PME du cybercrime vs cybersécurité des grandes organisations :

qui est David, qui est Goliath ?

La cybermenace se maintient en 2022. Les attaquants ont du temps, de l'argent, cherchent toujours de nouveaux moyens d'arriver à leurs fins et affichent aujourd'hui plus de capacités à se spécialiser, s'organiser et à monter en expertise. Les gains sont colossaux pour les attaquants et par rebond les conséquences financières des attaques sont toujours plus importantes pour les organisations touchées. Quelles sont les attaques les plus courantes et où en sont les grandes organisations dans leurs investissements en cybersécurité ?

GÉROME BILLOIS,

Directeur de la practice Cybersécurité, société Wavestone

Des attaques majoritairement opportunistes et qui visent des gains financiers

La motivation première des attaquants reste financière. Ainsi, le *ransomware* (attaque visant à voler des données et à bloquer le système d'information en chiffrant les ordinateurs et les serveurs puis à demander une rançon) demeure la menace numéro une des organisations : 51% des incidents gérés par le CERT Wavestone (CERT-W) ont impliqué ce type d'attaque. La nature opportuniste des attaquants signifie que tous les secteurs et toutes les entreprises peuvent être touchées. Ces groupes d'attaquants **se sont largement professionnalisés pour devenir des PME du cybercrime.** Par exemple, lors du démantèlement du groupe de cybercriminels CONTI, les autorités ont pu évaluer leur revenu annuel à 160M$ en 2021 et que la structure comptait au moins 65 membres. Basés sur l'expérience terrain du CERT-W, nos calculs de rentabilité estiment qu'un attaquant peut percevoir un ROI compris entre 200% et 800% ! **Ces entreprises du crime sont aujourd'hui dotées de services de recrutement, RH, finance, expertises techniques, équipes d'intrusion…** Ils font largement de la publicité pour leurs activités afin de recruter de nouveaux cybercriminels, notamment en publiant des offres d'emplois.

Plus ciblés, les autorités relèvent aussi de **nombreux cas d'espionnage et de déstabilisation**, industriels et étatiques, tels que mentionnés dans le Panorama de la Cybermenace 2022 publié par l'Agence nationale de sécurité des systèmes d'informations (ANSSI).

Enfin, certains secteurs médiatiquement exposés sont particulièrement soumis à **des attaques de type « *hacktivismes* »** qui visent à faire passer des messages

idéologiques ou à nuire à une organisation ou à une marque. Ces attaques sont souvent de faible intensité mais peuvent être très visibles dans les médias.

Les attaquants pénètrent dans les systèmes majoritairement à cause d'un mail de *phishing* et/ou à l'utilisation de comptes utilisateurs volés. Il y a donc encore une marge de progression concernant la sensibilisation des collaborateurs et la protection de nos messageries. On note toutefois que ces dernières années des investissements massifs ont été réalisés dans de nombreuses grandes structures pour sécuriser leur SI (accès conditionnel, authentification à facteurs multiples, définition de règles de détection d'incidents cyber…), entraînant concrètement une réduction du temps de détection d'une attaque non-négligeable. A titre indicatif, le temps de détection d'une intrusion est passé en moyenne de 94 jours en 2020 à 35 jours en 2022 d'après le rapport CERT-W.

Quel est le niveau de maturité en cybersécurité des grandes organisations ?

Wavestone mesure régulièrement le niveau de maturité des grandes organisations. Pour ce faire, nous maintenons un benchmark auprès de 100 structures (représentant plus de 3 millions d'utilisateurs) afin d'évaluer leur niveau de maturité autour des 16 thèmes clés de la cybersécurité. Les résultats sont sans appel : **les organisations françaises n'engagent pas encore assez de moyens (humains et techniques) pour se protéger contre des attaques.** En effet, en moyenne et tous secteurs confondus, les organisations de notre échantillon ont obtenu la note de 46/100 en matière de maturité cyber par rapport aux exigences des normes internationales.

Les niveaux sont en revanche très disparates selon les filières. Les acteurs les plus matures sont ceux sur lesquels la pression réglementaire est la plus forte, en particulier le secteur financier et les structures soumises à la directive NIS (texte européen imposant des mesures de sécurité pour les infrastructures critiques) ou à la LPM (Loi de programmation militaire, imposant des niveaux de sécurité minimum aux structures identifiées comme d'importance vitale par l'Etat).

