Conseils de sécurité pour gestionnaires de sites web

Voici une sélection de techniques existantes pour limiter les risques. Il en existe bien évidemment encore des milliers. Nous nous sommes limités aux plus courantes.

Tenez simplement toujours compte du fait qu'Internet comprend des dangers et que vous devez être conscients de ce que vous faites au quotidien dans votre vie professionnelle. Cela signifie que vous devez aussi gardez confidentielles ces informations au sein de vos cercles publics et professionnels, étant donné que le Web est le plus grand réceptacle d'informations et que la communauté des pirates informatiques rassemble et contrôle ces informations pour en abuser ensuite.

1. Lisez « Surfer en toute sécurité sur le World Wide Web : les 10 commandements »

2. Fournir du contenu

L'une des contre-mesures possibles pour prévenir la publication de contenu erroné sur le Web est le développement d'un flux d'approbation. Dans le jargon, on parle du « principe des quatre yeux » ou de « segregation of duties », qui permet à une autre personne d'apporter une validation supplémentaire aux données sur le Net.

Quels risques limitez-vous ainsi ?

Vous limitez ainsi le risque que des informations erronées se retrouvent sur le Net avec toutes les conséquences possibles imaginables sur le plan financier et la réputation.

3. Moyens d'identification et d'authentification

L'**identification** est la manière d'attribuer une identité à quelqu'un. Il s'agit d'un processus qui dépend du risque de votre application, où la sécurité du lien entre l'identité et la personne doit être d'un niveau élevé ou faible. Il s'agit de garantir que la personne est bien celle qu'elle prétend être. En voici quelques exemples :

- Vous pouvez donner un nom d'utilisateur à une personne en tenant compte du fait que celle-ci peut se trouver à l'autre bout du monde. Pour ce faire, vous proposez une page d'enregistrement sur laquelle cette personne ne laisse qu'une adresse e-mail avec éventuellement un CAPTCHA. Ensuite, le responsable de l'enregistrement (« registrator ») envoie un e-mail pour achever le processus d'obtention d'une identité. C'est un processus **très faible.**
- Quasi le même processus, mais on utilise une banque de données supplémentaire de personnes accréditées et, en interne, quelqu'un procède à des contrôles supplémentaires, éventuellement via un autre canal, par exemple un appel téléphonique. Dans ce cadre, quelques contrôles de base sont exécutés. Ceci aussi est encore un processus **faible.**

- Un citoyen va, en utilisant les preuves nécessaires, retirer sa carte d'identité électronique ou sa carte de banque à la maison communale ou à l'agence bancaire. Cette personne se présente physiquement afin que le fonctionnaire ou l'employé de banque puisse contrôler son identité. C'est un processus **solide.**
- D'autres processus sont encore possibles.

Un **moyen d'authentification** est en général un élément que vous possédez, par exemple un nom d'utilisateur combiné à quelque chose que vous connaissez, comme un mot de passe. Plusieurs combinaisons sont possibles :

- Identifiant et mot de passe
- Mots de passe à usage unique ou « One Time Passwords » (OTP). Il peut s'agir d'une application sur votre *smartphone*, par exemple « Google authenticator », ou d'une combinaison envoyée par SMS.
- Les cartes à puce dans lesquelles une clé privée est insérée, combinées à un solide processus d'émission ainsi qu'un code PIN. Par exemple l'eID et la carte bancaire.
- Les « listes TAN » comprennent des combinaisons sur papier qui peuvent varier selon le choix de celui qui les met en œuvre. Par exemple le token en Belgique.
- Il existe encore d'autres possibilités.

Le moyen d'authentification et les processus d'émission et de validation sont intrinsèquement liés au niveau de sécurité requis avant de pouvoir octroyer l'accès. On ne peut donc pas dissocier ces facteurs.

Dès lors, essayez de respecter cette simple règle de conduite : décomposez le mot de passe, PIN, TAN, la carte à puce et l'identité émise en plusieurs envois, SMS ou e-mails et utilisez toujours différents canaux. Veillez toujours à ce qu'un intermédiaire dispose également de toutes les informations lorsque celles-ci sont émises.

