Six heures pour passer les défenses du FBI (et autres aventures)

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 29 mai 2008

Spyworld Actu

Il en faut beaucoup pour choquer Chris Goggans. Il réalise des tests d'intrusion depuis 1991. Mais il affirme que rien n'a jamais été aussi flagrant que les manques de sécurité à la fois dans les infrastructures et dans la gestion des correctifs, d'une agence civile gouvernementale sur laquelle il a récemment travaillé.

Un travail de routine au départ

Les failles étaient telles qu'il a pu aller jusqu'à une base de données sensibles du FBI sur des informations liées au crime, en moins de six heures. Chris Goggans est consultant chez PatchAdvisor. Il avait commencé par un travail de routine de passage en revue (« scan ») du réseau. Il a alors découvert une série de vulnérabilités non corrigées dans un serveur Web d'une agence gouvernementale, ainsi que dans d'autres parties de l'entreprise. A partir d'une faille dans le serveur Web, Chris Goggans a récupéré des noms d'utilisateurs et des mots de passe, qu'il a réutilisés sur d'autres systèmes de l'entreprise.

Prise de contrôle d'une machine de la Police

Sur ces systèmes, il trouvé d'autres détails sur les comptes des utilisateurs qui lui ont permis de récupérer des privilèges d'administration de domaines sur le réseau Windows. Dès lors, il a pu prendre le contrôle de quasiment toutes les machines Windows de l'entreprise, y compris un poste de travail utilisé par la Police. Il a ainsi remarqué que plusieurs des postes de travail des forces de police, possédaient une seconde carte réseau, selon le protocole SNA, directement connectée vers un Mainframe IBM. En installant clandestinement un logiciel ...

...de prise de contrôle à distance sur ces postes, il a trouvé des programmes qui se connectent automatiquement à la base de données NCIC (National Crime Information Center) du FBI.

Cela aurait pu être aisément éviter

« A partir de ce logiciel, couplé à un outil de capture des frappes clavier, on pourrait récupérer des droits afin de se connecter à la base du FBI, remarque-t-il. Comme la plupart des vulnérabilités, celle-ci aurait pu être aisément supprimée par quelques stratégies de sécurité basiques. Par exemple, le réseau de la Police aurait dû être isolé du réseau principal, par des pare-feux, et les postes des enquêteurs tenus à l'écart du plus grand domaine. De même, l'agence n'aurait pas dû autoriser des postes de travail à être destinés à la fois à des tâches sensibles sur la base NCIC et à un accès général au réseau. Enfin, les administrateurs systèmes auraient du effectuer le contrôle de la réutilisation des mots de passe, et les bloquer.

La conformité réglementaire n'est pas de la sécurité

Un autre consultant, Chris Nickerson, PDG de Lares Consulting, s'étonne aussi de la simplicité de la plupart des attaques, en particulier dans le domaine de la conformité. En fait, alors qu'il réalisait un test dans une très grosse société de conseil, il avait obtenu immédiatement tous les droits d'administration sur toutes les applications. "Cette société disait être conforme à Sarbanes Oxley, depuis plusieurs années. En 20 minutes, j'avais le contrôle de toute l'activité, dit-il. Il a également trouvé des problèmes chez les sociétés se revendiquant ...

... de la conformité avec PCI. « Ils ont dépensé des millions pour être conforme à PCI, et je suis arrivé à ouvrir leur principal système de traitement des cartes de crédit en 10 minutes ». Un avis que partage Serge Saghroune, RSSI du groupe Accor : « PCI DSS à la couleur de la sécurité, mais ce n'est pas de la sécurité. La conformité à PCI DSS donne une fausse impression de sécurité, c'est comme se promener avec un costume qui n'aurait que le devant

alors que l'on est nu par derrière ».

des outils automatiques d'intrusion

Chris Nickerson encourage ses clients à se focaliser sur deux tâches en matière de technologies : gérer les correctifs, et durcir les systèmes d'exploitation, pour par exemple, bloquer les ports inutilisés. Chris Nickerson est fan des outils automatiques d'intrusion, tels que Core Impact de Core Security. « Avec un outil comme Core Impact, il est facile de se promener dans tout un réseau, même sans connaissances »". Ceci dit, ce type d'outils n'est pas la panacée. Chris Nickerson combine des outils automatisés et des procédures d'attaque manuelles, afin de montrer à quel point on peut fusionner de l'ingénierie sociale (exploitant la candeur de ses interlocuteurs) et l'exploitation des vulnérabilités réseau.

Systématiser le test du code applicatif

Il existe, de plus, de nombreux endroits où les données peuvent être corrompues dans le cas des applications Web : le navigateur, le serveur frontal, le serveur de back office, et lors du stockage. Par exemple, on a pu observer qu'une petite banque intégrait l'identifiant de l'utilisateur comme une partie de l'URL donnant accès à son compte client. En changeant quelques signes dans l'URL, on accédait très facilement à un autre compte. « La moitié des applications Web que nous testons donne accès à des données d'autres utilisateurs que celui qui s'est authentifié, souligne Brad Johnson, vice président de la société de consultants sécurité SystemExperts. « De nombreuses applications Web ne protégent pas le port 80, prévient pour sa part, Robert Maley, responsable de la sécurité pour les systèmes gouvernementaux de l'état de Pennsylvanie. Et c'est à la suite d'une attaque réussie de portails Web de l'état via de l'injection SQL, en provenance de Chine, qui a fait la une de la presse, ainsi que la mise en évidence d'une vulnérabilité donnant accès à des données personnelles sur les citoyens, que le responsable a pu enfin faire prendre conscience à sa hiérarchie des risques. « Grâce à cette mauvaise presse, finalement, nous avons les moyens de travailler sur la protection du code applicatif que nous développons et de le tester via des tests d'intrusion pour l'ensemble d'une configuration (matériel, logiciel, systèmes d'exploitation, et l'application elle-même), se félicite le responsable. Une démarche que l'on retrouve chez le groupe Accor qui - sous l'impulsion de son RSSI - a mis en place une équipe interne chargée de systématiser des tests d'intrusion sur l'ensemble des applications du groupe ainsi que celles de ses partenaires.

Post-scriptum :

http://securite.reseaux-telecoms.ne...