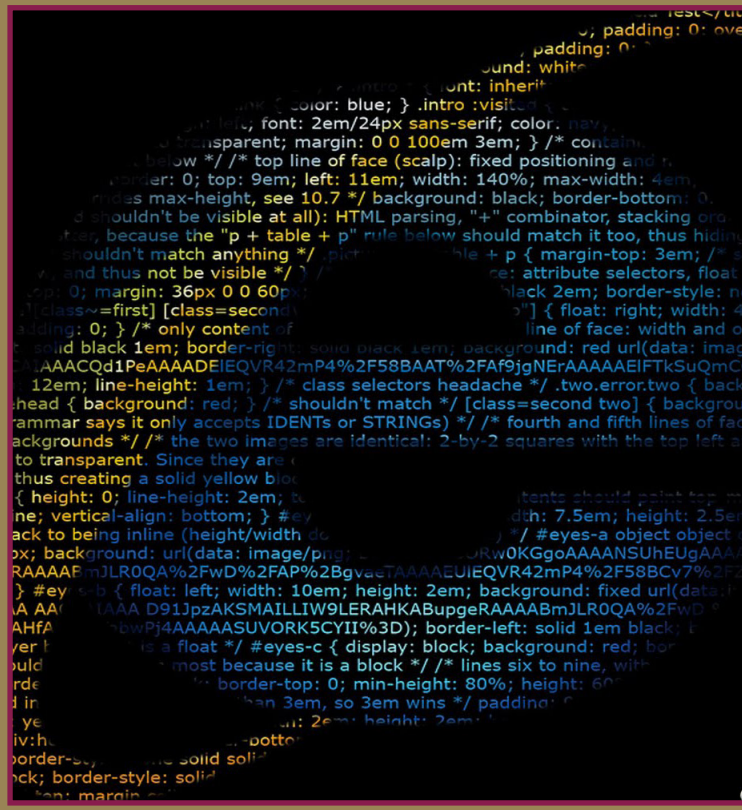
15

Bonnes pratiques pour le déploiement sécurisé du navigateur Internet Explorer



CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR INTERNET EXPLORER

Aujourd'hui, les navigateurs Web sont installés sur presque tous les ordinateurs, ceci les a rendus une cible privilégiée pour les attaquants. Ces derniers exploitent les vulnérabilités inhérentes au navigateur pour prendre le contrôle de votre ordinateur. La compromission d'un navigateur est attractive pour un attaquant car elle lui permet souvent de contourner les mesures de sécurité liées à l'architecture réseau et aux différentes passerelles de filtrage. Les vulnérabilités d'un navigateur peuvent avoir des origines différentes : le navigateur lui-même, les modules complémentaires (add-ons), les plug-ins ou extensions ou les actions de l'utilisateur.

Microsoft Internet Explorer

Microsoft Internet Explorer est un navigateur Web édité par Microsoft. C'est un navigateur qui dispose de puissants mécanismes de sécurité. Néanmoins, comme tout navigateur Web, il représente une cible privilégiée des attaquants du fait de leur utilisation massive sur Internet mais aussi en raison des vulnérabilités qui sont propres aux différents modules complémentaires intégrés aux navigateurs dont les processus de mise à jour sont généralement indépendants de ces derniers.

Mécanismes de sécurité pris en charge par Microsoft Internet Explorer

Depuis sa version 10, Internet explorer intègre de nouvelles fonctionnalités de filtrage et des mécanismes de protection avancés qui sont activés par défaut et qui lui donnent un niveau de sécurité accru. Les principaux mécanismes de sécurité pris en charge par les différentes versions de Microsoft Internet Explorer sont :

- Protected Mode (Mode Protégé), utilise des mécanismes de sécurité comme :

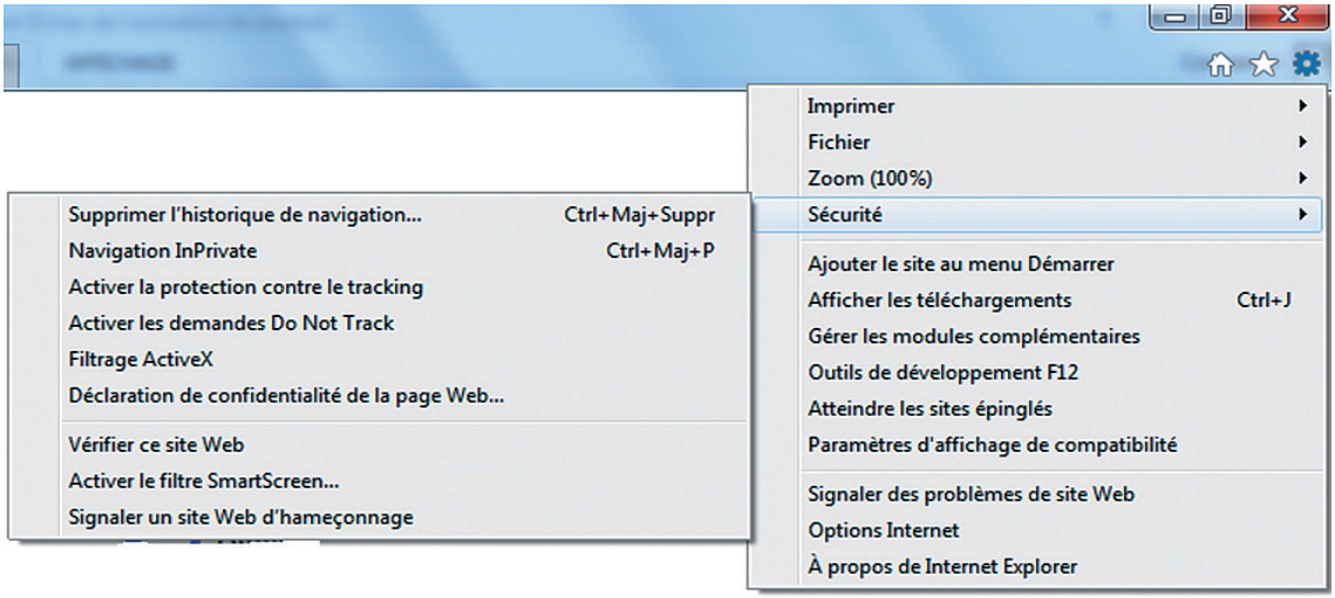
A. l'UAC (User Account Control) : à chaque fois qu'un programme veut faire un changement majeur à votre ordinateur, l'UAC informe l'utilisateur et demande la permission.

