



6% des visiteurs (anonymes) du salon Industrial Processing qualifient le niveau de protection de leur société de processus de 'passoire'.



Photo: Ahoy

Qui conduit le processus? Vous ou un pirate?

Par ir Walter Bergers

Un collaborateur licencié d'une installation d'épuration des eaux déverse des mois durant des eaux polluées dans des régions habitées. Des criminels qui réclament des millions pour taire une effraction. S'agit-il là de scénarios venus tout droit de Hollywood ou d'une réalité? L'effraction d'un réseau modbus nécessite une machine disposant des bons connecteurs et du support du protocole modbus. En revanche, s'il s'agit du protocole TCP/IP, un simple PC ou portable suffit.

Il est très difficile d'obtenir des données exactes sur les incidents relatifs à la protection (ICT), surtout dans l'industrie de processus où ces faits peuvent fortement nuire à l'image de la société. Des visiteurs du salon Industrial Processing ont parfois précisé de manière anonyme le niveau de protection au sein de leur

société. Six pour-cent d'entre eux le qualifiaient de 'passoire'.

Devons-nous nous inquiéter? Si vous recherchez sur internet ou via d'autres sources des problèmes de protection dans l'industrie de processus, vous retrouvez souvent les mêmes histoires, comme celle de l'employé de la

station d'épuration des eaux en Australie. Cet incident s'est déroulé en 2000. Après quelques recherches, nous remarquons que tous ces incidents proviennent d'une seule et même source : l'Industrial Security Incident Database (ISID) du British Columbia Institute of Technology (BCIT). Celui-ci conserve un résumé de tous les incidents survenant dans l'industrie de processus, parmi lesquels non seulement les effractions malveillantes mais aussi les erreurs commises par un opérateur. Les résumés sont accessibles à tous gratuitement, à condition qu'un nouvel incident soit annoncé.

Outre l'ISID, il est très difficile de trouver des données sur de tels incidents. Faut-il alors considérer tout cela comme des histoires venues tout droit d'Hollywood?



Il est effectivement fort difficile d'entrer par effraction dans un réseau de processus. Un tel réseau contient un équipement très sophistiqué comme des PLC et des systèmes embarqués. Nous retrouvons peu ou pas d'informations à leur sujet et les standards utilisés ne sont pas publiés. Tout cela doit donc présenter une garantie de grande sécurité. Eh bien non! Ne pas dévoiler comment est fait un système ou protocole, appelé également 'security through obscurity', est utile pour complexifier la violation. Toutefois, il ne faut pas croire que cela suffit pour arrêter les criminels. Les effractions sont également possibles avec des systèmes propriétaires aux standards fermés. Les experts qui approfondissent ce type de systèmes sont en mesure de trouver très vite leur fonctionnement, et donc leurs failles.

Un risque accru

Tant que personne ne s'intéresse à l'industrie de processus et qu'il subsiste le problème de recherche du fonctionnement des systèmes et de leurs failles, le risque reste minime. Toutefois, certaines évolutions actuelles tendent à accroître sensiblement le risque. Pensez par exemple à la nouvelle vague de criminels sur internet, au glissement vers des standards ouverts et aux liaisons toujours plus fréquentes des réseaux. Internet a démarré à l'époque comme outil pour les universités. Les protections n'étaient alors pas aussi importantes car il n'y avait pas encore de criminels sur Internet. Puis, dans les années 90, nous avons assisté à de nombreuses effractions par des personnes qui acquéraient ainsi du prestige au sein de leur groupe social. Des sites web étaient souvent attaqués et adaptés. Un tel 'website defacement' mentionnait dès lors toujours le nom de l'attaquant (ou du groupe d'attaquants).

