Services de sécurité managés (MSPP) 2.0 : 5 questions à se poser (Tribune)

Le manque de profils spécialisés en cybersécurité, associé à la complexité croissante des menaces et des réseaux, un environnement de plus en plus réglementé et une course à l'innovation conduisent les entreprises à externaliser leur sécurité. Le Gartner prévoit ainsi que le marché global de l'externalisation de la sécurité va passer de 12 milliards de dollars en 2013 à plus de 24, 5 milliards de dollars à l'horizon 2017.

Cependant, trouver les ressources nécessaires pour répondre au paysage changeant de la cybersécurité peut s'avérer difficile. Les attaques d'aujourd'hui sont plus discrètes que jamais. Pour les comprendre et se protéger contre elles, les entreprises ont besoin de mobiliser tous les aspects de leurs défenses pour se concentrer sur la menace, y compris les services. Il s'agit de gagner en visibilité et du contrôle au travers du réseau étendu et tout au long du continuum d'attaque – avant qu'une attaque ne se produise, pendant qu'elle se déroule et même après qu'une attaque ait eu lieu, avec un vol de données ou des systèmes endommagés. Ce nouveau modèle centré sur la menace entraine des changements pour les technologies de cybersécurité, les produits et les services.

Les premiers fournisseurs de services de sécurité managés (MSSPs) devaient prendre en charge des produits, mettre en place des outils, assurer leur maintenance, leurs mises à jour et les formations. Mais aujourd'hui, les MSSPs de cybersécurité efficaces doivent être établis sur une analyse approfondie et une connaissance en continu des menaces en elles-mêmes, pas seulement des technologies. Reflet d'une nouvelle ère dans la façon dont nous devons aborder la cybersécurité, certains analystes du secteur commencent à appeler cette prochaine vague de services de sécurité : MSSP 2.0.

Selon les compétences internes en sécurité, le budget et les priorités, vous pouvez choisir de plus ou moins externaliser vos besoins en matière de cybersécurité. Quel que soit le degré d'externalisation, lors de l'évaluation des services de sécurité managés, les 5 questions suivantes peuvent vous aider à vous assurer d'obtenir le support dont vous avez besoin pour rester concentré sur la menace.

1. Quels sont les types d'informations télémétriques utilisées pour obtenir une meilleure visibilité et augmenter les capacités de détection ?

Si la réponse est tout simplement le flux ou les logs, ce n'est pas suffisant. D'autres données, comme les métadonnées du protocole (ex. les données extraites directement des paquets qui traversent le réseau) sont une source d'information riche sur les méthodes d'attaques les plus utilisées aujourd'hui, telles que les infections par site web (watering hole) et les campagnes de phishing qui contiennent des liens vers des sites malveillants. Dans ces cas, la possibilité d'intégrer des métadonnées http dans un modèle de télémétrie fournit le degré d'information nécessaire pour aider à détecter les menaces web. Plus il disposera de données, plus le MSSP sera efficace dans la réduction des anomalies et aura la capacité à trouver une aiguille dans une botte de foin.

2. Comment les données vont être analysées ?

Avec la croissance des données, les modèles analytiques simples comme la corrélation des logs avec les ensembles de règles ne répondent plus aux besoins, surtout si elles ne fonctionnent pas en temps réel. Les techniques d'analyses avancées de Big Data en temps réel permettent d'exploiter de grandes quantités de données recueillies, pas seulement au niveau de l'entreprise mais au niveau mondial, au travers d'une communauté pour une gestion intelligente de la menace. Ce niveau d'analyse n'est pas fondé sur des règles que les pirates peuvent comprendre et contourner, mais il est prédictif et utilise un modèle statistique dynamique pour identifier les comportements anormaux, les réseaux et autres indices de compromission (IoCs) pour repérer les activités malveillantes potentielles. Peu importe le nombre de sources télémétriques utilisées, l'application d'analyses robustes aux données plutôt qu'une simple corrélation permettra d'obtenir une détection plus fiable.

3. Où les données sont-elles stockées et comment sont-elles protégées ?

Vous aurez besoin de savoir si les données seront stockées dans le datacenter du MSSP ou dans le Cloud. Selon le type de données de l'entreprise, les besoins en conformité, et les garanties offertes par le MSSP, vous devrez décider si la solution est adéquate ou sinon, s'ils peuvent proposer une approche alternative. Il s'agit d'un choix personnel pour chaque entreprise, qui doit être basé sur le niveau de confort de toutes les parties concernées : technique, juridique, et métier.

4. Quelles sont les données remontées ?

Les données sont importantes mais il s'agit d'être en mesure de les comprendre et de pouvoir agir selon elles. Vous devez être sûr que les données sont corrélées pour fournir un contexte afin que l'information que vous obtenez soit pertinente pour votre environnement et vos priorités. Dans ce cas, vous pouvez vous concentrer sur les menaces les plus importantes. Le temps est essentiel lorsqu'il s'agit d'attaques ciblées avancées, soit des attaques qui ont un but précis. Il s'agit de savoir si le MSSP est en mesure de vous présenter des informations pertinentes plutôt que des listes d'événements sans fin et qui requièrent une analyse approfondie et une recherche pour découvrir finalement qu'il s'agit d'alertes inutiles.

5. Comment pouvez-vous aider mon entreprise à se protéger contre les attaques zero-day et inconnues ?

Pour détecter et se protéger contre les menaces zero-day, vous devez être en mesure d'aller au-delà des approches traditionnelles qui permettent de surveiller et d'appliquer une protection à un moment donné au sein du réseau étendu. C'est ici que la valeur d'un grand ensemble de détection associé à l'analyse prédictive et la modélisation statistique devient nécessaire. Cela va au-delà de la simple corrélation d'événements que les MSSP ont offert pendant des années. Associées, ces fonctionnalités peuvent identifier les IoC presque imperceptibles et les anomalies pour vous aider à identifier ces attaques particulièrement furtives et nuisibles.

Compte tenu des enjeux business, réglementaires, et liés à la cybersécurité, de plus en plus d'entreprises sont à la recherche d'experts pour les aider à protéger leurs environnements contre les cyberattaques. En se posant les bonnes questions, vous pouvez vous assurer de rester concentré sur les menaces elles-mêmes, afin d'obtenir la protection dont vous avez besoin.