres du personnel qui fournissent un accès non autorisé à des parties externes – que ce soit intentionnel (sabotage) ou non (hameçonnage) – et les groupes coordonnés qui reçoivent un important financement et dont le but est de causer un dommage aux gens ou aux propriétés.

L'événement qui a sonné l'alarme pour les sociétés de services publics est l'attaque menée par le logiciel malveillant Stuxnet envers les centrales nucléaires iraniennes en 2008. Stuxnet a prouvé que les cyberattaques avaient le pouvoir de causer des dommages importants.

Celle-ci perturbé un cinquième des installations iraniennes et aurait retardé de deux ans les plans

D'ici à 2020, les dépenses de sécurité des TO doubleront en raison du nombre croissant d'attaques envers les infrastructures industrielles essentielles et de la réglementation visant à les contrer.

Guide de marché de la sécurité des technologies opérationnelles de Gartner, mai 2016.

nucléaires du pays, selon certains. Depuis cet événement hautement médiatisé, d'autres attaques ont émergé et leur fréquence a augmenté.

Bien que les fournisseurs d'électricité et même les États soient ciblés par ces offensives, les répercussions sur les citoyens ordinaires peuvent être considérables.

En 2015, quelque 230 000 résidents ukrainiens ont subi une panne de courant de 6 heures lorsque 60 postes électriques ont été déconnectés en raison d'une attaque de logiciel malveillant.

Selon l'agence de presse Reuters, un programme semblable a été détecté dans les réseaux d'au moins deux autres sociétés de services publics.

Ce type d'attaques a en effet le potentiel de poser un risque important pour des collectivités entières. En 2016, des pirates infiltrés ayant lancé une attaque contre une usine de traitement d'eau en Asie-Pacifique ont pu non seulement accéder aux dossiers de 2,5 millions de clients, mais aussi au système qui contrôle les produits chimiques utilisés pour traiter l'eau potable.

Heureusement, la menace a été détectée et l'attaque a pu être repoussée avant de causer des dommages.

UN SECTEUR HAUTEMENT CIBLÉ

Le secteur de l'énergie est une implorante cible des cyberattaques. Selon un sondage sur les défis de cybersécurité dans le secteur de l'énergie, mené en 2016 par Dimensional Research pour le compte de Tripwire, non seulement les attaques sont en hausse, mais elles le sont nettement plus dans le secteur de l'énergie qu'ailleurs.[1]

Même lorsque le réseau de TI d'une société de services publics dispose d'un système de cybersécurité sophistiqué, cette rigueur n'est pas nécessairement appliquée aux connexions au réseau de TO. Les éléments malveillants ont alors le champ libre pour s'infiltrer.

D'ailleurs, certains développeurs de logiciels malveillants semblent cibler les TO puisqu'elles n'ont pas été conçues pour être protégées sur Internet.

ÉVOLUTION DES ASPECTS JURIDIQUES DU SIGNALEMENT DES ATTEINTES À LA SÉCURITÉ

RLes exigences réglementaires sont également une source de défis pour les sociétés de services publics. Parmi les répondants du sondage CGI Global 1000 issus des services publics, 70 % ont indiqué que les lois relatives à la confidentialité et à la protection des données ont une incidence importante ou très importante sur leurs activités.

Partout sur la planète, on adopte de plus en plus de lois obligeant les fournisseurs de services publics à signaler les atteintes à la sécurité et auxquelles tout manquement a une incidence négative sur leurs finances et leur réputation.

