Les centres de contrôle sont-ils vulnérables?

Autor(en): **Link, Richard**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **102 (2011)**

Heft 10

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-856855

Les centres de contrôle sont-ils vulnérables ?

Remarques sur le ver informatique Stuxnet

En attaquant pour la première fois de manière ciblée des installations en dehors de l'environnement IT habituel, le ver informatique Stuxnet a apporté une nouvelle dimension à la menace existante sur les infrastructures critiques telles que les centres de contrôle des réseaux électriques. Quelles leçons pouvons-nous en tirer ? Qui doit assumer la responsabilité lors d'une attaque ? Et surtout, est-ce que ces systèmes de conduite réseau sont vulnérables ?

Richard Link

Stuxnet est un ver informatique découvert en 2010, qui a été spécialement développé pour un système SCADA (Supervisory Control and Data Acquisition) conçu pour la surveillance et le contrôle d'un processus industriel. Il est considéré comme exceptionnel en raison de sa complexité et de son objectif : saboter des systèmes de contrôle de processus industriels.

Avant l'apparition de Stuxnet, les logiciels malveillants tels que les troyens et vers informatiques avaient essentiellement pour but d'espionner certaines informations sauvegardées sur les PCs d'utilisateurs privés, par exemple les données de cartes de crédit, les coordonnées bancaires, et évidemment les mots de passe et données de connexion. Ces logiciels sont habituellement délivrés comme pièce jointe à un spam ou inclus dans une page Web, et l'utilisation de lacunes dans les systèmes d'exploitation et d'internet pour leur propagation leur permet d'entrer discrètement mais efficacement en action.

Figure 1 Les installations techniques ayant fait leurs preuves doivent relever le défi posé par l'utilisation de la technologie IT.

Une nouvelle dimension

Déjà du point de vue de sa stratégie de propagation, Stuxnet s'est montré novateur. S'ils sont protégés suivant les règles de l'art, les systèmes industriels ne sont pas accessibles via internet. Pourtant, Stuxnet a réussi à se propager, et ceci grâce à l'utilisation d'une faiblesse humaine : la curiosité. Il a probablement pu s'introduire dans le réseau de systèmes de contrôle industriels par l'intermédiaire de clefs USB « déposées » de manière ciblée à des lieux stratégiques. Celles-ci ont ensuite évidemment été examinées par leurs trouveurs sur l'ordinateur le plus proche. Grâce à l'utilisation simultanée de plusieurs lacunes de sécurité des systèmes d'exploitation en partie inconnues jusque-là, il a alors été possible d'installer un « Rootkit » qui a pu démarrer discrètement d'autres actions.

Une autre innovation a été l'utilisation de signatures digitales volées qui ont permis à ce logiciel malveillant de se nicher profondément dans le système, et ce, même sur des systèmes munis de toutes les mises à jour nécessaires. Même si l'énorme investissement qui a été indispensable au développement de Stuxnet sera difficile à réitérer et qu'une deuxième attaque sous cette forme soit peu probable, il a tout de même permis de localiser les vulnérabilités des systèmes actuels (figure 1).

Les auteurs changent

Extrêmement ingénieux, ce logiciel malveillant a probablement été développé par une équipe d'experts. Des compétences très particulières ont été nécessaires, à commencer par la connaissance des systèmes d'exploitation, de détails précis sur les appareils d'automatisation attaqués, de lacunes de sécurité alors inconnues, jusqu'à un savoir-faire très étendu et une connaissance de détails sur la configuration de l'installation particu-

lière des systèmes qui étaient l'objectif de l'attaque. Toutes ces qualifications, prises dans leur ensemble, ne peuvent être celles d'une seule personne, et certainement pas celles de soi-disant « script kiddies ».

