MOPS:
Analyse de risques
FONDERIE

Master 2 Cybersécurité

2018 - 2019

Encadré par :
Eric BORNETTE

Réalisé par :
Manon DEROCLES
Alexis LE MASLE

Table des Matières

I. Définition du périmètre du système et besoin de la société

1. Système de sécurité

a. Sécurité physique

Le site est totalement clos et il n'existe qu'une entrée/sortie possible. Le site est fermé par un périmètre de cinq cent mètres de long en forme de carré par trois mètres de grillage de haut. L'entrée est gardée par trois barrières automatique pour les véhicules, et par huit tourniquets pour les piétons. Il y a vingt-cinq personnes attribuées à la sécurité. Les matériaux précieux présents sur le site sont stockés dans des armoires fortes.

b. Sécurité non physique

La Fonderie possède un système d'identification en RFID basé sur des cartes Mifare 1k classic qui utilisent un protocole de sécurité propriétaire appelé CRYPTO1. Pour entrer dans le site il faut l'une de ces carte Mifare attribuée aux employés, si elle est valide cela autorise un tour du tourniquet qui permet l'accès du site. Pour entrer dans les bâtiments à l'intérieur du site, il faut de-nouveau utiliser le badge RFID ainsi qu'un code spécifique à chaque bâtiment. Pour se connecter sur un poste de travail dans les pièces à forte sécurité, il faut utiliser le même code que celui pour rentrer dans le bâtiment. Pour les pièces à moyenne sécurité il faut récupérer les clés qui sont dans des coffres à clé mécanique.

2. Le besoin

La société a besoin de garantir une certaine sécurité puisqu'elle s'occupe de contrats sensible incluant des contrats classés secret défense. L'entreprise doit s'assurer que les puces et les designs de celles-ci soient protégées contre des attaques d'un certain niveau. En ne respectant pas ses engagements, la société risque de perdre ses contrats importants, d'aller en justice ou de nuire à son pays de pars la nature des contrats.

II. Détermination des biens et caractérisation de leur valeur

1. Biens matériels

Pour la production de puces, il est nécessaire d'avoir en disponibilité certains composants. En effet la production de composants électronique nécessite des matériaux précieux, comme l'or ou l'argent. Ces matériaux sont coûteux et leur prix varie en fonction du marché actuelle. L'entreprise stock l'équivalent de trois mois de production en matières premières, ce qui équivaut à soixante kilogrammes d'or. Au prix du marché ces biens valent $2\,520\,000\,€$. Tous les mois la Fonderie s'apprivoise de nouveaux en matières premières pour pouvoir maintenir son stock de trois mois de production d'avance.

2. Biens intellectuels

La Fonderie possède des modèles de puces propriétaire, où l'intérêt premier est le secret, la confidentialité de leur fonctionnement. Les plans de ces puces sont estimés entre $150\,000€$ et $200\,000€$. Néanmoins, les contrats comme ceux de la défense reposent sur le faits que ces plans soient secrets, s'ils ne le sont plus, l'entreprise risque de perdre les contrats ainsi que leur revenu principal.

III. Identifier les menaces

Nous avons identifié trois menaces potentielles.

1. Entreprise concurrente

Une entreprise concurrente peut vouloir faire perdre la crédibilité et le sérieux de l'entreprise en faisant fuiter les concepts des composants. Cela provoquerait une perte du contrat avec l'état et potentiellement le récupérer.

2. Braqueurs

Une ou plusieurs personnes pourraient tenter de s'infiltrer dans l'entreprise pour voler l'or de l'armoire forte dans un but personnel. Le butin pouvant atteindre les 2,3 millions d'euros.

3. Attaque d'état

Un autre état ou organisation pourrait vouloir nuire à l'état en volant les secrets des designs de l'entreprise et ainsi affaiblir le pays par le biais de ses composantes cryptographique dont le secret pourrait être dévoilé.

IV. Les vulnérabilités

1. Mifare 1k classic

Il existe une faille sur les cartes Mifare 1k classic permettant l'accès aux mots de passes stockés dans cette carte ainsi que la copie de toutes les données contenue. Cette vulnérabilité rend obsolète son utilisation comme système de sécurité.

