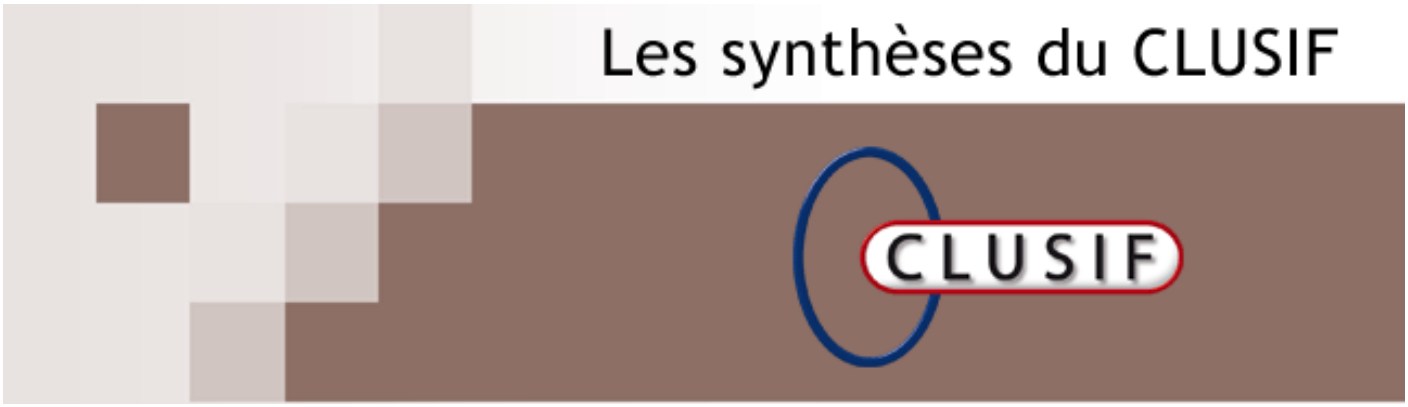

Applications mobiles et sécurité - *Synthèse de la conférence thématique du CLUSIF du 13 avril 2016.*

Bien que souvent présenté comme un sanctuaire, l'App Store d'Apple a accueilli en septembre 2015 des applications compromises après la diffusion d'une version d'Xcode modifiée. Cet épisode a rappelé à tous les professionnels de la sécurité qu'il n'existe pas de sécurité absolue dans le monde de l'application mobile, pas plus que dans celui du Web ou plus généralement, de l'informatique.

Dans le même temps, la technologie mobile est appelée à prendre de plus en place dans le paysage informatique. Comme le rappelle Thierry Chiofalo en introduction, en 2014, le nombre d'Internautes utilisant des terminaux mobiles a dépassé celui des utilisateurs se connectant depuis des terminaux fixes

La mobilité qui est donc au cœur des préoccupations de tous les acteurs économiques pose de nouvelles problématiques, de sécurité, bien entendu, mais également de développement, de déploiement ou de réactivité. Cette évolution vers les applications mobiles, sources d'enrichissement de la relation client et vecteur de fluidification de l'accès aux systèmes d'informations par les employés, touche alors les RSSI qui doivent l'accompagner tout en préservant les systèmes d'information.

Le CLUSIF, à travers cette conférence, a souhaité faire un point complet sur ce sujet qui a trait à la transformation du système d'information et à la façon dont il interagit avec ses utilisateurs, qu'ils soient internes ou externes.

Les risques identifiés par les RSSI

Par Henri CODRON, Responsable de l'Espace RSSI, CLUSIF

La sécurité des applications mobiles est un sujet qui est évidemment régulièrement abordé dans les réunions de l'Espace RSSI du CLUSIF, a indiqué Henri Codron. Si l'on était parvenu au fil des ans à sensibiliser les utilisateurs de postes fixes à un ensemble de bonnes pratiques en matière de sécurité, on est encore loin de cela dans le domaine des terminaux mobiles. Les utilisateurs s'éloignent au contraire de la charte d'utilisation signée au sein de leurs entreprises : ils téléchargent des applications sans mesurer les risques. Sans prendre en compte le fait que leur smartphone est connecté au système d'information de l'entreprise.

