



# CASES articles

Série d'articles CASES : Cyber attaques contre des pages Internet luxembourgeoises

## L'Internet est-il encore sûr ?

**Pour plus de sécurité, adoptez les réflexes CASES !**

**Comment les entreprises et personnes privées luxembourgeoises peuvent-elles protéger leurs applications web ?**

Qu'elles soient utilisées pour réserver un voyage, écouter de la musique ou lire les informations, toutes les pages Internet peuvent être considérées comme des applications web. Les cybercriminels recherchent systématiquement les points faibles de telles applications afin de perpétrer leurs méfaits. Les préjudices ainsi occasionnés peuvent atteindre des proportions importantes : cela peut aller de l'atteinte à la réputation, en passant par les pertes financières, jusqu'au dépôt de plainte par des tiers lésés. Les propriétaires d'applications web peuvent toutefois minimiser le risque de devenir les victimes de telles attaques. Ils contribuent ainsi également à rendre l'Internet plus sûr.

De nos jours, chaque usager d'Internet peut contribuer à son développement en plaçant sa propre application web sur la toile. Selon la société de sécurité Internet Netcraft, plus de 150 millions de ces applications sont désormais en ligne.

Les applications web sont de plus en plus populaires et ne sont pas seulement développées et mises en ligne par des entreprises, mais également par des personnes privées. Mais tous – personnes privées ou entreprises – s'exposent à certains dangers : les cybercriminels parcourent Internet à la recherche ciblée d'applications présentant des failles et pouvant être exploitées à des fins criminelles. La modification des contenus de pages Internet, la propagation de logiciels

malveillants ayant pour but de porter préjudice à des tiers (comme les attaques iframe), le vol de données ou encore la perturbation de la disponibilité d'un service figurent parmi les exemples connus de ces méfaits.

L'exploitation de failles d'applications web peut avoir des conséquences néfastes, que ce soit pour leur propriétaire ou pour les usagers d'Internet, et ceci est valable pour toutes les applications de ce type.

Pour les propriétaires d'applications web, il est donc recommandé d'appliquer certaines règles de sécurité, avant et pendant le développement, mais aussi durant l'exploitation de l'application.

### **Intégrité, confidentialité et disponibilité**

Un des défis qui se posent aux développeurs et hébergeurs d'applications web concerne la protection de l'intégrité des informations traitées et proposées. Lors d'un virement bancaire par le biais d'une application de banque en ligne par exemple, il ne doit pas être possible d'altérer le numéro de compte du destinataire du virement – il s'agirait d'une atteinte à l'intégrité des données. Les développeurs et hébergeurs doivent garantir que le fonctionnement du serveur web ne soit pas altéré par des actes involontaires ou malveillants.

Garantir la confidentialité représente également un défi. En 2007, l'application web du moteur de recherche monster.com a par exemple été attaquée. Des pirates informatiques ont alors réussi à obtenir l'accès à cette application et à une base de

données renfermant plusieurs milliers de curriculum vitæ. Selon des indications fournies par Symantec, les pirates ont ensuite exploité ces données personnelles afin d'effectuer des attaques ciblées de phishing (également appelé « spearphishing ») en combinaison avec du chantage. Dans le cadre de la préservation de la confidentialité, il importe donc tout particulièrement de veiller à la protection des données personnelles des utilisateurs enregistrées dans l'application web.

La disponibilité d'une application web doit également être garantie – en particulier lorsqu'il s'agit de processus critiques pour une organisation. Si le serveur web d'un important site d'e-commerce tombe par exemple en panne 5 jours avant Noël, tout achat devient impossible auprès de cette société et des pertes financières importantes ainsi qu'un préjudice non négligeable pour l'image de marque de la société en sont les conséquences.

Toutes les personnes et organisations qui souhaitent mettre en ligne une application web, ou qui l'ont déjà mise en ligne, devraient donc connaître les risques potentiels et les éventuelles répercussions.

### **Sécurité des applications web**

Certains principes de sécurité doivent être appliqués dès la conception d'une application web. Il convient par exemple d'éviter d'utiliser aveuglément les codes proposés sur Internet.

