



CASES articles

Adopter un comportement d'utilisateur responsable est une condition indispensable pour un e-commerce sécurisé

Les utilisateurs devraient vérifier les liens e-commerce

Pour plus de sécurité, adoptez les réflexes CASES !

Les pages web d'e-commerce doivent disposer de certificats de sécurité valides

Dans les domaines de l'Internet où la sécurisation des transmissions doit être garantie, des réflexes de protection doivent impérativement être adoptés par les utilisateurs. Le point faible « humain » devient, en effet, de plus en plus souvent la cible des cybercriminels. Les pirates exploitent alors le manque de connaissances des utilisateurs. Quelques réflexes de sécurité faciles à mettre en œuvre permettent aux utilisateurs de repousser les attaques ou d'éviter les points faibles. La vérification de la sécurité de pages web d'e-commerce fait partie de ces réflexes de sécurité.

Le comportement de l'utilisateur constitue le mécanisme de protection le plus important pour surfer sur l'Internet en toute sécurité. Afin de n'offrir aucun point d'attaque aux cybercriminels, chaque usager d'Internet devrait respecter les règles d'or de la sécurité informatique : choix de mots de passe adéquats, mise à jour régulière de tous les programmes installés sur l'ordinateur, utilisation d'un logiciel anti-virus régulièrement mis à jour et d'un pare-feu correctement paramétré, ainsi que l'analyse régulière de l'ordinateur à l'aide d'un programme anti-spyware. Lors de l'utilisation d'applications d'e-commerce, l'usager d'Internet devrait également adopter des réflexes de sécurité supplémentaires. Ces derniers peuvent être acquis facilement et ne nécessitent aucune connaissance informatique spécifique.

Réflexes de sécurité e-commerce

Un ordinateur utilisé pour des applications d'e-commerce devrait être réservé à ce seul usage. Une machine utilisée par toute la famille, et donc sou-

mise à différents comportements d'utilisateurs, est en effet exposée à un risque d'attaque plus important. Les logiciels de lecture vidéo peuvent par exemple comporter des failles de sécurité exploitables par les pirates. Des chevaux de Troie peuvent se dissimuler dans des jeux téléchargés gratuitement. Les pages Internet consultées peuvent installer des malwares sur l'ordinateur ou des virus peuvent l'infecter par le biais de MSN.

Le nombre de points faibles potentiels d'un ordinateur utilisé pour l'e-commerce peut toutefois être réduit de façon très importante : il suffit d'en limiter l'accès. Si l'utilisation d'un seul et même ordinateur par plusieurs personnes ne peut être évitée, il est alors recommandé de créer un compte utilisateur réservé aux seules applications d'e-commerce. Sous Windows, ceci est possible en cliquant sur [Démarrer] [Panneau de configuration] [Comptes d'utilisateurs]. L'utilisateur devrait néanmoins veiller à restreindre l'accès à cet ordinateur à un nombre de personnes aussi limité que possible.

De plus, il convient de veiller à ce que seuls les logiciels réellement nécessaires soient installés sur l'ordinateur. Avant toute installation, il est recommandé de vérifier que les logiciels ainsi que leurs supports proviennent de sources fiables. Une vigilance toute particulière est de rigueur lorsqu'il s'agit de CD gravés, de clés USB ou d'offres très alléchantes sur Internet.

Le protocole de sécurité https

La sécurisation des applications d'e-commerce doit être vérifiée. Le protocole de sécurité « https » est une des pierres angulaires pour leur mise en sécurité. Ce protocole se différencie de l'« HyperText Transport Protocol » ou http habituel, par des fonctions de sécurité supplémentaires.

Conseils de sécurité :

le permis commerce électronique
Les utilisateurs peuvent évaluer leurs connaissances et leurs réflexes en matière de sécurité en passant le permis commerce électronique sur le portail de sécurité CASES :

<https://epass.cases.lu>.

Définition : navigateur

Un navigateur est un programme permettant de consulter des pages web sur l'Internet.

Définition : plug-in

Un plug-in est un programme autonome apportant des fonctionnalités complémentaires à un autre logiciel auquel il est rattaché.

Définition : add-on

Un add-on est un module optionnel pouvant compléter un logiciel ou un matériel. Il ne s'agit pas d'un programme autonome.