Quelques exemples de la façon dont la situation peut déraper :

- Une combinaison de nom d'utilisateur et de mot de passe de 8 caractères se composant d'un mot d'un dictionnaire, par exemple « devoir », peut facilement être retrouvée avec une « dictionary attack ». Dans ce cadre, on utilise un ensemble de mots ou par exemple un dictionnaire et des combinaisons de mots. En cas d'attaque en ligne, les pirates informatiques peuvent retrouver la combinaison en 3 heures. Lorsqu'ils sont en possession de la banque de données, cela se produit en quelques secondes, selon la force de calcul bien entendu.
- Essayez de toujours crypter les données des utilisateurs en cas de combinaisons utilisateur/mot de passe, qui sont généralement enregistrées centralement, avec un cryptage de niveau suffisamment élevé. Si la banque de données est piratée, vous courez le risque que votre image soit rapidement atteinte et que vos données ne soient plus intègres ou confidentielles. Une conséquence supplémentaire est que vous devrez arrêter votre service pendant une durée illimitée.

Quels risques limitez-vous ainsi ?

Si vous tenez compte de ce qui est décrit ci-dessus et si vous suivez les étapes consciencieusement, vous limiterez les risques au niveau de la disponibilité, des conséquences financières, de la confidentialité et de la réputation.

4. Maintenir le contrôle sur les utilisateurs

Garder le contrôle sur les droits des utilisateurs est crucial car une communauté d'utilisateurs est une donnée vivante. Les gens et les organisations sont soumises à des changements : ils vont et viennent, changent de fonction, partent à la retraite, etc. Dans le jargon, on appelle cet aspect « User Life Cycle ».

Pour maintenir ce cycle de vie sous contrôle, il est crucial de développer quelques contrôles, comme :

- Pour la création d'un utilisateur, essayez d'utiliser un flux qu'une autre personne doit valider avant qu'un droit ne soit octroyé à une personne.
- Les gens qui s'occupent de tâches administratives comme la création d'un utilisateur/de mots de passe doivent de préférence utiliser un moyen d'authentification différent et plus sécurisé, par exemple l'eID.
- Ne communiquez jamais à personne des mots de passe et noms d'utilisateurs, surtout pour les éléments auxquels il convient d'appliquer le « principe des quatre yeux ».
- Si possible, utilisez des règles contraignantes pour les mots de passe.
- Vérifiez périodiquement les droits émis. Le contrôle sera de préférence effectué par une personne différente de celle qui a octroyé les droits.

Quels risques limitez-vous ainsi ?

Vous limitez ainsi le risque que des droits attribués continuent à exister après qu'un utilisateur ait quitté l'organisation et que le cycle de vie de l'utilisateur ne soit plus intègre.

5. Faiblesses des systèmes et applications

En tant qu'organisation, procédez régulièrement à des scans de sécurité sur les systèmes, comme les ordinateurs de bureau et portables, les systèmes et applications, avec un scan de vulnérabilités. Pour les environnements spécifiques qui sont à la disposition de l'organisation, suivez les faiblesses qui se trouvent sur exploit-db.com et www.security focus.com, cert.europa.eu, www.us-cert.gov et d'autres sites web.

Utilisez en outre le pare-feu standard ainsi que les pare-feux au niveau des applications. Utilisez des techniques et systèmes de détection d'intrusion pour limiter les attaques connues et suivez régulièrement les informations de journalisation, qui sont très utiles pour détecter des profils.

Quels risques limitez-vous ainsi ?

Vous limitez ainsi l'impact des pertes de données, de logiciels malveillants, d'espionnage, de disponibilité et d'autres problèmes.

6. Choisissez des mots de passe sécurisés, ne les réutilisez pas, ne les partagez jamais et renouvelez-les régulièrement

La règle d'or : au plus le mot de passe est long et complexe, au mieux il est protégé.

Pour vous souvenir facilement d'un mot de passe, vous pouvez utiliser une longue phrase, qui est en outre plus sûre qu'un simple mot.