2. Codes d'accès aux bureaux

Une vulnérabilité se présente aussi au niveau de l'accès aux bureaux. Un code permettant d'ouvrir le bâtiment et la porte d'un bureau semble inutile et potentiellement insécurisé. Un attaquant ayant vu ou copié le mot de passe de la carte d'un employé à l'entrée de ce bâtiment pourra par la suite accéder au bureau aussi comme si aucun mot de passe n'était nécessaire.

3. Entrées/Sorties du site

L'entreprise ne vérifie pas les sorties du site. Si un attaquant vole les identifiants d'un employé sur une carte Mifare, il pourra entrer sur le site (ou dans un bâtiment, bureau…) alors que l'employé est déjà sur le site.

V. Faits redoutés et scénarios de risques.

1. Faits redoutés

- La faille découverte dans l'algorithme Crypto1 peut provoquer le "Cassage" de la carte RFID des employés et l'intrusion d'un individu dans l'enceinte sécurisé de l'entreprise.

- Possibilité de vol des données de la carte RFID d'un responsable ayant accès aux armoires fortes contenant les métaux précieux.

- Avec le vol des données d'identification et d'authentification, le risque peut être l'accès aux bureaux fortement sécurisé des bâtiments. Par exemple le bureau d'ingénierie où se trouvent les concepts des composants secrets.

- Une altération des puces est possible, qui peut introduire une vulnérabilité dans celle-ci ou les rendre inutilisable.

2. Scénarios de risques

- Un attaquant vol les données d'identification du badge RFID d'une des personnes ayant accès aux postes d'ingénieur. L'algorithme Crypto1 utilisé par les cartes Mifare 1k classic est devenu inutile, la vulnérabilité a été publiée et elle permet de récupérer entre autre, les mots de passes contenu dans la carte. Grâce à ces mots de passes, l'attaquant peut ensuite s'introduire dans le bâtiment et dans les pièces à forte sécurité. Grâce au mots de passes de l'employé ayant accès aux salles d'ingénieries, il peut avoir accès aux plans secret des composants et les dérober ou les altérer.

- De la même manière que pour le premier scénario, l'attaquant va pouvoir exploiter la faille des cartes pour voler les données. Grâce aux mots de passes du responsable il peut ouvrir et dérober les matières précieuses contenues dans l'armoire forte.

VI. Vraisemblance des scénarios et leur impact

1. Vraisemblance des scénarios

Le premier scénario semble le plus vraisemblable. Ce scénario à un impact pouvant être national et peut être mis en oeuvre par une organisation malveillante.

Le second scénario concerne le vol d'or et de matières précieuse, ici on peut admettre que l'appât du gain en serait la raison. Or il s'agit d'un site contenant des plans secret défense et donc encore plus sécurisé qu'une entreprise normale utilisant des stocks de matières précieuses.

L'attaque de l'entreprise dans le but de compromettre les composants est plus probable car cela aurait un impact plus fort sur l'entreprise et/ou le pays.

L'attaque dans le but de voler des matières précieuses est moins vraisemblable car il existe des sites moins sécurisé et donc plus simple à voler.

2. Impact

- Dans le premier cas, la compromission d'un design entraînerait des pénalités supérieures ou égales à 500 000 euros. On peut donc considérer que la compromission d'une grande partie voire de la totalité des designs engendrera des pénalités en conséquence. De plus, ces composants étant utilisés dans le chiffrement par l'état Français seraient par conséquence compromis aussi. L'impact sera alors national et bien plus grand que de simple pénalités pour l'entreprise si le chiffrement de l'état entier s'en trouve impacté ainsi que la perte du contrat avec l'état.

- Dans le second cas, l'entreprise perdra 2 300 000 euros, soit la valeur des trois mois d'or stocké à raison de soixante kilos à 42 000 euros chacun. De plus, la production pourrait être temporairement arrêtée par manque de matière première. L'or étant livré une fois par mois, la production sera arrêtée jusqu'à un mois complet et les salaires seraient versés aux employés qui ne peuvent plus produire.

