Défense contre les cybermenaces sur les systèmes de gestion du bâtiment

par Daniel Paillet, CISSP, CEH

Résumé

Jusqu'à récemment, la surveillance de la sécurité des systèmes de gestion du bâtiment (SGB) ne posait jamais de problème. Mais les menaces imminentes de cyberattaques imposent d'accorder plus d'attention à l'intégrité des SGB. Alors que des protocoles bien connus existent pour la surveillance et la protection des ordinateurs et des centres de données, les SGB sont souvent ignorés. Cet article décrit les menaces existantes et recommande des approches de déploiement d'une méthodologie de « défense en profondeur » spécifique aux SGB.

Introduction

La menace de cyberattaques contre les systèmes de gestion du bâtiment (SGB) est un problème croissant, tant dans le secteur du bâtiment qu'en dehors de celui-ci. Un événement récent, l'attaque très médiatisée contre le géant de la vente au détail Target (près de 1800 grands magasins aux États-Unis), a abouti au vol de 40 millions de numéros de cartes de paiement pendant une durée de 19 jours. Cette faille s'est produite parce que Target avait accordé un accès externe au réseau à une entreprise tierce de chauffage, ventilation et climatisation (CVC). Celui-ci a ouvert à des pirates informatiques une voie leur permettant de lancer une attaque contre des systèmes plus critiques au sein du réseau de Target.[1]

Les systèmes de gestion du bâtiment et de contrôle d'accès sont des ordinateurs qui surveillent et contrôlent des fonctions opérationnelles dans le bâtiment telles que climatisation, alimentation électrique, lecteurs de cartes électroniques, ascenseurs, alarmes incendie et lutte contre l'incendie, chauffage, éclairage, ventilation et vidéosurveillance. Un nombre toujours croissant de ces systèmes est connecté à d'autres systèmes informatiques et à Internet. Alors que ces avancées technologiques améliorent l'automatisation et permettent des opérations à distance, elles exposent aussi ces systèmes à d'éventuelles cyberattaques. Jusqu'à très récemment, personne ne se souciait des cyber risques potentiels de ce type de systèmes au sein du réseau du gouvernement des États-Unis qui compte près de 9000 établissements fédéraux. Les cybermenaces sur ces systèmes étaient encore considérées comme un « problème émergent » et un cyber expert a informé des agences gouvernementales, comme le General Accounting Office (GAO), que de tels systèmes n'avaient pas été conçus en tenant compte de ces risques.

Ces menaces ont maintenant attiré l'attention du Département de la sécurité du territoire des Etats-Unis (U.S. Department of Homeland Security, DHS). Entre les années fiscales 2011 et 2014, le nombre de cyber incidents impliquant des systèmes de contrôle industriel, dont des systèmes de gestion du bâtiment et de contrôle d'accès, a augmenté de 140 à 243 incidents, soit une augmentation de 74 %. Les coûts financiers de ce type d'intrusion s'élèvent à des centaines de milliards de dollars par an. Un service international de répression estime que les victimes perdent près de 400 milliards de dollars chaque année dans le monde entier – ce qui en fait une plus grande activité criminelle que la vente mondiale combinée de marijuana, de cocaïne et d'héroïne.[2]

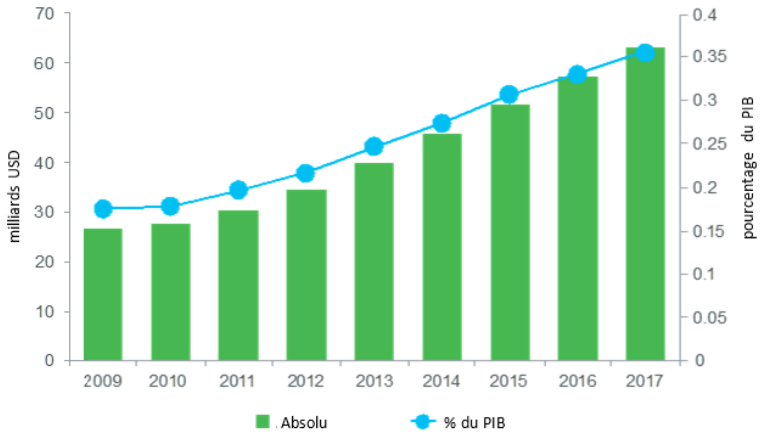

Figure 1

Croissance des dépenses en cybersécurité aux États-Unis (avec l'aimable autorisation de la Telecommunications Industry Association).

