Des donnÃ©es sensibles partagÃ©es avec ChatGPT en entreprise.
Info
PostÃ© par : JerryG
PubliÃ©e le : 26/7/2023 14:00:00

Netskope, leader sur le marchÃ© du SASE (Secure Access Service Edge), dÃ©voile les conclusions dâ□□une nouvelle Ã©tude selon laquelle pour 10â□□000 utilisateurs, les entreprises subissent chaque mois environ 183 incidents de partage de donnÃ©es sensibles avec lâ□□application ChatGPT. Le code source reprÃ©sente la part la plus importante des donnÃ©es sensibles compromises.

Cette information figure parmi les conclusions du rapport Cloud & Threat Report: AI Apps in the Enterprise, premiÃ¨re analyse complÃ¨te du Threat Labs de Netskope consacrÃ©e Ã lâ□□utilisation de lâ□□intelligence artificielle en entreprise et aux risques pour la sÃ©curitÃ©.

Sur la base des donnÃ©es gÃ©nÃ©rÃ©es par des millions dâ□□employÃ©s dâ□□organisations du monde entier, Netskope a constatÃ© que lâ□□utilisation des applications dâ□□IA gÃ©nÃ©rative augmente rapidement. Elle a en effet augmentÃ© de 22,5â□□% au cours des deux derniers mois, une accÃ©lÃ©ration qui entraine un risque croissant que des utilisateurs compromettent des donnÃ©es sensibles.

Lâ□□usage croissant des applications dâ□□IA

Netskope a constatÃ© que les entreprises dâ□□au moins 10â□□000 collaborateurs emploient en moyenne cinqâ□□IA applicatives par jour, ChatGPT comptant Ã elle seule plus de huit fois plus dâ□□utilisateurs quotidiens actifs que toute autre application. Au rythme actuel de croissance, ce nombre dâ□□utilisateurs devrait doubler au cours des sept prochains mois.

Au cours des deux derniers mois, Google Bard est lâ□□application dâ□□IA qui a enregistrÃ© la croissance la plus soutenue, avec une hausse hebdomadaire du nombre dâ□□utilisateurs de 7,1â□□%, contre 1,6â□□% pour ChatGPT.Â

A ce rythme, Google ne devrait pas rattraper ChatGPT avant plus dâ□□un an, sachant que le monde des applications dâ□□IA gÃ©nÃ©rative va probablement Ã©voluer de faÃ§on significative au cours de cette pÃ©riode, un grand nombre de plateformes Ã©tant en cours de dÃ©veloppement.

Les utilisateurs alimentent ChatGPT en donnÃ©es sensibles

Au cours de son Ã©tude, Netskope a constatÃ© que les codes source sont publiÃ©s dans ChatGPT, plus que tout autre type de donnÃ©es sensibles, avec un taux mensuel de 158 incidents pour 10â□□000 utilisateurs.Â

Parmi les autres donnÃ©es confidentielles partagÃ©es sur ChatGPT figurent des donnÃ©es rÃ©glementÃ©es, notamment financiÃ¨res, ou mÃ©dicales, et des informations personnellement identifiables (IPI).

Câ□□est aussi le cas de blocs de propriÃ©tÃ© intellectuelle, Ã lâ□□exclusion du code source et, ce qui est encore plus prÃ©occupant, des mots de passe et des clÃ©s gÃ©nÃ©ralement intÃ©grÃ©s dans le code source.

Â«â□□Il est inÃ©vitable que certains utilisateurs tÃ©lÃ©versent du code source propriÃ©taire ou

du texte contenant des donnÃ©es sensibles vers des outils dâ□□IA qui promettent de les aider Ã programmer ou Ã rÃ©diger des contenus, concÃ¨de Ray Canzanese, Threat Research Director, Netskope Threat Labs.

