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.

Table des matières

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.

I. Présentation détaillée de la notion de Honeypot.

La protection active ou dynamique entraine également une possibilité d'apporter des réponses à une menace de façon graduée et proportionnée. Mais quelle est la responsabilité des propriétaires de cet équipement et qu'est-il possible de faire en cas d'identification d'une intrusion.

A. La vision juridique et technologique.

1. Les limites technique et déontologiques de tels procédés

Le déploiement de systèmes de défense a un coût économique et humain en termes d'entretien, de maintien en activité et de maîtrise des outils, cette technique implique également de recourir à des outils de virtualisation.
La France fait la promotion d'une doctrine « l'interdiction du hack-back par les acteurs du secteur privé dans le cyberespace »[1]. Ou interdit une contre-attaque en cas de découverte d'une personne ou d'un *bot* sur le réseau.
Les entreprises ont souvent des intérêts dans différents Etats et le fait d'avoir des locaux sur différents territoires rend la notion de cyber défense et hack-back complexe.
Pour résumer la convention de Budapest : seul les Etats ont l'obligation de lutter contre la cybercriminalité, d'ériger en infraction pénale les atteintes à l'intégrité de systèmes informatiques. Des groupes d'experts intergouvernementaux des Nations Unis sur la cybersécurité (UN GGN), préconisent aux Etats de « veiller à ce que les acteurs non-étatiques n'utilisent pas leur territoire pour commettre » des « faits internationalement illicites à l'aide des technologies de l'information et des communications »[2].

En effet en matière de contremesure, seul les Etats ont qualité à agir en adoptant des contre-mesures en réaction aux faits internationalement illicites commis par un autre Etat qui affecte leurs droits ou ceux de leurs ressortissants. Néanmoins un projet de loi aux USA intitulé ACDC pour Active Cyber Defense Certainty Act, vise à autoriser exceptionnellement les victimes d'une cyberattaque (section 1030) « access without authorization the computer of the attacker », de recourir à des mesures de cyberdéfense et d'accéder sans autorisation à l'ordinateur dit attaquant. Une autorisation sera émise formellement si une entité est victime d'une intrusion persistante et non autorisée de ses systèmes ou réseaux : « victim of a persistent unauthorized intrusion ».
En l'Etat actuelle, en France. C'est l'Etat au travers de ses entités et les juges qui donneront une autorisation à apporter une réponse défensive dynamique à une attaque. La jurisprudence est vague, mais l'on peut imaginer des actions en référé ou une information de l'Agence Nationale de la sécurité des systèmes d'information en fonction de la nature de l'attaque et de

[1] SGDSN, *Revue stratégique de cyberdéfense*, 12 février, 2018. disponible à l'url : publication.pdf
http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-
[22] Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, rapport de 2015. Note du Secrétaire général, A/70/174, 22 juillet 2015, p15

l'organisation ciblée. Une notion de légitime défense s'applique difficilement aux entreprises. Le risque de dommage collatéraux à des installations tierces, lors d'actions de hack-back d'une société lésée, l'expose à des dommages et intérêts. En outre des réactions instantanées, symétriques et disproportionnées risquent de faire peser des menaces sur les réseaux, tant en termes de bon fonctionnement des infrastructures, que de fonctionnement des services proposés par certains agents économiques comme les fournisseurs d'accès à l'internet (FAI).

2. Les normes, les pratiques et la technologie dans ce domaine

Les organisations ne sont pas sans défense pour autant. Le hack-back est distinct de la cyberdéfense passive des entreprises *« simple recours aux systèmes automatiques de protection des réseaux (…), placés à la frontière entre ceux-ci et l'extérieur »*. Les techniques de défense passive couvrent à elles seules un large spectre d'activité (fournisseur d'antivirus, parefeu…) et leurs menaces associées : virus, cheval de troie, ver informatique.

Actuellement seul les Etats ont réellement vocation à régler les conflits en cas d'extraterritorialité des dommages ou faits. Le développement de myriades de « corsaires numériques » est un fait. La question de leur légitimé à se considérer habilité par l'Etat à exercer un droit de représailles se pose[3].

Le "*hack back*" est fondé sur l'idée que "*the best defense is a good offense*". Le terme de "*hack back*" ou "*hacking back*" ou *"reverse hacking"* ne connaît pas vraiment de définition officielle et pratiquement aucune organisation internationale ne s'est jusqu'à présent véritablement penchée sur cette question capitale mais hautement sensible. Ce terme, qui pourrait être traduit en français par « *contre-piratage* », « *piratage en retour* » ou encore « *contre fouiner*[4] », décrit le fait, pour la victime d'une cyberattaque, de riposter.

Seul les Etats ont vocation *in fine* à agir en exerçant leur monopole de la violence légitime qu'ils détiennent légitimement, notamment en agissant à travers des autorités compétentes. Le risque est que des comportements entrainent une escalade de la violence et la problématique des dommages collatéraux reste ouverte.

