Quand chaque minute compte

	**Quand chaque minute compte..**

McAfee, filiale d'Intel Security, publie aujourd'hui un nouveau rapport, « Prévention des menaces : chaque minute compte ! », qui évalue la capacité des entreprises à détecter et à détourner les attaques ciblées.

Ce dernier révèle également le Top 8 des indicateurs d'attaques les plus critiques et examine les meilleures pratiques proactives en matière de réponse aux incidents. Il illustre combien les entreprises sont plus efficaces lorsqu'elles effectuent des analyses des attaques subtiles en temps réel en prenant en compte plusieurs variables mais surtout dès lors qu'elles ont intégré et priorisé le temps de détection et les menaces intelligentes dans leur évaluation des risques.
Conjointement au rapport, une étude menée par Evalueserve, révèle que la majorité des entreprises interrogées manquent de confiance en leur capacité à détecter les attaques ciblées dans un temps opportun. Même les entreprises les mieux préparées à gérer les attaques ciblées passent beaucoup trop de temps à enquêter sur des événements, contribuant à un sentiment d'urgence, plutôt qu'à se concentrer pro-activement à la détection et à l'atténuation des menaces.
Le rapport met en évidence le fait qu'en France :
• Seulement 26 % des entreprises sont confiantes dans leur capacité à détecter une attaque en quelques minutes, et 29 % ont déclaré que cela pouvait leur prendre des jours, des semaines, voire des mois avant qu'elles ne remarquent un comportement suspect.
• 71 % des DSI interrogés ont indiqué que les attaques ciblées sont une préoccupation majeure pour leur entreprise.
• 54 % des entreprises ont enquêté sur plus de 10 attaques l'an dernier.
• 95 % de celles qui sont capables de détecter les attaques en quelques minutes possèdent une solution de gestion des évènements et des informations de sécurité (SIEM).
• Plus de la moitié des entreprises interrogées (61 %) ont indiqué qu'elles sont équipées des outils et des technologies nécessaires pour fournir une réponse rapide aux attaques. Cependant, les indicateurs critiques ne sont généralement pas isolés de la masse des alertes générées et provoquent une charge de travail supplémentaire aux équipes qui doivent passer au crible toutes les données des menaces.
« Pour garder la main sur les attaquants il faut relever le défi du temps dans la détection », déclare David Grout, Directeur Europe du Sud de McAfee, filiale d'Intel Security. « En simplifiant, grâce à une analyse intelligente et en temps réel, le travail frénétique de filtrage d'un large volume d'alertes et d'indicateurs d'attaques vous pourrez plus efficacement appréhender des événements pertinents et prendre des mesures pour contenir et détourner les attaques plus rapidement. »
Compte tenu de l'importance de l'identification des indicateurs critiques, le rapport de McAfee Intel Security a révélé le Top 8 des indicateurs d'attaque les plus courants.
Parmi ceux-ci, cinq reflètent le suivi des événements à travers le temps écoulé et montrent l'importance de la corrélation contextuelle :
1. Des hôtes internes communiquent vers des destinations inconnues ou mal connues ou vers un pays étranger où il n'y a pas d'affaire en cours.
2. Des hôtes internes communiquent vers des hôtes externes qui utilisent des ports non standards ou en inéquation avec le protocole/port, tels que l'envoi d'interpréteurs de commandes (SSH) plutôt que du trafic HTTP sur le port 80, qui est le port Web par défaut.
3. Des accès publiques ou en zone démilitarisée (DMZ) communiquant vers des hôtes internes. Cela permet de brûler les étapes de l'extérieur vers l'intérieur et en arrière-plan, permet l'exfiltration de données et l'accès à distance à des actifs. Il neutralise la valeur de la DMZ.
4. Détection de logiciels malveillants en heures Off. Ces alertes qui peuvent se produire en dehors des heures standards d'ouverture de l'entreprise (la nuit ou le week-end) et qui pourraient signaler un hôte compromis.
5. Scans de réseau par les hôtes internes communiquant avec plusieurs hôtes dans un court laps de temps, qui pourrait révéler une attaque se déplaçant latéralement au sein du réseau. Les défenses du périmètre réseau, tels que pare-feu et IPS, sont rarement configurées pour surveiller le trafic sur le réseau interne (mais pourrait l'être).
6. Plusieurs événements alarmants à partir d'un seul hôte ou à répétition sur une période de 24 heures sur plusieurs machines dans le même sous-réseau, tels que les échecs d'authentification.
7. Après avoir été nettoyé, un système est réinfecté par des logiciels malveillants dans les cinq minutes qui suivent – les réinfections répétées signalent la présence d'un rootkit ou d'une compromission persistante.
8. Un compte utilisateur tente de se connecter à de multiples ressources en quelques minutes à partir de ou vers différentes régions – signe que les informations d'identification de l'utilisateur ont été volées ou que l'utilisateur a des intentions suspectes.
« Un jour, nous avons remarqué qu'un poste de travail subissait des demandes d'authentification du contrôleur de domaine à deux heures du matin. Cela pouvait bien sur être tout à fait normal, mais il se pouvait aussi que cela soit un signe d'alerte malveillante », commente Lance Wright, directeur principal de l'information de sécurité et de conformité à Volusion, un fournisseur de solutions de commerce contributeur de l'élaboration du rapport. *« Suite à cet incident, nous avons créé une règle pour nous alerter si un poste de travail avait plus de cinq demandes d'authentification en dehors des heures ouvrables pour nous aider à identifier le début de l'attaque, avant que les données ne soient compromises. »*

« La veille en temps-réel, la bonne intelligence et les solutions de gestion des évènements et des informations de sécurité (SIEM), permettent de minimiser le temps de détection, d'éviter de manière proactive les violations fondées sur la contextualisation des indicateurs lors de l'analyse et d'apporter des réponses en matière d'action automatisés », précise David Grout *« Grâce aux solutions qui permettent d'accélérer la capacité de détection, de réaction et d'apprentissage sur les attaques, les entreprises peuvent grandement changer leur posture de sécurité et passer de 'traquées' à 'traqueuses'. »*

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.itrnews.com/articles/152073/chaque-minute-compte.html