- Aux États-Unis, la North American Electric Reliability Corporation (NERC) a mis en place des normes de fiabilité, y compris les normes de protection obligatoire des infrastructures essentielles (normes CIP) dont l'objectif est d'assurer la sécurité des actifs de TI vitales au fonctionnement fiable du réseau électrique. La norme CIP-008 englobe la détection, la classification, la gestion et le signalement des incidents de cybersécurité en lien avec les actifs de TI essentiels.[2]
- Au Canada, la Loi sur la protection des renseignements personnels numériques de 2015[3] a créé de nouvelles obligations pour les entreprises qui sont aux prises avec une atteinte à la sécurité touchant aux renseignements personnels. De plus, chaque province dispose d'une loi en matière de confidentialité et, dans la plupart des cas, un commissaire à la protection de la vie privée.[4]
- En Europe, la directive sur la sécurité des réseaux et de l'information (SRI), qui soumet les fournisseurs nationaux d'infrastructures essentielles à l'obligation de signaler les atteintes à la sécurité, en est actuellement aux dernières étapes de ratification.
- Certains États doivent encore ratifier le texte législatif, mais il ne fait aucun doute que les sociétés de services publics seront tenues responsables des failles dans leurs mesures de sécurité. Le Règlement général sur la protection des données (RGPD)[5] de l'UE, qui impose aux entreprises de signaler toute violation des données personnelles sur les clients, est en vigueur depuis janvier 2016 aux Pays-Bas.
- Un fournisseur de services publics a récemment été la cible d'une atteinte à la protection des données (dans le domaine des TI), et il a dû signaler l'incident rapidement et avec exactitude en vertu du RGPD.

1. http://www.tripwire.com/company/research/tripwire-2016-energy-survey-attacks-on-the-rise/
2. http://www.nerc.com/files/CIP-008-4.pdf
3. https://openparliament.ca/bills/41-2/S-4/
4. Personal Information Protection and Electronic Documents Act (PIPEDA)
5. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Facteurs de convergence des réseaux de TO et de TI

Les tâches effectuées par les systèmes de TO et de TI étaient auparavant entièrement distinctes. Il n'était pas nécessaire de combiner ces réseaux puisqu'ils n'étaient pas associés aux mêmes activités. Par ailleurs, les priorités et l'infrastructure différaient d'un type de réseau à l'autre. Le besoin croissant de données, les avancées technologiques et l'évolution du cadre réglementaire ont toutefois entraîné un changement de paradigme.

Le secteur des services publics reconnaît la valeur de la convergence des TO et des TI. Éliminer les activités en vases clos créées par le personnel, les systèmes et les données permettra de simplifier le flux d'information en vue de soutenir le contrôle automatique du réseau distribué. De même, en combinant les TO et les TI à d'autres sources de données internes, les organisations deviendront véritablement agiles et proactives.

Grâce à la convergence, les données recueillies dans différents secteurs du réseau de TO pourront être analysées dans le réseau de TI et contribuer à prévoir les sommets et les creux en ce qui concerne la demande. Les centrales électriques qui ont dû réduire le nombre d'employés chargés de surveiller les actifs, le matériel et le service sur place en raison de pressions budgétaires peuvent tout de même fonctionner efficacement grâce à la connexion entre les réseaux de TO et de TI.

Le projet SHINE (SHodan INtelligence Extraction) a permis de découvrir que plus d'un million de systèmes de télésurveillance et d'acquisition de données (SCADA) sont connectés à Internet au moyen d'IP uniques, un nombre qui augmente de 2 000 à 8 000 par jour.

Rapport Cyber Security for SCADA Systems de Thales (automne 2013)

En résumé, la convergence des TO et des TI offre une panoplie de moyens d'améliorer l'offre et la demande.

RISQUES ÉMERGENTS LIÉS AUX TO

Chaque élément ajouté à un réseau de TO crée un nouveau risque pouvant être exploité, ce qui expose l'infrastructure, auparavant dissimulée, à des attaques potentielles.

Par exemple, de nombreuses sociétés de services publics utilisent maintenant des technologies de pointe qui intègrent des protocoles et du code leur permettant de se connecter au réseau de TI.

Dans ce type de situation, un réseau de TO pourrait accidentellement exposer le système à Internet.

