Avis d'expert sécurité : Le périmètre ne meurt jamais, il s'adapte

Internet, les nouveaux usages et leur impact en matière de sécurité. Un vaste sujet qu'aborde aujourd'hui **Laurent Hausermann**, CTO d'Arkoon Network Security.

Les réseaux : des origines à nos jours

Dans le jardin d'Éden de l'Internet, les choses étaient simples. TCP/IP venait d'apparaitre et les premiers utilisateurs, issus de la communauté scientifique, étaient bienveillants. Personne n'exprimait un besoin de sécurité ; les systèmes restaient ouverts, les protocoles en clair et les réseaux décloisonnés. C'était l'époque de l'insouciance.

Puis vient l'époque des invasions barbares, période moyenâgeuse des réseaux. Le volume des courriers électroniques échangés explosa, les premiers sites web marchands firent leur apparition ; la nouvelle économie était née. Avec l'arrivée de ces utilisateurs économiques, les premiers brigands de l'Internet apparurent. Depuis leurs postes, ils pouvaient prendre le contrôle à distance des réseaux d'entreprises. Ainsi, connecter son réseau à Internet sans installer un Bastion relevait-il de l'hérésie même si la pratique était courante.

Désormais, nous sommes de plain-pied dans l'Âge d'or des réseaux. Nous possédons tous plusieurs périphériques (tablettes, station de travail, ordinateur portable, *smartphone*) connectés à Internet. Les données et les applications de l'entreprise sont hébergées dans les réseaux de l'entreprise, mais aussi chez des prestataires ou même sur des systèmes SaaS livrés via Internet. La complexité des organisations, dont les structures hiérarchiques évoluent rapidement, renforce cette complexité. Avec le « mode projet », les personnes ayant « le droit d'en connaître » ne sont plus organisées de manière hiérarchique, mais en étoile, chaque projet fonctionnant de façon transversale.

Mais le changement le plus important, cependant, est d'ordre conceptuel. Comme à l'époque moyenâgeuse, nous continuons à penser les réseaux comme des forteresses. Les « gentils » seraient à l'intérieur et les « méchants » à l'extérieur ; il suffirait d'installer des murs, des portes et les gardes pour s'assurer que seules les « bonnes personnes » entrent à l'intérieur depuis l'extérieur.

Cette idée persistante est fausse. Les réseaux d'aujourd'hui s'assimilent plutôt à des villes modernes, des entités dynamiques et complexes avec de nombreuses frontières et une multitude de voies pour y entrer et en sortir. L'usage généralisé d'Internet, des périphériques mobiles, des services *Cloud* ou bien même la structure des organisations contemporaines accélèrent cette mutation.

Quel est l'impact sur les architectures de sécurité ?

Pour répondre à cette question, procédons au travers d'une étude de cas. En décembre 2011, les

hacktivistes d'Anonymous ont révélé l'attaque massive sur l'entreprise Stratfor. Stratfor Global Intelligence est une entreprise américaine (Austin, Texas) à mi-chemin entre le « *think tank* » et l'agence de renseignement. Elle édite une *newsletter* quotidienne contenant de l'information grise et les dernières informations mondiales. La plupart des agences américaines (CIA, NSA) sont des clients, voire des partenaires – agissant comme une source – de Startfor. L'attaque a révélé en décembre 2011, et a vu plus de 200 Go de données ainsi que plus de 2,7 millions d'adresses *email* dérobées. Anonymous, comme à son habitude, a fait une grande publicité des faits, a publié certaines informations, ainsi que les *logs* de l'attaque sur les réseaux sociaux. Les experts des Labs Arkoon se sont procuré le journal de l'attaque.

Qu'y apprend-on ? Que tout d'abord, le niveau technique de l'attaque n'est pas élevé, tant les erreurs de mise en œuvre des systèmes étaient nombreuses chez Stratfor. L'attaquant n'a pas eu besoin d'utiliser plusieurs APT pour pénétrer sauf peut-être pour l'attaque initiale, malheureusement inconnue. Mais le reste du journal est fort instructif et nous permet de découvrir le mode opératoire.