Vous pouvez également recourir à des programmes spéciaux, baptisés « coffres-forts à mots de passe », qui créeront et se souviendront du mot de passe pour vous.

Renouvelez régulièrement vos mots de passe. Lorsque vous vous enregistrez sur des sites web, utilisez toujours des mots de passe et adresses e-mail différents.

Outre votre mot de passe, on peut également vous demander d'introduire un code qui vous est envoyé directement sur votre GSM personnel. Vous pouvez souvent activer vous-même cette fonctionnalité dans le programme ou sur le site web que vous utilisez.

Il est facile de deviner les réponses aux questions secrètes que vous pouvez choisir pour mieux protéger ou réinitialiser votre mot de passe. Si vous devez néanmoins le faire, le mieux est de ne pas répondre à la question mais de donner une réponse fictive. Veillez toutefois à bien vous souvenir de votre réponse ou à utiliser un coffre-fort à mots de passe.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact en cas d'abus de votre compte. En effet, si vos mots de passe et comptes ont été piratés sur le Net, il sera plus difficile pour les « hackers » de les réutiliser.

7. L'utilisation de SSL

Lorsque https:// est indiqué au début de votre adresse Internet, cela signifie que la connexion est sécurisée. Si vous recevez un message d'erreur signalant que le certificat n'est pas correct, cette connexion n'est plus sécurisée.

Tenez aussi systématiquement à jour l'implémentation SSL. Depuis 2013-14, SSL a commencé à présenter quelques faiblesses. De ce fait, des millions de sites web ont pu être espionnés. Attention, le problème ne se limite cependant pas à l'implémentation de SSL. Il convient en effet d'adapter aussi la force de cryptage que vous avez choisie à un moment donné dans le temps.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et l'interception de la communication.

8. Sécurisez toujours vos réseaux Wi-Fi

Sécurisez votre réseau à domicile ou au bureau avec un mot de passe que vous modifierez régulièrement. Soyez vigilants avec les réseaux Wi-Fi publics. Méfiez-vous en constamment et essayez toujours et en toutes circonstances d'exécuter vos tâches au moyen d'une connexion sécurisée par le biais de la technologie VPN.

Vous empêcherez ainsi aussi bien les cybercriminels que vos voisins (par exemple d'autres entreprises dans le même bureau ou d'autres membres du personnel) d'utiliser votre connexion Internet sans fil.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et l'interception de la communication.

9. Veillez à effacer complètement la mémoire de votre appareil et/ou serveur

Vous pouvez vider la mémoire de votre *smartphone* ou tablette via l'option « Effacer » de votre appareil. Pour votre ordinateur de bureau ou ordinateur portable, il est préférable de procéder à un effacement et à un formatage complet. Vous pouvez faire appel aux départements ICT pour procéder à cette opération rapidement et avec précision. Un formatage rapide n'est pas une bonne idée car il reste toujours des données.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et empêchez que des noms d'utilisateur et mots de passe tombent dans de mauvaises mains.

10. Procédure de sauvegarde et restauration

Veillez à toujours sauvegarder vos systèmes et données. Vérifiez toujours l'exactitude de votre sauvegarde et procédez régulièrement, par exemple avant qu'un site ne soit mis en ligne, à une restauration. Procédez au moins 2 fois par an à une restauration de la sauvegarde et validez l'exactitude de la procédure de restauration.

Sécurisez aussi vos sauvegardes puisqu'elles contiennent les mêmes infos que les données qui se trouvent dans les différents environnements.

Dans la mesure du possible, documentez le déroulement de la procédure de « back-up and restore » afin que les personnes qui ne connaissent pas les environnements puissent aussi exécuter la restauration.

Quels risques limitez-vous ainsi ?

Vous limitez ainsi les risques de pertes de données et de disponibilité.

Sources

(https://www.safeonweb.be/nl/tips)

(https://cert.europa.eu/cert/alertedition/en/malware.html)

(https://pentestmag.com/the-cyberwar)