Paris le 26 mai 2020

Alexis
Savva
Master 1 Cybersécurité

Université de Paris

Rapport d'analyse de risques

Paris le 26 mai 2020

Table des matières

Paris le 26 mai 2020

Introduction

Cette analyse de risques est réalisée dans le cadre d'un projet de rénovation d'un système de conduite d'une chaîne de production dans lequel l'ensemble des équipements matériels et logiciels sont de marque SIEMENS.

Elle a pour objet la sécurisation de activités tant en interne qu'en externe.

Les mesures présentées dans ce rapport seront transmises à la direction de l'entreprise afin que les équipes techniques prennent connaissance des mesures de sécurité préconisées.

Les principales activités de l'entreprise sont :

- le pilotage
- la supervision industrielle
- la surveillance industrielle

Il ne nous a pas été demandé de procéder à l'analyse de risques en adoptant une méthode d'étude particulière (EBIOS, EBIOS RM, MEHARI).

Nous procèderons donc avec une méthode en 2 étapes.

La première étape consiste à définir les besoins de sécurité, c'est-à-dire, définir le niveau d'exigences opérationnelles relatif aux biens essentiels. Les différents impacts sur la continuité, l'image de marque, le cadre juridique et financier, seront analysés.

Les événements redoutés en phase avec les besoins de sécurité seront aussi abordés.

La deuxième étape consiste dans l'approche technique sur les biens supports. Nous chercherons les différentes failles et vulnérabilités de chaque bien support (logiciel, matériel) et les risques en découlant en fonction de la gravité et de la vraisemblance. Cela impliquera un plan d'actions pour permettre de réduire les scénarii d'attaques.

Nous devrions normalement inclure une étape supplémentaire qui est métier et fonctionnelle, pour laquelle nous aurions dû solliciter les personnes ayant des activités sur ces périmètres.

Cette étape nous permettrait de comprendre, le fonctionnement métier et leurs besoins, pour commencer à cibler les critères de sécurité sur la base de la disponibilité, l'intégrité, la confidentialité et de la traçabilité.

Il s'agit d'une étape importante du processus métier, dans notre cas nous ne pourrons pas faire cette étape.

Ce rapport a pour but de mesurer le niveau de sécurité à mettre en place, si cela le permet, afin d'avoir un niveau de sécurité suffisant et opérationnel. L'approche intègre la dimension métier de

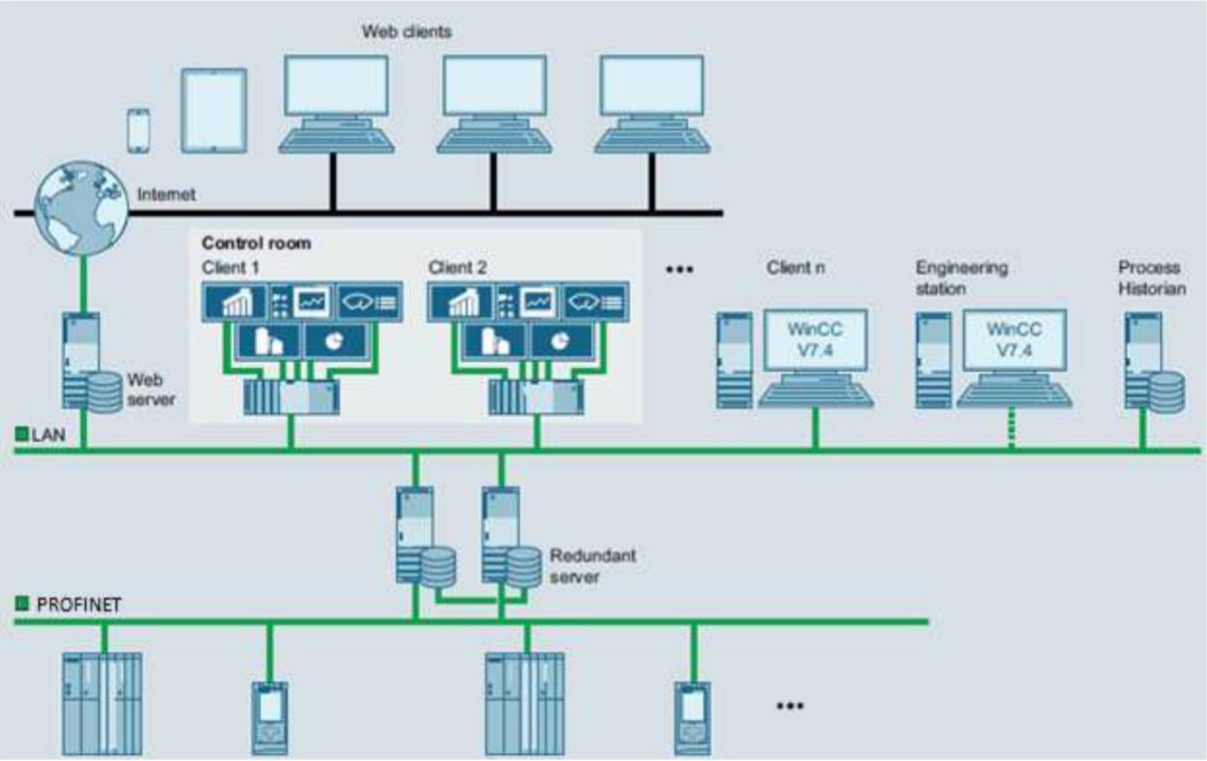
l'entreprise ainsi que les aspects humains, organisationnels et techniques. Comme nous l'avons précédemment évoqué l'analyse porte sur les informations que nous détenons n'ayant pas procédé à un échange avec les personnes au sein de l'entreprise, nous n'avons pas pu évaluer les mesures déjà existantes sur les systèmes d'information.

Notre cotation des impacts de la gravité et de vraisemblance est basée sur les grilles d'EBIOS RM que vous trouverez ci-dessous.

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Échelle	Description
Niveau 4 : Quasi certain	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
Niveau 3 : Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
Niveau 2 : Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
Niveau 1 : Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

Architecture de la chaîne de production :



L'analyse de risques porte sur l'étude des composants logiciels et matériels :

- Automates SIEMENS S7-1500
- Réseau PROFINET
- Serveurs redondé
- Réseau filaire LAN
- Serveur de journalisation
- PCs sous WinCC Portal
- Écrans tactiles Comfort Simatic HMI
- Tablettes HMI Mobile Panel connectées en Wifi avec un équipement USB
- Réseau Wifi
- Simatic Logon
- Une équipe de développeur
- Serveur web

Paris le 26 mai 2020

Partie 1 : Analyse de risques

1/ A partir des orientations énoncées précédemment, il vous est demandé de procéder à une analyse de risque cyber sur l'architecture et les équipements (Matériel et logiciel).

Comme évoqué dans l'introduction, nous manquons dans l'analyse de risques de l'étude du comportement des équipes opérationnelles nous permettant d'appréhender la réalité terrain en matière de sécurité. Cependant l'étude des documents matériels et logiciels ainsi que les plans de l'architecture nous renseignent suffisamment pour conduire notre analyse de risques. Nous présenterons donc l'analyse de risques en détail pour chaque équipement et les risques associés. Enfin un tableau de synthèse regroupant les matériels et logiciels, nous donnera une vue d'ensemble des composants en fonction de la vraisemblance et de la gravité des risques.

Le SIMATIC S7-1500 comporte un écran tactile, la fuite d'information due à des regards indiscrets est une vulnérabilité exploitable. Le manque de protection physique et de surveillance permettraient à une personne mal intentionnée d'accéder aux composants et de les remplacer, de détériorer en y introduisant des logiciels malveillants tels que des fichiers corrompus, malware et cheval de Troie. De plus, l'absence de contrôle d'accès et d'authentification permettra à un utilisateur non habilité de naviguer, de télécharger sur internet des fichiers et de corrompre le système. Enfin une surcharge électrique, coupure de courant pourrait endommager l'appareil ce qui aurait pour conséquence de rendre le matériel indisponible et entraverait la disponibilité des données.

Les réseaux PROFINET et LAN peuvent subir des coupures de courant. L'injection de faux messages, de dénis de service ou d'interception de messages sont des scénarii d'attaque possible. L'absence de protection des prises électriques et prises internet donnerait accès à un attaquant à des vulnérabilités exploitables. La perturbation des trames internet causée par un dénis de service entraînerait une indisponibilité des données. L'interception des trames quant à elle entraverait l'intégrité des données. A noter que le réseau PROFINET a été touché sur des versions antérieures par des attaques informatiques permettant d'exécuter des codes à distance.