1http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
2https://news.clearancejobs/01/26/dhs-eyes-cybersecurity-issues-building-control-systems/

Un autre rapport aboutit à la même conclusion en estimant que le coût mondial des cyber activités malveillantes se situe entre 300 milliards de dollars et 1 milliard de dollars.3 L'impact financier sur les entreprises varie d'un pays à l'autre et selon les secteurs, mais le point commun est que les cyberattaques coûtent chaque année plus d'argent aux entreprises.[4]

« Défense en profondeur » appliquée aux fonctions opérationnelles

La défense en profondeur est une stratégie liée à la sécurité des systèmes d'information qui intègre les personnes, la technologie et les fonctions opérationnelles, en vue d'établir des barrières aux cyber menaces sur plusieurs couches de protection afin d'assister les missions critiques d'une organisation.[5]

Bien qu'elle soit normalement associée à la sécurité des technologies de l'information (TI), la défense en profondeur devrait aussi être appliquée aux systèmes de technologie opérationnelle tels que les systèmes de gestion du bâtiment (SGB). L'application de cette approche diffère selon qu'il s'agit des technologies de l'information ou des technologies liées aux opérations. Les systèmes de TI se concentrent sur la triade de la sécurité de base formée par la confidentialité, l'intégrité et la disponibilité de l'***information*** (dans cet ordre de priorité). Toutefois, dans le cas d'un SGB, la triade de la sécurité est composée en première priorité de la disponibilité des moyens opérationnels, puis de l'intégrité/la fiabilité du processus opérationnel et, enfin, de la confidentialité des informations opérationnelles.

Le déploiement d'une telle approche de défense multidisciplinaire sur plusieurs niveaux du système nécessite de se focaliser sur les trois niveaux primaires que sont les personnes, la technologie et les fonctions opérationnelles en tenant compte du ratio coûts/avantages.[6] Le **tableau 1** regroupe les principales étapes à accomplir à chacun de ces niveaux.

Tableau 1

Étapes clés au sein des trois piliers de la triade de la sécurité.

Personnes	Technologie	Fonctions opérationnelles
Support de la direction	Fournir et déployer les bonnes technologies	Créer et implémenter les activités nécessaires pour soutenir la position de sécurité des fonctions opérationnelles au jour le jour[7]
Le personnel de gestion du bâtiment (ou toute autre personne ayant accès au système) est formé et conscient des problèmes de cybersécurité	Une défense est disponible en plusieurs points	
Les responsabilités en matière de sécurité sont convenues et les rôles sont attribués au sein des services de TI et de gestion du bâtiment	Les défenses sont déployées en couches, l'accès au SGB via le réseau informatique est isolé/limité	
Des consignes et des procédures de sécurité sont établies	Des technologies de détection d'intrusion sont déployées	

[3]http://oreo.schneider-electric.com/flipFlop/695962877/files/docs/all.pdf

[4]« Understanding the economics of IT risk and reputation, » IBM, novembre 2013.

[5]http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[6]https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[7]https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Les sources de menaces ne proviennent pas uniquement de pirates invisibles explorant l'Internet à la recherche de cibles faciles. La catégorie de menace par des personnes peut englober tant des employés internes que des agents externes. Les techniques utilisées par des personnes pour menacer des systèmes comprennent :

- Hameçonnage (phishing) – dans ce cas, l'escroquerie visant un compte d'informations financières en ligne est réalisée par le fraudeur qui se fait passer pour une entreprise ou un site web légitime.
- Spear Phishing – un e-mail qui semble provenir d'une entreprise ou d'une personne légitime. En fait, il vient d'une organisation criminelle qui veut récupérer un numéro de carte de crédit, un mot de passe ou une information financière sur votre ordinateur personnel.
- Advance Persistent Threats (APT) – des attaques du réseau où une personne non autorisée obtient un accès à un réseau cible et y demeure sans être détectée pendant une longue période. Le but des attaques APT est de voler des informations à des organisations.