Un autre risque réside dans l'absence de compétences internes en matière de cybersécurité. Il arrive que des services exploitant des génératrices diesel ou des centrales électriques n'aient pas d'architecte de sécurité attitré parce que leur attention se porte sur les activités plutôt que sur les TI. Il est alors possible que les concepteurs de systèmes ne soient pas conscients des vulnérabilités et des risques actuels et qu'ils utilisent des protocoles désuets ou des logiciels sans cryptage.

L'Internet des objets (IoT) est également une nouvelle source de risques. La surveillance des appareils, de leur connexion au nuage et de leur accès par les utilisateurs nécessite la mise en œuvre de mesures de protection et l'intégration à un cadre de sécurité global au sein de la société.

De plus, bon nombre de fournisseurs de services publics ont mis en place une main-d'œuvre mobile afin d'accroître la productivité des ingénieurs qui travaillent sur place. Par conséquent, les données de TO circulent librement dans les applications et les plateformes mobiles et de TI.

Il arrive parfois que les mesures de sécurité requises pour régler ces problèmes soient bien implantées. Parmi celles-ci, on retrouve notamment le profilage de données et les droits d'utilisateur. Dans d'autres cas, l'intégration des appareils patrimoniaux exige une évaluation rigoureuse des risques visant à vérifier que les éléments auparavant non connectés sont sécurisés.

Il est important de reconnaître que tandis que les violations visant les systèmes de TI entraînent des risques sur le plan des finances et de la réputation, celles visant les systèmes de TO représentent des risques opérationnels et de sécurité.

État de préparation actuel des sociétés de services publics

Dans quelle mesure les sociétés de services publics sont-elles préparées à atténuer les menaces à la sécurité? Selon les perspectives contenues dans l'analyse CGI Global 1000[6], issues de 1 000 entrevues en personne auprès de dirigeants des fonctions d'affaires et informatiques, la plupart des répondants du secteur des services publics considèrent être modérément préparés aux menaces à la sécurité et seulement 9 % se disent hautement préparés.

Plusieurs organisations ne possèdent pas les capacités avancées dont elles ont besoin pour contrer rapidement les menaces émergentes.

Il ne fait aucun doute que les sociétés de services publics subissent d'importantes pressions en raison des diverses priorités qui se font concurrence dans un contexte de restrictions budgétaires. Ces priorités comprennent la conformité réglementaire, le vieillissement de la main-d'œuvre et des infrastructures, le besoin de devenir des organisations numériques davantage axées sur le client et, particulièrement en Europe, la concurrence accrue.

Les répondants de l'analyse CGI Global 1000 issus du secteur des services publics considèrent l'obligation de se conformer aux exigences continuelles en matière de risque et de conformité comme le principal obstacle à l'évolution et au financement de leurs cyberprogrammes. En outre, 67 % ont indiqué que les initiatives se rapportant à la transformation numérique font concurrence aux programmes de sécurité sur le plan budgétaire.

« Le pire scénario possible est une attaque contre une infrastructure essentielle, ce à quoi les organisations sont mal préparées. »

Dr. Larry Ponemon, founder of the Ponemon Institute

6. L'analyse CGI Global 1000 présente les perspectives et le point de vue de CGI concernant les sujets stratégiques qui se sont dégagés d'entrevues en profondeur. Celles-ci ont été réalisées par les conseillers de CGI auprès de 1 000 dirigeants des fonctions d'affaires et des TI dans 10 secteurs d'activité et 20 pays entre janvier et avril 2016.

Mesures recommandées

Qu'est-ce que les sociétés de services publics peuvent faire pour améliorer leur posture de sécurité des TO et des TI? Bien qu'elles dépassent les attentes en matière de conformité, elles doivent faire plus afin d'assurer une cybersécurité intégrée à l'ensemble de leurs activités. L'approche fragmentée fondée sur les activités courantes n'est plus viable, particulièrement pour les systèmes essentiels. Pour atteindre le niveau élevé de préparation nécessaire afin d'atténuer à la fois les menaces internes et externes, les organisations doivent appliquer une approche qui englobe le personnel, les processus, les technologies et la gouvernance.

