Flash n° 5 – 5 juin 2013

Flash
ingérence économique

Ce « flash » de l'ingérence économique relate un fait dont une entreprise française a récemment été victime. Ayant vocation à illustrer la diversité des comportements offensifs susceptibles de viser les sociétés, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité au sein de votre entreprise.

Vous comprendrez que par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier l'entreprise visée.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de nous écrire à l'adresse :
securite-economique@interieur.gouv.fr

Vigilance sur les outils de pilotage de sites industriels.

Récemment, un hacker a pu accéder à l'interface de gestion de la turbine d'un petit barrage hydraulique destiné à fournir de l'électricité à un site industriel. Particulièrement ingénieux, le hacker s'est introduit par la « porte informatique » de la société de maintenance dont l'accès lui est normalement réservé, grâce à un login et un mot de passe. Or, par méconnaissance ou absence de responsable sécurité informatique, ce mot de passe « constructeur » n'avait pas été modifié par l'exploitant, alors que sa connaissance est aisée via internet ou par la brochure du fabriquant.

Cette technique est fréquemment utilisée dans le domaine des télécoms, lorsque des individus profitent de la mauvaise configuration de l'autocommutateur d'une société, pour le piloter à distance et générer des appels surtaxés multiples vers l'étranger.

Si ce dernier exemple ne relève que de l'escroquerie classique, la multiplication des outils de pilotage de site industriels connectés à l'Internet fait naître une nouvelle vulnérabilité aux entreprises qui ne prendraient pas les mesures adéquates. Elle pourrait avoir un impact sur l'environnement (ouverture de vannes d'évacuation d'effluent), nuire à leurs relations commerciales (arrêt des installations le jour d'une visite importante) ou à leur image si la faille venait à être exploitée par un opposant.

Commentaire :

Trop de sociétés limitent la gestion des outils de pilotage industriel au seul responsable de la production. Or, ces outils informatiques sont de plus en plus interconnectés et peuvent devenir la cible d'attaquants aux motivations variées.

La DCRI préconise donc que leur gestion relève des compétences du responsable de la sécurité informatique qui aura à cœur d'appliquer la même politique de sécurité que pour le reste du matériel informatique (mise à jour des logiciels et des systèmes d'exploitation, anti-virus, gestion des mots de passe, exploitation des fichiers log d'accès, etc.).

Dans la situation évoquée supra, il est de la plus haute importance de veiller au bon paramétrage de l'accès à distance du logiciel :
1- changer les mots de passe prévus par défaut par le constructeur ;

2- recourir à des mots de passe robustes afin d'éviter les attaques classiques (attaques par dictionnaire ou par force brute) ;
3- si l'accès à distance n'est pas nécessaire, le désactiver ;
4- si l'accès à distance est nécessaire, une gradation de l'accès peut être mise en place en respectant quelques précautions : envisager de n'ouvrir l'accès que lorsqu'une opération de maintenance est prévue. Si cette solution n'est pas adoptée, en limiter l'accès grâce au mot de passe et à une politique de filtrage de l'adresse MAC et / ou de l'adresse IP des ordinateurs autorisés, afin que le système soit accessible exclusivement par des utilisateurs légitimes ;
5- maintenir les logiciels et autres serveurs à jour.

Pour plus de précisions sur les recommandations et configurations à mettre en place, nous vous recommandons le site Internet (www.ssi.gouv.fr) de l'agence nationale de la sécurité des systèmes informatique (ANSSI) qui a publié un guide relatif à « la cybersécurité des systèmes industriels ».

Plus globalement, cette politique doit être appliquée à l'ensemble des outils connectés, quelques soient leurs finalités, au risque d'ouvrir une brèche dans le dispositif de sécurité de l'entreprise : ordinateurs fixes ou nomades, outils communicants (smartphone et tablettes numériques), ainsi que les photocopieurs modernes dotés des fonctions scanner - fax qui stockent sur leurs disques durs l'ensemble des documents photocopiés.