Veille : La Gestion des identités et des accès en entreprise

Gérer les accès, c'est savoir qui se connecte, que ce soit une personne ou un logiciel. Avec tous nos outils sur internet, mettre une double sécurité (MFA) est devenu obligatoire pour ne pas se faire pirater. Mais avec l'arrivée de l'IA, les règles du jeu ont changé. On ne surveille plus seulement des humains, mais aussi des programmes intelligents qui peuvent agir tout seuls dans notre dos.

L'IA permet maintenant aux pirates de créer des mails de piège (phishing) tellement parfaits qu'on ne voit plus la différence avec les vrais. Ça va beaucoup plus vite qu'avant et ça rend nos protections habituelles beaucoup moins solides. C'est fou, mais une simple invitation dans ton calendrier peut suffire à vider les mots de passe si un assistant IA mal réglé s'en occupe. Les attaquants utilisent ces nouveaux outils pour s'incruster dans nos comptes sans qu'on s'en rende compte.

Le vrai danger, c'est le "Shadow AI" : quand des employés utilisent des outils d'IA sans prévenir la boîte. Ces programmes automatiques ont souvent des droits énormes sur nos fichiers et personne ne les surveille. Pour éviter le carnage, il existe maintenant des solutions pour repérer ces "robots" fantômes et voir ce qu'ils ont le droit de faire. C'est devenu le seul moyen de garder un œil sur ce que font ces algorithmes dans notre réseau.

Pour répondre, les outils de sécurité doivent eux aussi devenir plus intelligents et capables de repérer les pièges de l'IA. Certains systèmes analysent maintenant comment on se comporte d'habitude pour bloquer un compte dès qu'il fait un truc louche. Grâce à l'IA défensive, on peut trier les alertes plus vite et stopper les pirates avant qu'ils ne se baladent partout dans nos serveurs. Le défi, c'est de surveiller ces nouveaux outils sans nous empêcher de travailler avec.

https://www.lemondeinformatique.fr/actualites/lire-ibm-x-force-alerte-sur-l-efficacitedes-attaques-dopees-a-l-ia-99499.html
https://korben.info/perplexity-comet-une-invitation-de-calendrier-suffisait-pour-pillervos-mots-de-passe-1password.html
https://www.ictjournal.ch/news/2026-02-19/okta-cible-les-risques-du-shadow-ai-avecagent-discovery
https://www.globalsecuritymag.fr/sentinelone-r-devoile-de-nouvelles-offres-dediees-ala-securisation-des.html