Les menaces faisant davantage appel à la technologie comprennent :

- Logiciel malveillant – un code ou un programme malveillant conçu pour endommager un ordinateur ou y exécuter des actions non autorisées.
- Enregistreurs de frappe – des programmes qui enregistrent les touches frappées sur un ordinateur et créent un journal de ces détails. Ces journaux peuvent être envoyés à distance sur Internet pour y être examinés par la personne malveillante qui a installé le logiciel.
- Arnaque à la clé USB – des clés USB sont déposées intentionnellement sur des parkings ou dans des garages dans l'espoir que quelqu'un les ramassera et les connectera à un ordinateur de bureau. La clé peut contenir un logiciel malveillant, charger des virus, voire envoyer des informations du PC infecté sur Internet.
- Pwnie Plug – un petit dispositif blanc carré ressemblant à un bloc secteur qui est branché au mur et en fait utilisé pour pirater des réseaux avoisinants.
- Pineapple – un dispositif de piratage sans fil sur pile qui peut être utilisé contre des réseaux ou des appareils sans fil.

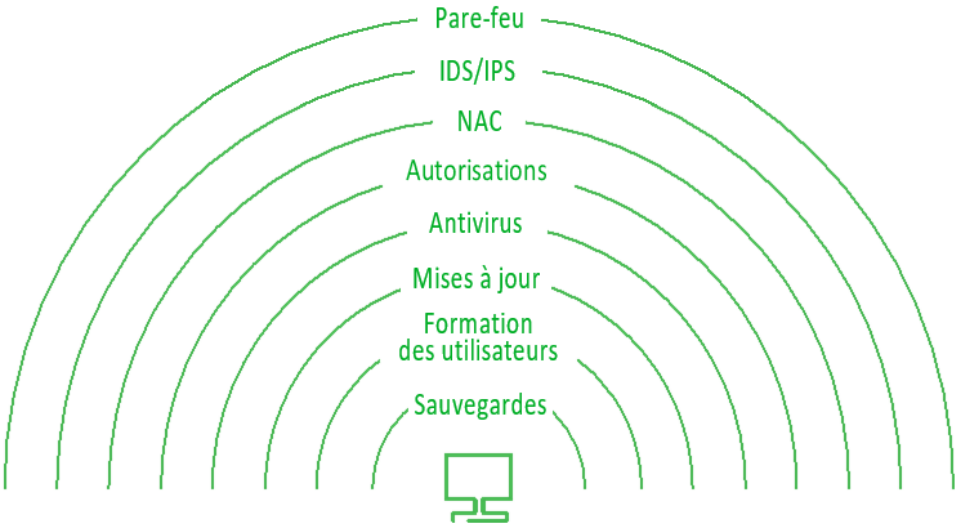

Figure 2

Exemple d'approche de défense par couches.

L'approche par couches de protection décrite dans la figure 2 a été développée par le United States Control Systems Security Program (CSSP). Cet exemple d'implémentation de la sécurité avec défense en profondeur fait appel à diverses stratégies de gestion des risques. Si une couche de défense ne remplit pas son rôle, une autre couche est déjà présente pour empêcher une faille complète.[8]

Défense en largeur

La défense en largeur, qui est un complément de la défense en profondeur, peut être définie comme suit : un ensemble systématique planifié d'activités multidisciplinaires qui cherchent à identifier, gérer et réduire les risques de vulnérabilités exploitables à chaque niveau du système, du réseau ou du cycle de vie de sous-composants (système, réseau ou conception et développement de produit ; fabrication ; packaging ; assemblage ; intégration système ; distribution ; fonctions opérationnelles ; maintenance et fin de vie). [9] En résumé, la défense en largeur fait appel à plusieurs types d'équipements de sécurité au sein de chaque couche de sécurité.[10]

Afin de comprendre les différences entre la défense en largeur et la défense en profondeur, considérons l'exemple suivant de protection contre les virus : la défense en profondeur utilise un logiciel antivirus comme un type de défense. La défense en largeur peut recourir à plusieurs anti-virus. Il est prudent de déployer les deux approches, car un logiciel anti-virus donné peut détecter un virus qu'un autre anti-virus ne reconnaîtra pas. L'utilisation d'un logiciel anti-virus d'un éditeur sur un serveur de messagerie et celle d'un anti-virus d'un autre éditeur sur les PC, stations de travail et serveurs tend potentiellement un meilleur filet de protection (contre les virus dans ce cas).

