22/11/2012
EPR21/2012

www.enisa.europa.eu

La Cyber sécurité selon Winnie l'ourson: le nouveau rapport de l'Agence européenne ENISA sur les « pièges pot de miel numériques (Honeypot) » pour détecter les cyber attaques crée le buzz

L'agence de cyber-sécurité de l'Union Européenne, ENISA, lance une étude en profondeur sur 30 différents pièges numériques « pot de miel » ou « honeypot » qui peuvent être utilisés par les équipes de sécurité et d'urgences informatiques privées et gouvernementales pour détecter proactivement les cyber-attaques. L'étude révèle des freins à la compréhension des concepts de base de ces pièges et présente des recommandations sur les meilleures techniques à utiliser.

Le nombre croissant de cyber-attaques et leur complexité exigent une meilleure capacité de détection précoce d'alerte pour les CERT. Les pièges « honeypots » sont un leurre pour les attaquants, en imitant une ressource de calcul réel (par exemple, un service, une application, un système ou des données). Toute entité entrée en connexion à un « honeypot » est alors considérée comme suspecte, et son activité est surveillée pour détecter une malveillance.

Cette étude fait suite à un rapport de l'ENISA récent sur la détection proactive des incidents de sécurité réseau. Le précédent rapport concluait que les pots à miel ont été reconnus par tous les CERT comme un moyen efficace de recueillir des informations sur le comportement des hackers, mais leur utilisation pour détecter et enquêter sur les attaques n'était pas encore aussi répandue qu'on pourrait le croire, en raison d'obstacles à leur déploiement.

Cette nouvelle étude présente des stratégies de déploiement pratiques et les nouveaux enjeux critiques pour les CERT. Au total, 30 « honeypots » de différentes catégories ont été testés et évalués. Objectif: offrir un aperçu des solutions open source et de la technologie des « honeypots » qui sont les plus judicieuses en terme de déploiement et d'utilisation. Sans l'existence de solution miracle, cette nouvelle étude a identifié certaines lacunes et obstacles de déploiement pour les pièges « honeypots »: la difficulté d'utilisation, la documentation, le manque de stabilité du logiciel, le manque d'assistance aux développeurs, peu de standardisation, et l'obligation de faire appel à des personnes hautement qualifiées, et la difficulté de compréhension des concepts de base de la technologie de ces pièges. L'étude présente aussi un classement et explore l'avenir des « honeypots ».

Le directeur exécutif de l'ENISA, le Professeur Udo Helmbrecht a commenté:

"Les pièges « honeypots » offrent un outil puissant pour les CERT pour recueillir des renseignements sur les menaces sans aucun impact sur l'infrastructure de production. Correctement déployés, les « honeypots » offrent des avantages considérables pour les CERT : l'activité malveillante dans la circonscription d'un CERT peut être suivie pour assurer une alerte précoce des infections de logiciels malveillants, l'exploitation par les hackers de nouvelles vulnérabilités et les comportements malveillants, ainsi que donner l'occasion d'en apprendre davantage sur les tactiques des attaquants. Par conséquent, si le CERT en Europe connaissent mieux les « honeypots » comme une option de choix, ils pourraient mieux défendre leurs infrastrustures. "

Pour le rapport complet
Pour des renseignements complémentaires : COM(2009)149 et incidences juridiques de l'OTAN de botnets Contrer

22/11/2012
EPR21/2012

www.enisa.europa.eu

Pour toute demande d'interview, veuillez contacter : Ulf Bergstrom, Porte-parole, press@enisa.europa.eu- mobile: +30 6948 460 143, ou Cosmin Cioabanu, l'ENISA d'experts, à opsec@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu