AKERVA

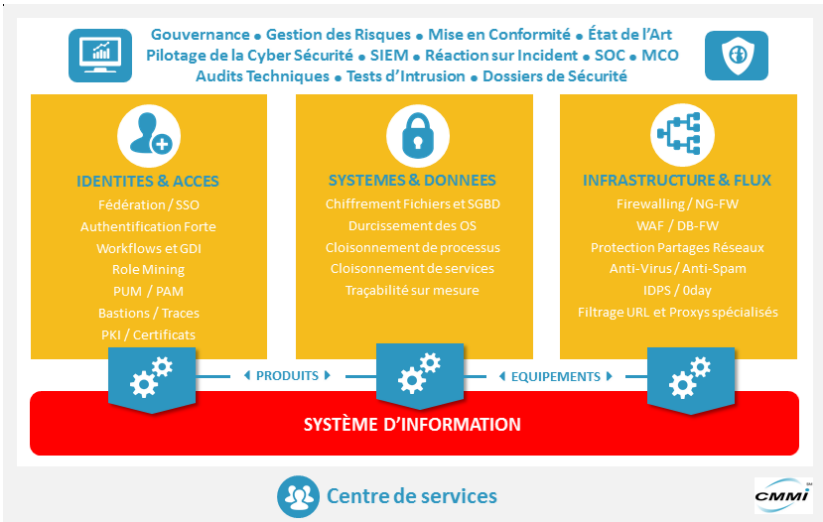
INFORMATION PRESSE
MARS 2015

Test d'intrusion/cyber-sécurité

Akerva propose des prestations d'audit toujours plus pointues

Société de conseil et d'expertise en Sécurité Informatique, Akerva a développé depuis plusieurs années un savoir-faire poussé en terme d'audit de sécurité et de test d'intrusion. Le recrutement de nouveaux consultants et la création d'une joint-venture avec le groupe Alten permettent notamment à Akerva de proposer des prestations encore plus pointues dans ce domaine.

A l'heure où les entreprises sont soumises à des attaques informatiques incessantes venant de l'extérieur ou de l'intérieur, protéger et garantir la sécurité des données devient critique. Les prestations dans ce domaine sont de plus en plus demandées par les sociétés et Akerva adapte régulièrement son offre afin d'apporter une réponse en adéquation avec le besoin des professionnels.



Dans cette optique, Akerva vient d'intégrer quatre nouveaux consultants au sein de son département "pentest" (test d'intrusion). Depuis deux ans, près de 40 audits ont été réalisés auprès de structures à forte valeur ajoutée dans les télécoms, dans la finance et l'assurance, auprès d'établissements de santé (CHU et cliniques) et sur le secteur des transports. De par sa spécialisation SSI, Akerva intervient également auprès d'industriels français de la sécurité et des structures étatiques.
"*La cyber-sécurité concerne chaque RSSI (Responsable de la Sécurité des Systèmes d'Information). De nos jours, cela parait difficile de passer, même une année, sans déclencher un audit de vulnérabilité sur au moins un de ses périmètres*" explique Cédric Thellier, Directeur Technique d'Akerva.

DES PROFESSIONNELS SENSIBILISÉS

Akerva possède une expérience solide concernant les audits, un savoir-faire qui fait partie de l'ADN de l'entreprise. De plus, la création récente d'une joint-venture avec Alten devrait rapidement apporter de nouvelles opportunités. Le Portfolio des solutions et prestations proposées apparait de plus en plus large, tout en étant basé sur une approche experte.

"*Afin d'obtenir une crédibilité et être identifié comme un interlocuteur sérieux en matière de pentest, il est nécessaire d'avoir déjà une certaine reconnaissance et expérience en matière de protection des données et de durcissement d'architecture. Nous sommes davantage considérés par nos clients comme un cabinet de conseil. Nous possédons un savoir-faire relatif à l'audit ponctuel qui fait office de valeur ajoutée sur nos prestations complémentaires*" indique Cédric Thellier.

DE LA BOÎTE NOIRE A LA BOITE BLANCHE

Akerva propose trois types de tests d'intrusion. Pour le premier, baptisé "Boîte noire", l'attaquant ne dispose d'aucune information, uniquement du périmètre cible. L'objectif est de constater quel niveau de compromission peut être atteint par une personne totalement externe à la société, dans le temps imparti par la prestation.