Dans le domaine des SGB, la défense en profondeur/largeur, comprend la sécurité des passerelles, des compteurs et des contrôleurs. La construction d'une telle architecture de défense commence quand les producteurs de ces composants suivent un cycle de vie de développement sécurisé au niveau de la fabrication des équipements et des logiciels destinés aux SGB (voir la figure 3). Une telle procédure permet le développement d'équipements et de logiciels renforcés qui sont en mesure de résister à des attaques. La figure 3 représente les différentes couches et processus qui permettent le durcissement de SGB qui sont sécurisés par conception, sécurisés par défaut et sécurisés en déploiement.

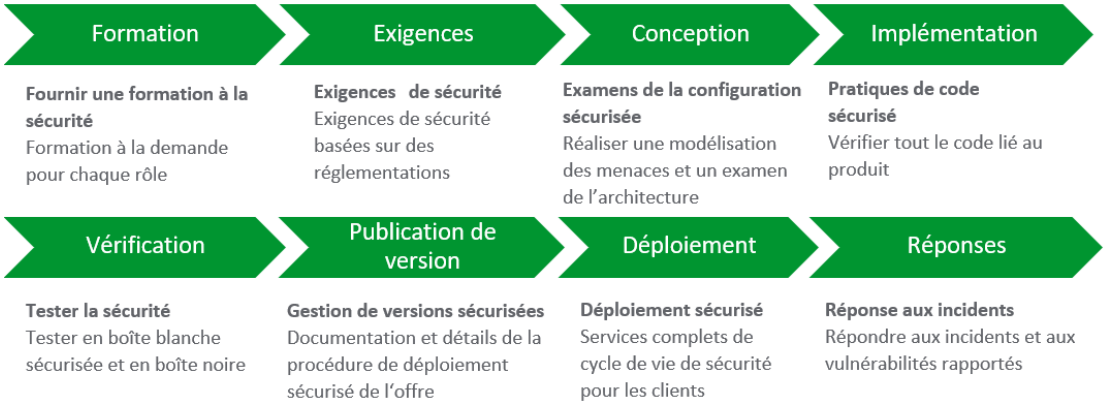

Figure 3
Cycle de vie de développement sécurisé.

[8]Viega and McGraw [Viega 02] au chapitre 5, « Guiding Principles for Software Security » dans « Principle 2: Practice Defense in Depth » aux pages 96 à 97_

[9]http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[10]Official (ISC2) Guide to CISSP-ISSMP CBK, Second Edition, page 198

Sécurité des SGB

Dans le domaine des systèmes de gestion du bâtiment (SGB), les réponses apportées par la cybersécurité doivent aller au-delà des problèmes reconnus tels que les attaques délibérées des employés mécontents, l'espionnage industriel et/ou les terroristes. Dans certains cas, des erreurs des utilisateurs, des pannes des équipements ou des catastrophes naturelles peuvent rendre le système vulnérable. Cela peut créer, dans le périmètre de défense du système, des points faibles permettant à un attaquant de pénétrer dans le réseau, d'accéder à des logiciels de commande et de modifier les conditions de charge pour déstabiliser le système de manière imprévisible.[11]

Le tableau 2 montre comment les réseaux des SGB peuvent être rendus plus résistants aux menaces grâce à une gestion ciblée des processus et des procédures des systèmes de sécurité.

Tableau 2

Meilleures pratiques pour renforcer la sécurité des réseaux de SGB.