Le protocole http permet, certes, la navigation sur l'Internet, mais les personnes intervenant dans la communication http (ou l'interceptant) à des fins malveillantes sont en mesure d'obtenir des informations sensibles par ce biais, telles que les mots de passe de l'utilisateur. Une personne malintentionnée peut également modifier les informations transmises ou même se faire passer pour l'un des interlocuteurs. Ce genre d'agissement est possible car le protocole http ne crypte pas les données transmises et n'exige pas l'identification du serveur.

Afin de sécuriser la navigation sur l'Internet, le protocole http a été doté de fonctions de sécurité supplémentaires. Ces fonctions sont regroupées sous la dénomination SSL/TLS (Secure Socket Layer / Transport Layer Security), le protocole de sécurité est

quant à lui dénommé « https ». SSL/TLS a recours à des procédés de chiffrement. La sécurité du protocole https est attestée par un certificat émis par une autorité de certification.

Le protocole de sécurité https se distingue du protocole http normal par les caractéristiques complémentaires suivantes : authentification, confidentialité et intégrité. Les fonctions de sécurité supplémentaires du protocole https permettent d'authentifier sans équivoque les parties en communication. L'utilisateur est donc en mesure de vérifier l'identité de son interlocuteur. La confidentialité des données échangées est garantie par le biais d'un procédé de chiffrement. Les informations transmises sont donc inaccessibles pour des tiers. Leur modification par des tiers est également impossible. L'intégrité des données est ainsi garantie.

En raison de ses caractéristiques, le protocole https est utilisé dans de nombreux domaines de l'Internet, en particulier celui du commerce électronique. Les usagers d'Internet devraient éviter les applications d'e-commerce qui n'utilisent pas le protocole de sécurité https. Il est donc nécessaire de pouvoir reconnaître les pages Internet qui l'utilisent effectivement.

Les cybercriminels tentent, entre autres, d'utiliser des certificats de sécurité falsifiés pour bernier les usagers d'Internet. Il est donc indispensable pour les usagers de connaître et d'appliquer la méthode permettant de vérifier la sécurité d'une page Internet d'e-commerce.

Pages d'e-commerce : vérification de sécurité par l'utilisateur

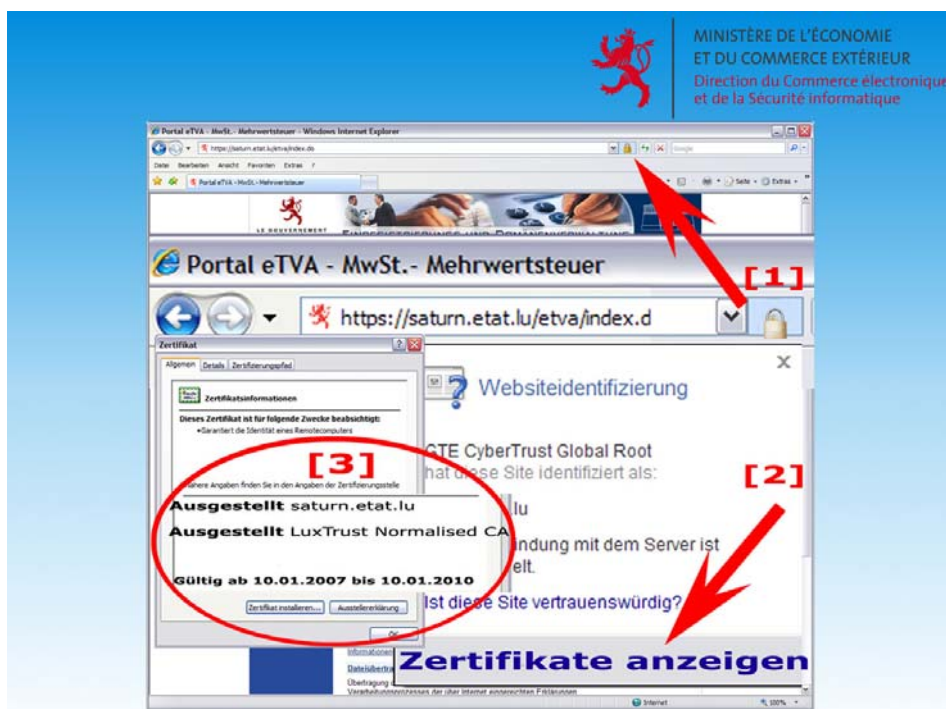
Une page web utilisant le protocole de sécurité https peut être identifiée grâce au petit cadenas fermé figurant dans la fenêtre du navigateur. Dans la version actuelle d'Internet Explorer, ce cadenas figure à droite de la barre d'adresse. Dans Mozilla Firefox, il apparaît non seulement à droite de la barre d'adresse, mais également en bas à droite de la fenêtre du navigateur. Dans les deux navigateurs, l'adresse (URL) saisie est surlignée en jaune lorsque le protocole https est utilisé et que le certificat de sécurité a été reconnu comme valide. Lorsque le