Concernant le second, "Boîte grise", l'attaquant ne dispose que de comptes de test et/ou de comptes génériques fournis par le client comme celui d'un stagiaire ou d'un partenaire, par exemple. Le but est de réaliser des tests plus approfondis et d'évaluer le bon cloisonnement des droits entre les différents comptes fournis aux collaborateurs ou clients de l'entreprise.

Pour le troisième, nommé "Boîte Blanche", l'auditeur a accès à l'ensemble des configurations et même, si possible, aux documents d'architecture décrivant l'existant et aux codes sources. L'objectif est d'exploiter directement l'ensemble des lacunes de configuration et les risques de compromission.

Ces tests peuvent être réalisés avec différentes variantes : test applicatif et/ou Web, Wifi, Téléphone mobile, accès VPN, poste de travail suffisamment sécurisé ou non….

Pour faire face à l'ensemble de ces menaces, les experts du pôle pentest ne se contentent pas de laisser travailler les différents outils de scan et 30 à 40% des tests sont réalisées manuellement. Ils mettent en œuvre de véritables tests d'investigation, à la méthodologie plus poussée. Sécurité des process, méthode de fonctionnement, mécanismes de cloisonnement, éléments ne pouvant pas être détectés par un Firewall/IPS/Antivirus… le nombre de points vérifiés et testés sont très nombreux et demande un vrai savoir-faire. Cette surcouche d'investigation va permettre d'affiner les résultats et le diagnostic, d'établir une véritable cartographie des secteurs d'exposition.

SE METTRE DANS LA PEAU DE L'ATTAQUANT

Les questions centrales étudiées lors d'un audit sont multiples : les outils de protection ont-ils fait leur travail ? Pourquoi ce composant, hors de prix, n'a pas agi correctement ? Est-il bien adapté, configuré ? Le retour sur investissement peut-il être amélioré ?

Comprendre l'attaquant, se mettre à sa place est la clé d'un audit réussi, tout comme intervenir rapidement pour fermer les vannes les plus ouvertes, à savoir les failles "critiques". "*Il est important de comprendre – lorsque ce n'est pas encore acquis – qu'avec quelques jours d'intervention nous pouvons limiter la casse*" soutient Cédric Thellier. "*Nous insistons sur l'importance de la complémentarité entre le responsable de l'administration des systèmes et le consultant Akerva. Ce travail en binôme participe activement à l'élaboration de l'éco-système sécuritaire".*

Actuellement Akerva constate une augmentation du volume et de la qualité des offensives avec des composants de sécurité qui peuvent être contournés. L'intérêt de "jouer" des attaques plus proches de la réalité, plus matures.

Un SoC (centre de supervision et d'administration de la sécurité) pertinent permet également de rentabiliser des équipements ou solutions déjà en place. Akerva fait également le lien entre ce type

d'expertise et l'activité Cyber Sécurité d'un SoC. Néanmoins, la plateforme apportera une réelle efficience seulement si les experts qui interviennent sont armés pour faire face à l'attaquant, que ce soit au niveau du bagage technique ou au niveau de l'expertise pour le durcissement des systèmes et de la configuration des équipements.

C'est dans cette optique qu'Akerva remet au client une feuille de route sous forme d'une matrice opérationnelle de suivi de l'application des préconisations. Cela permet, au final, aux équipes de production d'avoir une ligne directrice technique et organisationnelle en combinant l'expertise Akerva, l'expertise des équipes internes et les enjeux métiers.

C'est dans ce cas précis que les profils "Consultant Pentest" proposés par Akerva dans le cadre de missions longues d'Assistance Technique prennent tout leur sens.

A PROPOS D'AKERVA : Dirigée par Laurent Delaporte, Akerva développe un ensemble de services à très forte valeur ajoutée dans le domaine de la Sécurité des Systèmes d'Information dans des environnements complexes et déportés (Saas, virtualisation, Cloud Computing). L'entreprise intervient également dans les domaines de la Gestion des Identités et des accès (IAM).
En 2014, Akerva rachète Confluences IT, société spécialisée dans la transformation des systèmes d'information et la confiance numérique. A la fin de cette même année, Akerva crée avec ALTEN leader européen de l'Ingénierie et du Conseil en Technologies, une joint-venture spécialisée dans la cyber sécurité.
www.akerva.com.