Les différents risques pour le serveur de journalisation seraient l'interception de trames, l'attaque DDOS et la divulgation de son adresse IP. L'absence de contrôle d'accès pourrait permettre l'effacement ou la falsification des données par un utilisateur non habilité ce qui entraînerait une indisponibilité du serveur et une perte de traçabilité. Le manque de protection physique, pour tous les serveurs, permettrait la surcharge de courant pouvant nuire à la disponibilité des données. Les mêmes risques sont encourus pour les serveurs. La confidentialité des données n'est pas assurée sans chiffrement.
Concernant le serveur Web, une vulnérabilité sur ce serveur permettrait à une personne extérieure au site d'accéder directement à la couche dédiée à la supervision. L'architecture de l'infrastructure est donc à revoir. Enfin la situation géographique des serveurs redondés est importante ; une catastrophe naturelle pourrait entraîner une indisponibilité des données.

La solution WinCC Portal V7.4 comporte comme la solution PROFINET, des failles de sécurité critique. De la fuite de données à la destruction d'informations en passant par la compromission des données est à craindre avec la solution WinCC Portal. Des logiciels malveillants pourront être installés via l'application ou par le biais des ports USB. Le manque de protection physique

permettrait d'y accéder facilement. La fuite d'informations par des personnes non-autorisées est un scénario envisageable.

Les tablettes Advanced HMI MOBILE PANEL KTP900F Mobile disposent quant à elles d'un écran. Une fuite de données est tout à fait possible par le biais de regards indiscrets. La tablette comporte aussi un port USB. L'installation de logiciels malveillants par l'entré USB est à redouter pour l'intégrité des données et leurs disponibilités. Le stockage des tablettes sans surveillance, le manque de protection ou encore l'utilisation de ces tablettes en-dehors de l'entreprise permettraient de modifier les composants afin de récupérer les données ou de saboter la chaîne de production. Enfin le manque de contrôle d'accès permettrait à un utilisateur non-autorisé de se connecter à la tablette.

Le réseau WIFI pourrait se faire pirater. Les utilisateurs pouvant se connecter au réseau WIFI avec leurs appareils personnels pourraient saturer le réseau et importer des logiciels malveillants. L'accès aux composants physiques pourrait perturber les trames ce qui altérerait l'intégrité et la disponibilité des données. Des brouilleurs pourront stopper l'émission du signal WIFI. Le manque de sécurité tels que mot de passe trop faible ou algorithme WPE entraineraîent une attaque sur le WIFI pour récupérer des informations (adresse MAC, IP). Des attaques du type DDOS, Evil twin ou encore de Man in the middle permettraient de voler des informations confidentielles.

Les postes de travail et pupitres laissés sans surveillance pourront être volés ou hackés. La suppression de logiciel ou le remplacement de composant est aussi un scénario d'attaque. Une indisponibilité des postes de travail et pupitres entraînerait une perte d'activité. Le vol de composant sans sécurité ou chiffrement est redouté. La non mise à jour des logiciels sur les postes de travail et les pupitres est un vecteur d'attaque important.

Avec le logiciel SIMATIC Logon, sans authentification, pourrait déboucher sur de la fuite d'information. L'interception de données pourrait entraver la confidentialité et l'intégrité des données ainsi que leur disponibilité. L'absence de chiffrement permettrait de lire les trames réseaux. L'utilisation d'anciennes versions du logiciel comportant des failles de sécurité pourrait engendrer une fuite dans la confidentialité des données. Enfin le manque de protection physique des équipements permettrait à un utilisateur non autorisé de brancher ou débrancher des appareils, de modifier des composants et d'y installer des logiciels malveillants.

Le site SIEMENS permettra de faire les mises à jour des systèmes d'information. L'indisponibilité du site internet du constructeur suite à un DDOS, une attaque informatique ou un problème de réseau de l'entreprise empêchera la mise à jour de se faire.

Dans cette première partie, les différents scénarii d'attaque ont été expliqués. Le tableau récapitulatif permet d'avoir une vue globale des attaques en ajoutant la gravité et la vraisemblance de ces attaques (annexe page 27). Nous avons considéré pour chaque équipement que les mesures de sécurité étaient au plus bas. Nous allons voir dans la partie suivante quelles sont les mesures à mettre en place, comment les mettre en place et l'importance de leur mise en place.

Partie 2 : Mesures de sécurité

2/ A partir des conclusions de l'analyse de risque, il vous est demandé de proposer des mesures de sécurité pour réduire l'impact et/ou la vraisemblance des risques et leurs variantes dans les périodes d'exploitation et de maintenance de la chaîne de production.

Nous commençons par noter que la marque SIEMENS a été touchée par un ver informatique appelé Stuxnet en 2010. Ce ver espionnait et reprogrammait des systèmes industriels, ce qui comportait un risque élevé. Il ciblait spécifiquement les systèmes SCADA utilisés pour le contrôle commande de procédés industriels. Stuxnet est capable de reprogrammer des automates industriels (API) produit par Siemens et de camoufler ses modifications. Le virus s'attaque aux systèmes Windows à l'aide de quatre attaques « zero day » et vise les systèmes utilisant les logiciels SCADA WinCC/PCS 7 de Siemens. En juillet 2010, Siemens met à disposition de ses clients un outil capable de détecter et de supprimer Stuxnet. Plus récemment d'autres failles de sécurité, comme celles permettant d'accéder au DOS, ont été découvertes. Là encore le constructeur a mis en place des correctifs.

Pour le S7-1500 nous remarquons que le fournisseur propose des solutions de sécurité configurable lors de l'installation. La première étape que nous proposons est de désactiver les options par défaut et de mettre des mesures de sécurité en fonction de vos besoins. Ces mesures de sécurité sont facilement et clairement expliquées dans la documentation de la marque dans la rubrique « Protection » (annexe page 29). Nous conseillons d'activer, par exemple, les mesures suivantes :

Fonctions de protection	S7-1500	ET 200MP
Protection d'accès	✓	---
Protection Know-How	✓	---
Protection contre la copie	✓	---
Protection par verrouillage de la CPU/du module d'interface	✓	✓

Ces options se configurent avec des mots de passe lors du démarrage de la machine.

Protection d'accès par mot de passe pour l'écran

Vous paramétrez un mot de passe pour l'utilisation de l'écran dans les propriétés de la CPU dans STEP 7. L'accès en local est ainsi protégé par un mot de passe local.

Nous conseillons de générer des mots de passe d'au moins 12 caractères aléatoires, crées par un logiciel, comportant des minuscules, majuscules, chiffres et caractères spéciaux ainsi que de changer les mots de passe tous les 90 jours et enfin de les sauvegarder dans un logiciel de type KeePass, permettant la protection détaillée ci-dessous :

Les solutions annoncées sont très facilement réalisables et nécessitent peu de supervision.
Le S7-1500 comporte un écran tactile comme présenté sur l'image ci-dessous :

L'ajout d'un filtre de confidentialité sur l'écran a pour but d'empêcher la fuite d'information. L'importance de placer ce matériel dans une salle des machines avec des sécurités physiques telles que caméras de vidéosurveillance, badges pour accéder aux machines avec contrôle et sensibilisation des techniciens sont des solutions simples permettant de sécuriser le matériel.

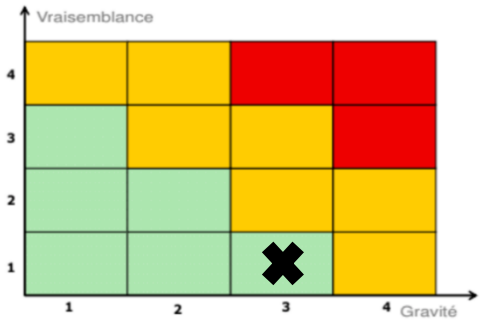
Le S7-1500 comporte peu de protection physique comme le montre l'image suivante :

Ce matériel placé dans une salle des machines avec contrôle et protection des connectiques permettrait de pallier une surcharge de courant électrique entraînant la surchauffe du matériel, le branchement de câble non autorisé, la casse, le sabotage ou encore vol du matériel.

L'équipement permet aussi d'avoir un serveur web et dispose d'enregistrement de documentation et de fichiers csv. Ici encore, pour le serveur web le constructeur a pensé mettre des mesures de sécurité comme la désactivation du serveur web, la désactivation de la communication PUT/GET, le changement d'adresse IP, protection pare-feu (voir annexe 30). Toutefois, pour compléter ces mesures de sécurité il est important d'interdire la navigation web aux utilisateurs non habilités sur cet appareil (interdiction de site web), limiter l'accès de navigation aux administrateurs, et interdire le téléchargement de fichiers Ensuite pour les fichiers csv et documentations nous recommandons de limiter les accès à certains profils habilités afin d'éviter d'accéder/importer des fichiers corrompus, des ransomwares, et d'ajouter une sécurité supplémentaire qui protège les documents.

