Veille Technologique : Sécurité Web et Mobile

1. DEFINITION

La **sécurité** Web & Mobile est le processus qui consiste à développer, ajouter et tester des fonctionnalités de **sécurité** au sein des **applications** et sites afin d'éviter les vulnérabilités face à des menaces telles que les accès et les modifications non autorisés.

1. Sécurité Web et Mobile

Les données personnelles stockées sur votre smartphone valent souvent bien plus que le smartphone lui-même. Il en va de même pour les ordinateurs portables et les tablettes. Avec l'avènement des smartphones et de la technologie mobile, de plus en plus de personnes ont entre leurs mains des menaces de sécurité potentielles.

La technologie mobile s'est infiltrée dans tous les aspects de notre vie quotidienne. On l'utilise dans le cadre d'une multitude d'activités, notamment la localisation GPS, le divertissement, le stockage, et bien plus encore. Alors que les fonctionnalités des téléphones mobiles sont infinies, les risques liés à notre confidentialité sont bien réels.

Plus nous stockons d'informations sensibles sur nos appareils mobiles, plus la protection de ces données devient cruciale. Des photos et adresses personnelles aux informations de carte de crédit et numéros de téléphone, les pirates informatiques qui accèdent à nos téléphones ont aujourd'hui plus d'informations personnelles à leur disposition que jamais.

Les attaques mobiles peuvent être classées en quatre catégories : les attaques de système d'exploitation, les attaques d'application, les attaques par malware et les attaques par réseaux de communication (par Wi-Fi ou Bluetooth, notamment).

Les attaques de système d'exploitation utilisent les faiblesses trouvées au niveau du système d'exploitation. Les attaques d'application sont généralement permises par une erreur de développement ou de code. Les attaques par réseaux de communication se produisent lorsque des utilisateurs se connectent à un réseau défectueux ou non sécurisé. Les attaques par malware, de plus en plus nombreuses, permettent à quelqu'un de voler vos photos, de détourner votre appareil photo et d'effacer des fichiers importants.



* Une nouvelle époque

Les failles de sécurité mobile sont très différentes des attaques portant sur votre ordinateur de bureau. Premièrement, l'étape de connexion n'existe plus. Les utilisateurs ne se connectent pas à leurs appareils, ce qui rend l'accès et le partage de données entre diverses applications problématiques.

En plus de vos photos, contacts et fichiers personnels, les applications mobiles stockent également des informations sensibles, telles que des mots de passe, des jetons d'authentification, et bien plus encore. Il est essentiel de protéger ces fichiers pour empêcher les pirates informatiques d'accéder à vos comptes personnels.

Contrairement aux utilisateurs d'ordinateur de bureau, les utilisateurs mobiles ne peuvent pas voir l'URL complète d'un site qu'ils visitent, ce qui permet aux escrocs sur Internet d'utiliser facilement des attaques de phishing contre des utilisateurs non avertis.

* Renforcement de la gouvernance en matière de sécurité mobile

Certaines mesures peuvent vous aider à préserver la sécurité de vos appareils mobiles. La première mesure consiste à savoir exactement quelles données sont collectées par les applications que vous utilisez, notamment les contacts, photos, données Internet et journaux d'appel. Vous devriez également comprendre comment vos données sont utilisées par ces applications.

Utilisez des mots de passe différents pour des applications et sites distincts. Créez des mots de passe longs et compliqués, comportant des lettres, des chiffres et des symboles. Pour ajouter un deuxième niveau de protection, utilisez un système d'authentification à deux facteurs.

N'utilisez jamais une connexion Wi-Fi ou Bluetooth non sécurisée et mettez à jour votre système d'exploitation et vos applications dès qu'une nouvelle version est disponible.

Il est possible de vous protéger et d'optimiser la sécurité de vos appareils mobiles. En comprenant parfaitement les risques et en prenant les précautions nécessaires, vous pouvez préserver votre vie privée et votre sécurité.

1. EXEMPLE D’ATTAQUE

# En Irlande, un rançongiciel à l’origine d’une attaque informatique contre le service de santé

C’est l’une des menaces informatiques les plus pesantes sur les entreprises et les institutions. Une nouvelle attaque au rançongiciel a été menée, vendredi 14 mai, contre le service public de santé irlandais (Health Service Executive, HSE). Il a dû arrêter l’ensemble de son système informatique en raison de cette « importante » cyberattaque.

Les cyberattaques à l’aide de rançongiciel sont un phénomène qui a explosé ces dernières années. Jeudi soir, Colonial Pipeline, [l’opérateur de l’immense oléoduc américain,](https://www.lemonde.fr/pixels/article/2021/05/10/comment-un-rancongiciel-a-seme-la-panique-dans-un-grand-reseau-d-oleoducs-aux-etats-unis_6079752_4408996.html) a relancé l’ensemble de son système, après avoir été paralysé le week-end dernier.

Un rançongiciel est un virus qui verrouille les ordinateurs et réseaux informatiques des entreprises qui en sont victimes. Tous les fichiers des ordinateurs touchés sont chiffrés, c’est-à-dire qu’ils sont illisibles et inutilisables par l’utilisateur. Les opérateurs de ces logiciels malveillants demandent alors une rançon en laissant une note sur les ordinateurs des victimes : en échange de cette rançon, qui peut se chiffrer en millions de dollars, ils promettent d’envoyer aux victimes une clé de déchiffrement censée leur permettre de récupérer l’usage de leur réseau.

1. CONSEILS

L’un des défis lorsqu’on **développe des applications mobiles** est la sécurité. Chaque fois que vous créez une application mobile pour une entreprise, vous devez vous assurer qu’elle est protégée contre tout type de [cyberattaque](https://www.codeur.com/blog/eviter-cyberattaque-repandues/). En cas d’atteinte à la sécurité, l’entreprise en question peut pâtir d’une mauvaise réputation.

Si vous n’assurez pas la sécurité des données des utilisateurs, ces dernières pourraient être manipulées ou volées et être utilisées à mauvais escient. Une application mal sécurisée peut aussi être infectée par un virus, ou même clonée. Vos efforts bénéficieraient à des gens mal intentionnés, qui se seraient contentés de se jouer de vos lacunes en matière de sécurité.



**Voici 6 conseils pour vous aider à protéger l’application contre les brèches :**

1. **Éliminer les failles côté serveur**
2. **Sécuriser le stockage de données**
3. **Considérer une forte authentification**
4. **Prévenir l’injection côté client**
5. **Limiter l’accès au code**
6. **Tester régulièrement**

**Conclusion**

En Définitive, la Sécurité Web et Mobile est primordiale dans cet environnement, de ce fait les conseils listés ci-dessus ne sont que le **b.a.-ba de la sécurité web mobile** . À la fin de 2018, il y avait plus de 30 millions de logiciels malveillants à destination des appareils mobiles. Ce chiffre grossit de manière constante. N’hésitez pas à [faire appel à un professionnel](https://www.codeur.com/fonctionnement-codeur) pour sécuriser votre application !