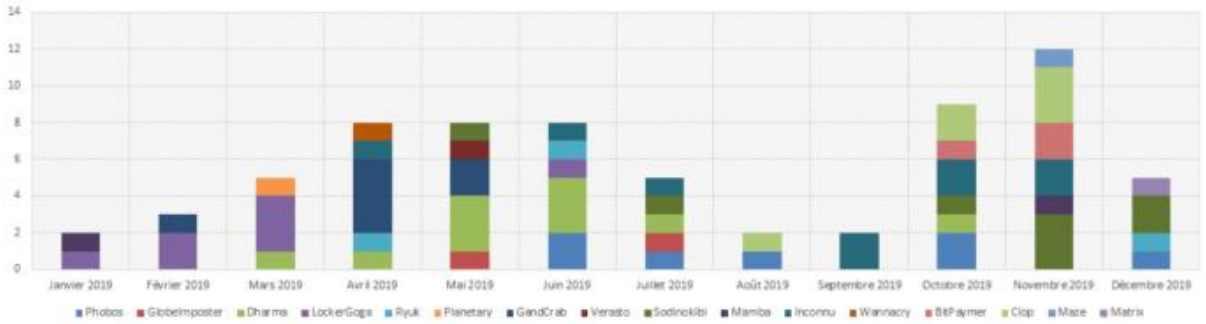
[3] *Cyberdéfense active par des entreprises privées ?Le* hack-back *entre l'hostilitéde la* Revue Stratégique de cyberdéfense *de la France et le projet de loi ACDC aux États-Unis* Karinne BANNELIER, Théodore CHRISTAKIS p.118

[4] la Commission générale de terminologie et l'Académie française, propose comme traduction française pour le nom « *hacker* » le mot « *fouineur* » (voir par exemple < http://www.gouvernement.fr/top-10-des-mots-d-internet-que-vous-allez-oser-dire-en-francais >). Si on suivait cette proposition, il faudrait ici traduire « *hacking-back* » par « contrefouiner
». Pour des raisons de commodité et pour éviter les confusions nous allons utiliser ici le terme anglais « *hack-back* ».

B. Un risque d'intrusion réel et un coût technologique et économique souvent pertinent

1. La maitrise des instruments de surveillances permet de contrôler en instantanée et d'enregistrer l'état d'un réseau

Il est avéré que les agents économiques ont besoins d'équipement informatiques pour mener à bien ses missions et son activité. Les menaces qui pèsent sur les installations informatiques sont bien réelles. De nombreuses installations ont été touchées, à des degrés de gravité variable, des administrations, des ministères ou des entreprises sensibles. Les cyber gendarmes de l'agence nationale de la sécurité des systèmes d'information, (ci-après l'ANSSI) ne communique pas toujours de façon transparente. Cet organisme, composé de près de 600 ingénieurs spécialisés, est sans doute tenu à la réserve en raison de sa fonction de publication, de veille et de participation aux mécanismes de défense. *« Tout juste apprend-on qu'une majorité d'incidents a eu lieu dans les domaines de la santé (un incident sur quatre) et des collectivités territoriales (un incident sur cinq). Une prévalence qui peut s'expliquer par la sensibilité de ces secteurs ainsi que par leur manque de moyens pour parer l'attaque seuls.*



Le nombre d'incidents, par mois, liés à des rançongiciels qu'a dû traiter l'Anssi indique une prévalence pour ce type d'attaque. C'est donc les données qui sont souvent prisent pour cible lors d'acte malveillant.
Selon l'ANSSI même si elle concède manquer d'informations exhaustives en ce qui concerne les rançongiciels sur l'ensemble du territoire français, estime qu'ils constituent aujourd'hui « la menace informatique la plus sérieuse pour les entreprises et institutions[5] *».*

Pour illustrer le caractère tangible de cette menace et sa proximité. Les serveurs de la région Grand-Est a entrainé des dénis de services et des retards de fonctionnement. La recrudescence de ces actions ou tentative de captation de données informatique, montre qu'une bonne défense est indispensable. Grace à la mise en place d'équipement adéquate cette attaque n'a eu qu'un impact limité et les données ont été préservées. Néanmoins cette intrusion a entrainé des retards dans les marchés publics et ont induit un certain retard dans le traitement de dossiers[6].

Les actes sont généralement repérés rapidement par les victimes. Cependant le vol de données peut réellement causer des préjudices, même si l'infrastructure reste intacte et peut

[5] Rançons exorbitantes, attaques ciblées : 2019, année « faste » pour le rançongiciel, Martin Untersinger, Article paru à l'url : https://www.lemonde.fr/pixels/article/2020/01/31/rancons-exorbitantes-attaques-ciblees-2019-annee-faste-pour-le-rancongiciel_6027913_4408996.html
[6] La région Grand-Est embourbée dans un cyberattaque, article de Jacques Cheminat, url : https://www.lemondeinformatique.fr/actualites/lire-la-region-grand-est-embourbee-dans-une-cyberattaque-78192.html

induire des retards. Les retards pour les entreprises ou leurs clients peut se traduire rapidement en un préjudice économique ou moral.