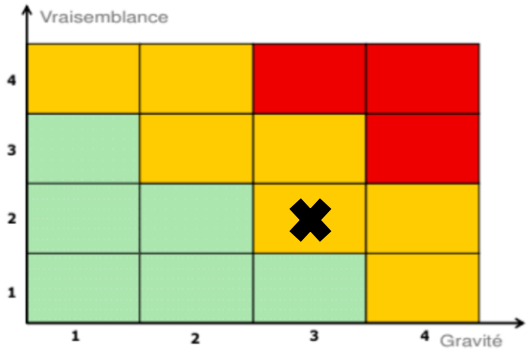
Dans un second temps, lors de la maintenance et/ou retrait du matériel, il faut garder à l'esprit que la chaîne de production ne pourra pas être arrêtée pour maintenance en-dehors des périodes estivales t/ou des périodes d'indisponibilité (exemple une panne). Il faut donc prévoir et anticiper en amont les tests avec des référentiels. Là encore SIEMENS intègre des mécanismes de diagnostic (annexe page 30) et de mise à jour. L'utilisation de ces fonctionnalités couplées avec des tests d'intrusion sont des mesures de sécurité importante à mettre en place. Toujours lors de la maintenance des appareils nous préconisons de bien chiffrer ou de supprimer les données contenues (csv, script) et de stocker le matériel dans un endroit sûr avec un contrôle d'accès par badges, caméras de surveillance et sensibilisation des techniciens. Enfin lors de l'effacement de données sur le matériel, le constructeur a encore pensé à des solutions (voir page 31). Il est important de noter que lors de l'effacement des données sur l'appareil certains paramètres confidentiels sont conservés. Nous recommandons donc la destruction de l'appareil avec des machines adéquates ou encore l'effacement de données aux différentes couches qui peuvent être mises en place grâce à la norme ISO 27040.

Pour conclure sur le S7-1500, les mesures de sécurité du constructeur permettent facilement d'installer des règles de sécurité importantes et continues. Les mesures proposées plus celles du constructeur nous situent dans le tableau de vraisemblance et gravité d'un scénario de risques :



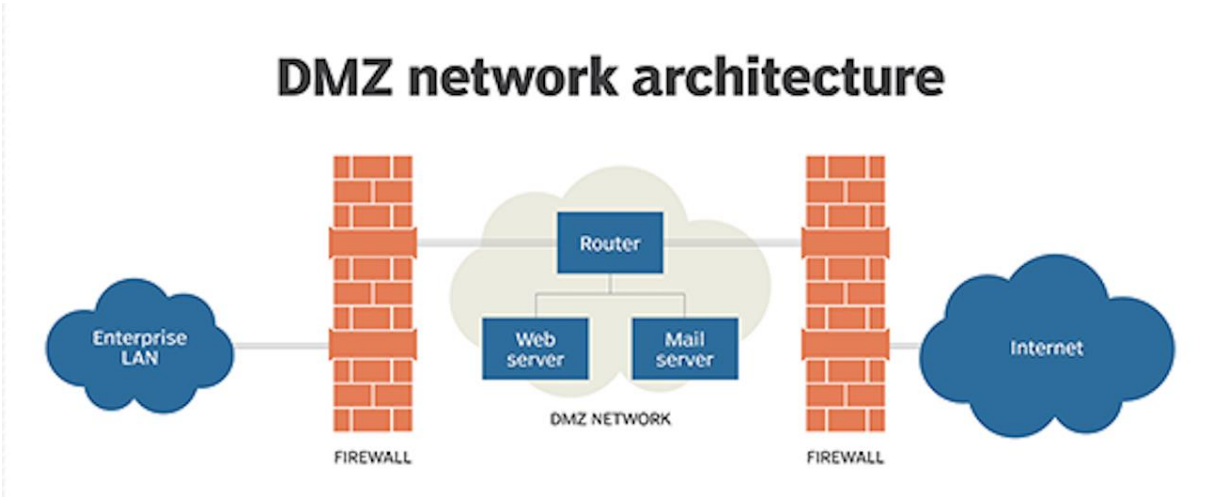
Les manques de sécurité sur le S7-1500 peuvent engendrer une perte de continuité d'activité, le vol de données et du sabotage. Cependant les mesures qui en découlent sont très faciles à mettre en place mais nécessitent de la supervision. Cela nous conduit donc à placer ce matériel en critère de sécurité vert.

Pour le réseau PROFINET et le réseau LAN, nous recommandons d'utiliser les mises à jour des logiciels avec test d'intrusion et référentiel. La désactivation des prises, serveurs et appareils inutiles au bon fonctionnement du réseau est indispensable. Pour pallier l'indisponibilité (DDOS, coupure de courant) nous proposons d'avoir des serveurs de secours et des générateurs électriques situés à des endroits différents géographiquement. Il est recommandé d'utiliser les solutions proposées par le constructeur PROFINET qui offre de la redondance de réseaux informatiques, du diagnostic flexible fournissant des informations sur la topologie du réseau et des périphériques. Une liste blanche des appareils et logiciels ayant le droit d'accéder au réseau ou une structure PKI (Public Key Infrastructure) sont vivement recommandés. Il est important de noter que le système PROFINET a révélé une faille de sécurité qui expose les produits de SIEMENS à une attaque DDOS. Nous recommandons de mettre à jour le système car le constructeur a mis en place un correctif (voir annexe page 30).
Enfin le serveur faisant l'interconnexion du réseau Ethernet (LAN) et le réseau PROFINET est redondé pour assurer une continuité de fonctionnement et d'activité. Nous préconisons de choisir des serveurs européens, d'utiliser des outils de détection des vulnérabilités, de placer les serveurs à des lieux géographiquement éloignés pour éviter qu'une catastrophe naturelle ou humaine entraînant l'arrêt des deux serveurs en même temps. De limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées puis de désactiver les services et logiciels non utilisés. Enfin effectuer des sauvegardes et les vérifier régulièrement sur le serveur permet de prévenir et de faire face aux situations difficiles. L'Installation de vlan pour séparer le réseau est recommandé. L'accès à ces serveurs (physique et virtuel) doit être contrôlé à l'aide d'un badge mais aussi couplé à une sécurité physique comme des codes d'accès et portes fermées à clef sont nécessaires.
Il faut également que l'adresse IP de ces serveurs, et les flux des informations y transitant soit chiffré. Une traçabilité des connexions par des fichiers de log, un load balancer pour prévenir des attaques DDOS sont des mesures nécessaires.
Toutes ces opérations de sécurité sont à mettre en place en période d'exploitation mais aussi en période de maintenance.
Pour conclure sur le réseau PROFINET et LAN, nous avons vu des mesures simples à mettre en place, qu'il s'agisse soit de corriger la faille de sécurité PROFINET ou encore soit pour protéger physiquement le réseau. Le serveur redondé faisant l'interconnexion entre les deux, nécessite des mesures de sécurité à surveillance régulière et doit être chiffré. Ainsi donc nous plaçons dans le tableau de vraisemblance et gravité d'un scénario de risques en critère orange.

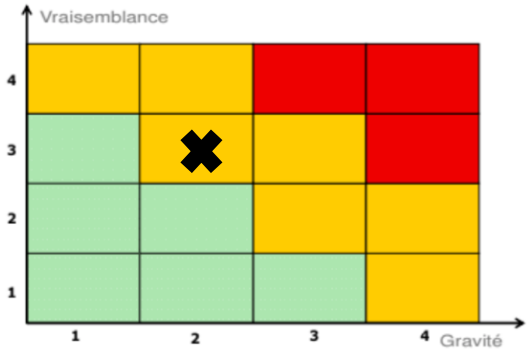


Le serveur Web interconnecte les couches de supervision et de surveillance externe. Il permet de mettre à disposition les informations de supervision à des clients légers Web se trouvant en dehors du site. Dans l'architecture retenue nous constatons que le serveur Web est situé au niveau de la couche supervision, cela présente une faille réelle de sécurité importante car un attaquant peut, s'il

arrive à prendre la main sur le serveur Web, accéder à la couche dédiée à la supervision. Les mesures de sécurité de base concernant l'architecture seraient de placer ce serveur Web dans une DMZ avec des pare feux pour protéger l'infrastructure interne de la société comme indiqué dans le schéma :

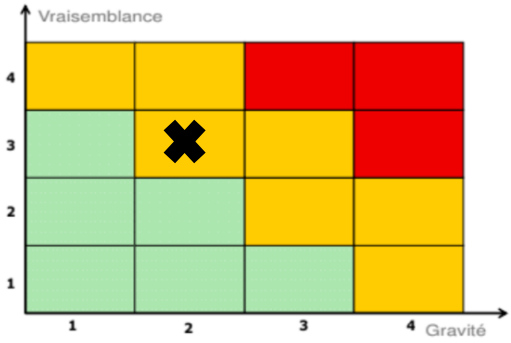


De plus l'utilisation d'authentification forte, de VPN professionnel pour les utilisateurs externes, de la gestion d'accès, de load balancer et de pare feu protègeront le site Web contre, la fuite d'informations sensibles, le DDOS et de l'interruption de service.
Comme évoqué précédemment, les mises à jour, détection de vulnérabilités, Secure By Design, enregistrement fichier de log et autres mesures de sécurité évoquées seront à mettre en place.
Enfin des tests d'intrusion et de bascule par rapport à un référentiel devront être mis en place pour garantir la sécurité du site Web et des utilisateurs.
Pour conclure, les mesures de sécurité proposées pour le serveur Web sont facilement implémentables et permettent de garder un niveau de sécurité convenable. Cependant l'installation du serveur Web dans la couche de supervision et non dans une DMZ constitue une faille critique pour la sécurité de l'infrastructure. Nous plaçons le niveau de sécurité dans le tableau de vraisemblance et gravité d'un scénario de risques en critère orange car les risques et l'exploitation de cette faille de sécurité sont critique cependant les solutions disponibles sont faciles à implémenter.