Il est par consÃ©quent impÃ©ratif que les entreprises mettent en place des contrÃ´les autour de lâ□□IA afin de pallier toute fuite de donnÃ©es sensibles, lâ□□objectif ultime Ã©tant de dÃ©ployer des contrÃ´les qui permettent aux utilisateurs de bÃ©nÃ©ficier des avantages de lâ□□intelligence artificielle en rationalisant les opÃ©rations et en amÃ©liorant leur efficacitÃ©, tout en attÃ©nuant les risques.Â

Les contrÃ´les les plus efficaces combinent la prÃ©vention des pertes de donnÃ©es (DLP) et un encadrement interactif des utilisateurs.â□□Â»

Bloquer ou permettre lâ□□accÃ¨s Ã ChatGPT

Le Threat Labs de Netskope suit actuellement les proxies de ChatGPT ainsi que plus dâ□□un millier dâ□□adresses URL et de domaines malveillants associÃ©s Ã des cybercriminels opportunistes qui cherchent Ã exploiter lâ□□engouement suscitÃ© par lâ□□IA au travers de campagnes de phishing et de distribution de malware, ou de la crÃ©ation de spam et de sites internet frauduleux.

Le blocage de lâ□□accÃ¨s aux applications dâ□□IA et aux contenus liÃ©s Ã lâ□□intelligence artificielle est une solution Ã court terme pour minimiser les risques au dÃ©triment des avantages potentiels quâ□□offrent ces nouvelles applications pour lâ□□innovation des entreprises et la productivitÃ© de leurs employÃ©s.

Les donnÃ©es collectÃ©es par Netskope montrent que dans des secteurs fortement rÃ©glementÃ©s tels que les services financiers et la santÃ©, prÃ¨s dâ□□une entreprise sur cinq interdit purement et simplement Ã ses employÃ©s dâ□□utiliser ChatGPT, contre seulement une sur vingt dans le secteur technologique.

Â«â□□En tant que leaders sur le marchÃ© de la sÃ©curitÃ©, nous ne pouvons tout simplement pas dÃ©cider dâ□□interdire des applications sans influencer sur lâ□□expÃ©rience et la productivitÃ© des utilisateurs, ajoute James Robinson, Deputy Chief Information Security Officer.

Les entreprises doivent se concentrer sur la sensibilisation de leurs collaborateurs et leurs politiques de donnÃ©es afin de rÃ©pondre aux besoins des employÃ©s qui utilisent ces technologies de maniÃ¨re productive. En conjuguant les bons outils et le bon Ã©tat dâ□□esprit, il est tout Ã fait possible de profiter des atouts de lâ□□intelligence artificielle gÃ©nÃ©rative en toute sÃ©curitÃ©.â□□Â»

Pour pouvoir adopter les applications dâ□□IA dans des conditions de sÃ©curitÃ© maximales, les entreprises doivent centrer leur approche sur lâ□□identification des applications autorisÃ©es et la mise en place de contrÃ´les permettant aux utilisateurs dâ□□en exploiter pleinement le potentiel, tout en se protÃ©geant contre les risques.

Une telle approche inclut le filtrage de domaines, le filtrage des adresses URL et lâ□□inspection des contenus pour neutraliser les attaques. Dâ□□autres mesures permettent de dÃ©fendre les donnÃ©es et dâ□□utiliser les outils dâ□□IA en toute sÃ©curitÃ©â□□:

â□¢ Le blocage de lâ□□accÃ¨s aux applications qui ne rÃ©pondent Ã aucun objectif professionnel lÃ©gitime ou prÃ©sentent un risque disproportionnÃ© pour lâ□□entrepriseâ□□;
â□¢ Lâ□□encadrement des utilisateurs et le rappel des rÃ¨gles de lâ□□entreprise relatives Ã lâ□□utilisation des applications dâ□□IAâ□□;

â¢ Lâutilisation de technologies de prÃ©vention des pertes de donnÃ©es (DLP) de nouvelle gÃ©nÃ©ration pour dÃ©tecter les publications contenant des informations potentiellement sensibles.

Plus d'info.