Veille : La Gestion des identités et des accès en entreprise

L'IAM (Identity and Acces Management), c'est tout simplement ce qui permet de gérer qui a le droit d'entrer dans nos logiciels et nos réseaux. Face aux piratages en série, verrouiller ces accès est devenu une urgence absolue pour protéger nos dossiers. Utiliser une double vérification (MFA) et limiter les droits de chacun, c'est la base pour être tranquille. L'idée, c'est de faire de notre identité un vrai bouclier qui s'adapte aux menaces en temps réel.

Les récentes fuites de données, comme celle qui a secoué la DGFiP, prouvent qu'on ne peut plus prendre nos accès à la légère. Les attaquants profitent de la moindre petite faille dans l'attribution des droits pour s'infiltrer discrètement. Cet incident rappelle brutalement qu'il est urgent de revoir comment on distribue nos autorisations en interne. Ce n'est plus juste un petit problème informatique, c'est une vraie crise qui touche toutes les organisations.

Le pire, c'est que même avec une double vérification active, les pirates arrivent encore à se connecter à nos comptes. Ils utilisent des petits virus pour voler nos sessions de connexion directement dans nos navigateurs web. Avec ces informations, ils font croire au système qu'ils sont déjà reconnus et contournent totalement nos protections. Cela prouve bien qu'un simple mot de passe renforcé par téléphone ne suffit plus pour empêcher les intrus de rentrer.

L'une des plus grosses erreurs aujourd'hui, c'est de laisser des droits d'accès ouverts en permanence sur nos outils. Pour corriger ça, de nouvelles solutions suppriment ces privilèges illimités qui sont du pain béni pour les pirates. Le principe est simple : on donne les clés uniquement quand la personne en a besoin, et pour une durée très courte. En faisant ça, même si un pirate vole un compte, il se retrouve vite bloqué devant une porte fermée.

Enfin, pour être vraiment serein, il faut repérer tout de suite quand un compte fait quelque chose d'anormal sur le réseau. C'est pour ça que nos systèmes de protection intègrent maintenant la surveillance directe de nos identités. En clair, si un pirate utilise un identifiant volé, le système le remarque immédiatement et isole la machine. Ça nous permet de bloquer l'attaque dans la seconde, avant que l'intrus n'ait le temps de vider nos serveurs.

https://www.zdnet.fr/actualites/fuite-a-la-dgfip-apres-les-excuses-du-ministre-lurgence-de-revoir-liam-face-aux-cyberattaques-en-serie-500205.htm

https://www.solutions-numeriques.com/avis-dexpert-pourquoi-les-identifiants-voles-continuent-de-fonctionner-meme-lorsque-lauthentification-multifactorielle-est-activee/

https://presseagence.fr/paris-cybersecurite-keeper-security-sattaque-a-la-faille-des-privileges-permanents-dans-le-cloud/

https://itsocial.fr/cybersecurite/cybersecurite-actualites/harfanglab-etend-sa-detection-aux-identites-en-ladossant-a-son-edr/