GUIDE

SECURISER L'USAGE DES MACROS

Quel risques ? Les macros peuvent contenir du code malveillant capable de modifier, chiffrer ou ouvrir la porte à une cyberattaque. Avec la généralisation des outils d'IA, leur création et leur diffusion deviennent encore plus faciles, ce qui augmente fortement le risque d'usage non maîtrisé.

Macros téléchargées d'Internet (hors code généré par IA) : éviter

- Les macros téléchargées d'Internet devraient être bloquées par défaut, et leur exécution ne devrait être autorisée que si elles sont signées et justifiées.
- Leur utilisation devrait être soumise à un processus de contrôle préalable, incluant la vérification du besoin légitime, de l'origine et, le cas échéant, une revue de code.
- Leur exécution devrait être limitée à un environnement isolé ou sandboxé, afin d'éviter tout impact sur les postes de production ou des données sensibles.
- Les utilisateurs devraient être sensibilisés aux risques spécifiques liés à ces macros, notamment leur rôle fréquent dans l'introduction de malwares ou ransomwares.

Macros à impact significatif : contrôler

- Lorsqu'une macro automatise un processus critique ou traite des données sensibles, son remplacement par une application dédiée devrait être prévu.
- Le code des macros devrait être systématique revu, par l'informatique interne ou, à défaut, par un prestataire externe qualifié.
- Leur accès et leurs droits d'exécution devraient être strictement limités, par exemple via les droits NTFS/partage et des rôles différenciés entre exécution et modification.
- Les modifications de ces macros devraient être intégrées dans un cycle de développement sécurisé, comprenant notamment des tests fonctionnels et une validation métier avant mise en production.

Macros locales et non critiques : sensibiliser

- Leur utilisation devrait être encadrée par des règles claires, définies dans la charte sécurité ou la charte informatique.
- Les utilisateurs devraient être notamment sensibilisés aux IA recommandées, à l'importance de n'utiliser que des macros issues d'une source fiable, de ne jamais les exécuter par simple réflexe, et d'appliquer une vigilance renforcée pour les macros générées par l'IA, en les testant d'abord sur des données fictives.
- Les utilisateurs devraient être encouragés à signaler à l'instance gestionnaire des événements et des incidents de sécurité toute macro suspecte, non documentée ou imprévisible.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information