Maitriser ses processus de gestion à incidents : une donnée stratégique en matière de Cybersécurité

Le management de la réaction est un point rarement évoqué en matière de sécurité IT, il est pourtant fondamental et nécessite d'être mené dans les règles de l'art. Cap sur ce sujet et rappel de ses fondamentaux.

Définir un cadre

En cas d'attaque, il est tout d'abord utile de recenser l'ensemble des contremesures locales activables, d'évaluer l'impact de l'attaque sur le fonctionnement du système, ainsi que la pertinence des contre-mesures envisageables, de mesurer l'impact de leur activation sur le fonctionnement optimal du système, puis de proposer un ensemble de stratégies de réponses à l'opérateur de sécurité.

Dans ce contexte, lors d'une attaque, l'opérateur de sécurité doit pouvoir bénéficier du meilleur éclairage afin d'être en mesure de forger et prendre sa décision sur les contremesures à appliquer à l'incident. La meilleure réponse est celle qui offre une coordination globale large, assurant la pertinence de la réaction, sa cohérence dans le contexte de l'incident, et la préservation des politiques de sécurité en vigueur dans l'environnement concerné. En effet, de nombreuses solutions offrent aujourd'hui des fonctions activables dans un objectif de sécurité des systèmes, mais elles souffrent de limitations liées notamment à leur méconnaissance du contexte complet, et notamment de l'impact de leurs mécanismes propres de réaction, souvent statiques et prédéterminés. Il est donc crucial de faciliter la collaboration de ces « éléments activables » dans une stratégie de réponse aux attaques mieux coordonnée et d'offrir à l'opérateur de sécurité une précieuse aide à la décision.

Valorisation des dispositifs existants

Dans un premier temps, il sera donc nécessaire de recenser les éléments actifs à disposition sur le SI de l'entreprise. Ces éléments actifs recouvrent l'ensemble des systèmes matériels et logiciels capables de mettre en oeuvre des configurations de réponse aux attaques : équipements du réseau (routeurs, switches), dispositifs de sécurité (pare-feux, IDS/IPS), annuaires des autorisations utilisateurs (LDAP, AD), systèmes d'authentification, configuration des postes applicatifs (droits d'accès).

Lors de l'occurrence d'une attaque, il faut identifier les parties prenantes de la menace (sources, cibles, relais et vecteurs de l'attaque), et évaluer les différentes stratégies de réponse possibles en fonction de la nature de l'événement, de la forme et la topologie de l'attaque, et des moyens de réaction mobilisables parmi les éléments actifs préalablement répertoriés. Cette évaluation doit intégrer l'estimation du rapport entre l'efficacité des contremesures proposées en regard de la nocivité de l'attaque, et le calcul de l'impact de la réponse sur l'intégrité et le fonctionnement des services et des réseaux sous-jacents.

L’opérateur de sécurité dispose ainsi instantanément de tous les éléments de décision permettant de pousser les configurations de réaction appropriées. Il devient alors possible de réagir en quasi-temps réel à une attaque en cours en activant des combinaisons intelligentes de contremesures à l’impact et l’efficacité mesurés : filtrage et contrôle d’accès, compartimentation, nettoyage chirurgical de flux nocifs.

La Threat Intelligence est fondamentale en matière d’aide à la décision et fait apparaître des notions d’intelligence artificielle, qui prouve bien que cette dernière s’applique depuis déjà plusieurs années dans les processus de gestion des incidents de cybersécurité.

Par Fabrice CLERC, Président de 6Cure