« Cette affaire rappelle que nul n'est à l'abri d'une cyberattaque et remonte les questions du niveau de sécurité au sein des administrations au centre des débats. L'impact des ransomwares devient de plus en plus important et surtout coûte cher aux entreprises et aux collectivités. Un rapport de Deep Instinct estime à 11,5 milliards de dollars les dommages générés par les ransomwares et une moyenne de 141 000 dollars par incidents (contre 46 800 dollars un an plus tôt). Parmi les rançongiciels les plus actifs en 2019, on retrouve Sodinokibi et GrandCrab »[7]. Certains faits nous rappel que ce ne sont pas que les organismes qui sont visés par ces actions, mais que les célébrités ou les personnes représentant les institutions. Cette menace reste d'actualité : le piratage de personnalité montre le caractère organisé des actions[8].

Les organisations publiques et privées ont donc particulièrement intérêt à mettre en place des procédures et équipements en vue de se prémunir contre les « hack » et notamment pour prouver qu'il y a bien eu des manœuvres en vue de soustraire une information ou de saboter des équipements. *A fortiori* cela permettra de constituer des preuves pour agir *in fine* devant un juge et auprès des autorités compétentes, en vue de réclamer la cessation d'un acte continu ou de prévoir des actions de « hack back ». Seuls certains instruments dont le honeypot et l'hypervision ont vocation à permettre d'identifier en direct un éventuel assaillant ou d'archiver une éventuelle intrusion.

2. Un moyen de réduire le temps à consacrer à la gestion des failles de sécurité du système.

Le nombre d'attaque par déni de service augmente par exemple avec les ordinateurs zombis, qui peuvent être utilisés à l'insu de leurs propriétaires par des pirates. Veiller à l'intégrité des infrastructures durant une période non travaillé, comme de nuit, concours également à sécuriser une organisation.
Cette question est particulièrement pertinente pour les ordinateurs zombies ou ordinateurs qui exécute en arrière-plan des services plus ou moins légaux.
En effet la mise hors service de tels *botnets* lors d'une opération de hack-back pourrait alors affecter des équipements de parties innocentes.
En ce qui concerne l'exemple de l'institution, la Région Grand Est a été aidée par un prestataire externe et a reçu le soutien de l'ANSSI pour réparer les dégâts. Après près d'une semaine de remédiation, les agents peuvent à nouveau envoyer des mails[9].

Pourtant la sophistication des moyens mis en œuvre par les attaquants et les moyens déployés pour réaliser de tels actes sont de plus en plus élaborés, instantanés et risquent de devenir coordonnés. Le droit international préconise aux Etats des mécanismes de règlement pacifique des différends (ou de ceux affectant leurs nationaux et leurs biens). De nos jours 200

[7] Ibid. Jacques Cheminat
[8] Le mondeinformatique, REvIL/Sodinokibi : Trump et Madonna victimes du ransomware as a business, Jacques Cheminat url : https://www.lemondeinformatique.fr/actualites/lire-revil-sodinokibi-trump-et-madonna-victimes-du-ransomware-as-a-business-79155.html
[9] Op. cit. La région Grand-Est embourbée dans un cyberattaque, article de Jacques Cheminat

millions d'entreprises existent de par le monde, réparties sur près de 200 Etats. Donner licence à tous ces organismes de se faire justice tout seul aurait de fâcheuses conséquences.

II. L'intérêt de l'outil pour les organisations

Tous les Etats et organisations sont potentiellement des cibles d'attaques informatiques. Pour la dernière décennie, les attaques de Wannacry ou NotPetya sont des marqueurs cités dans tous les articles en lien avec les attaques informatiques[10]. L'UE dénombrait 4000 attaques de rançongiciels lancées quotidiennement à travers le monde en 2016[11], pour la même année 80% des entreprises européennes avaient été touchées par une cyber-attaque au cours de l'année écoulée. Les conséquences économiques de ces attaques ont quintuplé entre 2013 et 2017 et pourraient quadrupler d'ici à 2019. L'année 2020 a notamment été marqué par une cyberattaque contre Bouygues construction[12].

A. Quelles données protéger de quels risques

Les entreprises spécialisées dans le domaine de la cybersécurité estiment en 2017 que le coût mondial des cyberattaques pourrait atteindre la somme de 6 trillions de dollars d'ici 2021[13]. Les données clients sont essentielles, préserver les projets et travaux réalisés par les différents services de l'organisation.
Presque tous les postes d'une entreprise ou d'une association peuvent de nos jours être organisés autour d'équipement numérique et dématérialisé en vue de faciliter les échanges entre les différents employés, les différents services ou les différents bénévoles.

Les organisations doivent s'adapter aux demandes qui nécessite souvent une recrudescence des moyens humains ou matériels et une notion d'immédiateté. L'hypervision permet au moins de dissuader les menaces internes et de veiller aux menaces extérieures. La virtualisation d'infrastructures sont des méthodes qui permettent de limiter les risques et de limiter les dénis de service en cas d'attaque par déni de service.
Les outils informatiques permettent aux organisations d'être plus flexibles et réactives, mais implique également qu'elles doivent se prémunir face à de nouveaux risques d'intrusion. Cette vulnérabilité des infrastructures numérique oblige les acteurs à investir dans ce domaine et implique de s'organiser de façon à prévenir le risque de cyber-attaque.