Processus	Procédures	Avantages
• Respecter les normes et règlements • Gestion des accréditations • Administration du système • Gestion des correctifs • Réponse aux incidents	• Formation du personnel • Évaluations régulières	• Prévenir l'introduction accidentelle de logiciels malveillants • Éviter les failles par ingénierie sociale • Conformité aux normes

Le lien en bas de cette page permet d'accéder à des détails sur les points mentionnés dans le tableau 2.[12]

Pour une protection maximale, des solutions conventionnelles de sécurité informatique devraient être incorporées aux réseaux des systèmes de gestion du bâtiment. Quelques-uns des domaines à prendre en compte dans le plan de sécurité global sont indiqués ci-après :

Contrôles d'accès

- Contrôles d'accès physiques : barrières, verrous de sécurité, lecteurs de cartes, caméras vidéo
- Contrôles à la frontière du réseau : pares-feux, VPN, passerelles unidirectionnelles

Durcissement du réseau

- Processus et procédures d'installation des logiciels et des équipements intégrés couvrant des éléments tels que la modification des identifiants par défaut et la désactivation des services inutilisés des systèmes d'exploitation
- Implémentation de systèmes de prévention d'intrusion dans l'hôte sur les points terminaux, mise en œuvre de « listes blanches » (utilisation d'un logiciel de filtrage antispam pour ne laisser passer que les adresses e-mail spécifiées) afin d'empêcher que des chevaux de Troie et des logiciels malveillants ne s'exécutent sur les serveurs/stations de travail

[11] NIST Smart Interoperability Panel: Cyber Security Group

[12] http://iom.invensys.com/EN/pdfLibrary/NERCCIPComplianceChecklist.pdf

Authentification et autorisation

- Gestion centralisée des comptes pour l'autorisation et l'authentification des utilisateurs
- Contrôle d'accès basé sur des rôles pour les droits et privilèges des utilisateurs finaux
- Surveillance et audit des événements système
- Journalisation centralisée des événements de sécurité relatifs à l'accès au réseau et au système
- Systèmes de détection et de prévention d'intrusion pour détecter le trafic anormal sur le réseau
- Gestionnaire d'incidents de sécurité avec alerte en temps réel et surveillance 24/7

L'amélioration de la disponibilité et de la fiabilité du réseau contribue à renforcer la confiance des clients dans les caractéristiques de cybersécurité du SGB.

Le National Institute of Standards and Technology (NIST) a fourni des conseils sur l'élaboration d'un cadre pour l'amélioration de la cybersécurité applicable aux SGB. L'un de ces documents, *« Framework for Improving Critical Infrastructure Cyber Security »,* décrit les principes de base pour le déploiement d'un tel cadre. Selon le NIST, un cadre permet aux organisations – quelles que soient leur taille, le degré du risque de cybersécurité ou la sophistication de la cybersécurité – d'appliquer les principes et les meilleures pratiques de la gestion des risques en vue d'améliorer la sécurité et la résilience de l'infrastructure critique. Ce cadre permet d'organiser et de structurer diverses approches de cybersécurité en regroupant des normes, des guides et des pratiques dont l'efficacité est prouvée. Le cadre devrait englober des normes de cybersécurité reconnues à l'échelle mondiale. Il peut être utilisé au niveau global par les organisations et servir de modèle à une coopération internationale sur le renforcement de la cybersécurité d'infrastructures critiques.[13]

Le maillon le plus faible dans tout système informatique ou de gestion du bâtiment est constitué par les personnes qui administrent et utilisent les systèmes. Leurs actions, qu'elles soient intentionnelles ou involontaires, peuvent accroître le risque de sécurité pour les systèmes. On peut citer comme actions involontaires l'absence de sécurisation des ordinateurs portables, des stations et des postes de travail ainsi que le non-respect des processus et procédures convenables (p. ex. une gestion des mots de passe sans annulation des identifiants et de l'accès quand un employé quitte l'entreprise). Les actions intentionnelles comprennent les menaces d'initiés telles que sabotage, fraude, vol ou fuite de propriété intellectuelle ou d'informations classifiées/confidentielles.

La menace de l'« ingénierie sociale »

Dans le contexte de la cybersécurité, l'ingénierie sociale se réfère à une personne qui influence un autre individu en possession d'un ordinateur (et qui dispose d'un accès interne à des réseaux et/ou des bases de données particuliers) pour qu'il suive ses instructions sous de faux prétextes. Par exemple, un appelant pourrait se faire passer pour un membre du support informatique et demander des identifiants ou d'autres informations sensibles. D'autres exemples de ces types d'attaques sont détaillés ci-après :

[13]http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Exemple 1 : e-mail à un « ami »

Dans certains cas, l'utilisateur peut croire qu'il ou qu'elle reçoit un e-mail d'un ami connu. En fait, si un criminel réussit à pirater le mot de passe e-mail d'une personne, ou à l'obtenir par ingénierie sociale, il est très probable qu'il ait accès aux contacts de cette personne.