PERSONNEL

1. Créer une culture de vigilance

Les personnes les plus susceptibles de perturber un service public sont celles qui se trouvent dans la centrale. En effet, la majorité des atteintes à la sécurité proviennent de l'organisation même. Il est donc primordial que les organisations tiennent compte du personnel sur place lorsqu'elles augmentent leurs mesures de sécurité.
Les failles de sécurité peuvent être corrigées par la mise en place d'un processus de validation et par le contrôle des droits d'accès de tous les employés, principalement en ce qui concerne l'accès au modèle d'information ou aux dessins techniques de la centrale.

En plus des employés, les parties ayant occasionnellement accès aux lieux, comme les employés contractuels ou externes, doivent être soumises à cette supervision. De même, les invités et les personnes externes à l'organisation qui effectuent des réparations de machinerie doivent faire l'objet d'une surveillance étroite.

Un changement de mentalité est également nécessaire. À des fins d'atténuation des menaces internes, tous les employés doivent envisager les actions quotidiennes posées par leurs collègues, aussi normales semblent-elles, en ayant à l'esprit la possibilité d'une menace. Par exemple, lorsqu'un membre du personnel est aperçu alors qu'il accède à un système auquel il ne touche habituellement pas, il doit être acceptable de lui demander ce qu'il fait et pour quelle raison.

Il est crucial de mettre en place des protocoles rigoureux d'identification et de gestion des accès afin que les employés aient uniquement accès aux renseignements et aux lieux physiques dont ils ont besoin pour remplir leurs responsabilités.
Cette sensibilisation doit être intégrée à la culture de l'entreprise.

2 .Améliorer la formation

Bien que renforcer le premier point de contrôle soit un impératif, 68 % des leaders du secteur des services publics interrogés dans le cadre de l'analyse CGI Global 1000 considèrent la mise en place d'une formation en sécurité efficace comme un défi.

La formation des employés doit être axée sur la sécurité et la protection de même que sur les compromis qui s'y rattachent. Tous les employés qui sont appelés à prendre des décisions en matière de sécurité et de protection doivent connaître les points de contact entre les TO et les TI ainsi que les mesures connexes requises.

Les membres du personnel autorisés à accéder aux données de TO et de TI à distance ou d'utiliser des appareils sur le terrain doivent suivre une formation pointue en sécurité afin de réduire les risques d'une menace interne. Parfois, ceux-ci ne saisissent pas l'ampleur des conséquences que peut avoir l'ajout d'une imprimante Wi-Fi, par exemple, ou encore la création d'un lien entre deux systèmes visant à obtenir des données en apparence non essentielles aux fins d'un rapport.

Souvent, puisqu'ils ne travaillent pas dans le domaine de la sécurité, ils ne comprennent pas que chaque porte ouverte doit faire l'objet d'une protection complète.

Les organisations doivent intégrer la protection des TO aux programmes existants afin de se protéger contre les menaces pouvant avoir des répercussions sur la sécurité. Par exemple, une clé USB que transporte un employé pourrait être utilisée pour perturber la centrale ou le réseau électrique.
Près de 40 % des dirigeants des TO et des TI interrogés dans le cadre de l'analyse CGI Global 1000 ont indiqué avoir de la difficulté à communiquer efficacement à leurs cadres supérieurs et aux administrateurs l'urgence relative aux menaces croissantes. Aussi bien les dirigeants que leurs subordonnés doivent être au fait des menaces à la sécurité des TI et du risque associé aux connexions établies entre les TO et le réseau de l'entreprise.
Même s'il peut être difficile de propulser la sécurité au rang des préoccupations des cadres et des employés, les hauts dirigeants des TI doivent continuer à en

faire la promotion en partageant de l'information et en offrant une formation continue à tous les échelons de l'organisation.