D'autres aspects de sécurité doivent ensuite être considérés au cours de la phase de développement ; en voici quelques exemples : seules les don-

nées devant effectivement être traitées par l'application devraient être utilisées. Les sessions devraient être administrées correctement et les utilisateurs identifiés clairement. De plus, les usagers d'Internet devraient avoir la possibilité d'interrompre la session à tout moment. Il est recommandé de toujours documenter tous les aspects d'une application web.

Enfin, un ensemble de principes de sécurité doit être appliqué lors de la mise en place et de l'exploitation d'une application web, comme par exemple l'utilisation de mots de passe complexes, la protection de ceux-ci, ainsi que la mise en œuvre de méthodes de cryptage éprouvées.

Le système d'exploitation ainsi que les services et applications sur lesquels repose l'application web, devraient être mis à jour régulièrement. De plus, les droits d'accès devraient être définis de manière à garantir la sécurité de l'application.

Le serveur web doit également répondre à toute une série de règles de sécurité : il convient par exemple de désactiver toute fonction ou tout procédé pouvant comporter des risques.

Des prestataires professionnels, garantissant un niveau élevé de sécurité devraient être sollicités pour l'hébergement de l'application.

Il convient de procéder régulièrement à une sauvegarde de l'application web ainsi que des données gérées par celle-ci. Les supports de sauvegarde doivent ensuite être stockés de façon sécurisée.

Des tests de sécurité permettent de détecter la présence d'éventuelles failles de sécurité. Tout comme l'hébergement, ce service devrait être confié à un prestataire professionnel, ceci permettant l'application optimale de tous les aspects de sécurité.

Il convient de soumettre régulièrement les applications web à une analyse des risques.

Afin de garantir les principes de sécurité et de faciliter leur application, le portail de sécurité CASES a élaboré un dossier électronique ayant pour objet les règles de sécurité relatives aux applications web. Ce dossier propose une check-list conviviale et s'adresse aux personnes privées et aux entreprises. « Ce dossier librement utilisable est disponible sur le portail de sécurité [www.cases.lu](http://www.cases.lu). Il est conçu de manière à pouvoir intégrer un cahier des charges. Il propose également un référentiel à l'intention des développeurs et soutient la conception sécurisée d'Internet », explique Raymond Faber, de la Direction du commerce électronique et de la sécurité informatique du Ministère de l'Économie et du Commerce extérieur, qui précise encore qu'une version imprimée du document a été mise à la disposition des entreprises à l'occasion de la conférence relative à l'Internet Security Day, le 8 mai 2008.

#### Conseil de sécurité

Vérifiez les caractéristiques de sécurité de votre application web à l'aide de la check-list accompagnant le dossier « Référentiel de sécurité pour applications web » de CASES. Ce dossier ainsi que la check-list sont disponibles sur [www.cases.lu](http://www.cases.lu).

#### Conseil de sécurité pour les experts

L'OWASP (Open Web Application Security Project), [www.owasp.org](http://www.owasp.org), propose gratuitement un guide détaillé de test des applications web. L'OWASP établit également une liste des failles de sécurité des applications web les plus utilisées, avec explica-

#### Définition : application web

Une application web est un programme exécuté sur un serveur web. Un serveur web est alors utilisé pour la transmission de documents à des programmes informatiques en vue de la consultation de pages web sur Internet. L'interaction avec l'utilisateur s'effectue exclusivement par le biais d'un navigateur – programme informatique spécifique, utilisé pour la consultation de pages Internet sur le World Wide Web.

Exemples d'applications web : pages Internet ou sites d'e-banking.

#### Définition : hébergement

Stockage d'une application web ou d'une page internet sur un serveur. Ce serveur permet ensuite la consultation du contenu de l'application par le biais d'internet.

#### Définition : blog

Un blog est un journal ou journal intime consigné sur une page internet et pouvant ainsi être consulté par tous les utilisateurs.

#### Définition : live CD

Un live CD comporte un système d'exploitation à partir duquel un ordinateur peut être démarré sans installation et intervention du disque dur.

tions, solutions et matériels de référence, et met gratuitement à disposition un live CD comportant de nombreux outils de test, de la documentation et un grand nombre d'outils de protection.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)