Le serveur d'enregistrement de la couche supervision, nécessitera les mêmes critères de sécurité que les autres serveurs vus précédemment. Nous ajouterons cependant du chiffrement sur les données qui seront situées sur le serveur, la sauvegarde régulière des fichiers de log ainsi la signature pour les fichiers. Toutefois le serveur devra comporter des ressources nécessaires pour stocker les données à enregistrer. Le risque de sécurité et d'exploitation de ces informations nous place dans un critère

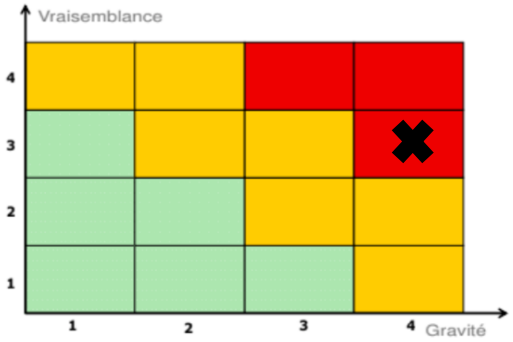
orange car la présence du serveur Web au même niveau que le serveur d'enregistrement augmente la vraisemblance de l'exploitation de ces données.



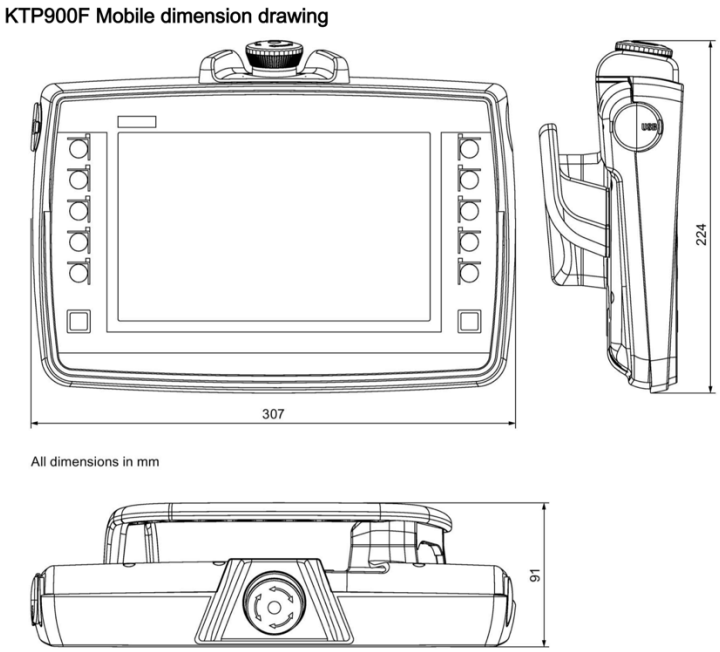
La solution WinCC Portal permettra la supervision du système. Cette solution sera mise en place sur les PC. La première mesure à prendre est de mettre à jour cette solution. En effet le constructeur a distribué un correctif permettant de corriger des vulnérabilités critiques dans ses produits SCADA. Notamment celles permettant à des utilisateurs non authentifiés d'exécuter à distance du code arbitraire sur un serveur SIMATIC WinCC SCADA. La faille a reçu l'indice 10 sur l'échelle de criticité CVSS (Common Vulnerability Scoring System), soit le plus élevé. Siemens a précisé dans un bulletin les produits affectés par les failles : plusieurs versions des solutions SIMANTIC WinCC et PCS 7, ainsi que toutes les versions du TIA Portal V13 avant la V13. L'activation des paramètres de base comme la redondance des serveurs, les tests d'audit durant la maintenance et des options de monitoring sont à mettre en place. Les solutions WinCC sont livrées avec un kit qui permet de coder en C# et C++.

La mise en place de test d'intrusion sera obligatoire. Une surveillance quotidienne et rigoureuse est importante pour la sécurité du système d'information pour ce logiciel. Ensuite la sécurisation des postes de travail est nécessaire. Les solutions de sécurité de base telles que l'utilisation de filtres de confidentialité, l'attachement des postes de travail avec des câbles de sécurité, la désactivation des ports. L'authentification par mot de passe et carte PKI, le renouvellement des mots de passe tous les 90 jours, la sensibilisation des collaborateurs est indispensable. Il faut procéder à l'installation des correctifs de sécurité, aux chiffrements des disques durs, à la limitation de tentative d'accès, aux verrouillages des PC après inactivation et enfin à l'utilisation de deux postes de travail. L'équipe de développement devra elle aussi respecter des règles de sécurité. Les documents confidentiels devront être rangés et sauvegardés pour éviter la fuite d'informations. La sensibilisation aux règles de sécurité par des formations qui devront être suivies par l'équipe. L'interdiction d'accéder à certains sites internet et de télécharger des logiciels devront être validés par des administrateurs et l'équipe sécurité. L'utilisation de gestionnaires de mot de passe, de droit d'accès, de logiciels permettant l'accès au code. Une copie du code sera réalisée pour pallier l'indisponibilité des serveurs. L'utilisation d'API sans faille lors de développement de code par l'équipe, l'utilisation de référentiels et la limitation de matériel qui permettent d'enregistrer (Google, Siri) sont des bonnes pratiques à mettre en place. Nous recommandons fortement d'interdire l'accès direct des PC à la couche de supervision et d'éviter toutes liaisons directes car il s'agit d'une opportunité pour un attaquant d'accéder au serveur de supervision et d'infecter le poste de travail d'un développeur. L'utilisation de serveurs de rebond permettraient de rajouter une couche de sécurité. Enfin le contrôle bienveillant d'une tierce personne sur les activités des développeurs serait une solution de sécurité supplémentaire pour s'assurer du respect des bonnes pratiques.

Pour conclure, les failles de sécurité du logiciel WinCC présentent premièrement des risques d'attaque qui permettent aux attaquants de prendre la main sur le système et de pouvoir exécuter du code à distance. Deuxièmement les solutions énoncées pour pallier les manques de sécurité des postes et de l'équipe de développement sont facilement réalisables mais nécessitent des contrôles permanents et rigoureux. Ainsi donc nous plaçons dans le tableau de vraisemblance et gravité d'un scénario de risques en termes de sécurité en critère rouge.



Les tablettes Advanced HMI Mobile Panel SIMATIC HMI KTP900F Mobile (référence : 6AV2125-2JB23-0AX0) servent à la surveillance des équipements lors de leurs rondes et des opérations de maintenance. Ce modèle ne dispose pas de capacité native de connexion Wifi. Pour y pallier, il sera utilisé un équipement inséré dans le port USB.

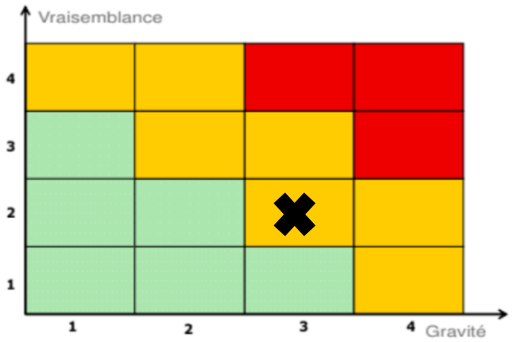


Les tablettes disposeront de filtre de confidentialité pour éviter la fuite d'informations. Elles devront être stockées dans des lieux avec du contrôle d'accès, de la vidéosurveillance, du contrôle de numéro de série, des puces de géolocalisation, du déverrouillage par mot de passe fort (12 caractères, etc…).