PROCESSUS

1. Établir une distinction claire entre la protection des TI et des TO en accordant la priorité à la sécurité

Lorsque des mesures de protection des TI sont appliquées à un environnement de TO, des incidents et des problèmes de sécurité sont inévitables. Par exemple, il peut arriver qu'une décision fondée sur les TI exige qu'une porte soit verrouillée à des fins de confidentialité, tandis qu'une décision prise en fonction des TO vise à garantir que les gens puissent fuir en situation d'urgence.

Il n'est pas viable pour une organisation de transposer des directives de protection des TI à des systèmes de TO. En effet, il est impossible de mettre en œuvre les mêmes mesures et contrôles de TI et d'exécuter les mêmes processus d'un environnement à l'autre, et le vocabulaire utilisé par ceux qui soutiennent ces environnements n'est pas harmonisé. L'ordre de priorité des facteurs de TI, à savoir la confidentialité, l'intégrité et l'accessibilité, est inversé dans l'environnement de TO pour devenir l'accessibilité, l'intégrité et la confidentialité. Les sociétés de services publics doivent mettre les facteurs de hiérarchisation au cœur de la série de normes ISA/CEI 62443 sur la protection des systèmes d'automatisation et de contrôle industriels.

La centrale ou le réseau de distribution d'électricité, par exemple, sont préoccupés par l'accessibilité : « Pouvons-nous contrôler le processus physique qui permet de produire ou de distribuer l'électricité et l'eau, ou encore de générer de l'électricité? ». Même dans le secteur manufacturier (la production d'acier, par exemple), la sécurité de l'usine est plus importante que le processus en tant que tel, bien que celui-ci soit évidemment un secret commercial.

2. Éliminer les vulnérabilités

Dans un souci de sécurité, les sociétés de services publics sont également tenues de s'assurer qu'il existe une séparation suffisante entre les technologies et les utilisateurs non autorisés. Les processus mis en place doivent contrôler les flux d'information, qu'ils soient automatiques ou manuels.
Ainsi, que le téléversement des données soit automatisé ou qu'un membre du personnel ait à se connecter pour le faire, chaque étape du processus doit être soigneusement documentée.
Dans le cadre des opérations de maintenance, un délai doit être convenu pour l'accès au système de TO, au terme duquel l'accès est automatiquement retiré.

De cette façon, un employé de maintenance ne peut pas ouvrir l'accès à des renseignements confidentiels en oubliant de réinitialiser correctement un système.

TECHNOLOGIES

1. Se préparer au pire scénario

En utilisant une approche proactive tirant parti des renseignements sur les menaces, les organisations sont en mesure d'en savoir plus sur les atteintes à la sécurité qui se sont produites récemment dans le secteur des services publics ou dans un secteur connexe en vue de se préparer à une menace semblable.

Lorsqu'une société de services publics signale une attaque de leurs systèmes de contrôle ayant entraîné un arrêt du service, les autres ont tout à gagner à prendre des précautions pour éviter qu'un incident du même type se produise dans leurs propres systèmes ainsi qu'à tester les mises à jour dans des conditions similaires.

2. Créer des redondances

Les sociétés de services publics sont aux prises avec des défis uniques en matière de protection des données. Elles ne peuvent tout simplement pas interrompre complètement leurs TO pour effectuer la maintenance ou apporter des mises à jour et des correctifs aux logiciels, comme c'est possible de le faire dans un environnement exclusivement fondé sur les TI. Comme le flux ne peut être suspendu, il est essentiel de concevoir une solution visant à endiguer la menace et à la tenir à l'écart jusqu'à ce qu'il soit possible de prendre des mesures complètes.
Dans un système conçu pour prendre en charge les redondances, chaque composante essentielle possède un double pouvant être mis hors ligne aux fins de mise à jour sans interrompre le service.

Il est également possible de permuter les éléments des réseaux redondants pour veiller à ce que l'eau ou l'électricité continue d'être distribuée pendant que des correctifs sont apportés aux appareils, puis de les permuter de nouveau lorsque le processus est terminé.

