L’apprentissage machine et l’intelligence artificielle pour améliorer la cybersécurité

5 juin 2020

Auteur

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Nouveaux enjeux

L’arrivée de la COVID-19 a bousculé le fonctionnement de plusieurs entreprises. Certaines se sont tournées vers le télétravail. D’autres ont été forcées de développer rapidement une offre de service en ligne. Cette évolution accélérée a propulsé la cybersécurité au premier plan, notamment quant aux renseignements personnels et aux secrets commerciaux qui peuvent ainsi faire l’objet de divulgations involontaires.

Les risques de cybersécurité proviennent des pirates informatiques, mais aussi souvent d’erreurs de configuration des outils déployés par une entreprise et d’usagers négligents. Afin de gérer les risques de cybersécurité, une des meilleures stratégies est souvent de tenter de trouver les failles d’un système avant une attaque, par exemple en effectuant des tests d’intrusions. Ce genre de tests a évolué grandement au cours des dernières années, passant d’essais-erreurs ciblés à des approches plus larges et systématiques.

Ce que l’apprentissage machine apporte à l'entreprise

L’apprentissage machine, et l’intelligence artificielle au sens plus large, permet entre autres de mieux reproduire le comportement humain, et donc celui d’un hypothétique usager négligent ou d’un pirate informatique. Les tests d’intrusion peuvent donc être plus efficaces lorsqu’ils sont infusés d’intelligence artificielle.

Arachni est un exemple d’apprentissage machine relativement simple. Il s’agit d’un logiciel libre (*open source*) visant à évaluer la sécurité d’applications Web, faisant notamment partie de la

distribution Kali Linux très connue pour les tests d'intrusion en informatique. *Arachni* utilise une variété de techniques avancées, mais il est de plus possible d'entraîner ce logiciel afin qu'il découvre plus efficacement les vecteurs d'attaques auxquels les applications sont le plus exposées[1]. Plusieurs autres logiciels de cybersécurité comportent maintenant de telles capacités d'apprentissage.

L'intelligence artificielle peut aller encore beaucoup plus loin. Les usages possibles de l'intelligence artificielle dans le cadre de la cybersécurité incluent notamment[2] :

la réduction du temps de réaction en cas d'attaques par des logiciels malveillants;
la détection plus efficace des tentatives d'hameçonnage (*phishing*);
une compréhension contextualisée des anomalies de comportement des usagers.

IBM a récemment produit un document expliquant comment sa suite *QRadar*, qui incorpore de l'intelligence artificielle, peut réduire le fardeau des gestionnaires en matière de cybersécurité.

À retenir :

L'être humain demeure central dans les enjeux de cybersécurité. Non seulement les gestionnaires doivent comprendre les enjeux de cybersécurité, y compris ceux qui sont créés par l'intelligence artificielle, mais ils doivent aussi instaurer des directives claires pour les usagers et s'assurer du respect de celles-ci.

À cet égard, il est important de sensibiliser ces gestionnaires informatiques aux enjeux juridiques liés aux mesures qui sont imposées aux usagers :

Il faut se garder d'une surveillance trop intrusive ou constante des employés d'une entreprise. Il peut être opportun de consulter un avocat en droit du travail pour s'assurer que les mesures envisagées sont compatibles avec le droit applicable.
Il faut comprendre les enjeux juridiques liés à une fuite de données ou à une brèche de sécurité. Certains renseignements personnels (par ex., les données médicales) sont plus sensibles et les conséquences d'une brèche de sécurité sont plus grandes. Il peut être utile d'établir un dialogue entre les responsables de la sécurité informatique et un avocat agissant en matière de renseignements personnels.
Enfin, les secrets commerciaux d'une entreprise nécessitent parfois des mesures de protection plus strictes que d'autres renseignements d'entreprise. Il peut être important que la stratégie de propriété intellectuelle de l'entreprise intègre les mesures de sécurité informatique.

---

1. https://resources.infosecinstitute.com/web-application-testing-with-arachni/#gref
2. https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/; https://towardsdatascience.com/cyber-security-ai-defined-explained-and-explored-79fd25c10bfa
3. *Beyond the Hype, AI in your SOC*, publié par IBM; voir aussi : https://www.ibm.com/ca-en/marketplace/cognitive-security-analytics/resources