Tour d'horizon

Fabrice PRIGENT a commencé la réunion par un tour d'horizon d'événements intéressants de ces derniers mois.

- Un « prestataire » propose de craquer les mots de passe d'accès à des comptes Webmail pour 100 $. Toutefois, il semble que le mode opératoire soit plus proche de l'ameçonnage bien organisé que de l'exploitation d'une faille dans les modules d'authentification des dits webmails.
- Dans au moins une situation, les données gérées par une Google Apps ont « débordé » vers le moteur de recherche et ont été indexées par ce dernier. Cet incident pose de nouveau la question de la segmentation des informations dans de gros systèmes de cloud computing – et d'une façon plus générale la question des données privées dont on délègue la gestion.
- La faille SMBv2 sera-t-elle un nouveau Conficker ? L'exploitabilité à distance, l'absence de correctif (mais présence d'un palliatif : désactiver SMBv2), l'éventualité d'un correctif hors calendrier habituel, font de cette faille un candidat sérieux à une exploitation massive.
- Un générateur de clés WPA qui repose sur un identifiant public n'est pas forcément une très bonne idée. Les BBox (Bouygues) ont récemment été victimes de cette faiblesse, et un outil spécifique de craquage de leur clé WPA existe.
- Deux documents intéressants : « Infiltrating a botnet » et un draft IETF sur le nettoyage de réseaux par rapport à d'éventuels botnets qui y seraient présents.

La norme ANSI TIA 942

M. Jean-Pierre Yché nous a présenté la norme ANSI TIA 942, une norme « du monde réel » définissant comment bien « construire » un centre de données (datacenter). Il s'agit d'un document reconnu par la communauté internationale, très orienté vers les télécommunications, relativement peu vers la sécurité de l'information, et insuffisant quant à la sécurité physique.

Cette norme a pour objectif d'éviter le désordre et d'organiser l'espace (au sens le plus général du terme) dans un centre de données. Cela signifie qu'elle aborde entre autres

- l'organisation de l'espace physique du centre de données,
- les faux-planchers et plafonds, et les contenus de ceux-ci,
- les aires de chargement ou de déchargement de matériel,
- les entrées et sorties physiques des salles,
- l'organisation des baies (travées chaudes et travées froides) et des câbles (courants forts et courants faibles),
- l'environnement physique (y compris sous l'angle sismique, pollutions industrielles voisines, lignes aériennes, etc.)

- et bien d'autres aspects qui peuvent directement influer sur la résistance d'un centre de données.

Cette norme est donc très axée sur le monde physique, mais elle apporte des points de vue qui sont tout à fait pertinents quant à l'organisation et la sécurité d'un centre de données ou d'une simple salle serveur. On y retrouve les mêmes notions que celles que nous rencontrons quotidiennement en matière de sécurité informatique :

- limitation des accès
- segmentation de l'espace physique
- suivi et contrôle des intervenants

Les exemples présentés ou évoqués par M. Yché montrent que l'on rencontre aussi les mêmes difficultés dans l'organisation et l'exploitation des centres de données que nous rencontrons souvent en sécurité informatique :

- problèmes comportementaux et humains
- problèmes quant à la sécurité des informations (parlées, stockées, écrites, archivées...)

Aspects juridiques du scan de port et des tests d'intrusion

M. Yoann Garot, juriste chez Itrust, a présenté ou rappelé quelques aspects juridiques des scans de ports et des tests d'intrusion.

Après la présentation de quelques éléments de vocabulaire, il a abordé les différences entre un pirate et un expert en sécurité (black hat et white hat), sans omettre les zones de flou qui peuvent exister quant aux actions des uns et des autres.

La présentation a ensuite abordé les aspects plus directs du droit de l'informatique, et tout particulièrement la loi Godfrain de janvier 1988 (aujourd'hui articles 323-1 à 323-7 du Code Pénal). Il nous a notamment exposé quelques situations qui ont amené à des condamnations ou, au contraire, à une relaxe des prévenus – tout en explicitant le pourquoi de la décision de justice. Au niveau jurisprudentiel, M. Garot a souligné qu'il existait une dissociation réelle entre un éventuel niveau de sécurité en place (ou absent) et une infraction commise. L'absence de sécurité ne constitue donc pas un blanc-seing pour un agresseur.

Les tests d'intrusion posent donc un ensemble de difficultés potentielles qu'il faut résoudre avant de commencer les opérations. La légalité des actions doit être certaine (pour l'intervenant), d'où la nécessité d'un contrat spécifique bornant clairement le test et sa portée (systèmes concernés et dates de validité de l'autorisation de tests) et définissant le protocole d'action du prestataire et celui d'information du client. Au-delà de cet aspect contractuel, il est impératif que le prestataire se tienne strictement aux clauses du contrat – et qu'en cas de doute il arrête ses opérations pour en aviser son client.

Le scan de port est-il légal ? Cela dépend clairement du contexte. Un simple parcours des ports ouverts ne constitue en soi pas un accès, mais juste l'envoi de paquets et l'examen des éventuelles

réponses (une opération de reconnaissance). Cela amène à penser qu'il n'y a pas d'infraction. Lorsque l'on passe de la reconnaissance à l'identification (quel est le serveur qui écoute sur le port TCP/80 ? quel est le système d'exploitation ?), la réponse est moins tranchée.

Pour l'identification du système d'exploitation, s'agissant d'une collecte et analyse de la « structure » des paquets reçus (tout particulièrement les en-têtes TCP), on peut considérer qu'il n'y a pas d'accès au système d'informations et donc pas d'infraction mais il ne s'agit malgré tout pas de requêtes habituelles. Pour l'identification des services (Apache sur port 80, Postfix sur port 25, etc.), il peut y avoir des actions exécutées sur le système cible (traitement de la requête HTTP ou d'un début de transaction SMTP) ; on peut alors considérer qu'il y a accès au système d'informations, et donc infraction potentielle.

Il s'avère que, malgré toutes les questions et les cas auxquels on peut penser, la question n'a jamais été tranchée par un tribunal français. La réponse viendra certainement de là, le jour où un tel dossier arrivera devant une cour française. M. Garot a cité quelques exemples issus de cours non-françaises et des interprétations divergentes de la légalité d'un scan de port.

Enfin, M. Garot a présenté les questions gravitant autour de la recherche et l'exploitation de vulnérabilités, ainsi que leur publication.