Le fait que les auteurs n'aient pas été découverts jusqu'à ce jour, suggère non seulement que les commanditaires disposent de moyens suffisants, mais qu'ils sont aussi en mesure de protéger les auteurs. La supposition largement répandue qu'il s'agisse des services secrets est à classer comme tout à fait probable. Un général des services secrets israéliens se serait d'ailleurs vanté d'avoir été responsable de cette attaque. Mais, étant donné le débat actuel autour de l'utilisation pacifique de l'énergie nucléaire, des militants environnementalistes ne sont également plus à exclure comme instigateurs potentiels de telles attaques ciblées contre les systèmes des producteurs d'énergie, sans compter les vulgaires criminels prêts à extorquer pour le moins des avantages financiers. Autrement dit, les hypothèses à l'avenir ne manqueront pas.

But probable

Stuxnet a probablement été programmé avec pour objectif le sabotage des installations atomiques iraniennes, bien qu'il n'y ait jusqu'à présent pas de confirmation officielle. En raison de l'investissement énorme nécessaire non seulement au développement, mais aussi à l'introduction et à la propagation de ce ver, cette supposition a l'air parfaitement plausible. Des rapports de presse de médias américains et israéliens vont également dans ce sens.

Mutation des scénarios d'attaque

Jusqu'à présent, les objectifs des attaques de logiciels malveillants ont principalement été les PCs à usage privé, mais une tendance est observée depuis Stuxnet. D'une part, des exploitants de systèmes avec de très grosses banques de données clients ont été attaqués et des données ont été effectivement dérobées – même les banques et entreprises de sécurité ne sont pas épargnées. D'autre part, les infrastructures critiques peuvent à présent être aussi considérées comme cibles potentielles. Mais il a également été démontré que les systèmes d'automatisation sont tout aussi concernés, de même que les systèmes intégrés comme les automates programmables industriels (PLC ou Programmable Logic Controller).

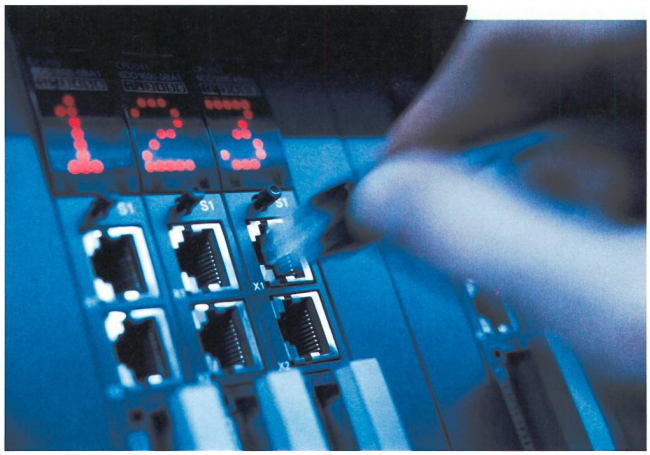


Figure 2 La mise en réseau met en danger les systèmes de commande industriels.

Autrement dit, il ne s'agit plus que d'une question de temps avant que les systèmes de téléconduite utilisés aujourd'hui ne deviennent la cible d'une attaque (figure 2). Les systèmes SCADA pour la surveillance et la commande de notre infrastructure énergétique sont donc directement menacés. Au vu de ces faits, beaucoup d'experts envisagent avec inquiétude un black-out étendu et le prévoient dans un avenir proche.

Cyberwar

Les auteurs de telles actions (et leurs commanditaires) évoluent, tout comme le degré de complexité de ces offensives en fonction de leurs intérêts politiques et économiques. Ce n'est donc pas un hasard si le terme « Cyberwar » est souvent utilisé pour caractériser ces attaques menées à l'aide de la technologie informatique.

Les moyens habituels de sécurité IT n'offrent pas une défense effective contre ces méthodes. Stuxnet l'a clairement démontré. Les exploitants se doivent donc de réduire ces risques autant que possible. Un système maintenu parfaitement, un personnel formé et une architecture élaborée de l'infrastructure IT feront bien sûr partie des moyens mis en œuvre pour empêcher ou du moins minimiser le risque qu'une telle attaque soit couronnée de succès.

Les responsabilités évoluent

Mais qui doit assumer la responsabilité de la sécurité d'une infrastructure critique ? La réponse semble être évidente : l'exploitant en tant que propriétaire et utilisateur de l'installation est également responsable de la sécurité de ses systèmes. Cependant, le fabricant se retrouve toujours également impliqué. Sa

Figure 3 Des systèmes SCADA modernes sont essentiels à la sécurité de l'approvisionnement électrique.

