Cyber terrorisme dans l'industrie, nouvelle menace ?

Le cyber terrorisme est un terme qui n'introduit encore que peu de crainte dans la population. Les implications possibles d'une cyber attaque sur l'économie d'un pays sont encore peu connues du grand public. Appliquée au secteur de l'industrie, la conscience d'un risque potentiel est encore plus lointaine. Est-il réellement possible d'infecter des systèmes de production dans le but de bloquer tout ou partie d'une économie ? Beaucoup de mesures de sécurité sont mises en place dans ce secteur pour limiter les capacités de nuisances de personnes non autorisées. Non seulement des mesures de sécurité physiques sont appliquées dans toute grande industrie, mais ses ordinateurs et son réseau sont aussi logiquement protégés. Mais qu'en est-il de la protection des systèmes de production ? L'idée selon laquelle tous les dispositifs avec une adresse IP comportent un risque de sécurité est de plus en plus répandue. Aurora et Stuxnet, les deux plus importantes attaques ciblées jamais identifiées jusqu'alors, montrent sur deux approches différentes qu'à l'avenir ceci pourrait bien se révéler exact.

Eddy Willems, Security Evangelist chez G Data Software est de nationalité belge. Dans le domaine de la sécurité depuis plus de 20 ans, il a collaboré avec des instituts influents, tels qu'EICAR, dont il est le cofondateur et le directeur de l'information et de la communication, ou différentes associations CERT.

Aurora : quand technicité et ingéniosité se rencontrent

En décembre 2009 et janvier 2010, il est devenu évident que les grandes multinationales pouvaient être victimes d'attaques de malware. Les réseaux de plusieurs compagnies parmi les 100 premières mondiales ont été pénétrés par ce qui sera dénommé plus tard l'attaque Aurora. La victime la plus connue d'Aurora était Google en Chine. Google a alerté les médias du fait que leur réseau avait été envahi. Une discussion féroce au sujet de la censure chinoise s'en suivit. Cette polémique masqua totalement la question la plus importante d'Aurora : derrière Google, plus de 30 autres grandes entreprises ont vu leur réseau pénétré grâce au niveau de sophistication élevé de cette attaque.

Aurora a réussi à s'introduire dans les réseaux de ces entreprises par l'utilisation d'une faille de sécurité non découverte et donc non corrigée (appelée faille 0-day) dans Internet Explorer. Cette faille a fourni l'accès du système au malware. Une partie de ce malware, qui est composé de pas moins de 12 programmes différents, a été chiffré plusieurs fois afin de rester indétectable aussi longtemps que possible dans le système. Pour s'assurer la pleine capacité d'Aurora, ses auteurs ont voulu que le programme soit installé par des personnes possédant des droits suffisants et des autorisations sur le système. L'infection ne pouvait être était réussie seulement lorsque le virus pouvait gagner le contrôle des comptes utilisateurs avec un accès à un grand nombre d'informations critiques. Pour réaliser ceci, des liens vers des sites Web infectés ont été envoyés à des employés parfaitement ciblés dans les sociétés visées. Pour contourner les filtres antispam, les attaquants ont rivalisé d'ingéniosité. Ils ont piraté les comptes de réseaux sociaux des amis de la personne ciblée et diffusé des messages de statuts pointant vers le site Web infecté. Un coup de maitre : un lien signalé par un ami est habituellement considéré comme de confiance...

Les auteurs d'Aurora semblent avoir pensé à tout. Avant que le malware n'ait été détecté, les informations sur l'entreprise avaient déjà été volées. Après sa découverte, Aurora a été décrit par des experts comme « le malware le plus sophistiqué jamais créé ». Si pour les entreprises attaquées (et leurs clients) la situation a été incommodante, les conséquences n'ont toutefois pas été dévastatrices. Le but était l'espionnage de la société. Outre l'énorme stress placé sur les épaules des responsables IT des entreprises visées, aucun risque ne courait sur la population mondiale.

