note de VEILLE

janvier 2017

Diffusée aux membres et partenaires d'AEC et de Digital Aquitaine, cette Note de veille mensuelle sur les mondes numériques vous délivre un diptyque actualités territoriales – tendances globales à déguster très frais.

CYBERSÉCURITÉ, LE VIRUS DES ENTREPRISES

A l'heure où l'on apprend régulièrement dans les médias que des entreprises se sont fait pirater leurs données, mettant les informations confidentielles de leurs clients aux yeux de tous, la cybersécurité est au cœur des préoccupations. Dernier piratage majeur en date, Yahoo et la fuite de données de plus d'un milliard de clients. Cas sensationnel, il est malheureusement loin d'être isolé et beaucoup ne sont jamais dévoilés. Pour mieux comprendre les enjeux en matière de cybersecurité, nous tenterons d'en dresser un rapide état des lieux, puis de présenter certaines alternatives et moyens mis à disposition des entreprises pour se prémunir contre cette menace.

Etat des lieux de la cybersécurité

Pour mieux comprendre les enjeux autour de la cybersécurité, il semble important d'en avoir une vision chiffrée. En France selon une étude PwC[1], la sécurité informatique a représenté un investissement moyen de **3.9 millions d'euros par entreprise** sur les 12 derniers mois (contre 4.6 millions au niveau mondial). Marché colossal, qui n'est pas prêt de faiblir si on en croit les prévisions et l'évolution des attaques ces dernières années en France (+ de 51% entre 2014 et 2015 contre 38% au niveau mondial). En effet, **81% des entreprises françaises** ont été la cible de cyberattaques en 2015. Constat alarmant surtout si on prend l'exemple d'EDF et de ses **10 millions d'attaques** annuelles (en moyenne). Quand on connait le coût moyen d'une attaque « réussie » pour l'entreprise victime, (**entre 300 K€ et 1.3 M€ selon la taille),** il y a de quoi réfléchir. Pour exemple, l'an passé, TV5 a dû débourser pas moins de **4.6 millions d'euros** pour réparer les dégâts de l'attaque subie. Il semble également important de souligner que 35% des incidents de sécurité dans les entreprises seraient le fait des collaborateurs malgré eux (bien souvent par manque de sensibilisation).

2016, une année sous le signe de la cybermenace IoT

Récemment une partie du web (Amazon, Netflix, Twiter...) a été paralysée suite à une attaque DDoS (attaque par déni de service), contre la société Dyn, qui se charge de faire le pont entre les adresses IP et le nom des sites internet (autrement appelé service DNS). Cela a été rendu possible par les hackers en s'appuyant sur la masse d'objets connectés en circulation, transformés en botnets[2]. Ce type d'attaque sature les serveurs par un nombre de requêtes pour lesquelles ces derniers n'ont pas la capacité technique de répondre, ce qui finit par rendre inaccessible les services hébergés. La grande quantité d'objets connectés en circulation va rendre ce type d'attaque de plus en plus fréquente au cours des prochaines années. Pour illustrer ce propos, **3 chiffres** : 3.5 milliards d'internautes, 6 milliards d'objets connectés actuellement en circulation, 20 milliards d'ici 2020. Il semble donc primordial de s'interroger sur la nécessité de rendre cet Internet des Objets (IoT) sûr.

Il semble que la priorité soit donc à la protection des entreprises, mais quels sont les moyens de se prémunir ?

Se prémunir face à la menace

De nombreuses solutions existent aujourd'hui pour protéger les infrastructures ou prévenir les attaques. Elles ne sont pas toutes à la portée de toutes les entreprises, mais ont le mérite d'apporter leurs lots d'innovations.

La Threat intelligence

A l'origine issue du monde militaire et des renseignements, la Cyber Threat Intelligence (ou CTI) est l'étude et la compréhension des menaces informatiques. L'idée est de faire émerger des modèles type (schéma) exploitables afin de prévenir les menaces pour la sécurité des données d'une organisation. L'approche n'est plus autocentrée sur les propres ressources de l'organisation qui s'appuierait sur ce type de solution mais, au contraire, ouverte sur la compréhension de l'origine des cyberattaques et des motivations des hackers, permettant d'adapter les modèles de cyber sécurité à l'évolution de la cybercriminalité. Concrètement, la threat intelligence va s'appuyer sur des flux de renseignements, de la veille sur des forums de cybercriminels, des analystes chargés d'établir des modèles concernant la récurrence des attaques, leurs modes opératoires, la méthodologie des hackers, dans le but d'anticiper les attaques. Ainsi, des entreprises comme **cybelangel**,

1 « The Global State of Information Security® Survey 2016 » réalisée par le cabinet d'audit et de conseil PwC, CIO et CSO réalisée en ligne du 4 avril 2016 au 3 juin 2016. Les résultats présentés ici se basent sur les réponses de plus de 10 000 CEO, CFO, CIO, RSSI, OSC, vice-présidents et directeurs de l'information et des pratiques de sécurité de plus de 133 pays.

2 Objets infectés et contrôlés à distance par le(s) hacker(s) à l'insu des propriétaires.

Réalisé par AEC l'agence aquitaine du numérique — En partenariat avec DIGITAL AQUITAINE — Avec le soutien de Région Nouvelle-Aquitaine

se charge par exemple de scanner le darknet[3] (ou deep web) afin d'identifier les informations sensibles des entreprises qui y circulent et d'agir en conséquence. Demandant de nombreuses ressources, la threat intelligence n'est pas à la portée de toutes les entreprises et ne peut se résoudre à une simple collecte de données sans une surcouche d' « intelligence ».