Cela est possible, car la plupart des individus utilisent le même mot de passe partout ; le pirate dispose donc très probablement d'un accès aux contacts de cet individu dans les réseaux sociaux.

Une fois que le criminel a pris le contrôle de ce compte e-mail, il envoie des e-mails à tous les contacts de la personne concernée ou poste des messages sur toutes les pages de ses amis dans les réseaux sociaux, voire sur les pages des amis de ses amis.

Les messages provenant du pirate sont conçus pour abuser de la confiance et piquer la curiosité. Ils peuvent juste contenir un lien indiquant *« regarde ici ! »*. Comme le lien provient d'un ami et que vous êtes curieux, vous faites confiance au lien et cliquez. Cela conduit à une infection par un logiciel malveillant qui permet au criminel de prendre le contrôle de votre ordinateur et de récupérer vos contacts afin de les abuser comme vous l'avez été.

Dans d'autres cas, l'e-mail peut inciter à un téléchargement de photos, de musique, de film ou de document contenant un logiciel malveillant. Si vous téléchargez, ce qui est probable, car vous pensez que cela provient d'un de vos amis, vous êtes infecté. Le criminel dispose alors d'un accès à votre ordinateur, à votre compte e-mail, à vos comptes de réseaux sociaux et à vos contacts, et l'attaque s'étend à toutes vos connaissances.

Les messages reçus du pirate peuvent décrire une histoire ou un prétexte convaincant. Ainsi, vous pouvez recevoir une demande d'aide urgente de votre « ami » parce qu'il est bloqué quelque part, a été volé et a un besoin urgent d'argent pour rentrer à la maison. Ou bien, vous êtes sollicité pour une collecte de fonds à des fins caritatives ou autres – avec des instructions précisant comment envoyer l'argent (au criminel).

Exemple 2 : essai d'hameçonnage

Un pirate informatique qui pratique « l'hameçonnage » envoie un e-mail, un message instantané ou un texto qui semble provenir d'une entreprise, d'une banque, d'une école ou d'une institution légitime et bien connue. Ces messages présentent en général au lecteur un scénario ou une histoire. Le message peut expliquer qu'il y a un problème qui vous oblige à « vérifier » les informations en cliquant sur le lien affiché et en fournissant des données personnelles dans son formulaire. L'emplacement du lien peut sembler tout à fait légitime avec tous les logos et le contenu appropriés (en fait, les criminels peuvent avoir copié le format et le contenu exacts du site légitime). Comme tout semble légitime, vous faites confiance à l'e-mail et au site factice et fournissez toutes les informations que le criminel demande. Les escroqueries par hameçonnage de ce type comprennent souvent un avertissement indiquant ce qui se passera si vous n'agissez pas rapidement. En effet, les criminels savent que s'ils peuvent vous faire agir avant que vous ne réfléchissiez, vous risquez davantage de tomber dans le panneau.

Le message reçu peut aussi indiquer que vous avez « gagné » quelque chose. L'e-mail peut prétendre provenir d'une loterie, d'un parent décédé ou que vous êtes la millionième personne à cliquer sur leur site. Pour obtenir ce que vous avez « gagné », vous devez fournir votre relevé bancaire pour qu'ils puissent faire un virement, ou bien indiquer votre adresse et votre numéro de téléphone pour qu'ils puissent envoyer le cadeau et vous devez souvent aussi prouver votre identité, y compris votre numéro de sécurité sociale. Ce sont les « hameçonnages à l'avidité », car même si le prétexte est faible, les gens veulent obtenir ce qui est offert et tombent dans le piège en donnant leurs informations. Ils se retrouvent ensuite avec leur compte bancaire vidé et leur identité volée.

