



16ème législature

Question N° : 17184	De M. Philippe Latombe (Démocrate (MoDem et Indépendants) - Vendée)	Question écrite
Ministère interrogé > Numérique		Ministère attributaire > Numérique
Rubrique >numérique	Tête d'analyse >Sécurisation des annuaires Active Directory des structures publiques et privées	Analyse > Sécurisation des annuaires Active Directory des structures publiques et privées.
Question publiée au JO le : 16/04/2024 Question retirée le : 11/06/2024 (fin de mandat)		

Texte de la question

M. Philippe Latombe alerte Mme la secrétaire d'État auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargée du numérique, sur l'urgence de sécuriser les annuaires *Active Directory* des structures publiques et privées. L'*Active Directory* (AD) gère l'annuaire de 90 % des entreprises françaises : son administrateur est donc celui de toutes les machines qui utilisent l'annuaire AD (en général 80 % de celles d'une entreprise). Pourtant, moins de 10 % des annuaires AD sont correctement sécurisés. Or si un annuaire AD ne l'est pas en configuration par défaut, un attaquant peut en prendre le contrôle en moins de deux heures. L'AD des systèmes constitue donc une cible privilégiée pour les cybercriminels qui cherchent à élever les privilèges pour pénétrer dans un réseau compromis. Les attaquants savent que cette compromission ouvre la porte à toutes sortes d'activités malveillantes, du vol de données au rançongiciel. Les erreurs de configuration, les utilisateurs disposant d'autorisations excessives et les vulnérabilités non corrigées sont autant de facteurs qui permettent aux cyberattaquants d'exploiter l'AD. Il sera donc essentiel de prioriser la sécurité des annuaires AD dans la transposition française de la réglementation NIS 2 (*Network and Information Security, version 2*). Dans le contexte à haut risque que l'on connaît actuellement et, notamment, dans celui imminent des jeux Olympiques et Paralympiques 2024 (JOP 2024), il souhaite savoir quelles mesures le Gouvernement envisage de prendre en urgence pour que l'ensemble des administrations, organisations publiques ou parapubliques, ainsi que les entreprises, fassent l'audit de leur *Active Directory* et corrigent les failles trouvées pour éviter que cela n'engendre des vulnérabilités et des catastrophes au moment des JOP 2024.