Mairies, hôpitaux, PME… comment rétablir le rapport de force entre gangs de cybercriminels, collectivités et entreprises.

Sébastien VIOU
Directeur Cybersécurité & Management Produits
Cyber-Evangéliste
Stormshield

Vincent NICAISE
Industrial Partnership and
Ecosystem Manager
Stormshield

Un état des lieux de la menace cyber

La cybercriminalité a encore fait les gros titres en 2022. Secteur public comme privé, grands groupes comme TPE : tout l'univers économique est concerné. Et la sur-représentation médiatique des vulnérabilités du secteur public ne doit pas laisser croire que seul ce secteur est ciblé, malgré l'attrait médiatique des multiples cyberattaques contre les hôpitaux et les collectivités. Rien qu'au niveau des collectivités, ce sont donc plus d'une dizaine d'hôpitaux et une trentaine de grandes mairies, régions et départements[1] qui ont été victimes de cyberattaques en 2022. Et au niveau du privé, ce sont la moitié des PME attaquées qui feront faillite dans les 18 mois.

Il ne faut pas non plus laisser croire à une incompétence de ces différentes institutions, mais plutôt insister sur la puissance actuelle des groupes de cybercriminels. L'image du geek seul dans son garage est dépassée depuis longtemps et laisse désormais place à un véritable écosystème de professionnels du cybercrime, générant plusieurs millions de dollars. En 2022, l'industrie du ransomware (rançongiciel) aurait rapporté pas moins de 457 millions de dollars[2] aux groupes de cybercriminels. Et il n'est ici question que des sommes déclarées par les victimes… Des entreprises cybercriminelles, comme Lockbit, Conti, Blackbasta ou encore Hive, réussissent par exemple à générer plusieurs dizaines de millions d'euros par an. Des premiers chiffres à mettre en regard des 20 millions d'euros débloqués en France en 2022 pour aider les seuls hôpitaux.

Conséquence : un rapport de force complètement déséquilibré. Là où les entreprises disposent de ressources limitées pour assurer leur cybersécurité (en matière de compétences humaines comme de budget), les groupes de cybercriminels ne sont pas tenus par les mêmes limites. Une tendance se dégage même chez ses derniers depuis quelques années, avec la création d'une réelle industrie via la répartition des tâches d'une cyberattaque : découverte des vulnérabilités, conception des malwares, analyse du système de la future victime, collecte des données et enfin déclenchement de l'attaque sont désormais attribués à autant de sous-

[1] https://www.numerama.com/cyberguerre/1208398-cyberattaques-la-liste-des-regions-departements-et-villes-impactes-en-2022.html
https://www.numerama.com/cyberguerre/1219264-cyberattaque-la-liste-des-hopitaux-touches-en-2022.html

[2] https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay/

groupes. Mais ces groupes ne s'arrêtent pas là et se structurent également comme de vraies entreprises, avec leur propre service RH permettant de recruter les meilleurs éléments, un service financier et même un service commercial pour gérer les achats et les ventes d'exploits et d'outils.

Au niveau des entreprises françaises, la part du budget informatique attribué à la cybersécurité représente en général 5% - divisant par deux le taux recommandé par l'ANSSI[3] . Une part qui grandit sensiblement dès qu'il est question de grands groupes – avec une protection sensiblement plus efficace également. Pour autant, ces différentes entités gèrent des données d'une sensibilité identiques : les mairies gèrent des données personnelles comme des listes électorales, des pièces d'identités, les laboratoires gèrent eux des données médicales et de santé, là où les banques gèrent des données financières. Toutes ces entités devraient donc toutes faire l'objet du même niveau d'attention quant à leur protection. Pourtant, ce n'est pas encore le cas aujourd'hui. Les petites structures sont alors des cibles plus faciles, tenues en plus de respecter des contraintes légales fortes. Mais est-il encore possible de rétablir le rapport de force ?

La nécessaire prise de conscience et l'organisation qui en découle

L'intense actualité des cyberattaques sur les entreprises privées et publiques a permis une véritable prise de conscience des impacts. Et surtout, elle a sensibilisé chacun à la possibilité d'être pris pour cible.