---

[10] *Ibidem Unis*, Karinne BANNELIER, Théodore CHRISTAKIS
La cyber-riposte des entreprises privées, Laura Baudin Programme de doctorat en droit site, Fonds d'investissement des cycles supérieurs de l'Université de Montréal, url, https://www.ficsum.com/dire-archives/automne-2019/societe-la-cyber-riposte-des-entreprises-privees/
[11] Auteurs de l'étude « Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés » (*Les Cahiers de la Revue défense Nationale*) préparatoire à la conférence internationale « Construire la paix et la sécurité internationale de la société numérique. Acteurs publics, acteurs privés : rôles et responsabilités » organisée par le gouvernement français à l'UNESCO les 6-7 avril 2017, ouvrage qui a été honoré du prix du livre « Cyberdéfense » décerné par le Forum International de Cybersécurité 2018 et remis aux auteurs par la ministre des Armées, madame Florence Parly. Cet article a bénéficié du
support l'Agence nationale de la recherche dans le cadre du programme « Investissements d'avenir » (ANR-15-IDEX-02).
[12] Le « back-office » de Bouygues Construction paralysé par une cyberattaque, article des Echos par Myriam Chauvot, url https://www.lesechos.fr/tech-medias/hightech/le-back-office-de-bouygues-construction-paralyse-par-une-cyberattaque-1169428
[13] Rapport, url https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

B. Quelles réponses apporter aux risques, incidents ou comportements illicites

La réticence de la France s'explique probablement par les risques d'un hack-back « sauvage » laissé à la discrétion des acteurs privés et sans contrôle de l'État, pratique qui le différencie d'un *hack-back* « sage » lancé par l'Etat avec l'aide, si nécessaire, d'acteurs privés.

Le droit n'autorise que des actions purement « réactive ». Le Etats sont seuls détenteurs de l'autorité de police et ont le monopole de la contrainte légitime. Les acteurs privés doivent se prémunir et éviter de se faire justice privée, mais une certaine défiance à l'égard des Etats se fait ressentir en raison d'une incapacité de ces derniers à protéger efficacement les personnes morales ou physiques contre les cyberattaques.

Le honeypot permet donc aux équipes victimes d'une cyberattaque de pouvoir agir lorsque celle-ci est déceler. Le temps de réaction offre la possibilité de mettre en œuvre des moyens matériels et humains afin de prévenir un vol d'information ou une dégradation d'équipement réseaux.

III. Les honeypot en serveur local

La force du honeypot est à la fois une faiblesse. Le honeypot peut-être sur un serveur physique directement relié à la production. Cette architecture induit un risque de passage d'une menace réelle confinée sur un équipement dédié à la repérer et capter les indices, sur le réseau des équipements liées à une activité économique.

A. Une mise en place rigoureuse et un suivi méticuleux

1. Un suivi technique et technologique des installations

Une mise à jour système qui modifie une règle, un port mal configuré… ce n'est que quelques exemples d'une situation qui peut permettre le passage de l'assaillant à la production. Autant d'arguments qui incitent à réaliser une installation rigoureuse et de réaliser un suivi régulier des mises à jour, des modifications à effectuer ou des évolutions techniques à implémenter. Les outils de protection et de virtualisation orienté honeypot se multiplient.

Les pistes pour installer le honeypot sur un serveur local. Il est possible de placer le honeypot à l'entrée de l'infrastructure au niveau du routeur qui a accès au World Area Network ou WAN. L'avantage de cette stratégie est de réduire le risque pour les réseaux internes. Ainsi le honeypot extérieur réduit les problèmes de conflits avec le pare-feu. L'inconvénient est qu'il ne capture pas les attaquants internes.
La seconde stratégie est de l'installer au niveau des serveurs de fonctionnement de service ou DMZ[14]. Cependant le honeypot ne couvrira pas entièrement la DMZ de façon efficace. De

[14] Guide digital, présentation de la notion de DMZ, IONOS url : https://www.ionos.fr/digitalguide/serveur/securite/quest-ce-quune-zone-demilitarisee-dmz/

plus de présence de pare-feu extérieur le honeypot ne peut remplir son rôle que si des ports supplémentaires sont ouverts dans ce but. Cela implique d'augmenter le risque d'intrusion.