cadenas est ouvert ou barré, cela signifie que le certificat de sécurité utilisé ne respecte pas l'ensemble des critères de validité : il peut par exemple être périmé ou provenir d'un organisme non reconnu. Si le cadenas est fermé, le certificat doit faire l'objet d'étapes de vérification supplémentaires. La méthode simple et rapide pour effectuer le contrôle de sécurité d'une page d'e-commerce est présentée à l'aide de l'exemple des navigateurs Internet Explorer et Mozilla Firefox. Dans cet exemple, la page à vérifier sera celle du système eTVA luxem-

bourgeois : <https://saturn.etat.lu/etva/index.do>.

La transmission de données sensibles devrait toujours donner lieu à une vérification de la sécurité de la communication par l'utilisateur d'Internet. Cette vérification est très simple et rapide.

Les pages web frauduleuses peuvent également acheter et mettre en œuvre des certificats de sécurité. C'est pourquoi l'utilisateur d'Internet devrait impérativement vérifier le contenu du certificat concerné. Lorsque



Avec Internet Explorer

Lors de l'ouverture de l'application, il convient de vérifier qu'un cadenas fermé est affiché en bas à droite de la fenêtre du navigateur. Comme mentionné précédemment, ce cadenas ne doit être ni ouvert, ni barré. Si le cadenas est fermé, il convient de vérifier le certificat. Il suffit de cliquer sur le cadenas à l'aide du bouton gauche de la souris pour ouvrir le certificat.

Dans l'onglet [Général], l'utilisateur peut trouver une description du certificat concerné. Celle-ci énumère le détenteur du certificat, l'organisme ayant délivré ce dernier, ainsi que la période de validité. Il s'agit là d'informations que l'utilisateur devrait vérifier avant de faire confiance à la communication. Dans notre exemple, le détenteur du certificat est identique au serveur sur lequel se trouve l'utilisateur : saturn.etat.lu, et le certificat est toujours valide. L'organisme LuxTrust ayant délivré le certificat est, de plus, mondialement reconnu. Sous [Détails], l'utilisateur pourra trouver de plus amples renseignements concernant le certificat. Sous l'onglet [Chemin d'accès de certification], l'utilisateur peut également vérifier le statut du certificat : celui-ci doit être valide.

l'utilisateur pense être sur la page Internet de sa banque et que le certificat de sécurité affiché n'est pas établi au nom de celle-ci, cela signifie que des cybercriminels tentent de le tromper.

Réflexes de sécurité : navigateur

La bonne utilisation du navigateur permet également de combler certaines failles de sécurité. L'utilisateur devrait par exemple mettre à jour régulièrement son navigateur. Les failles de sécurité du logiciel sont ainsi corrigées. De plus, de nouvelles fonctionnalités de protection sont à la disposition de l'utilisateur.