Risque de dommage

Nous notons aujourd'hui un glissement des attaques 'pour le plaisir' vers des attaques pour l'argent. Nous n'enregistrons quasiment plus d'effractions de sites web se limitant au simple changement de contenu. Il existe de nombreuses façons de gagner de l'argent. Par exemple en mettant sur pied un réseau comptant des centaines voire des milliers de systèmes craqués à partir desquels sont envoyés des pollupostages, contre paiement naturellement. Ou encore en extorquant de l'argent à des sociétés. Le chantage qui fonctionne le mieux est celui opéré auprès des sociétés qui courent un grand risque de dommage. Les criminels entrent par effraction et promettent de ne rien faire, moyennant la remise d'une grosse somme d'argent. Ces criminels ont entre-temps aussi découvert l'industrie de processus. On y retrouve souvent pas mal d'argent, ce qui motive le chantage. Le risque de dommage étant grand, la société abusée aura plutôt tendance à ne pas porter plainte



Nous notons aujourd'hui un glissement des attaques 'pour le plaisir' vers des attaques pour l'argent. Ces criminels ont entre-temps aussi découvert l'industrie de processus. On y retrouve souvent pas mal d'argent, ce qui motive le chantage. Le risque de dommage étant grand, la société abusée aura plutôt tendance à ne pas porter plainte et à payer.

et à payer.

Deux réseaux

On parle souvent de deux réseaux dans l'industrie de processus: le réseau de contrôle de processus et le réseau d'automatisation bureautique. Sur le réseau de contrôle de processus, nous retrouvons les PLC et systèmes embarqués qui pilotent la production. Sur le réseau d'automatisation bureautique, nous retrouvons les stations de travail des collaborateurs et l'infrastructure pour les courriels et le web par exemple. L'effraction du serveur web de l'entreprise est une chose, l'effraction du réseau de contrôle de processus en est une autre. Ou devrais-je dire 'en était une autre'? Nous voyons en effet un glissement des standards fermés vers des standards ouverts qui se trouvent aussi sur Internet: TCP/IP, Ethernet, HTTP. Un appareil embarqué qui soutient tous ces protocoles se gère ainsi très simplement à l'aide d'un navigateur web. Nous voyons aussi un glissement des systèmes spécialisés vers des systèmes courants. Nous voyons déjà apparaître dans les réseaux de processus des systèmes qui utilisent Windows comme système d'exploitation. De par ce glissement vers des standards ouverts et des systèmes COTS (Common Off The Shelf), l'effraction devient soudainement plus simple. Comme je le disais déjà précédemment, l'utilisation de

standards fermés ne suffit pas à repousser les criminels mais les standards ouverts augmentent sérieusement le risque en raison de la disponibilité de nombreux outils et méthodes pour entrer par effraction sur ces protocoles et systèmes connus.

L'effraction d'un réseau modbus nécessite une machine disposant des bons connecteurs et du support du protocole modbus. En revanche, s'il s'agit du protocole TCP/IP, un simple PC ou portable suffit. L'effraction effective est aussi beaucoup plus facile avec les systèmes COTS. Il existe suffisamment d'outils permettant d'entrer par effraction sans que le pirate ne doive disposer de connaissances spécifiques. De fait, lorsqu'une faille est découverte dans le logiciel, il ne faut pas attendre bien longtemps pour que sorte un 'exploit', c'est-à-dire un programme malicieux qui exploite une faille pour entrer par effraction. De tels exploits se trouvent difficilement pour les systèmes fermés car ils sont moins utilisés (donc moins intéressants). En revanche, les exploits pour le système d'exploitation Windows sont largement disponibles. En remplaçant des systèmes spécifiques, comme des variantes UNIX temps réel adaptées à l'industrie de processus, par des systèmes courants comme Windows, les attaques deviennent si simples qu'elles sont à la portée de n'importe quel enfant de dix ans.

Exemple pratique

L'exemple de James Cupps en dit long à ce sujet. Cet homme a été nommé en 2004 Security Officer d'une grande usine de papeterie aux Etats-Unis. Il a remarqué que les PLC dans l'usine ne communiquaient plus via des connexions sérieuses mais via Ethernet et s'est demandé si cela comportait des risques. Il a raccordé un PC standard au réseau et a lancé un 'renifleur de réseau', c'est-à-dire un programme qui analyse le trafic de données sur le réseau. De tels programmes se trouvent très facilement et gratuitement. James Cupps a identifié une liaison entre une station de commande et un PLC où l'on reconnaissait clairement le mot de passe 'hihihi'. Ce mot de passe était la clé vers toute l'usine et pouvait être intercepté sans aucune difficulté. Le mot de passe était fortement imbriqué dans les systèmes, il n'était pas possible de le changer. Tous ceux qui trouvent à un moment donné que les PLC d'une entreprise X ont comme mot de passe 'hihihi', ont donc libre jeu. On rencontre souvent ce type de problèmes dans des situations où l'on utilise des systèmes fermés. Le fournisseur se fie au fait qu'on ne saura jamais comment fonctionne le système. Dans ces cas, les systèmes sont conçus de telle sorte que l'ajout ultérieur d'une protection devient quasiment impossible, comme dans cet exemple où la modification ultérieure du mot de passe imbriqué n'était plus possible.



Diffusion

Le partage rapide de ce type de connaissances via Internet constitue un problème supplémentaire. Il existe des programmes qui recherchent les vulnérabilités en confrontant les systèmes et les logiciels aux problèmes connus. Le scanner de vulnérabilités 'Nessus' en est un exemple. Cet outil (gratuit) peut par exemple découvrir l'absence de patches. Il a été récemment étendu avec toutes sortes de vérifications de vulnérabilités dans les réseaux SCADA. Avec l'utilisation de Windows dans le réseau de processus par exemple, celui-ci devient aussi plus vulnérable aux attaques des virus et autres vers. Nous en retrouvons de nombreux exemples dans la littérature. Il n'est guère étonnant des lors que 97% des entreprises utilisent des programmes antivirus. Le coupe-feu est une technique de protection qui est encore plus fréquemment utilisée.

Les coupe-feu servent de contrôle de frontière entre deux réseaux. Ils sont quasi toujours utilisés entre le réseau d'automatisation bureautique et Internet. Un coupe-feu est également indispensable entre le réseau de processus et le réseau d'automatisation bureautique, surtout maintenant qu'il est tellement simple de les relier. Beaucoup de gens pensent que l'achat d'un coupe-feu résout leur problème mais ce n'est malheureusement pas le cas. Outre de fréquentes mauvaises configurations, il y a encore bien d'autres problèmes.

Abus

Les personnes qui peuvent accéder physiquement au réseau de processus ont toute la latitude d'abuser des erreurs de configuration et de l'absence de patches de protection. Il arrive souvent qu'une personne malveillante puisse aussi pénétrer dans un site en saluant de loin le portier sans se faire arrêter. Elle peut s'inviter elle-même en inventant un prétexte (par exemple la présentation d'un nouveau produit). En se rendant aux toilettes, elle peut se repiquer sur une station de réseau sans fil placée dans un coin et accéder sans fil à tout le réseau à partir du parking. Heureusement, de telles attaques ne sont pas si fréquentes car elles nécessitent un accès physique et une bonne dose de bravoure. Malheureusement, les attaques au travers d'un coupe-feu sont souvent possibles. Pire encore, ces attaques figurent parmi les plus fréquentes sur Internet. La procédure standard consiste à abuser d'une application qui tourne sur un serveur web, en l'approchant via Internet et en 'usurpant' la connexion que le serveur web établit avec les systèmes internes. Ces attaques permettent de manipuler des systèmes internes au travers du coupe-feu. Les applications mal écrites sont malheureusement monnaie courante. Les applications ne doivent souvent répondre qu'à des exigences fonctionnelles (que

doit faire l'application?). Les exigences de protection (que ne doit-elle surtout pas faire) sont cependant cruciales. Les mauvaises configurations et l'absence des derniers patches de protection ne sont pas rares non plus.