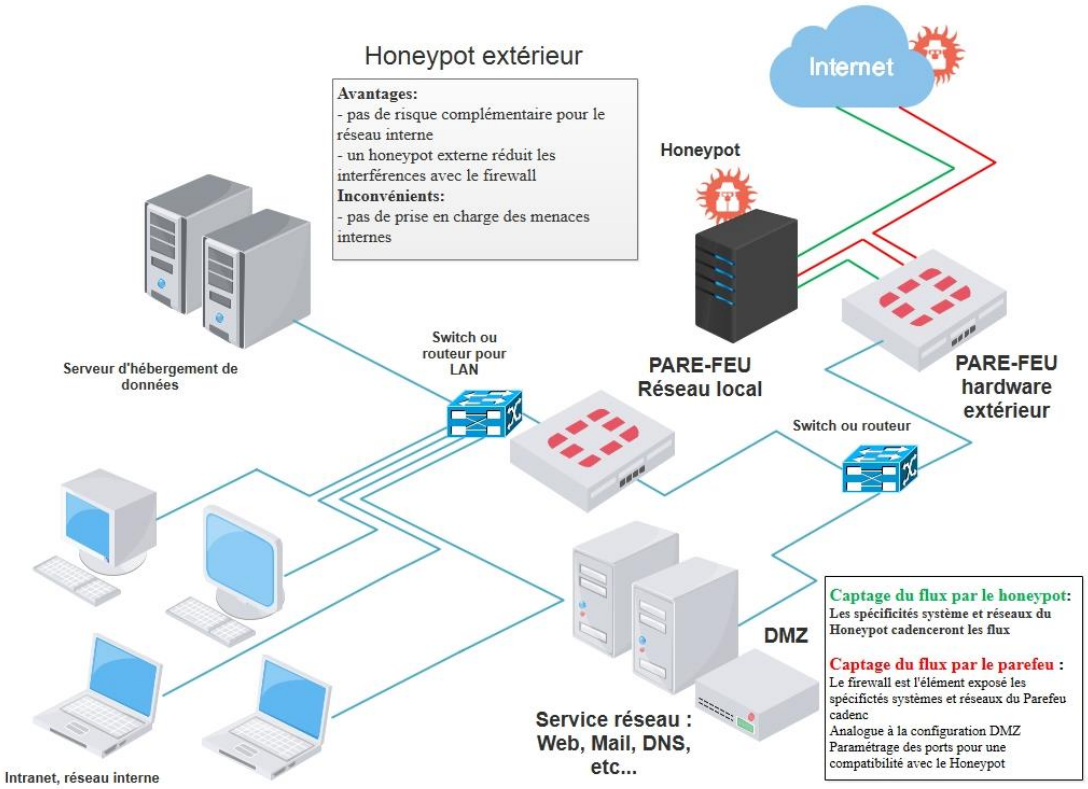
Enfin il est possible d'installer un honeypot au niveau du Local Area Network ou LAN. Cela permet notamment de détecter des défauts de configuration du pare-feu. Avec l'inconvénient de compromettre les autres systèmes. Malheureusement il peut lui-même servir de base à une attaque ou induire des conflits avec des services. Enfin, les règles de pare-feu doivent être préciser pour filtrer le trafic jusqu'au honeypot.

2. Optimiser le service en fonction des installations, préserver les locaux

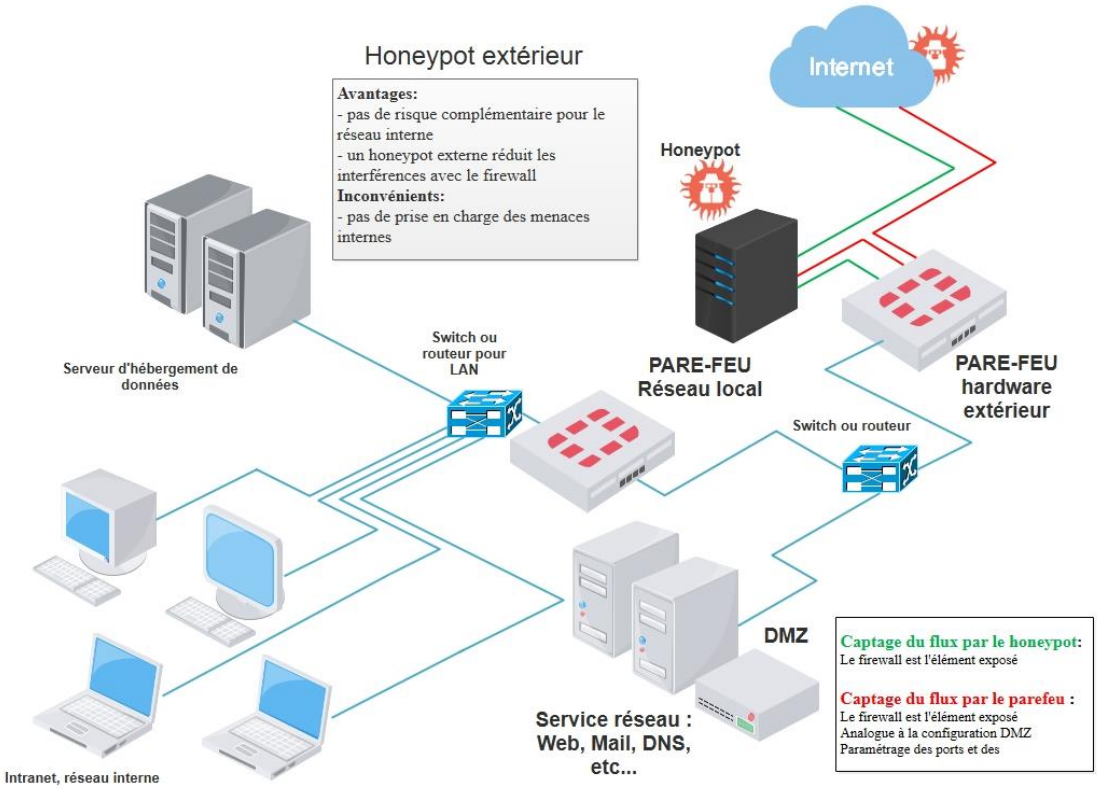
Où installer le système de honeypot ? "The next question is, where should you put your honeypots? Putting a honeypot outside of your DMZ and toward the internet is a popular option. That's an excellent location for watching external cyber-attacks on your network". Prévoir une topologie réseaux et instaurer des architectures dans ses configurations réseaux permet de faciliter la sécurisation des équipements et d'optimiser le fonctionnement des équipements de sécurité. Installer un honeypot prêt des interfaces réseaux des routeurs connectés en NAT à l'internet parait donc l'endroit le plus approprié.
"You probably don't want to put a honeypot inside your DMZ, because attacks to your DMZ can have terrible consequences. You should also consider putting a honeypot on the other side of your DMZ, in a location that's accessible to users in your private network".
Avoir accès au honeypot depuis le réseau local permet d'être alerté en direct en cas d'intrusion ou d'incident. Cependant il convient également d'établir quels utilisateurs auront accès au réseau privé. Déterminer des droits d'administration réseau clair est un bon moyen de réduire les menaces en interne.
Concrètement une DMZ ou zone démilitarisée est composé de serveurs ou systèmes qui ont besoin d'avoir un accès internet pour permettre le bon fonctionnement de l'organisation (messagerie, hébergement de domaine, etc…)[15].