3. Établir des priorités

Les sociétés de services publics doivent déterminer le risque le plus important pour leurs processus principaux (par exemple, la production d'électricité, le

transport de gaz ou le traitement et le transport d'eau) et veiller à ce que tous les employés affectés à la protection et à la sécurité soient sur la même longueur d'onde et utilisent la même terminologie. Les normes CEI-62264 et 62443 peuvent être utiles à cette fin.

Ces organisations auraient également avantage à repérer les éléments qui sont reliés aux actifs les plus précieux et ceux qui sont le plus vulnérables, puis à les sécuriser en faisant appel à la segmentation.
En matière de sécurité des TO et des TI, une approche multiniveaux est souvent la meilleure défense. Par exemple, il se peut qu'à la fin de la liste des mesures de protection figurent les mesures adéquates de cryptage et de surveillance des anomalies.

Par contre, la connectivité peut être priorisée afin d'assurer le cryptage approprié des communications et la mise à jour des diagnostics.
Dans le cadre de la protection du nuage, cela pourrait se traduire par la mise en place du bon type de systèmes de sécurité d'entreprise. Pour ce qui est de l'Internet des objets, l'organisation pourrait opter pour une approche progressive fondée sur des architectures existantes de protection des TI.
Il est ensuite possible d'utiliser cette base comme tremplin pour concevoir des solutions vitales de plus en plus complexes en y ajoutant des protocoles et des méthodologies, et ce, sans entraver les principes de sécurité déjà en place.

4. Surveiller et tester

Pour détecter les menaces et prévenir les attaques, les systèmes de TO et d'entreprise doivent faire l'objet d'une surveillance fondée sur des paramètres balisant un comportement considéré comme normal. Aussi minime soit l'écart, une enquête doit être lancée lorsqu'un comportement excède les paramètres. Les systèmes de contrôle industriels ont la capacité de repérer une anomalie par rapport au comportement quotidien et d'envoyer une alerte afin que des mesures soient prises.

Ainsi, si un terminal à distance commence subitement à communiquer avec un appareil d'un autre poste électrique ou que le volume de données générées par un appareil électronique connaît une hausse soudaine, il faut se demander si la situation s'est produite parce que le système a été piraté ou en raison d'un défaut dans l'environnement de TO.
Un programme de sécurité efficace comporte en outre un volet de tests continus. L'équipe de gouvernance a plusieurs responsabilités importantes, y compris celle de veiller à ce que le cadre de sécurité soit testé régulièrement par rapport à différents scénarios. Ces tests doivent être menés dans un environnement ouvert où le blâme n'a pas sa place et dont la priorité consiste à déterminer comment s'améliorer plutôt qu'à trouver le coupable. Il est possible de tirer des leçons de chaque exercice et de les partager au sein des divers services et, au besoin, auprès d'autres sociétés de services publics en vue de bâtir une base de connaissances collective.

GOUVERNANCE

1. Faire appel aux bonnes personnes

Dans le cadre de l'examen des politiques et des processus de cybersécurité, il est important de reconnaître que le réseau de TO ne peut pas être envisagé seul, mais plutôt aux côtés du réseau de TI. Les parties malveillantes peuvent très bien réussir à infiltrer le système grâce à la tablette d'un ingénieur ou à la liaison de données vers un système d'information de gestion, plutôt qu'à l'aide d'un appareil électronique destiné à surveiller le réseau de TO.

Pour cette raison, la responsabilité de cybersécurité ne se limite pas aux TO ou aux TI. Elle requiert le soutien du conseil d'administration et chaque partie prenante doit être représentée au sein de l'équipe de gouvernance.