Une criminalité si proche

Ce type d'attaques permet à un criminel aguerri de pénétrer en profondeur dans le réseau interne, le tout à partir d'un endroit sûr à la maison, à des milliers de kilomètres, tout simplement via Internet. Un collaborateur de Symantec expliquait lors d'une conversation comment il pénètre dans un serveur web via Internet et de là (à travers le coupe-feu) dans des systèmes internes. Ensuite, il sait - en regardant les noms des systèmes - trouver un système qui est le seul à avoir accès aux machines sur le réseau de processus. Le coupe-feu entre le réseau d'automatisation bureautique et le réseau de processus est paramétré de manière à ce qu'un seul système spécial puisse accéder au réseau de processus. Au lieu du responsable, c'est maintenant le collaborateur de Symantec qui se trouve sur la machine et peut aller sur le réseau de processus. Et puisque les noms d'utilisateur et les mots de passe y sont identiques, il peut sans aucun problème commander le contrôleur d'interface homme machine et prendre le plein contrôle de tout le réseau de processus. Tout cela via Internet, à partir de son propre PC.

Désormais, le glissement vers des standards ouverts facilite aussi la liaison des réseaux, ce qui implique à nouveau un danger. Les VPN peuvent relier différents sites mais un mot de passe qu'il est possible de deviner ou un mauvais paramétrage peut rendre ces VPN accessibles à des personnes non autorisées. Les modems installés pour permettre à un collaborateur de travailler le samedi soir de chez lui peuvent créer des portes de derrière indésirables. Les connexions aux réseaux sans fil qui utilisent un cryptage WEP standard peuvent être craquées en moins de dix minutes. Bref, toutes ces connexions de réseaux supplémentaires entraînent aussi des risques supplémentaires.

Portes de derrière

En guise de conclusion, je peux dire qu'avec la migration vers des standards ouverts et des systèmes COTS, la criminalisation sur Internet et la hausse des liaisons entre les réseaux, les risques peuvent rapidement prendre des proportions inacceptables. Connaissez-vous toutes les connexions de réseaux? Connaissez-vous toutes les portes de derrière? Peut-être devriez vous, sans tarder, examiner en détail votre réseau.<<

Les sociétés belges ne protègent pas leur innovation

De toutes les marques du Benelux déposées en 2005, il y avait sensiblement plus de demandes émanant des Pays-Bas que de la Belgique. Pas moins de 20.385 demandes provenaient des Pays-Bas contre 5.707 de la Belgique. Des études montrent en outre que 63% des entreprises belges ne considèrent pas l'enregistrement d'une marque comme important.

Les sociétés belges ont donc un énorme retard en matière de protection de marque par rapport à leurs collègues néerlandais. Un constat consternant pour un pays qui clame haut et fort que l'innovation est son avenir. Nos entreprises sont encouragées à se montrer innovantes et à mettre de nouveaux produits sur le marché. Les entrepreneurs belges s'efforcent de mettre sur le marché des produits qualitatifs et ils y parviennent. Cependant, l'étape suivante semble apparemment bénéficier de moins d'attention.

Les entreprises ne protègent pas suffisamment leurs produits contre la contrefaçon et nuisent ainsi à leur image de qualité. En effet, des produits de qualité inférieure sont mis sur le marché par des concurrents sous une marque qui ressemble fort à la marque originale. Et d'autres profitent de l'image de marque. En ne consacrant pas suffisamment de temps à la protection de la marque, l'entreprise perd bêtement l'argent et le temps qu'elle a investis dans le produit. Des études montrent que 63% des entreprises belges n'attachent pas beaucoup d'importance à l'enregistrement de la marque. Les marques non enregistrées peuvent toutefois être volées ou imitées. Sans enregistrement, la société n'a aucun droit probant sur une marque. Domage car les produits de contrefaçon semblent bel et bien inonder notre marché. Les chiffres sont révélateurs : en 2005, la douane belge a confisqué plus de 26 millions de contrefaçons.

Source: VLAO (Vlaams Agentschap Ondernemen)



Vous pouvez télécharger cet article sur www.mainpress.com