B. l'UIPI (User Interface Privilege Isolation) : est une technique de sécurité qui permet une protection contre les exploits d'injection de code.

- LCIE (Loosely-Coupled IE), qui consiste à séparer d'une part les processus de pilotage du navigateur (interface graphique, fenêtres, etc.) et d'autre part, les processus d'affichage de contenu (contenu HTML, contrôles ActiveX, exten

sions de barre d'outil, etc.). Cela permet de réduire la surface d'attaque des processus et de limiter ainsi les conséquences d'une exploitation de vulnérabilité.

- Filtre Smartscreen, mécanisme de protection contre le hameçonnage et les logiciels malveillants.
- Filtrage XSS 3 (anti-scripts de site à site), système de filtrage qui vise à repérer et bloquer le contenu malveillant injecté dans des pages Web par le biais de vulnérabilités.
- Filtrage ActiveX, système de filtrage qui permet de n'autoriser l'exécution de contrôles ActiveX que sur les sites de confiance.
- EPM (Enhanced Protected Mode), empêche les pages Web d'accéder en lecture/écriture au système d'exploitation.



LES RÈGLES À SUIVRE POUR UNE UTILISATION SÉCURISÉE DE MICROSOFT INTERNET EXPLORER

R1 Établir des listes de sites pour chaque niveau de confiance (zone intranet et zone des sites approuvés) auxquelles seront appliquées des configurations de sécurité spécifiques aux besoins de chaque zone.

R2 L'affectation des sites aux différentes zones de sécurité doit être faite par GPO (group policy object). Ces listes d'affectation doivent être verrouillées et non modifiables par les utilisateurs.

R3 Il est fortement conseillé de laisser le minimum possible de règles de sécurité dans un état non configurées.

R4 activation d'EPM pour que le niveau de sécurité atteint soit suffisant. Il en va de même pour le filtrage ActiveX et les autres fonctions visant à renforcer la sécurité d'exécution des modules complémentaires.

R5 Réduire la surface d'attaque du navigateur. Tout interdire puis renseigner exhaustivement par GPO une liste blanche de logiciel autorisés.

R6 Il est recommandé de désactiver l'utilisation SSL (ancien protocole) et de n'autoriser que les protocoles TLS qui offre une meilleure sécurité.

R7 Il est conseillé de désactiver le gestionnaire de mots de passe sur un réseau amené à traiter des données sensibles ou confidentielles.

R8 Il est recommandé d'activer toutes les « fonctionnalités de sécurité » facultatives.

R9 Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, etc.) de l'onglet sécurité dès lors que le navigateur n'est pas dédié à une navigation en Intranet.

R10 Il est recommandé d'interdire les fonctions de géolocalisation en configurant le navigateur Internet Explorer pour empêcher qu'il divulgue votre position géographique aux sites que vous visitez.

R11 Si la confidentialité des recherches est jugée primordiale, il convient de désactiver les fonctionnalités de recherche instantanée ou de suggestion de recherche.

R12 Pour des questions de respect de la vie privée, il est conseillé d'imposer un moteur de recherche s'appuyant sur une connexion chiffrée (HTTPS).

R13 Il est recommandé d'activer les fonctionnalités de filtrage de contenu telles que l'anti-hameçonnage ou le bloqueur de fenêtres publicitaires (« pops-ups ») sur la zone Internet.

R14 Lors du démarrage du navigateur, il est préférable de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une page connue et de confiance.

R15 Il est recommandé d'appliquer le modèle « niveau de sécurité haut » pour les sites que vous avez classé dans la « zone de sites sensibles » au niveau du navigateur.

R16 Si le navigateur est dédié à la navigation en intranet, il est plus pertinent d'appliquer directement le modèle de « niveau de sécurité haut » à la « zone Internet ».