Pour passer à l'action et mettre en œuvre une posture de cyberdéfense, il est essentiel de compter sur des experts du domaine et ainsi structurer la sécurité de ses propres systèmes d'information. Si les grandes entreprises ont déjà ajouté dans leur organigramme des équipes entières dédiées à la stratégie et à la mise en œuvre de cette cybersécurité, les plus petites structures (publiques comme privées) se retrouvent très souvent dépourvues de cette catégorie d'experts internes. Et lorsque, malgré tout, elles se lancent dans une démarche d'embauche, elles se retrouvent bien souvent confrontées à un marché de l'emploi en tension – et notamment une compétition impossible avec des entreprises privées qui proposent des salaires souvent plus intéressants.

Reste la possibilité de sous-traiter cette expertise à des sociétés de services. Celles-ci proposent de prendre en main la sécurisation des réseaux, de la mise en œuvre d'une politique de sécurité jusqu'à la gestion de crise en cas de compromission. De cette manière, même les plus petites structures peuvent bénéficier d'un service mutualisé, économiquement viable, et d'une expertise technique à l'état de l'art. Il est possible d'ajouter à cela les services d'un SOC mutualisé (centre opérationnel de sécurité, Security Operation Center) qui complètent les moyens humains en permettant d'identifier rapidement des comportements suspects ou une cyberattaque et les actions de remédiation à entreprendre.

S'il est essentiel d'investir dans ces moyens organisationnels, il est également primordial de sensibiliser collaborateurs, agents et élus afin d'accroitre leur vigilance et de leur donner les bons réflexes. Parce que les cyberattaques proviennent souvent de l'exploitation d'une faiblesse humaine, il faut donner les clés de lecture pertinentes à ces potentielles cibles comme savoir identifier un email frauduleux ou connaitre les dernières techniques de social engineering pour ne pas se faire duper. Pour cela, des pratiques de base existent comme le MOOC

[3] https://www.banquedesterritoires.fr/la-cybersecurite-parent-pauvre-des-budgets-informatiques-des-collectivites

de l'ANSSI[4] et sont à mettre en œuvre dès que possible. Peu coûteuses, ces pratiques peuvent réduire drastiquement les tentatives de compromission. Enfin, réagir rapidement permet de limiter la propagation de la cyberattaque et déclarer un incident aux autorités compétentes permet d'enrichir la base de connaissance commune.

Des moyens techniques en support de l'organisation

Une fois l'organisation opérationnelle, se pose la question des moyens techniques. Et c'est à ce moment-là que les éditeurs de cybersécurité entrent en jeu. Firewall, antivirus, VPN, sonde, EDR, XDR, IPS… toutes ces solutions sont autant d'éléments qui constituent une panoplie complète de cyberdéfense. Et qui concernent tout le monde.

Car les menaces cyber seront les mêmes, quel que soit l'utilisateur final : l'infrastructure d'une mairie et celle d'une banque seront toutes les deux autant vulnérables à une faille Proxyshell dans leurs outils Microsoft par exemple. Dans la même idée, le chiffrement IPsec des communications de télétravailleurs aura la même force (et la même importance) pour une entreprise de la Défense que pour un laboratoire pharmaceutique.

Une différence entre grands groupes et petites infrastructures tiendra plutôt au nombre d'outils de sécurité déployés, plus élevé chez les grands groupes. Une particularité qui découle de la complexité de leur infrastructure et de leur organisation décentralisée, davantage que de raisons de protection. Des solutions de micro-segmentation seront par exemple nécessaires à un datacenter ; des Web Application Firewalls seront utiles pour de l'hébergement ; un SOAR permettra de synchroniser la réponse à incident de plusieurs entités métiers ; autant d'éléments qui seront inutiles pour les collectivités. Reste à définir le minimum requis en matière de solution de cybersécurité qui doit être mis en œuvre. Liste non-exhaustive :

- une solution de firewall, proposant du cloisonnement, de la prévention d'intrusion, un anti-virus et un portail VPN ;
- une solution d'authentification forte pour les accès distants ;
- une solution de protection des postes et des serveurs ;
- une solution d'antispam et d'antiphishing ;
- une solution de chiffrement de surface et une autre pour les fichiers sensibles.