Elles doivent faire l'objet de contrôles, de tests d'intrusions à mettre en place régulièrement en suivant des référentiels. Il faudra mettre en place de l'authentification, des comptes individuels devront être présents, du verrouillage automatique ainsi que la sensibilisation des techniciens en sécurité informatique. Le port USB devra servir exclusivement à l'utilisation du matériel pour se connecter au wifi. Nous recommandons de sceller ces deux matériels pour éviter que tout autre logiciel et matériel puissent nuire à la sécurité du système d'information. De plus nous ajouterons une sécurité qui permettra de désactiver le port USB, si ce n'est pas le matériel qui permet de se connecter au wifi. Cependant, la solution de sécurité optimale consistera à changer les tablettes pour un modèle qui possèderait des capacités de connexion wifi. La connexion au réseau wifi devra se faire par authentification entre la tablette et le wifi de l'entreprise pour éviter tout piratage, comme une attaque de l'homme au milieu ou du jumeau maléfique. En ce qui concerne le maintien et le retrait des tablettes, nous préconisons de bien chiffrer ou de supprimer les données qui y sont contenues et de stocker le matériel dans un endroit sûr avec un contrôle d'accès par badge et caméra de vidéosurveillance.

Pour le réseau Wifi nous conseillons d'activer les normes de sécurité WPA-3 entreprise avec du chiffrement AES 192 bits et un mot de passe généré par KeePass, plusieurs bornes de secours pour éviter une attaque DDOS, des mécanismes pour éviter le spoofing, une identification des appareils connectés au réseau wifi avec une authentification avec l'active directory. Il faut également limiter les accès aux réseaux wifi de l'entreprise avec interdiction de certains sites internet. La mise en place d'un second réseaux wifi pour les collaborateurs à destination de leurs appareils personnels serait une bonne pratique. Le matériel physique (borne, routeur) doit avoir des protections physiques pour qu'on ne puisse pas ajouter ou débrancher des connectiques. Il ne faut laisser que les logiciels nécessaires pour se connecter au WIFI. Une sauvegarde des connexions infructueuse ou fructueuse devra être mis en place.

Pour résumer, sur les tablettes Advanced HMI Mobile Panel SIMATIC HMI KTP900F et le réseau wifi, les vulnérabilités énoncées et des précautions à mettre sur celles-ci et le wifi placent la sécurité en critère orange dans le tableau de vraisemblance et gravité d'un scénario de risques.



La solution SIMATIC Logon permettra la connexion avec le système de supervision, à relier à l'Active directory de l'entreprise. Le constructeur a pensé mettre des mesures de sécurité telles que :

Exigences importantes

Les exigences importantes permettant la validation d'installations sont les suivantes :

- la gestion des utilisateurs en vue d'accorder les droits d'accès afin que les accès non autorisés ou non intentionnels à l'installation soient impossibles,
- la création et l'archivage de justificatifs relatifs à des actions importantes ou critiques.

Enregistrement des événements

SIMATIC Logon enregistre les événements suivants avec SIMATIC Logon Eventlog Viewer :

- connexion aboutie,
- tentative avortée de connexion,
- authentification d'un utilisateur,
- déconnexion par l'utilisateur,
- déconnexion automatique,
- changement de mot de passe.

Nous recommandons d'installer ces mesures de sécurité pour avoir un premier niveau de sécurité et une traçabilité des événements. La mise à jour du logiciel couplée à des tests d'intrusions à intervalles réguliers sont nécessaires pour garantir un niveau de sécurité convenable. Les mesures de sécurité pour les mots de passe énoncés plus haut s'appliquent aussi dans notre situation (mot de passe à 12 caractères, renouvellement tous les 90 jours, limite de tentatives). Les communications entre les différents services devront être chiffrées en utilisant du LDAPS et non du LDAP. Il faudra limiter le nombre de comptes administrateur pour éviter la fuite d'information. La sauvegarde des données sur des serveurs internes devra être chiffrée et faite régulièrement. Enfin l'architecture de l'active directory doit être bien pensée pour pallier des failles de sécurité conceptuelles. Le constructeur a aussi pensé à la possibilité de signer les requêtes.

SIMATIC Electronic Signature

SIMATIC Electronic Signature est le composant de *SIMATIC Logon* permettant de saisir une signature électronique. Cette signature électronique est un justificatif créé et archivé à la suite d'une requête configurée (entre autres, dans le cadre d'interventions importantes ou critiques au sein d'une installation d'automatisation).

Ces justificatifs contiennent des informations sur une opération, p. ex. :

- le nom de/des agent(s),
- la date et l'heure de l'opération à exécuter,
- la signification des signatures (p. ex. : autorisation),
- l'auteur (p. ex. d'une recette batch).

Exemple

Une signature électronique est requise dans le cadre de l'intervention configurée "Démarrer un moteur".

Pour finir SIMATIC Logon permet d'utiliser la solution WinCC.

Une association aux composants de SIMATIC Logon est réalisée p. ex. dans les applications suivantes :

- Automation License Manager
- WinCC
- SIMATIC BATCH
- STEP 7

Comme vu précédemment, la compatibilité avec le logiciel WinCC présente une menace importante au vu des vulnérabilités du logiciel. Nous déconseillons d'utiliser le logiciel antérieur à la version V4.5 et de renforcer le contrôle lié à ce logiciel.

Enfin les comptes utilisateurs des personnes qui ne se sont pas connectées depuis 45 jours devront être désactivés puis supprimés. De plus pour garantir une sécurité optimale, les applications qui utilisent l'Active Directory doivent avoir un certificat partagé pour valider l'échange d'informations. Au niveau physique, il faudra mettre en place les mesures de sécurité déjà évoquées pour les autres matériels (code d'accès au locaux, vidéosurveillance) et tout particulièrement vis-à-vis du lecteur de carte à puce que le logiciel possède.

5.4.3.3 Connexion via un lecteur de carte à puce

Introduction

SIMATIC Logon prend en charge la connexion à une application SIMATIC avec carte à puce à l'aide d'un lecteur de carte à puce.

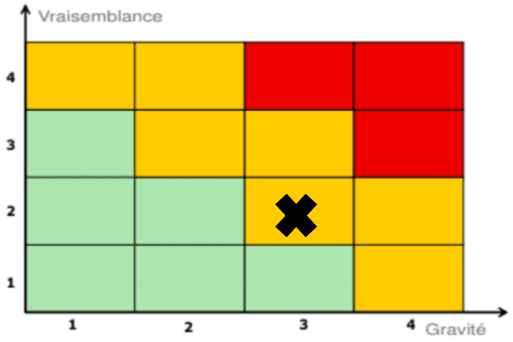
Ce paragraphe décrit les conditions à remplir et le mode de configuration de la carte à puce.

Remarque

Pour utiliser le lecteur de carte à puce comme appareil de connexion, **chaque** utilisateur doit disposer d'une telle carte.

Si cette option n'est pas utilisée il faudra souder le lecteur ou désactiver l'option. En cas de maintenance ou de retrait, les données devront être sauvegardées et chiffrées.

Pour résumer sur le logiciel SIMATIC Logon et l'Active Directory, la mise en place des solutions de sécurité au regard des failles du logiciel WinCC ainsi que les recommandations faites par le constructeur et par l'analyse de risques nous placent, en termes de sécurité, en critère orange dans le tableau de vraisemblance et gravité d'un scénario de risques.

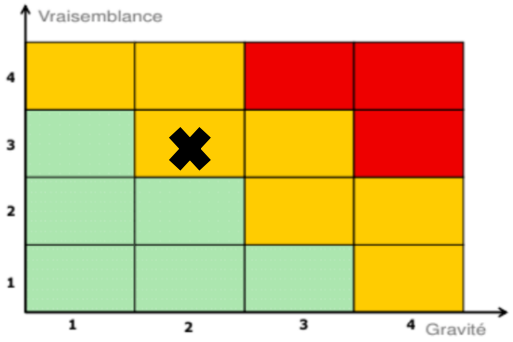


Les pupitres de la gamme Comfort SIMATIC HMI seront utilisés pour les postes de travail. Le constructeur prévoit dans l'usage de ces pupitres les options suivantes :

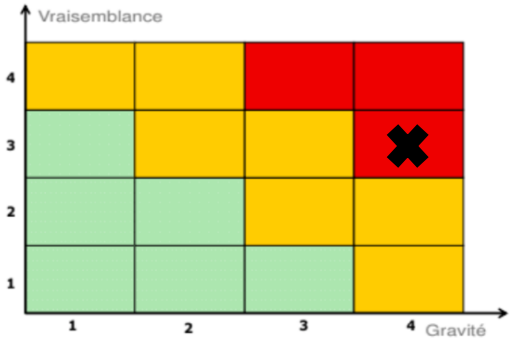
Comfort Panel :
La gamme Comfort SIMATIC propose des pupitres de dernière génération, innovants, très robustes, avec des fonctions HMI évoluées (Archives, scripts, viewers...) et homogènes sur la gamme.
- Écran large, 16 millions de couleurs, luminosité ajustable (LEDs).
- Interfaces : 1 port PROFIBUS, 1 ou 2 ports PROFINET, 2 ou 3 ports USB, port Audio (à partir du 7").
- Robuste : cadre en aluminium à partir de 7" et utilisable en Zone ATEX 2 et 22 (nous consulter).
- PROFIenergy (jusqu'à 80 % d'économie d'énergie durant les temps de pause).
- Nouvelles fonctionnalités de transfert d'applications (via Mini USB et carte SD).
- Outil de programmation : TIA PORTAL