Évidemment, les responsables des TO et des TI doivent figurer parmi les partenaires, tout comme les ressources humaines, les services juridiques, les divisions commerciales et les équipes de chaîne d'approvisionnement, afin de favoriser la création d'une culture de responsabilité collective en vue de prévenir les atteintes à la sécurité.
Pour vérifier qu'une gouvernance adéquate est en place, les sociétés de services publics doivent être en mesure de répondre à la question suivante : « Qui est responsable de la cybersécurité au sein de ce service, et cette personne a-t-elle les pouvoirs nécessaires pour agir rapidement lorsqu'un problème est détecté? »

2. Déterminer ce qui relève des TO et des TI

L'Internet des objets offre des possibilités qui brouillent les frontières entre les TO et les TI. Il est donc crucial de tenir compte des TO dans son approche des systèmes qui gèrent des données en temps réel et envoient des alertes aux clients ou à l'équipement sur le terrain, et de poser des questions comme « Ce système aura-t-il une incidence sur le processus physique que nous exécutons? » et « Qu'arriverait-il si le système connaissait une défaillance ou commettait une erreur? ». Les sociétés de services publics peuvent tirer parti de ces renseignements pour concevoir ou modifier les systèmes et pour éviter qu'ils soient compromis.

Conclusion

Bien que les sociétés de services publics aient plusieurs priorités qui se disputent le budget de transformation et l'attention de l'organisation, il n'existe pas de plus grand risque pour elles et pour les citoyens qu'une cyberattaque de logiciel malveillant à grande échelle. La solution à ce problème est complexe et nécessite une profonde compréhension des risques allant de pair avec la convergence des TO et des TI. Sa réussite repose sur la mise en place de changements de culture et de comportement ainsi que sur l'amélioration du contrôle et de la surveillance des activités. Seule une approche qui englobe le personnel, les processus, les technologies et la gouvernance procure la meilleure défense contre les atteintes à la cybersécurité. De cette manière, les services essentiels continuent d'être offerts, et les employés comme les collectivités demeurent en sécurité.

CGI

cgi.com

À propos de CGI

Fondée en 1976, CGI est l'une des plus importantes entreprises de services en technologies de l'information (TI) et en gestion des processus d'affaires au monde et offre des services-conseils en management, ainsi que des services d'intégration de systèmes et de gestion déléguée de grande qualité. Grâce à son solide engagement à offrir des solutions et services novateurs, CGI affiche un bilan inégalé de 95 % de projets réalisés selon les échéances et budgets prévus. Nos équipes s'arriment aux stratégies d'affaires des clients afin d'obtenir des résultats probants sur toute la ligne.

CGI et les services publics – CGI propose des services et des solutions à l'ensemble du secteur des services publics, notamment dans les domaines de l'électricité, des activités de gaz naturel en aval et de la gestion de l'eau et des déchets. Nous possédons une vaste expérience des marchés réglementés et non réglementés et nous avons tissé, au fil du temps, des relations d'affaires durables avec les plus importantes sociétés de services publics au monde. Cette collaboration de longue date avec le secteur des services publics nous permet de fournir à nos clients des technologies novatrices répondant à leurs exigences actuelles et futures et leur assurant croissance et succès à long terme.

CGI et la cybersécurité – Chez CGI, la sécurité fait partie intégrante de tout ce que nous faisons. Nous adoptons une approche axée sur les activités opérationnelles pour tous les volets de la sécurité, notamment les audits, les exigences en matière de conformité, les politiques et l'architecture. Notre offre complète comprend des services-conseils et des services de formation, l'intégration et la mise en œuvre, ainsi que la gestion déléguée des services de sécurité. Grâce à notre réseau mondial de centres de gestion de la sécurité, nous disposons d'une vue complète des menaces dans tous les secteurs d'activité et marchés géographiques. Nos équipes d'experts en sécurité conçoivent et déploient constamment des solutions avancées en vue de maintenir une infrastructure de pointe. Notre expérience à l'échelle mondiale nous aide à prédire les nouvelles attaques et à nous défendre contre celles-ci, et nous mettons ces connaissances à profit pour accroître nos capacités de première ligne.

Pour en savoir davantage, visitez www.cgi.com ou écrivez-nous à info@cgi.com.

© 2016 GROUPE CGI INC.