IA Act : stimuler lâ□□innovation tout en renforÃ§ant la cybersÃ©curitÃ©
Internet
PostÃ© par : JerryG
PubliÃ©e le : 22/1/2024 13:00:00

Le 8 dÃ©cembre dernier, le parlement europÃ©en est parvenu Ã un accord lÃ©gifÃ©rant lâ□□utilisation de lâ□□intelligence artificielle (IA). Ce rÃ¨glement vise Ã promouvoir lâ□□innovation dans le secteur mais aussi Ã protÃ©ger les droits fondamentaux, de la dÃ©mocratie, de l'Ã□tat de droit et de la durabilitÃ© environnementale face aux applications Ã haut risque de cette technologie.

Bien que cet accord soit destinÃ© Ã stimuler les progrÃ¨s dans le domaine, Ben Eichorst, principal ingÃ©nieur en sÃ©curitÃ© chez Yubico, souligne que les dirigeants doivent simultanÃ©ment renforcer leur posture en cybersÃ©curitÃ© pour mieux apprÃ©hender les risques induits par l'intelligence artificielle en 2024.

Â« En 2023, le paysage professionnel, et au-delÃ , a Ã©tÃ© fortement influencÃ© par une hausse significative de l'adoption des outils d'intelligence artificielle (IA) comme ChatGPT. Cependant, malgrÃ© les multiples avantages qu'elle offre, cette technologie a semÃ© des inquiÃ©tudes parmi les dirigeants d'entreprise, notamment en ce qui concerne la sÃ©curitÃ© informatique.

Les avancÃ©es dans les modÃ¨les d'IA gÃ©nÃ©rative, ciblant les sens primordiaux tels que la vue et l'ouÃ¯e des utilisateurs, sont exploitÃ©es par les cybercriminels. Cette tendance aggrave la complexitÃ© de la dÃ©tection des attaques, notamment du phishing.

En 2024, la mobilitÃ© de la main dâ□□oeuvre reprÃ©sentera un risque accru en ce qui concerne les outils d'IA, car les employÃ©s opÃ©reront Ã partir de leurs propres rÃ©seaux et appareils, qui sont souvent moins sÃ©curisÃ©s. Cette transition facilitera l'utilisation de mÃ©thodes de plus en plus crÃ©dibles par les cybercriminels pour mener Ã bien des attaques dâ□□ingÃ©nierie sociale.

Des mesures de sÃ©curitÃ© auparavant robustes, telles que la vÃ©rification vocale de l'identitÃ© lors de la rÃ©initialisation d'un mot de passe, deviendront obsolÃ¨tes Ã cause de l'IA gÃ©nÃ©rative. Bien que ChatGPT ne puisse pas encore produire des rÃ©sultats convaincants pour le spear phishing, il pourrait amÃ©liorer la qualitÃ© gÃ©nÃ©rale des campagnes de phishing en Ã©vitant les fautes de grammaire, dâ□□orthographe et les informations erronÃ©es, par exemple.

Alors que la technologie va continuer de progresser et de transformer la sociÃ©tÃ© en 2024, les entreprises doivent prendre des mesures adÃ©quates en dÃ©ployant des moyens adaptÃ©s aux cybermenaces, notamment lâ□□authentification multi-facteur (MFA) rÃ©sistante au phishing, telle que les clÃ©s de sÃ©curitÃ© physique.

Cela est crucial pour protÃ©ger les donnÃ©es sensibles ainsi que les actifs critiques. En parallÃ¨le, ces initiatives doivent Ãªtre accompagnÃ©es d'une formation continue en matiÃ¨re de sÃ©curitÃ© Ã l'intention du personnel, renforÃ§ant ainsi les dÃ©fenses et positionnant les entreprises de maniÃ¨re optimale pour contrer les cybermenaces Ã©mergentes. Â»