VII. Solutions

L'entreprise cherche une solution permettant de ne pas changer les cartes RFID dû au coûts important de remplacement des cartes et lecteurs associés, nous proposons les solutions suivantes:

L'entreprise doit mettre en place une surveillance des cartes RFID, en effet aucune surveillance des entrées et sorties sur le site ou dans les bâtiments n'est mise en place. Nous proposons de surveiller les allées et venues des employés. Par exemple, un employé s'étant authentifié pour entrer dans le bâtiment A ne peut donc pas entrer dans le bâtiment B si il n'a jamais authentifié sa sortie du bâtiment A. Si un employé authentifie son entrée dans le bâtiment A et que le même identifiant est authentifié dans le bâtiment B, nous pourrons donc savoir qu'un problème à eu lieu et que l'employé s'est probablement fait voler son identité sur le site. Il ne pourra donc plus y avoir deux entrées si il n'y a pas eu de sortie du bâtiment ou du site.

Cela permet de palier à la vulnérabilité principal de la carte mifare, la copie de carte. En effet si un intrus est sur le site lors de la venue du "vrai" employé cela entraînera une alerte déclenchée automatiquement pour deux entrées de suite sans sorties ou inversement deux sorties de bâtiments sans entrée. Deux identifications du même employé à l'entrée du site pourront donc être détectées et gérées instantanément avant même que l'intrus ne pénètre l'enceinte du site en bloquant le tourniquet ou la barrière et en appelant la sécurité.

Il faut aussi mettre en place des alarmes. Lors de la perte d'une carte, celle-ci doit être immédiatement bloqué. Une carte d'un employé doit être bloqué lors de ses congés, pendant ses jours de repos et hors de ses horaires de travail.

Au sein de l'entreprise, les employés qui ont accès à un certain bâtiment grâce à un code utilise le même pour pénétrer dans les bureaux. Nous proposons de modifier ce fonctionnement en dissociant le code d'entrée du bâtiment de celui du bureau, de ce fait, un attaquant réussissant à entrer dans un bâtiment en copiant un code ne pourra pas rentrer dans le bureau.

Les mots de passe que détiennent les employés doivent être générés aléatoirement pour éviter les mots de passe facilement cassable, malgré les conseils fait par l'administrateur (doit contenir des chiffres, des majuscules, des signes de ponctuations, une longueur minimum raisonnable…).

Une solution pour éviter le vol ou la copie d'une des cartes Mifare contenant les informations nécessaire à l'intrusion sur le site serait de séparer les cartes d'employés de celles utilisés pour le restaurant d'entreprise. Toujours dans l'optique de prévenir l'utilisation de la faille Mifare par un attaquant ayant compromis le système de paiement du restaurant, car même si il parvenait à copier cette carte, elle ne lui donnerai aucune informations pour se faire passer pour quelqu'un d'autre.

Enfin, une précaution supplémentaire serait de remplacer l'armoire forte de stockage des matériaux précieux par des coffres-forts reliés à une alarme ainsi qu'à la base de données des droits d'accès pour vérifier si la personne qui ouvre le coffre en a bien les droits et si le moment est bien propice et fait partie des horaires d'ouvertures autorisés.

VIII. Risques résiduels

Malgré toutes ces solutions, il existe une solution plus radicale mais coûteuse. En effet, le coeur du problème réside dans la faille de sécurité des puces Mifare 1k classic. Le plus efficace serait donc de changer toutes les cartes et lecteurs par une nouvelle version non vulnérable à ce jour et étant considérée comme sécurisé. En ajoutant à cela les mesures conseillées dans la partie “Solutions”, l’entreprise obtiendra une bien meilleure sécurité.

Nos solutions reposent aussi sur l’humain qui ne peut pas être considéré sans faille. En effet, les employés doivent être réactifs pour signaler une perte ou un vol de carte afin de les bloquer.

Sans le remplacement du système d’identification et d’authentification des cartes Mifare 1k classic par un autre système, il restera toujours cette faille dans le système et une potentielle erreur humaine pourrait bien laisser un intrus entrer.