Si les catalogues d'applications ont mis en place des processus de validation intégrant la notion de sécurité, il arrive, dans la pratique, qu'ils mettent à disposition des applications malveillantes.

Les RSSI ne disposent pas de liste précise de ces applications malveillantes et ont du mal à agir sur la gestion du parc, a ajouté Henri Codron. Si des progrès ont été faits, aucune solution permettant de sécuriser les terminaux mobiles n'émerge véritablement sur le marché.

Les risques sont multiples. Les applications développées par l'entreprises et ayant des accès au système d'information cohabitent sur des terminaux avec des applications tierces qui envoient des données dans le cloud. Le risque de fuite de données est réel.

La gestion des versions est complexe. Celles-ci ont généralement pour but de régler des problèmes de sécurité mais il faudrait dans l'absolu pouvoir vérifier qu'une nouvelle version peut coexister avec le système d'information ou les autres applications.

En outre, la pression métiers ou marketing sur les développeurs est désormais très forte. On les incite à mettre en place des cycles de développement très courts, qui ne sont pas forcément compatibles avec une composante sécurité poussée.

Qui plus est, les tests d'intrusion qui garantiraient une meilleure sécurité des applications et partant, des systèmes d'informations peuvent, dans le cadre de ces développements rapides, se révéler plus onéreux que le développement de l'application elle-même.

Tout cela pose une série de questions :

- Comment accompagner les nouveaux usages tout en sensibilisant à la sécurité ?
- Comment connaître le niveau de sécurité des applications publiques installées sur les terminaux mobiles ?
- Comment parvenir à sensibiliser les métiers aux problématiques de sécurité ?
- Comment obtenir les budgets nécessaires à une bonne analyse de sécurité pour ces nouvelles évolutions du système d'information ?

Ces questions sont d'autant plus prégnantes que l'on retire trois enseignements de l'évolution des applications mobiles :

- Les utilisateurs ne veulent pas de contraintes.
- Les métiers demandent de plus en plus d'applications mobiles.
- L'analyse de la sécurité des applications mobiles n'est pas un processus mature.

Les comportements cachés des applications mobiles

Par Renaud GRUCHET, PRADEO

Les applications mobiles ont un usage et des permissions demandées qui sont déclarées et affichées sur les catalogues. Mais pour Renaud Gruchet, cela cache souvent des comportements engendrant les problèmes évoqués précédemment. C'est ce que Pradeo a appelé le syndrome de l'Appsberg, contraction des mots Applications et Iceberg. Une application qui a accès aux contacts, récupère en fait des données personnelles, communique peut-être avec des serveurs non sécurisés, etc.

Plus on avance, plus les terminaux mobiles se connectent au système d'information. Pradeo a réalisé une étude avec OpinionWay sur ce qui est considéré comme confidentiel dans un smartphone. Les particuliers et les professionnels estiment à une très grande majorité (en moyenne 80%) que les photos, les vidéos, les mails, les contacts, les SMS, l'agenda, sont confidentiels.

Pour autant, 52% des personnes qui utilisent un smartphone pour un usage professionnel ont enregistré des identifiants et des mots de passe personnels sur leurs terminaux. Contre 33% pour ceux qui les utilisent pour un usage privé.

Il y a sans doute là une sorte de faux sentiment de sécurité, les utilisateurs imaginant que les entreprises qui leur confient les terminaux mobiles ont fait le nécessaire pour en assurer la sécurité.

Les applications mobiles sont un énorme marché et elles ont un avenir certain. Il va donc falloir composer avec elles.

Pradeo a par ailleurs réalisé un livre blanc sur ce sujet. Quelque 1.250.000 applications différentes ont été analysées. Apple ne facilite pas le travail des chercheurs de failles, c'est pourquoi 80% des applications étudiées proviennent du monde Android. De fait, Android concentre le plus d'applications malveillantes connues, étant l'environnement le plus ouvert et facile à analyser.