Les attaquants d'Anonymous n'ont pas eu à faire beaucoup d'efforts : depuis la machine exposée sur Internet toutes les autres machines de l'entreprise étaient joignables. Pire encore, un compte SSH non protégé – aucun mot de passe – permettait de s'y connecter. Il n'y avait aucune DMZ dans l'entreprise, juste un seul et même réseau « à plat ». Les serveurs n'étaient bien entendu pas à jour et s'y mélangeaient des services internes (avec du code source de programmes) et des applications web externes.

À la lecture du début du journal, on peut supposer que l'attaque initiale a été menée via un site web, et que là encore le serveur d'application n'était ni à jour, ni protégé par un mécanisme de protection *ad hoc* de type conformité protocolaire ou IPS. Par conséquent, une attaque de type injection SQL est probable.

Les architectures modernes ou l'impérieuse nécessité de démultiplier les zones de sécurité

Cette attaque aurait pu être évitée grâce à des mécanismes et des *process* de sécurité appropriés. Mais surtout, son impact aurait été moindre si l'architecture mise en place avait été mieux pensée : une plus grande segmentation aurait réduit les vols d'information et les conséquences désastreuses sur le business de l'entreprise.

Rappelons qu'une sécurité réseau sans mécanisme de sécurité périmétrique est utopique. La porte d'entrée du réseau doit rester un point de contrôle fort et assurer une étanchéité nette : protection des données et des topologiques des réseaux, filtrage des protocoles et des couches réseaux, établissement de tunnels sécurisés, un premier niveau de filtre *antimalware*. Ainsi, le concept de défense en profondeur continuera-t-il de s'appliquer.

Plutôt que de disparaitre, la notion de périmètre doit se généraliser et se multiplier. Il devrait y avoir plusieurs périmètres, plusieurs sas entre les zones du réseau de l'entreprise. Une zone regroupe des machines, des données et des utilisateurs d'un même niveau de sensibilité. Par exemple, dans une entreprise de biotechnologies, naturellement attachée à sa propriété

intellectuelle, son département R&D et ses données de recherche, son département commercial et sa base client, constituent deux zones. Les secteurs les plus sensibles pourraient vouloir créer des zones pour les serveurs d'applications d'une part, et pour les utilisateurs d'autre part. D'un point de vue technique, une zone peut être une interface Ethernet ou un VLAN.

Une fois les niveaux de risques contingentés dans des zones dans l'architecture des réseaux, il devient possible entre chacune d'appliquer une politique de sécurité stricte. Au-delà du simple *firewall* TCP/IP *Stateful*, il s'agira de garantir :

– l'application politique de sécurité basée sur des éléments techniques (zones, IP source/destination) ;

– l'authentification forte des utilisateurs, afin de réaliser une politique basée sur l'identité, et d'assurer une traçabilité à des fins de preuves et d'analyse *post mortem* ;

– le respect des standards et de l'implémentation des protocoles ;

– les attaques et comportements malveillants ;

– l'application employée par l'utilisateur, en gérant complètement les problématiques d'encapsulation et d'*obfuscation*.

À ce jour, des solutions émergent permettant d'assurer tout ou partie de ces contrôles. Elles manquent aujourd'hui de maturité et d'expérience. Elles ne possèdent aucune évaluation en matière de sécurité (aucune n'a reçu de qualification standard ANSSI par exemple). À titre d'exemple, la détection d'application est une évolution très intéressante, mais qui fait débat. Comment bâtir une politique de sécurité sur un mécanisme qui n'est pas évalué ? Peut-on faire confiance à une « boite noire » dont personne ne peut auditer le fonctionnement ? Quelle est la prédictibilité de ces mécanismes en termes de performance ? Autant de questions qui aujourd'hui demeurent sans réponses.

Les architectures et leurs composants doivent évoluer pour faire face à l'évolution des usages, des réseaux et des attaquants. Il est d'ores et déjà possible d'introduire plus de contrôle et de sécurité avec les outils actuels et de garantir une certaine étanchéité. Mais il reste un vaste champ d'innovation et de recherche afin de rester en avance face à la menace.

Près de vingt-cinq ans après leur invention, les systèmes de protection des réseaux doivent poursuivre leurs évolutions et suivre le rythme exponentiel de l'Internet.

Crédit photo : © Arkoon Network Security