[15]Guide digital, IONOS url : https://www.ionos.fr/digitalguide/serveur/securite/quest-ce-quune-zone-demilitarisee-dmz/

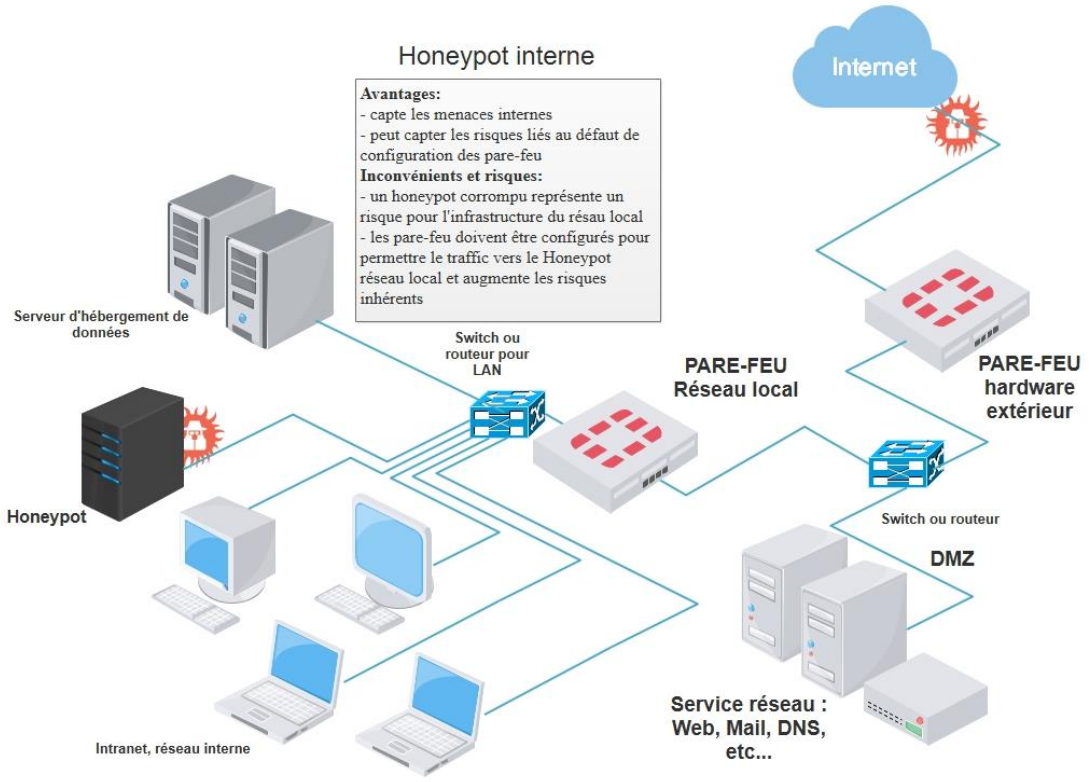
L'emplacement extérieur :



L'emplacement DMZ :



L'emplacement réseau interne ou réseau local :



"As long as you make sure as few employees and contractors know about the internal honeypot as possible, it can be an effective way to catch and analyze internal as well as external attacks". According to IBM"s 2016 Cyber Security Intelligence Survey, about 60% of cyber-attacks are done by insiders"[16].
Une installation sur un serveur à part permet de l'isoler et prévenir les attaques extérieures et de le préserver d'éventuelles intrusions internes.

B. Le honeypot en serveur en site propre

Centraliser les moyens de défense sur une place permet de réduire les menaces externes. Les serveurs honeypot ont essentiellement vocation à réguler et capter les menaces extérieures et est un moyen de prévention complémentaire à d'autres outils de protection : pare-feu software ou hardware, antivirus, service de régulation des sites à risque, etc…

Le honeypot ne protège pas contre des actes de malveillance en interne, qu'il soit volontaire ou involontaire. Le piratage par clé USB corrompue, ou la diffusion d'informations confidentielles par un employé à des tiers sont des points de sécurité à aborder par l'organisation en adoptant des règles de bonnes pratiques, en édictant un règlement précis ou en s'équipant d'infrastructures adaptées pour faire écran à ces menaces.

