COMMENT DÉTECTER ET METTRE FIN AUX COMPORTEMENTS À RISQUE SUSCEPTIBLES DE MENER À UNE FUITE DE DONNÉES

Les analyses ont démontré que dans 70 % à 80 % du temps, les cyberattaques proviennent du réseau interne des entreprises. Voilà une donnée qui incite à accorder une attention particulière à la gestion des activités internes, tout autant qu'à celles qui proviennent de l'extérieur.

Quelle méthode s'avère la plus efficace pour détecter des comportements à risque à l'intérieur d'un réseau d'entreprise? En gros, il faut associer l'analyse des fuites de données aux accès inhabituels.

Mesurer, suivre ou rapporter des éléments de base liés à la sécurité TI n'est pas la meilleure piste à suivre quand vient le temps de détecter des situations préoccupantes de fuite de données. Une approche beaucoup plus efficace consiste à concentrer les efforts sur les variantes et les exceptions observées par rapport aux activités habituelles.

CONCEVOIR, IMPLANTER ET EXPLOITER

En matière de sécurité TI, il s'avère essentiel de concevoir des architectures selon les cadres normatifs établis et les meilleures pratiques en vigueur. Par la suite, il faut effectuer des vérifications d'usage, procéder à des tests d'intrusion sur l'infrastructure technologique et les applications mises en place. Cette combinaison d'activités semble bien rassurante et devrait permettre de se sentir en contrôle. Illusoire? En effet, la réalité pourrait être tout à fait différente. Ces activités incontournables et d'une grande importance doivent impérativement être renforcées par d'autres mesures afin de pouvoir scruter de près l'ensemble des activités et être en mesure de détecter toute activité louche. On peut alors intervenir rapidement pour enrayer les dégâts, une situation plus réjouissante que de devoir assumer des conséquences coûteuses voire désastreuses.

Nous le savons tous, la plupart des organisations ou entreprises doivent composer avec des moyens limités en ce qui concerne le budget, le temps et les ressources. Raison de plus pour sélectionner soigneusement les activités les plus importantes à entreprendre à partir d'une liste exhaustive.

Il est impossible de tout faire, de tout contrôler et de tout voir. Fonder ses espoirs dans un modèle basé sur les lignes directrices habituelles et en assumer l'exploitation seraient tout simplement utopique.

EN PRIORITÉ : DEUX ACTIVITÉS ESSENTIELLES ET MÊME CRUCIALES

La plupart du temps, les mécanismes de surveillance sont conçus pour détecter un comportement normal ou anormal déjà défini. Il vaut mieux opter pour une approche différente qui ne met pas l'accent sur les tendances habituelles, mais qui permet plutôt de se concentrer sur les activités inhabituelles et les anomalies

ÉTAPE 1 : ANALYSER LE FLUX DES DONNÉES

L'analyse du flux des données vise à identifier, contrôler et protéger l'information sauvegardée ou en circulation. Le but principal est de limiter les risques de fuites de données sensibles, que ce soit accidentel ou intentionnel. Ce sont des actes criminels, des erreurs humaines ou de systèmes qui sont en cause dans les cas de fuites de données. La façon la plus optimale de se protéger contre la fuite des données est d'implanter une politique de sécurité, se doter de mécanismes technologiques et d'assurer des contrôles de sécurité.

Les tendances et les statistiques ne racontent pas toute l'histoire, elles révèlent toutefois l'information qui peut être souvent inquiétante en rapport avec le comportement de groupes d'utilisateurs et les utilisateurs et certains échanges sur le réseau (à titre d'exemple : courriels d'entreprise ou sur Internet, sites de sauvegarde, échanges, services de sauvegarde, etc.). À l'aide de ces analyses et statistiques, il devient possible de faire une sélection judicieuse d'échantillons basée sur un ensemble de paramètres qui permettent de creuser l'enquête et d'obtenir des indications sur les échanges sur le réseau et les façons de se comporter des utilisateurs. Certains flux de données complémentaires (Private VPNs, Telnet, Connections, http, Https, Databases, etc.) peuvent également être analysés pour identifier des échanges de données ambigus qui pourraient conduire à un problème de fuite de données. Il peut s'agir du type d'échange, de la source, de la destination, du volume des données, de la durée, de la fréquence, etc.

La solution n'est toutefois pas d'ajouter plus de technologies, mais plutôt d'analyser l'information déjà disponible. Il n'y a aucun avantage à générer plus de données si nous n'analysons pas celles dont nous disposons déjà et qui pourraient indiquer des anomalies.