Figure 4 La sécurité ne peut être garantie que par une étroite collaboration entre l'exploitant et le fournisseur.

responsabilité quant au produit est donc clairement établie, bien que la question se pose quant à son applicabilité aux systèmes complexes d'aujourd'hui. A noter que la responsabilité du fabricant n'entre en jeu qu'en bout de course, lorsqu'il est déjà trop tard, qu'un dommage est apparu et que les conséquences économiques doivent être supportées.

A l'avenir, les efforts devront se focaliser sur la sécurité de toute l'installation et surtout sur celle de l'infrastructure IT correspondante. Les systèmes de gestion de l'approvisionnement énergétique ne peuvent plus être gérés comme par le passé, en tant que simples appareils électrotechniques, mais doivent l'être comme un ensemble intégré. La complexité des installations d'aujourd'hui exige d'appliquer des règles strictes de sécurité IT. C'est pour ces raisons que les standards de sécurité comme le NERC-CIP[1)] en Amérique du Nord ou le BDEW-Whitebook[2)] en Allemagne comportent des directives claires pour l'exploitation et la configuration de tels systèmes. Mais si la responsabilité de l'exploitant est mise clairement en évidence dans ces documents, la responsabilité du fabricant quant au produit n'y est représentée qu'en relation avec l'exploitant.

La sécurité IT peut-elle être fournie sur commande ?

Un processus d'appel d'offres long et coûteux régit aujourd'hui encore la fourniture de systèmes complexes comme les systèmes de conduite réseau. Toutes les caractéristiques requises, y compris le niveau de sécurité, sont décrites dans le cahier des charges (figure 3). Mais aussi détaillée qu'en soit la description, les exigences en matière de sécurité IT mettent ce processus à rude épreuve.

D'autre part, des exigences générales (« doit satisfaire au standard XYZ ») n'augmentent pas nécessairement la sécurité. Ceci est dû notamment à la nature des standards : un standard décrit les conditions générales, or un système de conduite réseau ou de sous-station est souvent très spécifique aux besoins de l'exploitant. Une exigence de sécurité conforme aux besoins apparaît dans ce contexte comme une tâche herculéenne. Sans compter que les exigences complexes et détaillées en rapport avec l'infrastructure IT prennent beaucoup de temps et sont coûteuses.

Un autre aspect du processus d'appel d'offres est le facteur temps. Entre la publication des documents d'appel d'offres, et la livraison et mise en service, des mois, mais aussi souvent des années, se seront écoulés. Ceci a pour conséquence, qu'en particulier les critères de sécurité exigés dans l'appel d'offres initial ne sont plus à jour au moment de la mise en service. Le fabricant livre ce qui est spécifié dans l'appel d'offres. Une adaptation tardive des exigences du système est toujours liée à des frais supplémentaires. La pression générale exercée par les coûts et la pratique habituelle de sélectionner l'offre la moins chère ne coïncident souvent pas avec une solution optimale du point de vue de la sécurité IT du système délivré.

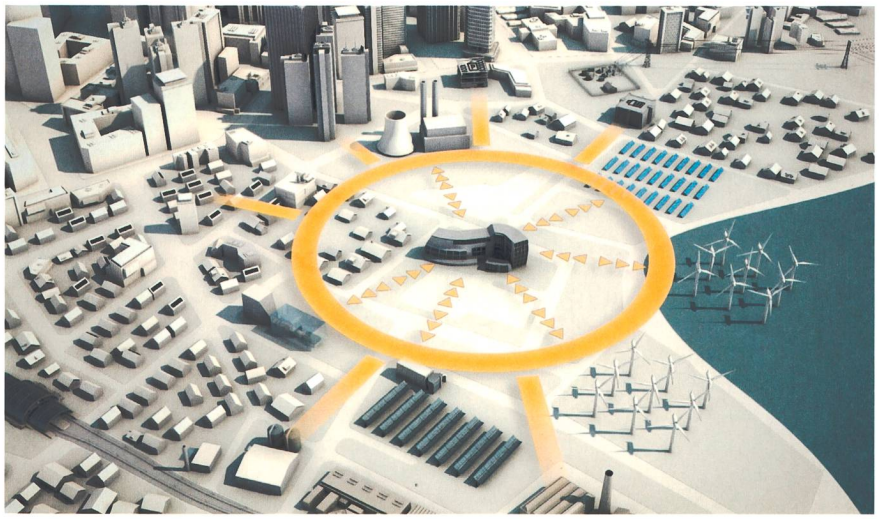
Pouvons-nous réorienter notre façon de penser ?

