***Biographie** : Jérémy RENARD exerce dans le milieu de la Cybersécurité depuis une quinzaine d'années, toujours au sein et pour de grands comptes. Successivement, il a occupé des fonctions de consultant, adjoint RSSI, Directeur du Conseil et Audit Cyber et actuellement Responsable de l'Offre Cybersécurité au sein du cabinet de conseil Capgemini Invent. Reconnu comme un expert de la cybersécurité[1], Jérémy est également passionné par le management et le capital humain. C'est sur la base de cette combinaison qu'il a construit ses convictions et en a fait une clé de succès unique pour la réussite des projets de ses clients.*

Titre : Les 3 raisons pour lesquelles les grandes entreprises devraient envier les OBL et OSBL

Quand il m'a été proposé d'écrire un article à propos de la cybersécurité des OBL et des OSBL, ma première réaction a été de … chercher la signification de cet acronyme sur Internet ! Après tout, je n'ai travaillé qu'au sein de et pour de très grands comptes et je me sentais bien loin de ce milieu. Alors qu'allais-je pouvoir apporter ?
Sans oublier que nous avons tous compris que nous ne pouvions pas appréhender la cybersécurité de la même manière dans une OBL et les OSBL qu'au sein d'une grande entreprise. C'est une évidence ne serait-ce que par la différence des moyens à disposition de part et d'autre[2].
Ensuite, de très bons écrits relatifs à la sécurité des petites et moyennes entreprises existent déjà, notamment ceux rédigés par l'ANSSI[3].
Finalement, je me suis rendu compte que j'aurais pu passer à côté de principes essentiels en termes de cybersécurité et cette demande est en réalité une véritable opportunité ! Ainsi, c'est justement sous l'angle des grandes entreprises et donc un un angle différent et original que je vais vous expliquer pourquoi la cybersécurité des OBL et des OSBL est si importante et devrait attirer l'attention de nos plus grands dirigeants d'entreprise, de la sécurité, du risque, des systèmes d'information, etc.

Raison n°1 : La dépendance entre les grandes entreprises et les OBL

La **dépendance entre les grandes entreprises** (y compris les plus grandes figurant au CAC 40) et les OBL est prégnante. En effet, quelle grande société ne travaille pas avec des OBL ? Exemple précis, l'un des progiciels les plus utilisés dans le monde bancaire est SAB[4] : il s'agit d'une entreprise de moins de 250 salariés. C'est-à-dire que pour traiter du cœur de l'activité d'une grande société comme les banques leur sécurité reposent en (grande) partie sur des OBL. Or, nous avons toujours en tête que la sécurité ne vaut que par le niveau de robustesse de son maillon le plus faible. Il convient évidemment à ce que l'OBL ne représente pas un maillon faible (au même titre que les composants de l'entreprise de la société elle-même bien entendu). Il est important de souligner ce point à la lumière des propos de Guillaume Poupard, patron de l'ANSSI. En effet, ce dernier rappelle que l'une des grandes menaces pesant sur les grandes entreprises est représentée par les attaques indirectes, c'est-à-dire en abusant des sous-traitants pour atteindre l'entreprise cible plus facilement[5]. Et l'actualité ne fait que lui donner raison jour après jour[6].

---

[1] https://www.capgemini.com/fr-fr/experts/cybersecurity/jeremy-renard/
[2] https://www.lemondeinformatique.fr/actualites/lire-les-tpe-pme-plus-vulnerables-aux-cybermenaces-51889.html
[3] https://www.ssi.gouv.fr/actualite/petites-et-moyennes-entreprises-decouvrez-le-guide-des-bonnes-pratiques-de-linformatique-adapte-a-vos-besoins/
[4] https://www.sab2i.com/fr/
[5] https://www.usinenouvelle.com/article/les-sous-traitants-le-nouveau-maillon-faible-de-la-chaine-de-la-cybersecurite.N796835
[6] https://www.franceinter.fr/emissions/histoires-economiques/histoires-economiques-07-fevrier-2019

Raison n°2 : Les OBL et OSBL représentent un modèle pour les grandes entreprises en termes de cybersécurité

Il existe au moins deux raisons pour lesquelles les OBL et OSBL représentent un modèle pour les grandes entreprises. La première est que les entreprises les plus innovantes en termes de cybersécurité sont bien souvent des OBL qui fournissent d'ailleurs les grands comptes. Il suffit pour s'en persuader de lire la liste des entreprises référencées par Hexatrust[7]. En complément, rappelons que l'une des deux seules sondes de détection des menaces qualifiées récemment par l'ANSSI est une OBL, nommément Gatewatcher[8]. Et celle-ci est donc vouée à équiper les entreprises françaises les plus sensibles, c'est-à-dire les Organismes d'Importance Vitale (OIV).