Nous remarquons que le constructeur prévoit la compatibilité avec le réseau PROFINET et met à disposition des ports USB, mini USB, carte SD ainsi que l'outil de programmation TIA PORTAL. La première mesure serait de désactiver les ports cités au-dessus pour éviter la fuite d'information et des logiciels malveillants insérés dans les pupitres. Un filtre de confidentialité devra être installé sur les écrans. Les failles de sécurité sur PROFINET et TIA PORTAL 13 sont de grandes menaces qui doivent être prises en compte. La mise à jour des logiciels et l'installation des correctifs de sécurité doivent être faits pour pouvoir utiliser les pupitres. Des protections physiques comme des câbles de sécurité sont nécessaires. La connexion avec HMI doit se faire avec un mot de passe. De plus, il faudra sensibiliser les intervenants, limiter le nombre de tentatives de connexion et chiffrer les disques. Lors de la maintenance, de la sauvegarde des données, le chiffrement des données est nécessaire. Des tests d'intrusions doivent être fait pour s'assurer de la sécurité. Pour la suppression des données, les mesures de sécurité telles que la destruction du matériel ou l'effacement des données à plusieurs couches seront mises en place.

Pour conclure sur les pupitres de la gamme Comfort SIMATIC HMI, nous avons vu des mesures simples à prendre, qu'il s'agisse de corriger la faille de sécurité PROFINET et de TIA PORTAL ou encore pour protéger physiquement le matériel. Ainsi donc nous plaçons dans le tableau de vraisemblance et gravité d'un scénario de risques en termes de sécurité, en critère orange.



Le site SIEMENS permettra de faire la mise à jour des produits et logiciels. Cette méthode de mise à jour via le site n'est pas recommandée. En effet, si le site du constructeur est en maintenance, subit une attaque ou se fait pirater, le système d'information ne pourra pas bénéficier du correctif. L'indisponibilité du constructeur à nous transmettre ce correctif peut engendre de sérieux problèmes de sécurité. Nous recommandons d'avoir des programmes automatiques qui permettent de savoir si un correctif est disponible et de le télécharger aussitôt, d'analyser les paquets des mises à jour du constructeur pour vérifier qu'il n'y ait pas de malwares. Une autre source permettant d'accéder aux correctifs serait une mesure de sécurité efficace. Le manque de solutions et de redondance pour accéder aux solutions et correctifs du constructeur nous place en critère de sécurité rouge dans le tableau de vraisemblance et gravité d'un scénario de risques.



Pour conclure si la maintenance est faite par un sous-traitant ou encore qu'elle nécessite un déplacement du matériel, nous insistons fortement sur les points suivants : sensibiliser les sous-traitants à la sécurité informatique et imposer une charte de sécurité. Mettre en place des formations de sécurité à destination des sous-traitants. Sécuriser le transport des pièces et matériels par un traçage de suivi, chiffrer les données sortantes, s'assurer du suivi des procédures, supprimer les données sortantes et le faire à différentes couches. Pour les logiciels il faut bien prendre en compte les APIs qu'on utilise, en faire une sauvegarde complète et chiffrer des données. Mettre à jour et prendre soin des outils qui servent à la maintenance, faire du contrôle avec des référentiels, faire de l'inventaire, sécuriser l'accès, avoir des stocks et des pièces de rechange sous scellé pour garantir la disponibilité des pièces. La centralisation et la création d'alertes en cas d'événements est conseillé. Utiliser les équipements recommandés par l'ANSSI. Tester le nouveau matériel avec un référentiel en veillant à la perte, casse. Il faudra prévoir des tests d'intrusion en amont et suivre les référentiels car la chaîne de production ne pourra pas être arrêtée pour maintenance en dehors des périodes estivales de nettoyage et/ou des périodes d'indisponibilité suite à une panne. La maintenance des serveurs devra se faire une par une pour garantir la continuité de service. Toutes les mesures proposées permettent de limiter la surface d'attaque mais ne garantissent pas une sécurité des

systèmes d'information entière. L'importance de savoir ce qui doit être surveillé et les risques qui en découlent permettent de mieux se préparer en cas de crise. Des plans de continuité d'activité et de reprise d'activité seront à mettre en place pour garantir un niveau de sécurité en cas de crise importante. L'importance des sauvegardes, des serveurs redondants permettra une reprise d'activité plus rapide et mieux organisée.

Partie 3 : Actions à réaliser

3/ Compte tenu des constats réalisés aux questions 1 et 2, indiquez les actions à réaliser sur l'ensemble du cycle de vie des équipements, d'une part, et sur celui de la chaîne de production, d'autre part, pour garantir leurs besoins de sécurité

L'étude de la question 2 nous a permis de préconiser des mesures de sécurité sur la période d'exploitation et de maintenance.

Nous présenterons dans cette partie, sous la forme d'un tableau, les besoins de sécurité à mettre en place pour les autres périodes du cycle de vie.

	Conception
Matériel Logicielle	• Mise en place d'un référentiel • Définition des enjeux • Sensibilisation et formation à la cybersécurité • Niveau de confidentialité des documents • Sécuriser les documents confidentiels • Gestion d'accès aux différents documents de conception • Sauvegardes • Chiffrement • Choix du sous-traitant • Cycle de vie du document • Génie logiciel • Contre la fuite d'infos : vérifier les résultats dans les moteurs de recherche • Segmenter le réseau et mettre en place des zones • Sécuriser les dépôts pour les logiciels • Signature numérique

	Fabrication
Matériel	• Fabrication des pièces • Référentiel • Gestion d'accès au matériel • Contrôles d'intégrité • Test /Test d'intrusion • Matériaux robustes • Antivol, faire attention contre la casse • Assurer le transport des matériaux (suivi, signature), mettre en sous-scellé • Se mettre d'accord sur le rôle de sécurité des sous-traitants (s'assurer qu'il ne vole pas le savoir, règles strictes)
Logiciel	• S'assurer que les APIs n'ont pas de failles • Gestion d'accès au code • Utilisation saine de logiciels à jour • Mettre en place un référentiel et s'y tenir, le mettre à jour si nécessaire • Backup (avec signature) • Deux postes pour les développeurs (un seul avec le projet dessus) • Pas de copier-coller de code d'internet • Définition de bonnes pratiques de développement (éventuellement formations pour les développeurs) • Imposer du contrôle automatisé ou humain (RÉFÉRENTIEL) • Prendre en compte l'environnement • PRA et PCA • Redondance • Contrôles d'intégrité • Test unitaire/Test d'intrusion • Vérifier/tester les mises à jour • Faire de préférence des serveurs européens (Cloud Act) • Sécuriser les postes de travail • Savoir qui a qu'elle droit • Autoriser la connexion au réseau de l'entité aux seuls équipements de l'entreprise • Segmenter le réseau et mettre en place des zones

	Intégration
Matériel	• Référentiel des pièces • Plan de configuration • Gestion d'accès aux pièces • Suivre le plan de construction • Inventaire • Vidéosurveillance • Sceller les pièces • Assurer le transport de pièces/matériel (suivi, signature), mettre en sous-scellé • Contrôles d'intégrité des pièces • Sécuriser le stockage : changement de pièces, vol des composants, destruction des composants, perte, casse, logiciels espions • S'assurer que les sous-traitants aient respecté leur part de sécurité
Logiciel	• S'assurer que les APIs n'ont pas de failles (mises à jour des APIs) • Protection du réseau (MITM, DDoS, signatures numériques, PKI) • S'assurer que les sous-traitants aient respecté leur part de sécurité • Assurer le transport de données (suivi, signature), attention aux Backdoors, etc... • Test/d'intrusion intelligent • Savoir qui à quel droit • Savoir ce que l'on cherche • Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés • Chiffrer les données sensibles • Transmises par voie Internet • Segmenter le réseau et mettre en place des zones

	Retrait (mort)
Matériel	• Détruire le matériel (avec son propre système de destruction), s'assurer de la destruction • Backup des données • Démontage du matériel • Sécuriser l'accès au matériel • Vider/Détruire les disques • Entrepôt sécurisé • Contrôles
Logiciel	• Effacer les données dans les différentes couches • Sensibilisation/formations • Contrôles • Tests unitaires • Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés • Chiffrer les données sensibles transmises par voie Internet

Partie 4 : Maturité de sécurité

4/ Il vous est demandé de vous prononcer sur la maturité d'un point de vue cybersécurité des matériels de la marque SIEMENS.