Une fois que le choix de fournisseur a été effectué et que les propriétés du système délivré ont été établies, un autre sujet, lui aussi digne de discussion, vient s'ajouter : la mise en service du système. La pratique courante, tout du moins pour les moyens et grands systèmes de conduite réseau, est l'acceptation en plusieurs étapes :

- Le système est d'abord testé chez le fournisseur, notamment pour vérifier qu'il est en accord avec le cahier des charges (Factory Acceptance Test, FAT).
- Ensuite le système est envoyé chez l'exploitant où il est testé encore une fois très intensivement (Site Acceptance Test, SAT).
- Finalement, la réception définitive est effectuée après une période d'essai de mise en service.

Cette procédure permet le test du système en profondeur, mais elle présente cependant un désavantage décisif : elle suppose que le système ne change plus pendant et surtout après la mise en service. L'état du logiciel est alors « gelé ». Tout changement du système, y compris les mises à jour (patches) de sécurité, implique que le système ne peut plus être considéré comme fiable étant donné que les tests ont été effectués sur une tout autre base. Ceci mène à un dilemme : soit le système qui a été testé en profondeur reste tel quel mais devient vite obsolète, soit le système utilisé en opération diffère rapidement de celui complètement testé. Les deux variantes ne sont en fait pas acceptables pour une infrastructure critique.

Un autre aspect est la question de l'étendue des tests. Le niveau des tests est très élevé, en fin de compte souvent tous les équipements interconnectés au travers d'interfaces de communication sont testés point par point. D'un autre côté, les systèmes actuels sont la plupart du temps intégrés dans une infrastructure d'entreprise dans laquelle ils sont soumis aux règles des systèmes IT et leur vulnérabilité doit être évaluée du point de vue d'une installation informatique. De nombreuses questions doivent donc être éclaircies à l'avenir : Quelle étendue devraient avoir de tels tests ? Qui devrait les effectuer ? Le fournisseur ? L'exploitant ? Un fournisseur de services externe ? Dans ce contexte, une étroite collaboration entre tous les participants est indispensable (figure 4). En résumé, une chose est claire : la mise en service d'une infras-



Figures: Siemens AG

Figure 5 Les smart grids rendent notre approvisionnement électrique plus vulnérable.

tructure critique doit suivre d'autres règles que celles des années 80. Les règles valables pour les systèmes IT doivent aussi être applicables aux systèmes d'approvisionnement énergétique.

La sécurité exige un système à jour

Aujourd'hui un système de conduite réseau est interconnecté avec une multitude d'autres systèmes. Ceci est d'autant plus vrai avec la tendance actuelle en ce qui concerne la mise en place de réseaux électriques intelligents: les smart grids (figure 5). C'est pourquoi le devoir d'effectuer toutes les mises à jour de sécurité disponibles est valable pour un tel système comme pour tous les autres systèmes informatiques. Un « gel » de l'état du logiciel est inconcevable, puisqu'un système qui n'aurait pas été mis à jour du point vue de la sécurité IT pendant des années serait considéré comme peu sûr et ne devrait pas être exploité. La conséquence logique est donc la mise en place d'une gestion des mises à jour (patch management). Il est absolument nécessaire que le logiciel soit, à intervalle régulier, non seulement mis à jour, mais aussi muni de versions améliorées.

