Les 10 principales défaillances des systèmes Scada selon Lexsi

Pendant 4 ans, le cabinet Lexsi s'est penché sur les infrastructures de 50 de ses 500 clients sur la base d'un référentiel maison représentatif (celui de l'Anssi étendu). Un audit de longue haleine mené à travers des études annuellement mises à jour qui a permis au spécialiste de la cybersécurité de dresser un panorama des principales failles de sécurités qui touchent les systèmes industriels. Pour la plupart issues du CAC40, les sociétés auditées en question évoluent dans les secteurs de l'énergie, de l'aéronautique, industrie automobile, transport, environnement et administration. Autant de secteurs représentatifs de la réalité du terrain.

Lexsi s'est penché tant sur les réseaux ICS (Industrial Control System) de gestion des capteurs et actionneurs du monde physique des chaînes de production, que sur le Scada (Supervisory Control and Data Acquisition), l'ensemble des serveurs, poste de travail et applications de l'ICS pour superviser le procédé industriel. Plusieurs problématiques touchent les infrastructures industrielles. En premier lieu, *« l'idée d'un réseau Scada isolé est de moins en moins vrai*, avance le consultant expert sur la partie industrielle David Bigot chez Lexsi. *On voit sur certains terrains des réseaux connectés en cellulaires désormais. »*. D'autre part, les outils du Scada sont soumis aux problématiques de sécurité propre à l'informatique de gestion classique avec la nécessité de répondre à des cycles de vie courts (3-5 ans). En face, la plupart des réseaux industriels connaissent des cycles de vie longs de 15-20 ans dans des solutions logicielles et matérielles figées difficiles à faire évoluer. Enfin, la différence de culture informatique fait que les gens de l'IT ne se parlent pas nécessairement avec ceux des réseaux de contrôle des chaines de production, ce qui ne va pas dans le sens d'une approche préventive de la sécurité.

Des risques qui s'accentuent

Pourtant, les risques sont réels. Démontrés par le projet universitaire Aurora dès 2007, l'attaque de sites industriels s'est matérialisée en 2010 avec Stuxnet, un APT visant à dégrader la production nucléaire iranienne. En 2014, plusieurs failles de système Linux/Unix (Heartbleed, Shellshock) et l'apparition de malwares à portée industrielle (DragonFly, Sandworm…) ont probablement permis l'attaque de sites. Ce fut notamment le cas pour une aciérie allemande dont peu de détails ont filtré. Il a par ailleurs été démontré que le protocole industriel Modbus conçu en 1979 par Modicon (racheté par Schneider Electric) ne dispose d'aucun système de sécurité et donne accès aux mots de passe en clair, ainsi qu'à la reprogrammation des PLC (contrôleurs logiques des capteurs, actionneurs…).

Si des actions sont entreprises, notamment avec les publications de référentiels Anssi (Agence nationale de la sécurité des systèmes d'information), la constitution de groupes de travail ou un nouveau correctif de la faille exploitée par Stuxnet en 2014, Lexsi entend prendre également part à l'émergence des prises de conscience des industriels en publiant les 10 écueils les plus fréquemment rencontrés au cours de ces audits de terrain.

1. **Absence de développement sécurisé** dû à des développements internes qui répondent

aux besoins internes. Il en résulte des comptes d'accès stockés en clair ou encodés trivialement (le nom de la société comme mot de passe principal, par exemple).
2. **L'absence de test de sécurité** découle en toute logique de l'absence d'intégration de la sécurité informatique dans les projets.
3. Une **mauvaise gestion des comptes** où l'on retrouve l'usage d'identifiant par défaut (user/user…), des mots de passe trop faibles ou inexistant (vides, nom du client, mot du dictionnaire évident…) ou encore des utilisateurs disposant de privilèges administrateur sur l'OS.
4. **L'interconnexion des systèmes de gestion avec les systèmes industriels** pas assez sûre. Une perméabilité qui permet à un attaquant qui s'introduirait dans le système de gestion informatique de poursuivre sa route sur le réseau industriel.
5. **L'absence d'antivirus** sur les postes de travail et serveurs qui laisse tout loisir aux agents malveillants de se propager. Lexsi a ainsi constaté la présence du vers Conficker sur des postes de supervision industrielle dans 50% des cas.
6. **Absence de veille en cybersécurité** qui rend difficile la détection de signaux d'alerte et la remontée d'information. Au mieux, souligne Lexsi, les logs sont enregistrés par les firewall mais rarement analysés.
7. **Des sessions Windows non verrouillées** qui rendent l'accès permanent aux interfaces de contrôle (IHM) ou consoles de pilotage. Là encore, en cas d'attaque, la prise de commande distante est un jeu d'enfant pour l'assaillant.
8. **Absence d'outils de surveillance** des systèmes (sondes de détection/prévention d'intrusion) et pas de centralisation des journaux systèmes et de leur analyse.
9. **Des protocoles courants** (FTP, Telnet, VNC, SNMP…) utilisés sans chiffrement qui ouvre l'accès à la récupération de login/mot de passe, à des connexion illégitimes aux serveurs, à des attaques hors ligne, des dénis de service par modification des configurations réseau…
10. **Des OS et firmware obsolètes** et non mis à jour. Si Windows XP est encore très présent dans le monde industriel, Lexsi constate également encore la présence de Windows 2000 et même NT4. Une obsolescence qui permette des prise en main rapide sur le Scada avec pour conséquence des compromissions instantanée des équipements et le risque de rebondir sur d'autres périmètres.

Recommandation et prise de conscience

Face à ces défaillances d'approche, Lexsi propose ses recommandations. Lesquelles s'en tiennent aux lignes habituelles de conduite de projets sécurisés. A savoir la mise à jour des OS et applications, l'installation d'antivirus, l'usage de protocoles sécurisés et de solutions de détection d'intrusion (IPS/IDS), la déconnexion des IHM (consoles de contrôle) en cas d'inactivité, cloisonner les réseaux IT et industriels, utiliser des mots de passe complexes, retirer les privilèges administrateurs aux postes qui n'en n'ont pas besoin, instaurer une veille de sécurité et effectuer des audits, ou encore inclure des clauses de cybersécurité dans les contrats des éditeurs.

David Bigot reconnaît néanmoins qu'il *« est difficile d'appliquer ces recommandation dans le monde industriel car cela oblige à changer un certain nombre de choses qui entraînent inévitablement un impact sur la production et donc un coût »*. Sans parler des applications incompatibles avec les nouvelles

générations d'OS (de Windows XP à Windows 7 notamment) et oblige à des re-développements. Il faut donc *« faire évoluer les mentalités en évangélisant, obtenir le soutien de la direction et créer des groupes de travail multi-compétence »*, soutient l'expert. Il n'en reste pas moins que le problème est aujourd'hui pris en compte par le législateur (notamment à travers la Programmation de loi militaire) et des éditeurs industriels. S'il y a encore beaucoup de travail, *« la dynamique est bonne »*, assure David Bigot.

Lire également

Thomas Houdy, Lexsi : « Après Dragonfly, réagir sur la sécurité des Scada »
Sécurité des Scada : pourquoi la côte d'alerte est atteinte
Scada : un virus infecte le nucléaire sud coréen