Le machine learning, nouvel expert en cybersécurité ?

Malgré une protection des systèmes d'information (SI) et des utilisateurs de plus en plus vigilants, les cyberattaques se multiplient, sont de plus en plus sophistiquées et font davantage de dégâts. Comment les entreprises peuvent-elles faire face à ce défi ?

Les entreprises, plus vulnérables que jamais

Les cyberattaques se sont intensifiées ces dernières années à cause, entre autres, de l'augmentation du nombre d'appareils connecté [1] et la publication de code malveillant (ex : EternalBlue, Wanacry) qui augmentent les chances du hacker d'arriver à son but. Les entités semi-publiques[2] et publiques ainsi que les grandes et moyennes entreprises, tous secteurs confondus, sont aujourd'hui concernées, d'après l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[3].

Les entreprises ayant pourtant une forte culture de la sécurité de l'information ne sont pas hors de danger. Les attaques de masse, auparavant mal-ciblées, disparaissent au profit d'actions spécifiques, plus sophistiquées et donc plus difficiles à prévoir et à détecter. Les gains potentiels pour les hackers sont de plus en plus conséquents ; cela est d'autant plus vrai qu'aujourd'hui le régulateur met les acteurs économiques face à leurs responsabilités et obligations, avec par exemple l'application du RGPD et de la directive NIS[4]. Les entreprises qui ne prennent pas les mesures adéquates pour corriger les vulnérabilités de leurs SI s'exposent entre autres à un impact opérationnel sérieux et à de potentielles amendes.

Les protections périmétriques, longtemps déployées dans les entreprises, comme un maillage de mesures protégeant et compartimentant l'accès au site, au bureau, à l'ordinateur, aux réseaux, aux serveurs et à leurs données, tout en garantissant une grande granularité et souplesse d'utilisation ne répondent plus nécessairement aux menaces actuelles ou à venir. Par exemple, un exploit 0-day ou une exfiltration de données (volontaire ou non), peut compromettre l'intégrité du SI.

Certes, la prise de risque peut être acceptable pour ces deux exemples, mais alors quelles actions peut-on prendre si ce n'est pas le cas? On peut d'autant mieux se protéger contre des vulnérabilités quand elles sont précisément identifiées. Les entreprises ont des lacunes pour détecter les événements à risques (faut-il généraliser la mise en place de SIEM et de SOC ?); elles n'ont pas toujours le temps suffisant à consacrer à l'analyse de ces données et pour mettre en place les actions correctrices.

En moyenne, une entreprise met 201 jours pour découvrir qu'elle a été victime d'une cyberattaque [5]. Désormais, le constat est simple : il existe un réel décalage entre les technologies de détection d'intrusion et la sophistication grandissante des cyberattaques. Face à ces constats, la cybersécurité et la culture d'entreprise ont besoin d'évoluer.

Cyberattaques : quels risques et quelle(s) solution(s) ?

Les vecteurs d'attaquent ne cessent d'évoluer. Certains types d'attaques sont cependant plus fréquents que d'autres : Malware, Denial of Service, Browser & Pishing, Brute Force[6]. Ces menaces touchent l'ensemble et tous les niveaux de l'architecture d'un SI.

> Le Rançongiciel (ransomware / malware) logiciel pouvant détruire les données sur les ordinateurs comme sur un réseau tout entier, est souvent utilisé à des fins de chantage. Ils sont de plus en plus répandus et perfectionnés (les derniers en date sont Wanacry et NotPetYa).
> L'attaque par déni de service (DDOS) consiste à envoyer de nombreuses requêtes à un serveur pour saturer son activité et rendre un site inaccessible. Pour un acteur du e-commerce, du IaaS ou SaaS, cela peut représenter un manque à gagner très important.
> L'Hameçonnage (fishing) est également très utilisé pour extraire des données. Aujourd'hui, véhiculé par e-mail ou site web, il est difficilement détectable même par un expert.

De manière générale, toute attaque est préjudiciable pour l'entreprise : contacts, données clients, personnelles ou financières restent sensibles et soumises à la confidentialité. Un piratage peut également affaiblir l'image de l'entreprise. La première action, pour les entreprises, est d'adopter une vision d'ensemble de la sécurité informatique. En effet, une attaque peut survenir bien en amont, notamment via un logiciel ou un ordinateur corrompu, par l'internet et la connectivité en général, ou même via un partenaire ou un prestataire.

Pour aider les sociétés à réagir face aux cyberattaques, la seconde clé est l'expertise en cybersécurité. Néanmoins, bien qu'efficace car elle couvre un large spectre du SI, elle repose souvent sur une liste préétablie et assez générique de vulnérabilités ce qui n'est pas nécessairement adaptée à toutes les entreprises.

Afin de pallier cela, des outils prometteurs d'analyse comportementale intégrant du Machine Learning (une sous partie de l'IA – Intelligence Artificielle) se déploient peu à peu. Le cabinet Gartner projette que d'ici fin 2020 la part de Machine Learning dans le déploiement d'outils de détection d'intrusion (par exemple IDPS – Intrusion Detection and Prevention System) passera de 10% à 60%.[7] Cette technologie permet, sans croyance établie, d'étudier et de modéliser le fonctionnement du SI sous un angle comportemental et, ainsi, détecter en temps réel les usages et changements soudains, qui permettront d'informer ou de bloquer pro-activement les accès pour protéger les biens de l'entreprise. La possibilité de rejouer l'anomalie permettra d'analyser le comportement et mettre à jour la politique de sécurité.

L'évolution rapide des technologies ainsi que des comportements digitaux a créé un terreau fertile aux cyberattaques toujours plus sophistiquées et difficilement détectables. Il est aujourd'hui indispensable, pour les entreprises, d'investiguer de nouvelles approches complémentaires et d'investir dans des technologies auto-adaptatives capables de détecter les menaces en temps réel et d'enclencher des actions adéquates de protections immédiates.

[1] https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-france-2017-mai2017.pdf

[2]https://www.generation-nt.com/ransomware-hopital-rancon-cyberattaque-piratage-actualite-1942396.html

[3]https://www.ssi.gouv.fr/uploads/2018/04/rapport_annuel_2017_anssi.pdf

[4] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148

[5]Selon une étude de l'Institut Ponemon

[6]https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2017.pdf

[7][https://www.gartner.com/doc/reprints?id=1-4OOFSAC&ct=180112&st=sb&submissionGuid=2a07a204-0a2c-4e26-8ddb-826e8eb6d264