[16] Site AT&T business, entreprise de télécommunication, url : https://cybersecurity.att.com/blogs/security-essentials/explain-how-honeypots-work-to-me

Les outils d'hypervision, les outils de virtualisation d'infrastructure réseaux sont des éléments software qui permettent à un organisme de modéliser des infrastructures existantes pour leurrer des personnes malveillantes.

L'intérêt de réduire l'emprunte des bots qui sont responsables du spamming. Dématérialiser son honeypot est un pléonasme, mais le faire fonctionner à distance est une autre perspective de recours au software as a service.
Développe pourquoi il est intéressant de recourir à système cloud public ou SAAS pour y installer un honeypot, notamment pour isoler son installer des risques de débordement.

« Ces techniques consistent à augmenter virtuellement le ratio coût/effort nécessaire à une intrusion afin de détourner l'intérêt de l'attaquant. Ainsi, la dissuasion encourage un cybercriminel à s'intéresser à d'autres systèmes promettant plus de bénéfices à moindre coût. C'est l'application du principe " le jeu en vaut la chandelle " ... Aujourd'hui, l'efficacité de cette stratégie anti-intrusion est remise en cause dans un environnement moderne où la majorité des pirates sont animés par le "easy kill" et une "shotgun approach". En effet, les attaquants perdent rarement de temps à analyser les systèmes qu'ils visent, leur but étant de toucher le maximum de machines ou de voir simplement à quoi ils accèdent avant de recommencer. Pire encore, la plupart des attaques ne sont pas exécutées en direct par les pirates, mais bien de façon programmée par des outils automatisant les attaques (comme les vers par exemple). Seule exception notable, les attaquants aux " cibles choisies " par opposition aux " attaques par cible d'opportunité " susvisées, et qui concernent les rares pirates de haut vol, plus impliqués dans des actions proches de l'espionnage et du contre-espionnage industriel ou du sabotage »[17] ...

L'utilisation d'outils de sécurité permet d'assurer l'intégrité des équipements réseaux, d'assurer la sécurisation et de préserver l'intégrité des données transmises. En l'informatique le fait de réaliser des redondances ou des sauvegardes sur différents sites est un élément de sécurité passive. Le fait de garantir l'intégrité d'une installation avec des procédés de veille à distance à l'avantage de cloisonner les débordements possibles en cas de de piratage.

IV. Les principaux acteurs du marché des honeypot

A. Les GAFAMI et les projets honeypot pour protéger des technologies populaires.

Les technologies googles souffrent de certaines failles, des événements tels de Google Hack Honeypot a vocation à permettre aux participant de maîtriser les outils googles et contribuer à améliorer les procédures de sécurité. Il s'agit d'un projet PHP qui a vocation de permettre de répondre à certain type d'attaques[18].
IBM propose des technologies basées sur les honeypot : un tel mécanisme permet notamment de se prémunir contre les Honeypot « for spam protection »[19], ou d'autres « éléments indésirables »[20]. Le personnel qui y a recours doit être formé. Les différentes interventions à réaliser se font en respectant des limites de temps et des procédures[21].

[17] Marie Barel Juriste, spécialiste en droit des technologies de l'information et de la communication et sécurité de l'information
[18] Les 'Google hacks' ont désormais leur honeypot, url : https://www.silicon.fr/les-google-hacks-ont-desormais-leur-honeypot-9085.html
[19] Présentation du service anti-spam, url : https://www.ibm.com/support/knowledgecenter/SSMNED_5.0.0/com.ibm.apic.devportal.doc/tapic_portal_honeypot.html
[20] Présentation de sécurisation du réseau, AT&T, url : https://cybersecurity.att.com/blogs/security-essentials/explain-how-honeypots-work-to-me
[21] Présentation du service anti-intrusion, url : https://www.ibm.com/support/knowledgecenter/fr/SSFS6T/com.ibm.apic.devportal.doc/tapic_portal_honeypot.html

Enfin des guides de bonnes pratiques incitent à ne plus faire de cloisonnement entre les différentes infrastructures. Leaders and some advice : “Install your honeypot virtual machines from the same disc images you use to install operating systems in your production network. Configure its local firewall to have more open TCP/IP ports, and fewer filtered ports altogether. Leave more of the default OS and application settings. “That way, if an attacker OS fingerprints your honeypot, they can try exploiting some vulnerabilities that have been known for a long time. Or not”.

B. Le leader en matière de livraison de honeypot : Trend Micro

Trend Micro est une entreprise japonaise qui compte parmi les leaders dans le domaine des solutions de sécurité informatique. Cette entreprise réalise des enquêtes régulières, une enquête de janvier 2020 révèle que « les environnements industriels non sécurisés sont le plus souvent victimes de menaces courantes. Le honeypot a en effet été piraté à des fins de minage de crypto-monnaies, a été visé par deux attaques distinctes de ransomwares et a été détourné pour fraude à la consommation ».