Cela mène à des aspects qui n'ont jusqu'ici pas été discutés dans la branche. Actuellement, les cycles de mise à jour des fabricants de logiciel d'entreprise sont presque toujours mensuels. Par contre, les standards ne prévoient pas concrètement de tels cycles pour les infrastructures critiques. Ceci pour une bonne raison: les systèmes très étendus, avec plus d'une centaine d'ordinateurs, ne peuvent que difficilement être mis à jour toutes les quatre semaines. En particulier, l'absolue nécessité d'une exploitation sans interruption requiert un processus par étape qui prend du temps et augmente les risques. De plus, il est nécessaire de tester le système plusieurs fois: aussi bien les fabricants que les exploitants sont tenus de vérifier le nouvel état du logiciel avant de l'utiliser.

Partons maintenant du principe de la nécessité de la gestion des mises à jour: il est alors à consigner qu'autant les fabricants que les exploitants y soient impliqués. Mais parmi les points à éclaircir se trouvent encore les cycles de mises à jour, la procédure générale, ainsi que les conséquences pour l'opération et la maintenance des systèmes.

Comment aller de l'avant?

La sécurité des infrastructures critiques ne peut être garantie qu'avec une collaboration étroite entre l'exploitant et le fabricant. Le déroulement complet de l'opération, de l'appel d'offres en passant par la commande, à l'acceptation du système jusqu'à la mise en opération, a besoin d'être réévalué. L'exploitation d'une installation d'approvisionnement énergétique doit aussi à l'avenir prendre en considération le point de vue de la sécurité IT.

Le conflit entre les exigences opérationnelles et les exigences de sécurité IT nécessite toujours un compromis: même si la mise à jour régulière du logiciel va à l'encontre d'une exploitation stable et l'investissement pour les tests en est grandement augmenté, l'alternative – utiliser le même système inchangé pendant des années – n'est plus d'actualité et est surtout liée à un risque irresponsable.

La sécurité ne s'obtient pas gratuitement. Ce coût doit absolument être intégré dans les calculs dès le début, et cela pour tout le cycle de vie du système, par les exploitants comme par les fournisseurs. Une pure responsabilité quant au produit du fabricant est difficile à réaliser dans l'environnement IT; aussi, seule la coopération entre les fabricants et les exploitants peut aider à contenir les risques au cours des prochaines années.

Une chose est claire depuis Stuxnet: les systèmes d'approvisionnement électrique sont non seulement de plus en plus complexes – particulièrement en ces temps de mutation vers les smart grids – ils sont aussi devenus vulnérables. La protection des infrastructures critiques constitue l'un des défis les plus conséquents des années à venir.

Informations sur l'auteur

Richard Link est ingénieur diplômé en génie mécanique spécialisé en technique de production. Il est actif dans le domaine des systèmes de conduite réseau chez Siemens AG depuis 1998, entre autres en tant que développeur de logiciel et chef de projet pour le développement de plusieurs produits, et remplit à ce poste diverses fonctions de gestion. Depuis 2006, il est responsable de la gestion des produits pour la sécurité IT et collabore ainsi à plusieurs commissions telles que le Cigré et l'Oesterreichs Energie.

Siemens AG, D-90459 Nürnberg, richard.link@siemens.com

[1] NERC-CIP: North American Electric Reliability Council – Critical Infrastructure Protection.

[2] BDEW: Bundesverband der Energie- und Wasserwirtschaft; www.bdew.de/.

Zusammenfassung **Sind Leitsysteme angreifbar?**

Anmerkungen zum Computervirus Stuxnet

Durch den erstmaligen gezielten Angriff auf Anlagen ausserhalb der gewöhnlichen IT-Infrastruktur hat der Computervirus Stuxnet eine neue Dimension bei der bestehenden Bedrohung kritischer Infrastrukturen wie beispielsweise den Leitsystemen von Stromnetzen erreicht. Was können wir daraus lernen? Wer trägt bei einem Angriff die Verantwortung? Und vor allem, sind Systeme der Netzleittechnik angreifbar?

Dieser Artikel stellt die Herausforderungen im Bereich IT-Sicherheit heraus, durch die Notwendigkeit, die Vernetzung innerhalb von Netzleittechniksystemen zu erhöhen und zeigt neue Strategien auf, um die Risiken zu verringern. CHe