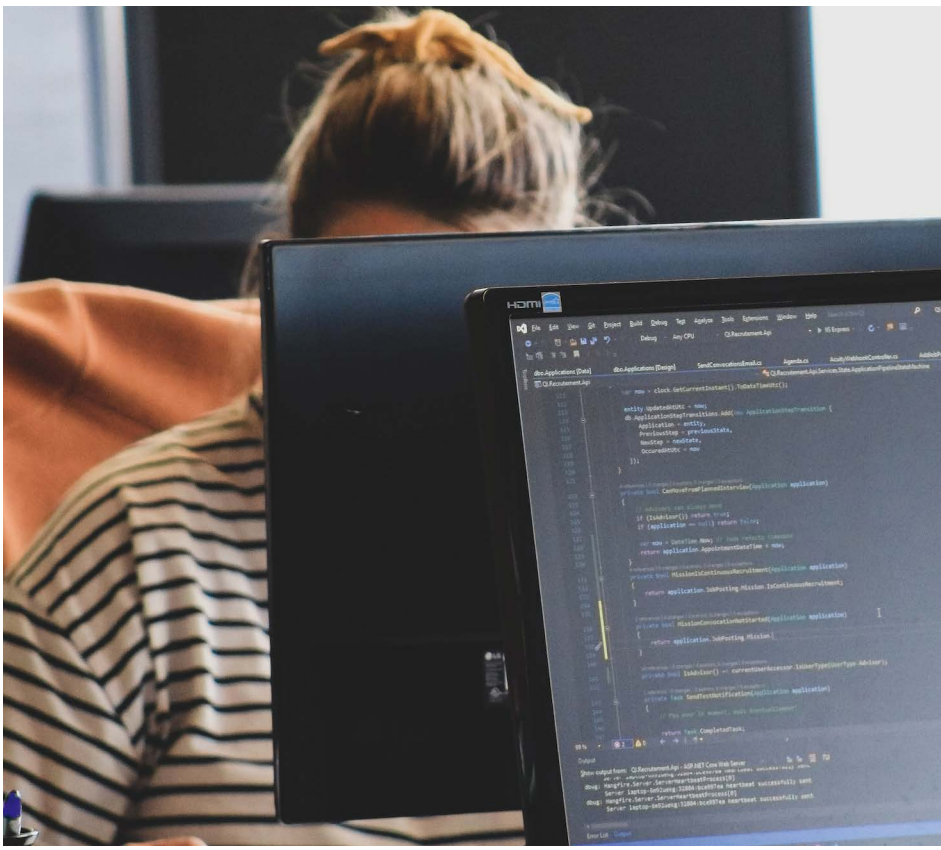
Le budget dédié à la cybersécurité est aussi trop faible : il est mesuré à 6,1% du budget informatique. Là encore les différences sectorielles sont importantes, le financement de grands programmes de cybersécurité varient entre 100 et 800M d'euros dans le secteur de la finance contre 15 à 80M d'euros pour l'industrie par exemple.

Quels sont les priorités d'investissement ?

S'assurer de la mise en œuvre des mesures essentielles

Il existe des défis techniques à relever pour bloquer les attaques les plus fréquentes. Sur les technologies de protection, les deux mesures phares que sont les EDR (outil de protection avancée des ordinateurs et serveurs) et **l'authentification multi-facteurs** (MFA) ont connu des déploiements importants ces dernières années.