Dans un premier temps, il est important de rappeler que les produits de la marques SIEMENS ont été victimes de plusieurs attaques informatiques dans le passé, que ce soit par le ver Stuxnet en 2010 en infectant les systèmes industriels SCADA, le logiciel WINCC en 2019 ou encore les systèmes PROFINET avec des versions antérieures à la V4.5.

Les failles de sécurité critiques sont nombreuses chez le constructeur et très récentes. L'importance de choisir l'ensemble des composants du même constructeur permet la compatibilité des composants et elle est plus facile à piloter.

De plus les correctifs et mises à jour sont disponibles seulement sur le site internet comme évoqué par la marque et énoncé au début du sujet.

La marque SIEMENS corrige les failles de sécurité sur les matériels et logiciels qui en ont besoin et met à disposition ce correctif sur son site internet. Le risque majeur de la solution proposée par le constructeur réside dans la disponibilité du correctif. Des problèmes de connexions réseaux, de DDOS et de piratage informatique du site internet peuvent empêcher de rendre ce correctif disponible dans son intégrité aux clients qui utilisent ces appareils.

Il aurait été plus judicieux, à mon sens, que SIEMENS notifie à ses les clients les nouvelles mises à jour et les correctifs lorsque qu'ils sont disponibles afin que les clients puissent les télécharger ou non.

En revanche, les produits matériels de la marque SIEMENS offrent des options de sécurité, de maintenance et de diagnostic. Certains constructeurs ne mettent pas la sécurité au premier plan, ce qui n'est pas la position la firme allemande. Elle propose, explique et notifie clairement dans la documentation les moyens et solutions à mettre en place lors de la configuration et de l'installation du matériel.

À noter qu'il est important de souligner que la marque SIEMENS est une marque allemande qui existe depuis 1847 de renommée mondiale avec des filiales présentes partout dans le monde. Enfin il faut dire également que *The Gartner* (entreprise américaine de conseil et de recherche dans le domaine des techniques) en 2017 et 2019 a placé SIEMENS parmi les leaders mondiaux du MES (Manufacturing Execution Systems) ce qui fait d'elle une entreprise leader dans son domaine.

De mon point de vue, je conseillerais d'utiliser les appareils de la marque SIEMENS comme les SIMATIC S7-1500 car leurs matériels respectent la norme IEC et les directives européennes. Ces appareils permettent d'avoir un contrôle d'accès avec gestion de mot de passe, système de protection de la mémoire en accès physique que ce soit par le biais d'une personne ou d'un logiciel lors du démarrage, protection du micro logiciel contre une mise à jour frauduleuse.

> De plus ces automates ont reçu la Certification de Sécurité de Premier Niveau (CSPN) prononcée par l'ANSSI le 25 avril 2016 (certificat ANSSI-CSPN-2016-5) qui atteste du niveau de sécurité de ces automates et qui prouve la pertinence des fonctions évaluées pour les besoins de la sécurité nationale et de la confiance résultant des processus de développement au sein de la marque SIEMENS.

En revanche en matière de cyber sécurité, le nombre de failles de sécurité critiques sur des anciennes versions mais aussi sur certaines versions récentes dans les logiciels WINCC, SCADA présentent un risque élevé et sont des éléments alarmants qu'il me semble important de rappeler et dont il faut tenir compte c'est pourquoi je ne recommande pas d'utiliser les logiciels de la firme allemande.

Ma recommandation est qu'il conviendrait d'utiliser un logiciel présentant un risque beaucoup moins élevé d'un point de vue intégrité, traçabilité et disponibilité tout en s'assurant de la bonne compatibilité avec le matériel SIEMENS. Malgré tout un risque le risque 0 n'existe pas.

Du côté maintenance SIEMENS offre des options de diagnostics et de tests sur ses appareils. En effet les tests lors de maintenances sont des opérations qui ne peuvent pas être négligées. Il s'agit d'un point fort. Le constructeur permet de faire des tests sur un produit qu'il connait et qu'il a conçu, basé sur un référentiel propre au constructeur. C'est un point lors de contrôle en période de maintenance sur le matériel pour ensuite enchainer sur des tests d'intrusion plus spécifique.

Pour conclure, malgré des faiblesses mises en lumière par le ver informatique Stuxnet et les vulnérabilités des logiciels du constructeur, les produits matériels de la marque SIEMENS sont des produits recommandés par l'ANSII. Ils mettent en place de la sécurité en profondeur. Il est classé dans les meilleurs MES par *The Gartner.* SIEMENS s'évertue, en outre, à mettre en service et à maintenir dans des conditions de sécurité sa progression constante via des équipes formées et compétentes. Pour ce faire, le géant allemand se base sur le référentiel de l'ANSSI concernant les prestataires d'intégration et de maintenance pour les systèmes industriels, garantissant d'un niveau de compétences particulièrement élevé. Une surveillance quotidienne du matériel et logiciel est nécessaire pour avoir un niveau de sécurité maximal. Ainsi les produits sécurisés, alliés à des mesures de mise en service et de maintenance optimisées, permettent à SIEMENS de s'imposer comme référent auprès des industriels soucieux de préparer sereinement l'homologation de leurs installations industrielles.

Annexes

Équipements concernés	Risques	Gravité	Vraisemblance
Disponibilité			
S7-1500, Réseaux filaires, PC WinCC, Écran Comfort, Tablettes	Perte ou modification de continuité d'activité/de la production (au niveau pilotage des actionneurs)	2	2
Réseaux, Serveur, PC WinCC, Écran Comfort, Tablettes, Logon	Atteinte à la bonne conduite de la supervision	1	2
Tout	Absence de surveillance	3	2
Réseaux filaires, réseau Wifi, Tablettes	Indisponibilité du réseau	2	3
S7-1500, Serveurs, PC WinCC, Écran Comfort, Tablettes, IHM	Injection de code malveillant	3	2
PC WinCC, Écran Comfort, Tablettes	Injection logicielle par port USB	3	2
S7-1500, Serveurs, PC WinCC, Écran Comfort, Tablettes, Logon	Compromission, sabotage, vol	4	1
Serveurs, reseaux filaire et Wifi	DDOS	2	4
IHM	Développement d'application malveillante	3	2

S7-1500, PC WinCC, Écran Comfort, Tablettes	Téléchargement de logicielles/ documentation	3	2
Confidentialité			
S7-1500, Réseaux, Serveurs, PC WinCC, Écran Comfort, Tablettes, IHM, Logon	Fuite d'informations	2	3
S7-1500, Réseaux, Serveurs, PC WinCC, Écran Comfort, Tablettes, Logon	Pas de contrôle d'accès	3	4
Réseaux, Serveurs, Réseau Wifi	Interception des communications	2	3
S7-1500, Serveurs, PC WinCC, Écran Comfort, Tablettes, IHM	Injection de code malveillant	3	2
PC WinCC, Écran Comfort, Tablettes	Injection de logiciel	3	2
S7-1500, Serveurs, PC WinCC, Écran Comfort, Tablettes	Corruption des appareils	4	1
S7-1500, Réseaux filaires, Serveur interco	Fuite d'informations lors de la remontée des paramètres	2	2
IHM	Développement d'application malveillante (Fuite d'informations)	3	2
S7-1500, PC WinCC, Écran Comfort, Tablettes	Téléchargement de mises à jour malveillantes	3	2
Tout	Manque de protection physique		
Intégrité			
Réseaux, Serveurs, PC WinCC, Écran Comfort, Tablettes, Réseau Wifi	Injection de faux messages et falsification d'informations	2	2

S7-1500, Réseau Profinet, Serveur interco	Remontée de mauvais paramètres vers la couche supervision	2	2
S7-1500, PC WinCC, Écran Comfort, Tablettes	Remplacement, effacement de logiciel	3	2
S7-1500, Serveurs, PC WinCC, Écran Comfort, Tablettes, IHM	Injection de code malveillant	3	2
PC WinCC, Écran Comfort, Tablettes	Injection logicielle (par USB)	3	2
IHM	Développement d'application malveillante	3	2
Tout	Coupure de courant	3	3
Traçabilité			
Tout	Effacement des fichiers de log		

9.2 Configurer la protection d'accès de la CPU

Introduction

La CPU offre quatre différents niveaux d'accès permettant de limiter l'accès à des fonctions déterminées.

En définissant le niveau d'accès et les mots de passe correspondants, vous restreignez les fonctions et les zones de mémoire qui sont accessibles sans saisie de mot de passe. Vous définissez les différents niveaux d'accès et les mots de passe associés dans les propriétés d'objet de la CPU.