Dans le même temps, les OBL et OSBL pourraient servir d'exemple de par leur pragmatisme. En effet, leurs moyens étant limités – sous réserve d'un niveau de sensibilisation à la cybersécurité qui n'est pas toujours présent – sont en quelque sorte « forcée » de travailler selon les priorités fortes systématiquement. Comment ? En sécurisant l'essentiel. Cela impose effectivement de se focaliser sur les actifs les plus critiques. Alors, certes, faut-il encore bien le faire. Pour cela, la fameuse revue Harvard Business Review France[9] nous guide dans une démarche par scénario, bien loin des modèles « château fort » désuets et même du modèle « aéroport » qui trouve ses limites dans un monde de plus en plus connectés, liés avec de tierces parties et dont les données sont de plus en plus exploitées (ex : big data, open data, etc.). Enfin, certes parce qu'elles n'ont pas les mêmes contraintes, quand les grandes entreprises entreprennent des chantiers de « move-to-cloud » ou tentent désespérément de réduire leur niveau d'obsolescence au sein de leur système d'information, si ce n'est de surveiller le taux d'actifs à jour (correctifs de sécurité, mise à jour de la base de signature des programmes contre les codes malveillants, …), les OBL et OSBL ont souvent fait le choix, nativement, de s'orienter vers des solutions cloud (e.g. GCP, Azure ou AWS) leur fournissant souvent un niveau de sécurité moyen plus élevé que grand nombre de grandes entreprises.

Raison n°3 : Les grandes entreprises comptent sur les OBL pour faire avancer leurs projets devant la pénurie de ressources spécialisées en cybersécurité

Si nous avons évoqué les solutions et produits de cybersécurité dans le paragraphe précédent, de manière plus globale, elles ne manquent pas (il suffit de compter le nombre de stands dédiées aux solutions et produits de cybersécurité aux Assises pour s'en persuader). Non, ce qui est communément admis par toutes les entreprises et notamment les grands comptes, c'est la pénurie de **ressources qualifiées** en cybersécurité[10] et c'est cela qui inquiète. Alors, devant cette demande croissante de profils, florissent (ou ont déjà flori) de nombreux cabinets de Cybersécurité de moins de 250 personnes. A cela, s'ajoutent la tendance des profils cybersécurité à créer leur propre société en tant qu'indépendant et les sociétés de portage spécialisée ou avec une composante cybersécurité. Ainsi, les grandes entreprises comptent grandement sur les OBL pour subvenir à leur besoin de ressources spécialisées, les grands cabinets et ESN étant submergés par les demandes et arrivant difficilement à répondre à la demande (ou alors, s'inquiéter de la qualité de service de cette entreprise qui pourrait vous fournir si facilement des ressources spécialisées en cybersécurité, ESN ou cabinet). La bonne nouvelle, c'est que nombre d'entre elles sont qualifiées par l'ANSSI[11], gage de leur niveau de compétence.

---

[7] https://www.hexatrust.com/

[8] https://www.lemondeinformatique.fr/actualites/lire-l-anssi-qualifie-les-sondes-de-detection-des-menaces-de-thales-et-gatewatcher-74884.html

[9] https://www.hbrfrance.fr/magazine/2019/03/24739-les-tendances-en-matiere-de-securite-digitale/

[10] https://itsocial.fr/enjeux/securite-dsi/cybersecurite/penurie-dexperts-cybersecurite-situation-inquietante/

[11] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

Si bien entendu les enjeux, le niveau d'exposition, les moyens sont très différents en termes de cybersécurité entre les OBL et OSBL d'une part et les grandes entreprises d'autre part, ces deux mondes tendent à se rejoindre car elles font partie d'un écosystème commun, d'une même chaîne sécuritaire. Quant on sait que les cyberattaques ciblent de plus en plus les sous-traitants et qu'aucune grande entreprise ne peut s'en passer, la menace reste prégnante, et de plus en plus forte. Enfin, regarder de plus près la façon de travailler des OSBL et OBL en termes de cybersécurité est certainement l'opportunité pour les grandes entreprises de voir sa cybersécurité « out of the box » et trouver des solutions qui fonctionnent vraiment.