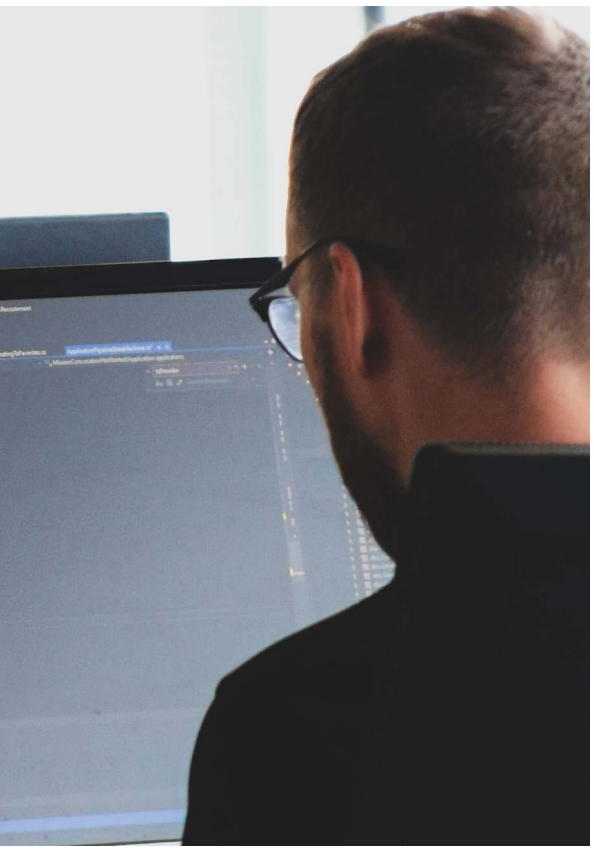
Toutefois beaucoup reste à faire, notamment sur la **sécurité de *l'Active Directory*** (brique technique peu visible



qui gère l'ensemble des droits d'accès aux informations et aux ordinateurs dans la plupart de systèmes d'information), cible numéro un des attaquants puisque ce composant est impliqué dans 90% des crises gérées par le CERT-W l'année dernière. Dans votre plan d'investissement n'oubliez pas non plus d'inclure les **sauvegardes**, et en particulier d'étudier leur externalisation et leur capacité à résister à une attaque *ransomware*. Enfin, les sujets les plus en difficulté aujourd'hui restent la **sécurité des applications et des données**, en particulier du fait du volume d'actifs concernés, et, de manière plus surprenante, **la sécurité cloud.** Sur ce dernier point, de très mauvaises pratiques sont en vigueur, souvent car il y a un faux sentiment de sécurité du fait des discours des fournisseurs. Un exemple concret : plus de 42% des organisations évaluées permettent l'accès d'administration à leur système cloud avec un simple login / mot de passe.

S'entourer d'une équipe compétente

Mais ces boucliers et mesures techniques ne feront pas tout. Vous devez aussi disposer de compétences en cybersécurité… et elles sont rares actuellement : plus de 3 millions d'emplois vacants dans le monde, dont 15 000 en France et 700 000 aux Etats-Unis. Aussi d'après notre benchmark, seulement 1 personne pour 1500 employés en moyenne est dédiée à la cybersécurité, ce qui est loin d'être suffisant pour couvrir tous les nouveaux sujets associés : résilience, gestion du budget cyber, analyse des vulnérabilités, etc. Evidemment **le recrutement est une piste mais il ne faut pas négliger non plus les mobilités internes ou l'usage de sociétés spécialisées pour vous accompagner.** Dans tous les cas, vous devez savoir qui dans votre organisation est en charge de la cybersécurité.



Mettre en place des investissements pluriannuels

Vu l'ampleur des besoins et la durée des projets, il est souvent nécessaire de piloter un programme de remédiation cybersécurité sur plusieurs années. Il pourra s'appuyer sur les piliers du référentiel NIST quia vous aidera à prioriser vos projets en fonction des enjeux *Identify, Protect, Detect, Respond, Recover.*

Cette approche pluriannuelle permet de lisser ses investissements entre lancement de projets (phase de *Build*) et leur maintien (phase de *Run*). La gestion d'un budget cyber est un sujet complexe qui requiert l'adoption d'un cap et de la flexibilité. Pour le piloter efficacement il faut **connaître ses besoins présents et anticiper ses besoins futurs**, qui souvent évoluent rapidement au regard de la menace.

Conclusion

L'impact financier d'une attaque contre les organisations devient de plus en plus critique compte tenu des moyens importants mis en œuvre par les attaquants. Les menaces se multiplient aussi à cause du nombre d'applications utilisées pour produire et fournir leurs activités, dans un contexte d'organisation étendue. La guerre entre attaquants et responsable de la cybersécurité est donc loin d'être terminée. Pour se prémunir et réduire les impacts il faut **engager plus d'efforts dans la sensibilisation des collaborateurs, la protection de son SI et faire de la résilience sa priorité.** ■