ÉTAPE 2 : ANALYSER LES IDENTITÉS ET LES ACCÈS INHABITUELS

La tendance est d'observer et de compter le nombre de comptes, accès, demandes de changement, temps de résolution, etc.; mais produire ce type de rapport a une valeur limitée compte tenu de la charge de travail et des coûts qui y sont associés. Bien entendu, un tel travail est utile et même essentiel pour exploiter les environnements; par contre, cette façon de faire n'est pas à privilégier pour détecter des activités anormales, des comportements à risque et des comptes utilisés dans la fuite des données.

L'approche la plus efficace consiste à se concentrer sur les activités qui provoquent les soupçons : les exceptions, les contradictions, les alertes, les échecs dans les vérifications, les accès atypiques, les utilisations hors-normes, suspectes, inconnues, les comportements à risque, l'augmentation anormale du volume de données, l'usage bizarre des données, l'utilisation de comptes à des fins autres que celles dans le cadre des fonctions, etc. Afin d'obtenir encore plus de précisions, il faut intensifier les activités de gestion afin de cibler les comptes privilégiés, les comptes comprenant de multiples profils ou soudainement réutilisés, les activités non conformes, la gestion utilisée pour les fonctions d'application, les accès à plusieurs dossiers non associés, les comptes orphelins utilisés ou ceux qui frôlent ou franchissent les limites définies.

Il est évident que la surveillance de toutes ces activités ne s'effectue pas en une seule étape; mais il est important de se servir de cette base pour lancer les travaux quitte à ajouter graduellement des éléments spécifiques et plus complets. Cette information permettra également la mise à jour des

procédures, la définition des cas types d'utilisation et la validation des vérifications requises et leur remplacement si elles sont dépassées ou non pertinentes.

COMMENT LES ATTAQUANTS TROUVENT-ILS ENCORE DES FAILLES DANS LES APPLICATIONS, L'EXPLOITATION ET LA SURVEILLANCE?

En fait, ils ne contraignent pas leur pensée dans un cadre basé sur l'usage normal. Ils savent sortir des sentiers battus et osent penser différemment. Ils examinent toutes les possibilités. C'est d'ailleurs l'approche que nous devons nous-mêmes préconiser quand nous analysons une situation potentielle de fuite de données. Construisons un modèle, découpons des modules et des fonctions en pensant comme un cyber attaquant! Comment outrepassent-ils les règles établies?

CONCLUSION

L'histoire nous a clairement démontré que la fuite des données et les utilisations hors normes ne sont pas identifiables par des activités de surveillance conventionnelles. Même avec une solution bien conçue et bien gérée, il est primordial de la renforcer avec des activités de mesure complémentaires afin de déceler si un environnement est la cible de fuites de données

Ne renions pas les approches conventionnelles, elles sont toujours utiles dans l'exploitation des environnements. Par contre, elles doivent être soutenues par des approches innovantes liées à la détection d'activités soupçonneuses. Il est préférable de produire des tableaux de bord avec une vision globale en se basant sur un modèle et de les alimenter ensuite avec des métriques précises qui permettront de rechercher, travailler et analyser les éléments d'exception.

Bien sûr, il faut éviter d'ajouter des solutions dispendieuses et de générer plus de données si vous ne misez pas sur l'information que vous possédez déjà. Elle pourrait vous en dire long à la condition d'être soumise à une analyse rigoureuse.

Partie 2 : Le prochain article portera sur l'élaboration de notre approche et sur nos tableaux de bord spécialisés dans la production de l'information requise pour détecter l'indétectable… au-delà des efforts actuels.

Partie 3 : Cette parution abordera la gestion globale de la cybersécurité. Comment peut-on obtenir un aperçu de la cybersécurité et suivre les tendances à l'intérieur d'une entreprise grâce à des métriques spécifiques?

Nous serons heureux de vous offrir une rencontre gratuite pour établir comment INDIK peut aider votre entreprise. Nous vous invitons à communiquer avec nous.

Alain Scherrer, président
Alain.Scherrer@securecom.ca
Téléphone : 514 544-0442, poste 2320

SECURECOM indiK

D’autres capsules d’information sur INDIK[MC] 2.0 seront diffusées régulièrement.

Surveillez les prochaines publications!

+ Information utile à l’intention des gestionnaires de TI : INDIK 2.0 TI Management.pdf

https://www.indik-dashboard.com/sites/default/files/images/pdf/INDIK%202.0%20Gestion%20TI.pdf

+ Information utile à l’intention des gestionnaires en cybersécurité : INDIK 2.0 Cybersecurity.pdf

https://www.indik-dashboard.com/sites/default/files/images/pdf/INDIK%202.0%20Cybers%C3%A9curit%C3%A9.pdf

Pour plus de renseignements : www.indik-dashboard.com

INDIK[MC] une division de SecurEcom Services Conseils inc.
368, rue Notre-Dame O, bureau 101
Montréal (Québec)
H2Y 1T9