Règles pour les mots de passe

Veillez à ce que le mot de passe soit suffisamment sûr. Tenez compte des règles suivantes :

- Choisissez un mot de passe d'une longueur minimum de 8 caractères.
- Mélangez différents types de caractères : lettres en majuscule et en minuscule, chiffres et caractères spéciaux.

Niveaux d'accès de la CPU

Tableau 9- 1 Niveaux d'accès et leurs limitations d'accès

Niveaux d'accès	Limitations des accès
Accès complet (pas de protection)	Chaque utilisateur peut lire et modifier la configuration matérielle et les blocs.
Accès en lecture	Ce niveau d'accès n'autorise, sans saisie de mot de passe, que l'accès en lecture à la configuration matérielle et aux blocs. Vous pouvez changer la configuration matérielle et les blocs dans la console de programmation. L'accès IHM et l'accès aux données de diagnostic est également possible. Sans saisie du mot de passe, vous n'avez pas la possibilité de charger de blocs ni de configuration matérielle dans les CPU. Sans saisie du mot de passe, les actions suivantes ne sont également **pas** possibles : fonctions de test en écriture et mise à jour du firmware (en ligne).
Accès IHM	Ce niveau d'accès, sans saisie de mot de passe, n'autorise que l'accès IHM et l'accès aux données de diagnostic. Sans saisie du mot de passe vous ne pouvez charger dans la CPU ni blocs, ni configuration matérielle ; vous ne pouvez pas non plus charger de blocs ni de configuration matérielle de la CPU vers la console de programmation. Sans saisie du mot de passe, les actions suivantes ne sont également **pas** possibles : Fonctions de test, changement d'état de fonctionnement (MARCHE/ARRET), mise à jour du firmware et affichage des résultats de comparaison en ligne/hors ligne.
Aucun accès (protection complète)	Si la CPU est entièrement protégée, l'accès en écriture ou en lecture à la configuration matérielle et aux blocs est impossible, sauf avec autorisation d'accès et mot de passe. L'accès IHM n'est pas possible non plus. La fonction de serveur pour la communication PUT/GET est désactivée pour ce niveau d'accès (non modifiable). La légitimation par le biais du mot de passe vous permet d'obtenir à nouveau un accès intégral à la CPU.

Vous trouverez une liste énumérant les fonctions possibles dans les différents niveaux d'accès sous l'entrée "Paramétrages possibles pour la protection" dans l'aide en ligne de STEP 7.

9.7 Protection par verrouillage de la CPU/du module d'interface

Possibilités de verrouillage

Protégez votre CPU/votre module d'interface des accès non autorisés (par ex. à la carte mémoire SIMATIC) en les munissant en outre d'un volet avant suffisamment sécurisé.

Vous avez p. ex. les possibilités suivantes :

- Placer un scellé
- Verrouillez le volet frontal avec un cadenas (diamètre de l'anse : 3 mm)

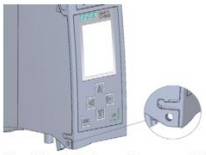


Figure 9-9 Patte de verrouillage sur une CPU

Secure Communication

En matière de communication, il existe de plus en plus un besoin de transférer des données sous forme chiffrée à des ordinateurs externes, par l'intranet ou des réseaux publics.

Les CPU SIMATIC S7-1500 et ET 200 à partir de la version 2.0 du firmware prennent en charge l'infrastructure à clé publique (PKI) Internet (RFC 5280) avec STEP 7 à partir de V14. Cela permet la configuration et l'utilisation de la communication sécurisée Secure Communication, par exemple :

- Hypertext Transfer Protocol Secure (HTTPS)
- Secure Open User Communication
- Secure Communication avec OPC UA

L'infrastructure à clé publique (PKI) peut délivrer, distribuer et vérifier des certificats numériques. Pour les CPU S7-1500, vous créez des certificats pour différentes applications dans les propriétés de la CPU dans STEP 7, par exemple : certificats TLS pour la communication Secure Open User Communication, certificats pour le serveur Web, certificats OPC UA.

Processeurs de communication à fonctions de sécurité intégrées

Pour des exigences spécifiques de votre installation, vous utiliserez des processeurs de communication à fonctions de sécurité intégrées, par exemple la protection d'accès par pare-feu, la protection contre la manipulation des données par VPN, FTPS, HTTPS, SNMPv3 et NTP sécurisé.

Avantages pour le client

Les fonctions de protection ci-dessus assurent la protection de vos investissements contre les accès et les modifications non autorisés, améliorant ainsi la disponibilité de l'installation de sécurité.

Mesures complémentaires de protection de la CPU

Les mesures suivantes améliorent considérablement la protection contre les accès non autorisés de l'extérieur et du réseau aux fonctions et données de la CPU S7-1500 :

- Désactivation du serveur Web
- Désactivation du serveur OPC UA (pour plus d'informations sur les mécanismes de sécurité pour OPC UA Server, voir la description fonctionnelle Communication (https://support.industry.siemens.com/cs/de/de/view/59192925/fr))
- Désactivation de la synchronisation de l'heure à l'aide du serveur NTP
- Désactivation de la communication PUT/GET

L'utilisation du serveur Web permet de protéger votre système d'automatisation S7-1500 contre les accès non autorisés :

- en vous donnant la possibilité de paramétrer, dans la gestion des utilisateurs, des droits d'accès protégés par mot de passe pour certains utilisateurs ;
- en vous permettant d'utiliser l'option prédéfinie "Autoriser l'accès uniquement via HTTPS".
  Cette option autorise l'accès au serveur Web uniquement avec le protocole de transmission sécurisé HTTPS.

3.4.6 Diagnostic

Dans le système d'automatisation SIMATIC S7-1500, le diagnostic intégré est présent à tous les niveaux de l'automatisation. Tous les produits SIMATIC possèdent des fonctions de diagnostic intégrées qui permettent une analyse et une localisation efficaces des défauts. Vous raccourcissez ainsi les temps de mise en service et réduisez les temps d'arrêt de la production.

Un concept de signalisation homogène permet de visualiser les messages d'erreur dans STEP 7, sur l'IHM, dans le serveur Web et sur l'écran de la CPU sous forme identique de textes en clair.

Vous pouvez également configurer des diagnostics de machines et d'installations. La logique de ces messages ou surveillances du diagnostic de processus dépend alors directement de l'état des installations et est définie par vous.

Modifier l'adresse IP d'un serveur NTP dans le programme utilisateur

Tâche d'automatisation

Vous changez de serveur NTP dans votre réseau. Le nouveau serveur a l'adresse "192.168.1.10".

Vous voulez modifier par le biais du programme utilisateur l'adresse IP du serveur NTP avec lequel votre CPU se synchronise.

L'exemple montre comment modifier l'adresse IP du serveur NTP en "192.168.1.10" avec l'instruction "T_CONFIG" dans le programme utilisateur.

Possibilités de test

- Test avec la visualisation de l'état du programme
- Test avec points d'arrêt
- Test avec la table de visualisation
- Test avec la table de forçage permanent
- Test avec la table des variables API
- Test avec l'éditeur de blocs de données
- Test avec le test de clignotement de LED
- Test avec la fonction Trace

Tableau 11- 5Objets mémoire après un effacement général

Objet mémoire	Contenu
Valeurs effectives des blocs de données, blocs de données d'instance	Initialisé
Mémentos, temporisations et compteurs	Initialisé
Variables rémanentes d'objets technologiques (p. ex. valeurs de référencement de codeurs absolus)	Conservé
Entrées dans le tampon de diagnostic	Conservé
Adresse IP	Conservé
Nom d'appareil	Conservé
Valeurs des compteurs d'heures de fonctionnement	Conservé
Heure	Conservé

- Effacement général de la CPU : automatique et manuel
- Sauvegarde et restauration de la configuration de la CPU
- Synchronisation de l'heure
- Données d'identification et de maintenance

Siemens Security Advisory by Siemens ProductCERT

SSA-780073: Denial-of-Service Vulnerability in PROFINET Devices via DCE-RPC Packets

Publication Date: 2020-02-11
Last Update: 2020-03-12
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

PROFINET Driver for Controller: All Versions < V2.1	Update to V2.1 Patch 03 https://support.industry.siemens.com/cs/ww/en/view/109768047/

Objet: SCADA Multiples vulnérabilités dans Siemens WinCC OA

GESTION DU DOCUMENT

Référence	CERTFR-2019-AVI-078
Titre	SCADA Multiples vulnérabilités dans Siemens WinCC OA
Date de la première version	26 février 2019
Date de la dernière version	26 février 2019
Source(s)	Bulletin de sécurité Siemens ssa-844562 du 25 février 2019
Pièce(s) jointe(s)	Aucune(s)

RISQUE(S)

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité des données
- Élévation de privilèges

RÉSUMÉ

De multiples vulnérabilités ont été découvertes dans Siemens WinCC OA. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges.

SOLUTION

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).