SEREIN MAIS RÉACTIF FACE AUX CYBER-ATTAQUES

« Pour se servir de sa raison, on a besoin de sécurité et de quiétude » - Patrick Süskind

QUELQUES CHIFFRES

75,4 $Mds	Budget mondial de la sécurité informatique en 2015 (soit une hausse de 4,7% par rapport à 2014) - Source Gartner
+29%	Augmentation du budget de cybersécurité des entreprises françaises en 2015 - Source PWC
+51%	Progression du nombre de cyber-attaques en France sur l'année 2015 - Source PWC
56 mn	Temps moyen au bout duquel un scan malveillant advient après la création d'un nouveau serveur visible sur internet - Source Université du Michigan

Ces chiffres ne sont que le reflet de la place occupé par la sécurité dans le budget informatique. La cyber-sécurité prend de plus en plus d'importance, tant les enjeux sont cruciaux en termes de protection des données et des infrastructures. L'envie pour chaque entreprise est d'être sereine mais réactive en matière de cyber-sécurité. C'est devenu une priorité.

Une préoccupation quotidienne

Parce que l'essentiel de son business en dépend, l'informatique est devenue aujourd'hui une ressource primordiale pour l'entreprise. C'est pourquoi il est nécessaire d'en assurer les règles de bonne santé et d'hygiène, non seulement en prévenant les pannes par une maintenance régulière, mais également en mettant en place une surveillance de ses vulnérabilités.

Une équation insoluble

Malgré cette prise de conscience, beaucoup se heurtent à des problèmes techniques pour répondre à ces besoins de sécurisation. Dans un secteur en évolution si rapide, la méthode traditionnelle, qui consiste à réaliser un audit de sécurité une à plusieurs fois par an, devient largement insuffisante. Alors que faire? Multiplier les audits ? Une démarche quasimement impossible en termes de ressources et difficilement supportable en termes de coût.

Vers une surveillance continue et automatique des vulnérabilités

Grâce à des innovations majeures et brevetées, il est maintenant possible de réaliser un audit continu des infrastructures informatiques et des serveurs, sans en impacter la production. Un logiciel de détection des failles, capable de trier et d'adresser les résultats aux bons interlocuteurs, couplé à une prestation d'analyse, permet de prendre les bonnes décisions et d'assurer un environnement sain.

Elastic Detector

Elastic Detector facilite l'audit de sécurité des infrastructures informatiques, qu'elles soient virtuelles, cloud ou physiques. Le produit maintient en condition de sécurité l'infrastructure en détectant tout changement. Il se met à jour automatiquement en évitant la majorité des actions manuelles.

Auto-découverte Réseaux et serveurs découverts automatiquement	Périmètre de sécurité mis à jour des changements Pas de configuration Pas de risque d'erreur
Auto-checks Test de sécurité mis à jour et lancés automatiquement	Nouveaux serveurs automatiquement surveillés Pas de configuration Pas de risque d'omission Base de tests jamais périmée
Sans agent Pas de logiciel à déployer sur les serveurs	Pas de coût de déploiement ni de maintenance Pas de ressource utilisée Pas de risque de cheval-de-Troie
Clonage Analyse approfondie, de l'intérieur du serveur	Analyse poussée sans impact sur la production Serveurs dormants inclus Moins de faux positifs
Multi-cible Utilisation Cloud, virtuelle, physique et hybride	Adaptatif à l'environnement Infrastructures physique, virtuelles, clouds et hybrides Support d'environnement cibles simultanés
Reporting Rapports détaillés et tableau de bord	Synthèse Rapports configurables Alertes et réactivité Archivage et tendances

SECLUD IT
AHEAD OF SECURITY

eaZySecure
powered by SECLUDIT

EaZySecure est un service applicatif proposé par Comaxess, utilisant le logiciel Elastic Detector pour lutter contre les failles et les vulnérabilités des infrastructures informatiques.

Libre choix du support	Hebergé sur les infrastructures Cloud COMAXESS Installé sur les infrastructures client
Souplesse Deux formules au choix	Mode expert pour une prise en charge autonome par le client Mode Protection Avancée pour une délégation totale du service
Mode Expert Analyse assurée par le client	Logiciel Elastic Detector Maintenance (bug, correction, upgrade) Mise à jour quotidienne des vulnérablilités Support téléphonique
Mode Protection Avancée Analyse assurée par nos soins	Mode Expert + Prestations d''expert sécurité Analyse approfondie des scans Monitoring des alertes
Ergonomie	Pas d'installation compliquée à réaliser Pas d'agent à installer Interface conviviale et intuitive
Prédictibilité des coûts	Abonnement mensuel Formule tout compris

comaXess
cloud & it services