Stuxnet : tout comme les PC, les systèmes de production peuvent aussi être infectés

Un peu plus tard cette même année 2010, Stuxnet était l'autre grande attaque. Stuxnet est, comme Aurora, un malware qui se compose de différentes pièces. Mais les concepteurs de Stuxnet ont de loin dépassé les concepteurs d'Aurora sur un aspect clé : à la différence d'Aurora, Stuxnet ne s'est pas fondé sur une seule faille zéro day, mais sur pas moins de quatre ! En outre, une vieille faille zéro a été utilisée. Celle-ci datait de 2008. Une faille corrigée cette même année par Microsoft, mais jamais installé sur beaucoup de systèmes, y compris des systèmes liés à la régulation de processus. Afin d'être classé par catégorie en tant que logiciel légitime par Windows, les auteurs de Stuxnet n'ont pas opté pour le chiffrage multi couche, comme Aurora. Au lieu de cela les développeurs ont volé des certificats Windows légitimes actifs dans les entreprises JMicron et Realtek Semiconductors.
Le malware n'était pas destiné à infecter beaucoup d'ordinateurs, mais seulement un groupe ciblé. Pour atteindre ce but, l'infection était possible de plusieurs manières exigeant le contact physique avec des périphériques infectés, par exemple le contact avec des clés USB ou des dispositifs supportant des scanners et des partages d'imprimante. Afin de rester inaperçu, le malware a adopté une approche particulière en se répandant seulement sur trois autres PC accessibles à partir du premier ordinateur infecté.
Une fois installé sur un système, Stuxnet est capable de réaliser un balayage des systèmes à jour sur lequel les activités du malware peuvent être rapidement découvertes. Il vérifie également si l'ordinateur a le programme SCADA (Supervisory Control and Data Acquisition) de Siemens installé. SCADA est employé très souvent dans l'industrie de transformation dans le système à régulation de processus pour commander tous les processus. Le malware se déploie seulement si SCADA est sur le système d'exploitation ciblé et reprogramme le contrôleur logique (PLC). Ceci exécuté, les attaquants ont non seulement accès à des informations critiques sur l'entreprise, mais aussi le contrôle complet sur la production.
En dépit de son système de déploiement et d'infection spécifique, Stuxnet a tout de même réussi à infecter des douzaines d'entreprises industrielles partout dans le monde. La cible principale semble être l'industrie iranienne, spécifiquement les réacteurs nucléaires de ce pays. Bien que ce malware ait été détecté juste à temps, il est possible que Stuxnet ait réussi à atteindre son objectif. La société iranienne a admis publiquement qu'elle avait été affectée par Stuxnet.

Repenser les pratiques pour améliorer la lutte

Aurora et Stuxnet nous amènent à diverses conclusions. Tout d'abord, le malware s'impose comme un système professionnel. L'écriture de code malicieux n'est pas seulement un passe-temps pour petits escrocs, il implique aussi des développeurs pointus, financièrement soutenus par des investisseurs, probablement même par des gouvernements. De cette situation découle deux autres conclusions : les cyber-attaques deviennent de plus en plus sophistiquée et leurs raisons évoluent. Le chantage, l'extorsion, le contrôle total des processus industriels ou leur destruction semblent être les prochains buts recherchés. Pour combattre cette menace et éviter qu'elle ne trouve un écho qui pourrait être dévastateur dans des industries dites « sensibles » il est important de considérer comme urgente la sécurité des systèmes à régulation de processus. Ceci passe d'une part par la mise en place de programmes de mises à jour planifiées et/ou systématiques des systèmes industriels, mais aussi par des tests de vulnérabilité sur l'ensemble des processus mis en place afin de les sécuriser rapidement et de

manière permanente. D'autre part, les employés doivent aussi prendre conscience qu'ils sont les cibles potentielles des cybercriminels, qu'ils soient impliqués ou non dans le processus de contrôle. Ceci signifie qu'ils doivent éviter de cliquer sur des liens dans les emails ou sur les réseaux sociaux, particulièrement quand ils sont au travail. En outre pour une meilleure sécurité, les clés USB doivent être mieux contrôlées sur le lieu de travail.

A propos de G Data Software AG

G Data Software AG dont le siège social est situé à Bochum (Allemagne), est un éditeur de logiciel innovant spécialisé dans les solutions de sécurité. Fondée en 1985, la société G Data a été pionnière dans le développement du logiciel antivirus. Depuis 5 ans, aucun autre éditeur de logiciels de sécurité européen n'a obtenu autant de distinctions nationales et internationales que G Data. La gamme de produits se compose de solutions de sécurité pour des particuliers et les entreprises. Les solutions G Data sont disponibles dans plus de 90 pays.

Informations : www.gdata.fr