En couplant ces outils et solutions, une organisation de la cybersécurité et la mise en œuvre des bonnes pratiques de configuration des systèmes et de sauvegardes de données, on obtient un niveau de protection suffisant pour éviter la majorité des cyberattaques, même pour les plus petites structures.

Les aides externes sur lesquelles s'appuyer

Mais autant de solutions à déployer implique forcément un budget conséquent. Un budget incompatible avec les finances de la plupart des petites structures…

Pour faire face à cette problématique financière, l'Etat français prévoit plusieurs dispositifs complémentaires permettant d'accompagner, d'aider et de sensibiliser le secteur public comme le privé. Il a notamment lancé en 2021 le projet France

[4] https://www.ssi.gouv.fr/actualite/secnumacademie-le-mooc-de-sensibilisation-a-la-cybersecurite-ouvre-ses-donnees/

Relance, un programme d'accompagnement avec l'ambition d'élever significativement et durablement le niveau de cybersécurité des acteurs publiques. Pas moins de 136 millions d'euros ont alors été débloqués, dont 60 millions exclusivement pour les collectivités locales et 20 millions pour le secteur de la Santé (complétés par 20 millions supplémentaires en 2022, suite à l'attaque de l'hôpital de Corbeil-Essonnes). Les bénéficiaires du projet se voient financer un « parcours de cybersécurité », équivalent d'audit simplifié et pragmatique du système d'information permettant de dégager les premières mesures de sécurité à mettre en œuvre. Une fois le parcours réalisé, les entités peuvent alors bénéficier d'un co-investissement pour des solutions de cybersécurité souveraines. L'agence française (ANSSI) pilote l'ensemble de ce dispositif sur le territoire, notamment via des délégués présents en région, dans un rôle d'accompagnement et de relai sur le territoire. Ces délégués sont par ailleurs un lien précieux pour les entreprises qui se questionnent sur leur sécurité et qui ont besoin d'être aiguillés ou accompagnés dans leurs démarches.

Également issu du projet France Relance, les CSIRT régionaux (Computer Security Incident Response Team) sont des centres de réponse aux incidents de cybersécurité. Ils traitent les demandes d'assistance des PME, ETI et collectivités de taille intermédiaire et les mettent en relation avec des partenaires de proximité comme des prestataires de réponse à incident par exemple. L'émergence de ces CSIRT permet de fournir des services locaux de premier niveau gratuit, prestation complémentaire de celle proposée par les prestataires et les services du CERT-FR.

Enfin, la plateforme cybermalveillance.gouv.fr vient compléter les actions de sécurisation et de détection. Ce dispositif national a pour mission la sensibilisation, la prévention et l'assistance aux victimes d'actes de cybermalveillance. Ce dispositif regroupe des représentants de l'Etat, des syndicats, des associations professionnelles avec des éditeurs, des constructeurs et des prestataires de services.

En dehors des actions de l'Etat, d'autres initiatives locales et nationales permettent d'aider et d'accompagner ces entreprises de taille intermédiaire, comme notamment :

- le CESIN, un groupement de RSSI qui propose un lieu d'échange, de partage d'expérience et de coopération pour les experts de la sécurité de l'information et du numérique ;
- le CyberCercle, un cercle de réflexion, d'expertise et d'échanges sur les questions de confiance et de sécurité numérique ;
- le CLUSIF, qui regroupe offreurs de solutions et utilisateurs et qui, à travers ces groupes de travail, produit de nombreux guides et conférences pour tous les domaines de la cybersécurité.

D'autres actions existent en parallèle, à l'échelle nationale (comme le groupement des RSSI territoriaux et le Club Cyber OT du GIMELEC) et à l'échelle régionale (avec par exemple le CLUSIR, déclinaison régionale du CLUSIF, ou encore la Mêlée Numérique à Toulouse).

Sur le papier, rétablir le rapport de force entre petites structures et cybercriminels a tout du mythe de Sisyphe. Et on le constate dans les faits. Mais ce n'est pas nécessairement inéluctable ; la prise de conscience, les niveaux de protection mis à disposition par les éditeurs de cybersécurité, les nouvelles offres des sociétés de service, les actions gouvernementales et les initiatives associatives forment ce qui devrait être un socle commun pour la sécurité de toutes les entreprises, publiques comme privées, sur le territoire, avec à terme, un rapport de force qui s'équilibre.