BTS SIO

Veille technologique : les honeypots

Philippe JUNDT

Abstract

Le honeypot est un piège numérique qui permet de leurrer et identifier des attaquants. Ce procédé consiste à virtualiser par mimétisme sur un serveur une installation physique réelle. La virtualisation d'une infrastructure sur un serveur permet de berner la personne qui souhaite en recueillir les données et d'identifier cette intrusion. Cette technique implique de mettre en place des outils et de recourir à de l'Hypervision d'infrastructure.

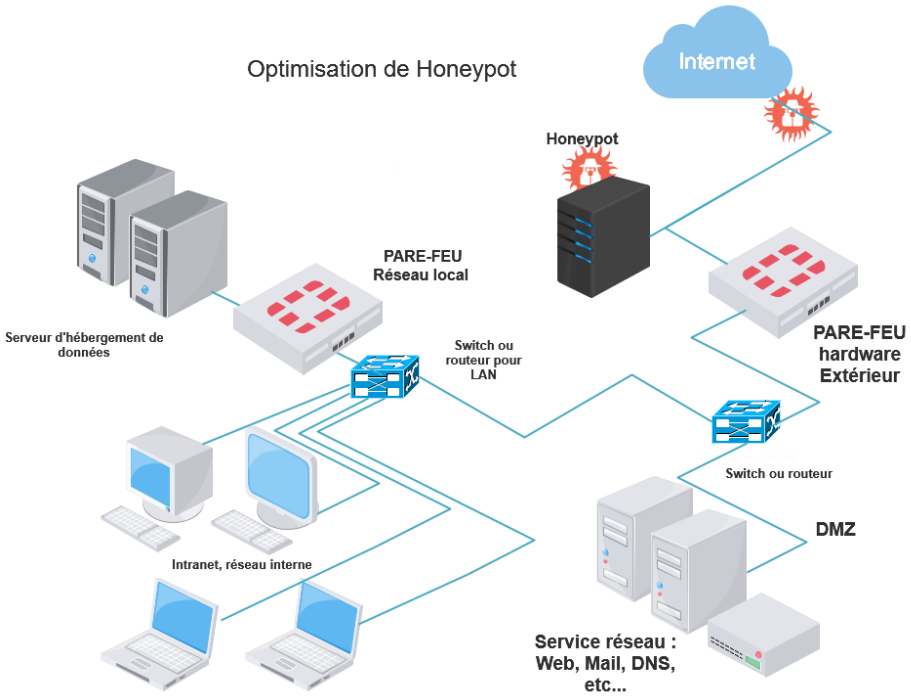
Les données enregistrées sur les serveurs d'une entreprise et les flux qui transitent sur son réseau interne ont de la valeur. L'utilité de ce procédé prend de plus en plus de sens pour sécuriser des installations informatiques. En effet les données ont de la valeur et font l'objet de convoitise, les organisations ont intérêt à les protéger. Aussi se prémunir de la sorte avec un honeypot contre les attaques par dénis de services, ou les attaques dont le but et la récupération d'information, prend tout son sens.

Ce type de sécurité est à prendre en complément d'autres mesures. L'intégrité de l'installation contre certaines menaces peut être assurée par divers éléments de sécurité, un code de bonne conduite des employés, des filtres pour réduire l'accès à des sites à risque, la mise en place d'anti-virus ou de pare-feu... Ce type d'équipements est à prévoir pour la prévention des attaques de serveurs qui stockent des informations sensibles (stratégie de développement, données bancaires, données médicales…) ou de valeur (factures, comptes clients, informations pour le paiement en ligne…).

Il s'agit notamment d'un élément lié à la sécurisation des systèmes et réseaux, un des moyens d'assurer leur intégrité et la sécurité des données sauvegardées dans les locaux d'une organisation.

Définition du Honeypot :

Il s'agit d'un piège numérique qui permet de leurrer et identifier des attaquants. Il reproduit par effet de mimétisme une installation physique réelle, par virtualisation de l'infrastructure.



<u>En résumé :</u>

Le honeypot est un équipement ou un outil de sécurisation de site qui a vocation à remplir une fonction de veille et de surveillance des intrusions. En cas d'incident ou d'attaque avéré le honeypot a plusieurs rôles : repérer l'incident, enregistrer de l'intrusion, retarder les actes de malveillance de soustraction d'information ou de dégradation d'infrastructure.
Les services installés sur le serveur honeypot permettront en principe d'apporter des éléments de preuve pour faciliter les actions de sécurisation future de l'infrastructure victime de l'acte de malveillance et faire cesser le préjudice, dans la mesure du possible en appréhendant les responsables.
Dans l'idéal cela permet de repérer l'assaillant, de le faire cesser ses actions et d'éviter la répétition du cyber-délit.