Le bug bounty : les hackers au service des entreprises

Initié en 1995 par Netscape aux Etats Unis, le « bug bounty » est une pratique qui consiste à rémunérer des « white Hats[4] » à la faille de sécurité trouvée. Les entreprises organisent des sessions avec des hackers afin qu'ils testent les nouveaux produits/services, qu'ils plongent dans les entrailles de la technologie, pour en comprendre le fonctionnement et en faire émerger les failles qui permettraient d'en détourner l'usage. L'entreprise doit alors périmétrer le domaine d'intervention des hackers et établir les règles du programme (et les limites à ne pas dépasser). La récompense quant à elle sera fonction des failles remontées, de leur complexité, de leur documentation et des préconisations voir des patchs[5] fournis pour y remédier. Très courante parmi les entreprises technologiques, cette pratique se généralise à d'autres secteurs. L'avantage est qu'elle force à une obligation de résultats, contrairement aux solutions de « **pentesting** » qui se proposent également d'identifier les failles de sécurité dans les systèmes, mais qui sont soumises à une obligation de moyens. Or, peu d'entreprise sont en mesure de pouvoir s'offrir ce type d'audit régulièrement. De fait, les sociétés de pentesting fournissent un rapport détaillé de la sécurité des systèmes mais uniquement pour un instant T contrairement à un programme de bug bounty qui peut être mis en place pour tester en continu ses systèmes.

Depuis 2011, Facebook et Microsoft propose leur programme international, **the Internet Bug Bounty**. Des plateformes se sont également montées, **HackerOne**, **BugCrowd** aux Etats Unis, Bug **bountyZone**, **Bountyfactory.io, Yogosha** en France, s'occupant de mettre en relation hackers et entreprises.

Antivirus et autres solutions de cyber sécurité ne sont plus d'actualités, l'IA est la prochaine (r)évolution.

Derrière l'utilisation des termes d'intelligence artificielle en matière de cyber sécurité, on entend la possibilité pour une machine de détecter les logiciels malveillants, et la mise en place d'algorithmes d'apprentissage automatique leur permettant de faire des prédictions basées sur des données connues. En outre, l'arrivée de l'IA dans le monde de la cybersécurité permet d'alléger la charge de travail grandissante des analystes et d'automatiser la détection d'attaques et donc l'efficacité des systèmes. Plus performant que les systèmes passés, ces solutions vont permettre de prévenir des menaces mais également de contrecarrer celles qui restaient jusqu'alors invisibles, telles que les attaques **APT** (Advanced Persistent Threat) supposées rester invisibles sur une longue période et travaillant en « sous-marin ». Les chercheurs du **MIT's Computer Science and Artificial Intelligence Laboratory** et la startup **PatternEx** ont mis au point une intelligence artificielle capable de prédire **85% des cyberattaques**. L'entreprise française **Darktrace** s'inspire elle des principes biologiques du système immunitaire humain et permet par l'auto-apprentissage de détecter en temps réel des menaces jusqu'alors ignorées, le tout indépendamment de leurs origines. La licorne californienne **Cylance**, a développé un logiciel en mesure de bloquer les malwares avant qu'ils n'aient d'effets sur les machines des utilisateurs. Le secteur n'est pas ignoré par les géants de la Tech. Le projet Google Brain basé sur le deep learning, ayant été récemment en mesure de **faire communiquer deux machines dans un langage indéchiffrable par l'homme**, permet de crypter des communications. **L'IA Watson d'IBM,** elle, est en mesure de croiser les données contextuelles (par l'apprentissage du langage de la cybersécurité) avec des données issues des solutions classiques et ainsi venir appuyer la compréhension des analystes et réduire considérablement les délais d'intervention.

Dans un futur proche il faut également envisager le fait que cette IA aujourd'hui pressentie comme étant au service de la cybersécurité, pourrait tout aussi bien être détournée au service de la cybercriminalité ou du cyberespionnage à l'image du **projet Sauron**, un programme à même de personnaliser son implantation et son infrastructure pour chaque cible, de s'adapter à son environnement afin de lui permettre d'aspirer les données des machines infectées.

Aujourd'hui aucune solution n'est sure à 100%, du simple fait de l'asymétrie qu'il existe entre la cybercriminalité et les moyens de s'en protéger, la première évoluant plus vite que l'autre. Néanmoins, une réflexion est à mener quant à la protection de ses données, qu'elles soient issues du monde de l'entreprise ou personnelles, et il semble nécessaire de trouver la solution la plus à même de répondre à ce besoin de protection. L'avenir de la confiance numérique étant en jeu. On peut cependant insister sur l'importance du social engineering et de l'humain dans la cybersécurité. Comme le souligne Frédérique Gouth, consultant en sécurité des SI, une bonne protection passe d'abord par une sensibilisation des collaborateurs et par de la prévention aux travers des bonnes pratiques à adopter. L'Agence Nationale de la Sécurité des Système d'Information (ANSSI), a ainsi mis au point **un guide à destination des petites et moyennes organisations.**

3 Le «Web profond» ou «Darknet » est une collection de pages non-indexées, non référencées sur les moteurs de recherche classiques.
4 Un white hat (en français : « chapeau blanc ») est un hacker éthique qui réalise des tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des systèmes d'information d'une organisation. Ils s'opposent aux black hats, qui sont les hackers mal intentionnés.
5 Un patch est une section de code que l'on ajoute à un logiciel, pour y apporter des modifications : correction d'un bug, traduction, crack. ...

Vous pouvez nous suggérer des thèmes que vous souhaiteriez voir traités dans une prochaine Note (ou Dossier) de Veille

Thèmes et rédaction//AEC
www.aecom.org
@agenceAEC
Contact : veille@aecom.org

Thèmes et diffusion//Digital Aquitaine
www.digital-aquitaine.com
@DigitAqui
Contact : communication@digital-aquitaine.com