Anatomie d'un exercice « Red Team »

Les enseignements qui en sont tirés vont de la détection d'une violation à sa résolution, en passant par l'enquête et la prévention des futures violations. L'équipe Red Team examine ainsi tout au long de l'exercice, les processus de contrôle des personnes et de la technologie en place dans l'organisation.

Par ailleurs, la Red Team permet également aux entreprises d'adapter leurs outils de sécurité aux attaques du monde réel ; les entreprises pourront notamment identifier leurs données les plus sensibles et le chemin que les attaquants emprunteront pour les atteindre. Prenons un exemple pour comprendre comment ces exercices se déroulent concrètement. Une entreprise a investi plusieurs millions de dollars dans la sécurité, essentiellement dans la protection des points d'accès et la sécurité périmétrique. Cette organisation a migré la majorité de ses données les plus sensibles dans le cloud public, tout en adoptant une méthodologie DevOps. Les données concernées comprennent des dossiers financiers, RH et des informations détaillées sur les clients. L'entreprise a contacté la Red Team pour simuler l'attaque d'un adversaire externe qui tenterait de pénétrer dans son infrastructure cloud public en vue d'accéder à ces données stratégiques.

La Red Team a donc commencé par de l'hameçonnage, en clonant le portail du courrier électronique. Certains employés ont saisi leurs informations d'identification sur ce site, à priori légitime. A ce stade, le réseau est déjà compromis, mais l'accès se limite à quelques endroits. Pour aller plus loin, l'équipe a d'abord collecté des informations dans l'Active Directory pour déterminer quels sont les comptes à privilèges, qui les possèdent et à quoi ils sont actuellement liés. Le constat est sans appel : des informations d'identification compromises sont partagées sur d'autres machines du réseau vers lesquelles des déplacements latéraux sont alors rendus possibles. L'une d'entre elles est le poste de travail d'un employé du service informatique, doté d'un compte d'administrateur domaine. Lors d'une attaque réelle, il pourrait s'agir d'une situation de « fin de partie » car, à ce stade, un cybercriminel aurait la possibilité de compromettre n'importe quelle autre machine du réseau.

Cependant, l'entreprise a migré toutes les informations sensibles auxquelles la Red Team doit accéder dans le cloud. L'objectif est désormais de trouver le moyen de passer de l'accès sur site à leur infrastructure cloud public. En utilisant les privilèges d'administrateur domaine nouvellement acquis, l'attaque se porte sur les développeurs. Un accès distant compromis permet l'exécution d'un malware sur la machine d'un ingénieur DevOps.

Bingo ! Un outil de connexion à distance, utilisé pour se connecter à un serveur cloud, y est découvert. A cela s'ajoutent des droits d'accès à privilèges, sous la forme d'une clé SSH (Secure Shell) stockée localement sur la machine. Cette clé est ensuite utilisée pour connecter une machine dans le cloud public de l'organisation.

Les fournisseurs de cloud permettent en effet d'attribuer certains privilèges aux ressources du cloud en créant une identité, avec un ensemble spécifique de permissions, et de l'affecter à différentes ressources. Cela permet, par exemple, à une machine de communiquer avec un périphérique de stockage. Cependant, ces privilèges sont stockés sous forme de clés API cloud-natives, pouvant être récupérées par n'importe quel utilisateur, quels que soient ses niveaux

d’accès au système d’exploitation de la machine. Il est donc essentiel d’attribuer le bon niveau de privilèges à l’identité.

La Red Team profite de son accès à cette machine unique pour récupérer ces API. Elle a désormais un contrôle total sur l’environnement et l’accès aux informations sensibles : son objectif est atteint ! Chaque serveur est ensuite sauvegardé et copié, 375 au total, puis relié à un nouveau compte, créé par la Red Team avec le même fournisseur de cloud public. L’organisation ne s’est même pas rendu compte que son environnement a été compromis. Tout ce dont la Red Team a eu besoin, pour copier l’ensemble de leur environnement, est l’accès à un seul serveur avec le bon accès API ; et l’utilisation abusive des privilèges tout au long de l’exercice.

Mais comment une telle attaque peut-elle être stoppée ? Dans ce cas spécifique, l’application du principe de moindre privilège sur tous les points d’accès aurait permis de contenir la tentative de compromission. En outre, dans la mesure où les mêmes identifiants à privilèges étaient utilisés dans l’environnement sur site, la Red Team a pu se déplacer latéralement dans le réseau. De plus, la sécurisation des clés SSH et API ne sont pas la responsabilité du fournisseur de cloud ; pourtant, la rigueur appliquée à la sécurité sur site doit également s’appliquer à l’environnement cloud qui doit être traité comme une extension de l’environnement existant, et non comme un élément distinct, que quelqu’un d’autre devrait sécuriser.

Les privilèges continueront de jouer un rôle dans la quasi-totalité des scénarios d’attaque, qu’il s’agisse de répandre un robot crypto-mineur, d’exfiltrer des données ou de voler de l’argent sur les comptes d’une entreprise. Les organisations doivent par conséquent en prendre consciences pour sécuriser pour de bon leurs informations sensibles en amont et garder une longueur d’avance sur les attaquants.