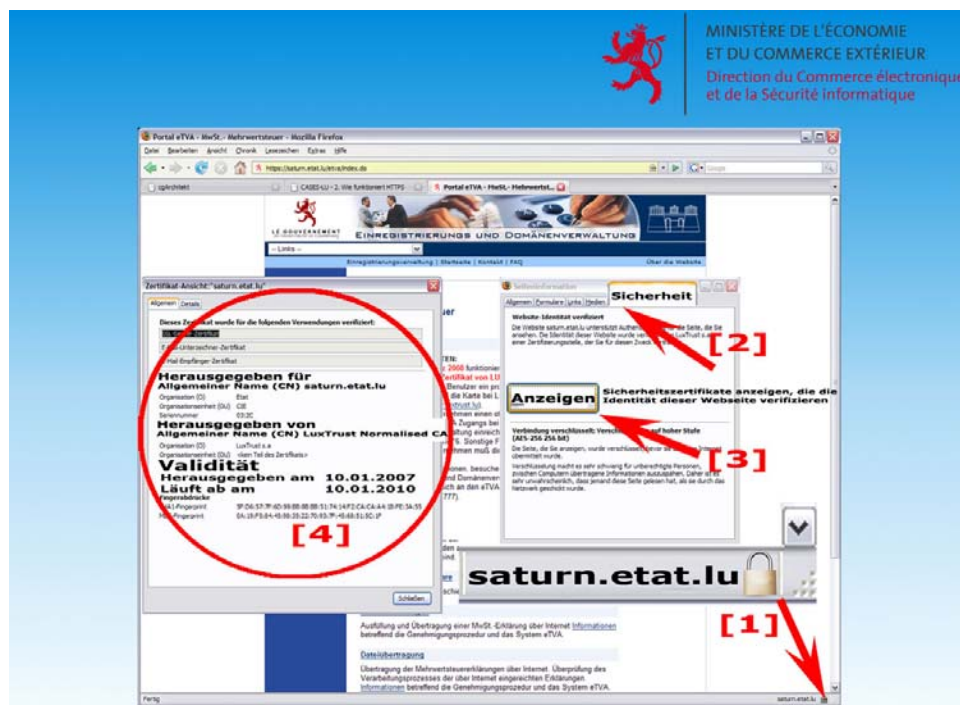
Les contenus enregistrés par le navigateur devraient être effacés après chaque session d'e-commerce ; il s'agit d'une opération simple : l'utilisateur peut suivre les indications figurant à la rubrique Conseils de sécurité du présent article à cet effet.

L'installation de programmes complémentaires tels que les plug-ins ou add-ons devrait être mûrement réfléchie. L'utilisation d'un nombre restreint de plug-ins et d'add-ons réduit en effet le risque lié aux failles de sécurité que peuvent comporter ces programmes. En outre, les utilisateurs ne devraient pas utiliser une version d'évaluation de leur navigateur.

Le portail de sécurité luxembourgeois CASES permet aux usagers d'Internet de s'informer sur les réflexes de sécurité adéquats et sur le comportement qu'il est recommandé d'adopter sur l'Internet.

Effacer des contenus dans la mémoire intermédiaire du navigateur

À l'aide de deux exemples, voici comment effacer les contenus enregistrés dans la mémoire intermédiaire du navigateur : dans le navigateur Internet Explorer, ces contenus peuvent être effacés en cliquant sur [Outils] dans la barre des menus, puis sur [Options]



Mozilla Firefox

Dans un premier temps, il convient de vérifier qu'un cadenas fermé est affiché à droite de la barre d'adresse ainsi qu'en bas à droite de la fenêtre du navigateur. Ce cadenas ne doit être ni ouvert, ni barré. Si le cadenas est fermé, il convient ensuite de vérifier le certificat. Un clic avec le bouton gauche de la souris sur le cadenas ouvre la fenêtre « Informations sur la page ». Dans l'onglet [Sécurité], l'utilisateur doit cliquer sur [Afficher le certificat]. Dans l'onglet [Général], l'utilisateur peut ensuite trouver une description du certificat employé. Le détenteur, l'organisme d'émission et la validité du certificat doivent être vérifiés. Le détenteur du certificat doit être identique au serveur sur lequel se trouve l'utilisateur. Dans notre exemple de l'application e-TVA, c'est bien le cas. La validité du certificat ne doit pas être arrivée à son terme, ce qui est également le cas. L'organisme de certification devrait être reconnu à l'échelle internationale, ce qui est le cas de l'entreprise LuxTrust. La communication est donc sécurisée.

Internet], et dans l'onglet [Général] sous *Historique de navigation* ; dans le navigateur Mozilla Firefox, ces contenus sont effacés en cliquant sur [Outils] dans la barre des menus, puis sur [Options], onglet [Vie privée] sous *Vie privée* [Paramètres] ou grâce au raccourci clavier [CTRL] [SHIFT] [SUPPR].

Informations complémentaires sur le protocole de sécurité https

Le portail de sécurité www.cases.lu propose des informations détaillées relatives à la sécurité des pages Internet. Un guide illustré présentant le mode de fonctionnement du protocole de sécurité https et permettant de vérifier la sécurisation d'une communication Internet est disponible dans le dossier HTTPS.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu