Sujet Analyse de risque
FONDERIE

Contexte

- Une société fabrique des composants électroniques dont certains sont destinés au chiffrement pour l'état français. Elle est installée sur un site géographique dont elle assure la sécurité physique. Une vulnérabilité sur l'un des composants de ce dispositif a été publiée. La direction du groupe souhaite donc très rapidement connaître l'impact de ce problème sur sa sécurité physique . Elle demande aussi qu'un plan de gestion du risque soit produit très rapidement.

Fabrication

- La société fabrique (fonderie) des composants électroniques orientés sécurité. Soit la société reçoit les design des composants et les fabrique uniquement, soit, sur la base d'un algorithme, conçoit le design du composant et le fabrique. Les séries vont de 2 000 composants par an jusqu'à 700 000 pièces pour d'autres. Elle fabrique environ 5 millions de composants par an. Pour fabriquer ces composants, la société utilise des matières précieuses (or, argent, …). Il y a 6 types de matières utilisés. Pour un mois de fabrication, la société utilise 20 kilos de ces matières (équivalent or). Elle possède un stock pour trois mois de fabrication. Les composants fabriqués sont livrés tous les mois. Les design des composants sont stockés sur un serveur informatique accessible depuis un vlan spécifique. Ils sont créés ou manipulés informatiquement depuis les postes informatiques du bureau d'ingénierie. Ils sont stockés sur le serveur. Au moment de la fabrication du composant, ils sont chargés sur la fonderie par le réseau.
- Le coût de concept et de réalisation d'un composant est d'environ 150 K à 200 k euros. Beaucoup de ces design sont à protéger car ils contiennent les algorithmes dont le secret doit être conservé. En ce qui concerne les composants fabriqués pour l'état, la compromission d'un design pourrait entraîner des pénalités >= 500 ke.
- Les composants sont stockés dans des armoires de la fonderie. Les matières précieuses sont stockées dans des armoires fortes de la fonderie. Seuls les responsables de la fabrication possèdent les clés de ces armoires fortes. Ce ne sont pas des coffres forts.

Description du site et de sa sécurité

- L'entreprise est installée sur un site de forme carrée d'environ 500 mètres de côté. Le périmètre est entièrement clos avec un grillage renforcé de 3 mètres de haut. Il existe une seule entrée principale qui donne sur l'avenue devant le site. Il y a un poste de sécurité principal. Sur sa gauche il y a les entrées sur le site, sur sa droite, les sorties. Au niveau de l'entrée, il y a 3 barrières automatiques en parralèle qui permettent l'entrée des voitures (3 simultanément). Il y aussi 8 tourniquets qui permettent l'entrée des piétons (8 personnes simultanément). Au niveau des sorties, le dispositif est identique à l'entrée. Il n'est pas possible de sortir par l'entrée et vice et versa. Pour rentrer sur le site, les permanents possèdent un badge RFID. Pour chaque barrière et chaque tourniquet, il y un lecteur de badge de type IP6. Pour rentrer, la personne présente son badge à proximité du lecteur. Si son badge et reconnu et qu'elle possède le droit d'accès, l'actionneur barrière s'ouvre ou le tourniquet se dévérouille pour un tour. Si le badge n'est pas reconnu, l'actionneur reste vérouillé.
- L'action de présenter le badge correspond à l'identification du porteur du badge. A l'intérieur du site, il y a 12 bâtiments sécurisés. La porte de chaque batiment est vérouillée. Il y a un lecteur de badge RFID doublé d'un clavier numérique. Quand une personne veut entrer dans un bâtiment, elle présente son badge devant le lecteur, elle s'identifie. Ensuite, elle tape son code secret sur le clavier, elle s'authentifie. Si les informations sont correctes, et que la personne possède les droits d'accès, la porte s'ouvre. Pour sortir du bâtiment, la personne appuie sur un bouton qui déverouille la porte.
- A l'intérieur des bâtiments, il y a des pièces à moyen niveau de sécurité et des pièces à fort niveau de sécurité. Les pièces à moyen niveau de sécurité sont fermées à clé. Les clés sont déposées dans un coffre à clé mécanique. Ces pièces sont équipées d'un dispositif de détection d'intrusion. Les pièces fortement sécurisées bénéficient du même dispositif que celui qui est installé sur les portes d'entrée des bâtiments. Ces pièces sont aussi protégées par un système de détection d'intrusion. Les fenêtres sont condammées par des barreaux en fer ou électroniques infra rouge.

Description du site et de sa sécurité

- Les lecteurs de RFID sont connectés par liaison ethernet via un vlan spécifique vers la base de données des accèdants, des droits d'accès et de la gestion des accès. En temps normal, le lecteur interroge la base de données pour savoir si la requête d'accès est légitime. En cas de coupure de réseau ou d'alimentation électrique, les lecteurs sont autonomes. Régulièrement la partie correspondante de la base de données de gestion des accès est recopiée localement dans la mémoire du lecteur. Les codes personnels d'authentification sont stockés dans la mémoire de la puce mifare 1k classic du badge RFID. Un code d'accès est spécifique pour une personne pour une seule porte. Une personne peut avoir une dizaine de codes à retenir. Cependant, la constitution de ces codes permet une mémorisation facile.
- Les badges sont personnels et remis à l'arrivée de chaque employé. Ils sont rendus au départ de la société. Ces badges servent aussi à payer les repas au sein du restaurant d'entreprise. En fin de journée, le week end ou durant les vacances les employés gardent leur badge avec eux.
- Les visteurs qui ne possèdent pas de droits d'accès doivent se présenter au poste de sécurité à l'entrée. Contre une pièce d'identité, ils peuvent recevoir un badge visiteur qui ne leur permettra que de franchir l'entrée du site. Le badge visiteur ne permet pas de rentrer dans un bâtiment ou dans une pièce fortement sécurisée.

Volumétrie et coûts.

- Le kilo d'or varie aux alentours de 42 k euros.
- Il y a environ 1 000 employés.
- Il y a environ 80 lecteurs de badge (opérationnels et stock de maintenance).
- Il y a un stock de 3 700 badges (personnels, personnels logistiques, badges neufs, badges usagés…).
- Un lecteur de badge coûte environ 3 500 euros installé. Un badge personnalisé (photo, nom…) coûte environ 2,7 euros pièce.
- Il y a environ 25 personnes qui gèrent la sécurité du site.

Vulnérabilité crypto1

- La communication entre le badge et le lecteur s'effectue par liaison radio. Afin d'éviter l'enregistrement et l'attaque par rejeu, cette communication est chiffrée par l'algorithme crypto1. Une bonne partie de la sécurité repose sur le secret de l'algorithme. Celui-ci vient d'être publié sur internet. C'est la vulnérabilité majeure du système de sécurité de ce site.

Documents à joindre au sujet.

- http://www.openpcd.org/OpenPICC_RFID_Emulator_Project
- http://www.openpcd.org
- http://www.nxp.com/documents/data_sheet/MF1S503x.pdf
- http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20Classic/The_MIFARE_Hack.pdf
- http://www.nicolascourtois.com/papers/mifare_all.pdf
- http://www.angelfire.com/co3/bog/documents_files/ACG_Mifare_v14e_module.pdf (les 6 premières pages).

Travail demandé

- Conduire l'analyse de risque dans le cadre de l'apparition de cette vulnérabilité jugée critique.
- Vous devez :
  - Définir le périmètre du système que vous allez étudier et reformuler le besoin attendu par la société.
  - Lister les biens et les caractériser.
  - Identifier les menaces et vecteurs de menace pour chacun des biens.
  - Identifier les composants du système en lien avec ces biens.
  - Lister les vulnérabilités qui affectent ces composants.
  - Identifier les faits redoutés et les scénarios de risques.
  - Classer ces scénarios en fonction de leur vraisemblance justifiée et de leur impact.
  - Proposer un ensemble de mesures adapté à la gestion des risques identifiés.
  - Lister les risques résiduels.

  - Vous allez avoir besoin d'informations complémentaires. Il faudra m'adresser votre question par la messagerie.

  - Ce travail est à rendre. Je vous donnerai rapidement des informations complémentaires sur ce point.

  - Bon travail.