Si des menaces sérieuses sont avérées comme la plus célèbre portant sur des ransomware : « S’il est vrai que ces attaques présentent un risque dans le contexte de l’industrie 4.0, notre enquête démontre que ce sont des menaces plus courantes qui sont le plus susceptibles de frapper », pour le Directeur technique Europe du Sud, Trend Micro « Les petites usines ou unités de fabrication auraient donc tort de penser que les cybercriminels les laisseront tranquilles. L’absence de dispositif de protection élémentaires pourrait notamment ouvrir la voie à des ransomwares ou à des tentatives de détournement des capacités de traitement informatique. Le but étant de miner des crypto-monnaies, attaques relativement peu sophistiquées mais qui pourraient avoir des conséquences fâcheuses pour les résultats de l’entreprise. »

Pour parer à ce type de menace sur les installations industrielles, l’entreprise Trend Micro Research a créé un prototype d’entreprise industrielle réaliste : avec des équipements de contrôle industriel, un mélange d’hôtes physiques et de machines virtuelles assurant le fonctionnement de l’usine, notamment plusieurs automates industriels programmables, des interfaces homme-machine, des postes de travail techniques et robotisés, ainsi qu’un serveur de fichiers.

Trend a optimisé ses solutions pour les principaux environnements du marché - parmi lesquels Amazon Web Services (AWS), Microsoft® et VMware®.

<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 avérée 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.

Eléments bibliographiques et sitographie

Articles de blogs spécialisés :

Using Dynamic Honeypot CyberSecurity : What do you need to know?
https://www.guardicore.com/2018/10/dynamic-honeypot-cyber-security/
What Is A Honeypot And How It Helps Improve Cybersecurity?
https://tweaklibrary.com/what-is-a-honeypot-and-how-it-helps-improve-cybersecurity/
Honeypots Catch Winnie-The-Pooh…And Hackers Too!
https://blog.ipswitch.com/honeypots-catch-winnie-the-pooh-and-hackers-too
Why use honeypot ?
https://resources.infosecinstitute.com/honeypots-in-the-cloud/#gref
How to Use Honeypot Traps to Fight Email and WordPress Spam
https://www.mailpoet.com/blog/email-honeypot-traps/
Honeypot-as-a-Service démontre que la sécurité IoT n'est encore et toujours pas satisfaisante
https://veille-technologie.mobivision.fr/2019/10/15/honeypot-as-a-service-dmontre-que-la-scurit-iot-nest-encore-et-toujours-pas-satisfaisante-data-news/
Honeypot un pot pourri… juridique, par Marie Barel, disponible en pdf :
http://actes.sstic.org/SSTIC04/Droit_et_honeypots/SSTIC04-article-Barel-Droit_et_honeypots.pdf
La zone démilitarisée : protéger le réseau interne
https://www.ionos.fr/digitalguide/serveur/securite/quest-ce-quune-zone-demilitarisee-dmz/
Les 'Google hacks' ont désormais leur Honeypot
https://www.silicon.fr/les-google-hacks-ont-desormais-leur-honeypot-9085.html
La protection par honeypots (et les risques couverts)
https://www.frameip.com/honeypots-honeynet/

Articles et comptes rendu ou documentation universitaire :

Cyberdéfense active par des entreprises privées ? Le Hackback entre l'hostilité de la revue stratégique de cyberdéfense de la France et le projet de loi ACDC aux Etats-Unis,
revue Institut de Stratégie Comparée, par Karinne Bannelier et Théodore Christakis
Disponible à l'url :
https://www.cairn.info/revue-strategique-2017-4-page-99.html

Onze thèses sur la transparence, revue multitude, traduit de l'italien par **André Salsedo**
https://www.cairn.info/revue-multitudes-2018-4-page-70.html

Communication d'entreprise :

Using honeypot for spam protection IBM
https://www.ibm.com/support/knowledgecenter/SSMNED_5.0.0/com.ibm.apic.devportal.doc/tapic_portal_honeypot.html
AT&T Business, Explain how honeypots work to me, par Kim Crawley, Guest Blogger
https://cybersecurity.att.com/blogs/security-essentials/explain-how-honeypots-work-to-me
How configure honeypot on a windows system :

https://answers.microsoft.com/en-us/windows/forum/all/how-to-configure-a-honeypot-server-on-a-windows/bcb0d450-b5b8-4b2e-b75a-5b8a8b4e665d

Trend Micro crée un honeypot industriel pour piéger les hackers : https://www.trendmicro.com/fr_fr/about/newsroom/press-releases/2020/20200121-trend-micro-cree-un-honeypot-industriel-pour-pieger-les-hackers.html

Article de journaux et sites spécialisés :

REvIL/Sodinokibi : Trump et Madonna victimes du ransomware as a business, Le monde informatique, par Jacques CHEMINAT, 20 mai 2020, url : https://www.lemondeinformatique.fr/actualites/lire-revil-sodinokibi-trump-et-madonna-victimes-du-ransomware-as-a-business-79155.html
La région grand est embourbée dans une cyberattaque, Le monde informatique, par Jacques CHEMINAT, 21 février 2020, url : https://www.lemondeinformatique.fr/actualites/lire-la-region-grand-est-embourbee-dans-une-cyberattaque-78192.html