Exemple 3 : scénarios d'appât

Ces escroqueries par ingénierie sociale s'appuient sur le désir de faire « une bonne affaire ». L'« appât » peut être un bon prix sur un article particulier ou un nouveau film ou une chanson très populaires. Souvent, ces escroqueries se trouvent sur des sites pair-à-pair, des sites de réseaux sociaux ou des sites malveillants trouvés dans des résultats de recherche. L'escroquerie peut se présenter sous forme d'une bonne affaire exceptionnelle sur des sites d'annonces ou de vente aux enchères. Pour dissiper les soupçons, le vendeur affiche une bonne évaluation (le tout ayant été planifié et réalisé à l'avance). Les personnes qui mordent à l'appât peuvent être infectées par un logiciel malveillant qui peut créer un nombre quelconque de nouveaux *exploits* contre elles-mêmes et leurs contacts. Elles risquent de perdre leur argent sans recevoir l'article acheté et de retrouver leur compte en banque vide si elles font l'erreur de payer par chèque.

Exemple 4 : réponse à une question que vous n'avez jamais posée

Des criminels peuvent prétendre répondre à votre « demande d'aide » de la part d'une entreprise tout en offrant davantage d'aide. Ils choisissent des entreprises utilisées par des millions de personnes, comme un éditeur de logiciels ou une banque. Si vous n'utilisez pas le produit ou le service, vous ignorerez l'e-mail, l'appel téléphonique ou le message. Mais, s'il se trouve que vous utilisez le service, il y a de bonnes chances pour que vous répondiez, parce que vous avez probablement besoin d'aide sur un problème (p. ex. un problème informatique).

Le représentant, qui est en fait un criminel, aura besoin de « vous authentifier », de vous faire vous connecter à « leur système » ou bien de vous faire connecter à votre ordinateur et soit leur accorder un accès à distance à celui-ci pour qu'ils puissent le « réparer » pour vous, soit vous indiquer les commandes pour le réparer vous-même avec leur aide. Cela peut permettre au criminel d'accéder à votre ordinateur plus tard.

Exemple 5 : créer la méfiance

Certaines techniques d'ingénierie sociale visent à créer la méfiance ou à déclencher des conflits. Celles-ci sont souvent mises en œuvre par des gens que vous connaissez et avec qui vous êtes fâché, ou par des fauteurs de troubles qui essaient simplement de semer la pagaille. Ces gens veulent tout d'abord susciter votre méfiance vis-à-vis d'autres personnes afin de se présenter ensuite de manière héroïque et gagner votre confiance. Dans certains cas, il peut s'agir d'extorqueurs qui veulent manipuler l'information et vous menacent ensuite de la divulguer. Cette forme d'ingénierie sociale commence souvent par l'obtention d'un accès à un compte e-mail ou à d'autres comptes de communication, comme un client de messagerie instantanée, des réseaux sociaux ou un forum de discussion. Cela est réalisé par piratage, par ingénierie sociale ou simplement en devinant des mots de passe particulièrement faibles.

La personne malveillante peut ensuite modifier des communications sensibles ou privées (notamment des images ou des enregistrements audio) à l'aide de techniques d'édition de base, puis les envoyer à d'autres personnes pour créer un drame, de la méfiance ou de l'embarras. Elle peut faire croire qu'il s'agit d'un envoi accidentel, ou donner l'impression de vous faire savoir ce qui se passe « vraiment ». Une autre possibilité est d'utiliser le matériel modifié pour extorquer de l'argent soit de la personne piratée, soit du destinataire présumé.

Il y a littéralement des milliers de variations des attaques d'ingénierie sociale. L'imagination du criminel est la seule limite au nombre de façons dont il peut manipuler les personnes touchées par ingénierie sociale. Le criminel est aussi susceptible de vendre vos informations à d'autres qui pourront alors exécuter leurs *exploits* contre vous, vos amis, les amis de vos amis etc.[14]

En général, on considère comme ingénierie sociale tout acte qui influence une personne pour qu'elle exécute une action qui peut être, ou ne pas être, dans son propre intérêt.[15] Elle représente « l'art et la science » d'un individu qui amène un autre individu à se conformer à ses désirs. Dans une attaque par ingénierie sociale, l'agresseur vise souvent le maillon le plus faible de la chaîne de sécurité informatique. En fait, on pourrait postuler que même un ordinateur débranché pourrait servir de vecteur à un acte d'ingénierie sociale. Si l'attaquant peut persuader une personne sans méfiance de brancher un ordinateur et de le mettre en marche, cet ordinateur « débranché » pourrait servir de vecteur vers une faille.[16]

L'ingénierie sociale est le moyen le plus simple d'accéder sans autorisation à un SGB. Pour se protéger contre de telles attaques, les entreprises doivent former leurs services, leurs sous-traitants et leurs partenaires commerciaux afin qu'ils puissent résister à de telles menaces. Il peut s'agir d'une formation de sensibilisation, dans le cadre du processus d'accueil lorsque de nouvelles personnes ou des entreprises externes sont intégrées à l'organisation.

Certaines organisations recourent à une modélisation des menaces afin d'anticiper les différentes séries d'événements qui pourraient conduire à une faille de sécurité. Dans le cas des SGB, la modélisation des menaces pourrait comprendre l'identification des points d'entrée accessibles et une définition claire des droits d'accès des sous-traitants et des utilisateurs (p. ex. principe du moindre privilège). Il faut ensuite élaborer des consignes, des processus et des formations à partir des résultats de ce modèle de menace.

Les menaces d'initiés peuvent avoir des conséquences désastreuses en cas de sabotage des équipements et des processus du SGB. Les programmes de formation constituent un moyen de défense important dans de telles circonstances. Le tableau 3 représente les principaux éléments à intégrer à un programme de formation à la sécurité des SGB :

---

[14] http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering#close

[15] Social-Engineering.org

[16] http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html

Tableau 3

Éléments pour renforcer la cybersécurité des SGB.

Ressources humaines	Éducation organisation-nelle	Consignes et procédures
• Commencer par le processus d'embauche, désactiver l'accès au moment de la résiliation	• Formation spéciale pour les managers et les ressources humaines	• Mise en œuvre du principe du moindre privilège, séparation des tâches, règles strictes de gestion des mots de passe, changer les contrôles
• Journaliser et surveiller les activités	• Rafraîchir la formation de sensibilisation une fois par an	• Sauvegarde et restauration
• Rechercher et anticiper les problèmes conduisant à des activités malveillantes	• Former les sous-traitants et les partenaires commerciaux	• Établir et communiquer des moyens de dissuasion en cas de non-conformité

Conclusion

La création d'une politique de sécurité et d'une infrastructure de réseau pour les systèmes de gestion des bâtiments nécessite l'appui de la direction. Le maintien d'une défense solide en profondeur et en largeur exige un travail continu. Alors que les attaques (y compris par ingénierie sociale) deviennent plus courantes et plus sophistiquées, il est nécessaire de développer des processus et des procédures qui sécurisent les réseaux des SGB. La formation des personnes chargées de la gestion des réseaux des SGB est un facteur critique de succès. La vigilance et une diligence raisonnable doivent comprendre une maintenance disciplinée des systèmes de SGB avec les dernières mises à jour et une évolution des stratégies relatives aux architectures de sécurité de la défense en profondeur et en largeur. La formation des utilisateurs finaux/des employés doit avoir lieu à intervalles réguliers afin de se prémunir contre les méfaits de l'ingénierie sociale. Ces investissements profiteront à l'organisation en réduisant les incidents conduisant à des pertes de revenus et en préservant la réputation de l'organisation auprès de ses clients et partenaires.

À propos de l'auteur

Daniel Paillet est actuellement Architecte en chef de la cybersécurité chez Schneider Electric, Unité opérationnelle Gestion de l'énergie. Il a notamment travaillé pour le département de la Défense des États-Unis dans le cadre de divers projets de sécurité. Il possède plus de 15 ans d'expérience en sécurité dans les domaines de la technologie de l'information, de la technologie opérationnelle, de la vente au détail, des services bancaires et des points de vente. Il est certifié CISSP, CEH et possède d'autres certifications indépendantes et spécifiques à des fournisseurs. Son rôle actuel est d'architecturer, d'améliorer et de développer des solutions et des offres sécurisées chez Schneider Electric.

Remarque : les liens Internet peuvent devenir obsolètes au fil du temps. Les liens référencés étaient disponibles au moment de la rédaction de cet article, mais peuvent ne plus l'être maintenant.

Schneider Electric GmbH
Gothaer Strasse 29, 40880 Ratingen / Allemagne

998-2095-12-08-15AR0_FR 11/19

Téléphone : +49 (0) 2102 404 6000

www.se.com