Sur le total des applications étudiées, 1% sont notoirement malveillantes. Mais ce sont les 15% d'applications « suspectes », classées dans une zone grise qui posent problème. Elles récupèrent des données personnelles non nécessaires à leur fonctionnement. Leur comportement sera jugé malveillant ou non, selon les règles personnalisées des entreprises.

Quelque 3500 applications du panel étudié sont des malwares de type screenlogger, cheval de Troie, keylogger, intercepteur OTP ou ransomware.

Enfin, on note que les applications natives des fabricants et des opérateurs ne sont pas irréprochables.

Sécuriser les applications mobiles : il y a un OWASP Top 10 pour ça

Par Sébastien GIORIA, French chapter leader, OWASP

L'OWASP (Open Web Application Security Project) est un organisme à but non lucratif désormais bien connue pour l'édition de son Top 10 associant les 10 risques les plus importants pour les sites Web, associés aux recommandations de correction correspondantes. Ce Top 10 est constitué grâce à l'ensemble de la communauté OWASP qui remonte des informations tirées d'audits ou des découvertes de failles

Aujourd'hui, ce projet est complété d'un projet Top 10 spécifique au contexte mobile. Ce Top 10 mobile est en release candidate et va donc encore probablement un peu évoluer. Il comprend aujourd'hui les points suivants :

1. Improper platform usage
   Mauvais usage de la plateforme de distribution (App store, Play store, etc.). Parfois l'application entre dans le store parce que l'éditeur est connu mais il peut ne pas avoir respecté les guidelines pour certaines de ses applications. Cela peut aboutir à des vols de données ou des fraudes au paiement.

2. Insecure data
   Risque de vol de données sur le terminal ou dans le cloud. Ce peut être le cas, par exemple, d'une application bancaire qui afficherait des informations sans authentification. Pourtant il existe des mécanismes de coffre-fort de plateforme permettant de sécuriser des données sensibles en les chiffrant. Mais de très nombreuses applications ne les utilisent pas. Les données sont stockées en clair dans des fichiers XML ou des bases SQL. Le coût de l'utilisation de ce type de coffre-fort est pourtant quasiment nul.

3. Insecure communication
   Risque de vol de données lors de leur transmission. La solution consiste à mettre en place TLS. C'est simple et peu coûteux.

4. Insecure authentication
   Il existe un risque d'exposition de données à un utilisateur non autorisé. Il n'est pas rare que des applications n'exigent pas de mot de passe, ou que ceux-ci soient trop simples. La solution passe par l'authentification multi-facteur, un système de déconnexion et une gestion correcte des sessions.

5. Insufficient cryptography
   Utilisation par les applis de cryptographie simple. La clef est parfois stockée dans l'application et elle est commune à l'ensemble des utilisateurs.

6. Insecure authorisation
   Il existe un risque d'accès à des opérations de type CRUD (Create, Read, Update and Delete) sans autorisation. Pour éviter cela, il faut mettre en place de l'habilitation et pas simplement de l'autorisation : OAuth 2.0 [1]par exemple.

7. Client code quality issues
   Risque de prise de contrôle sur le terminal. Solution : revue de code, bonnes pratiques de codage sécurisé.

8. Code tampering
   Bibliothèques vulnérables ou infectées ajoutées dans du code et faisant courir un risque de prise de contrôle du terminal. Solution : anti-virus, mécanismes de signatures. Complexe et coûteux à mettre en œuvre.

9. Reverse engineering
   Vérifier que la décompilation et l'analyse de l'application sont complexes. Attention à choisir une solution d'obfuscation complexe, pas simplement celles proposées par les plateformes.

10. Extraneous functionality
    Fonctionnalités non déclarées. C'est un risque par exemple lors d'une sous-traitance, si l'agence est peu professionnelle. Comme il s'agit de code non désiré dans l'application, il faut l'analyser, ainsi que les binaires, avant la mise en œuvre.

[1] Standard ouvert de gestion des autorisations

Enjeux et stratégie de protection

Par Christophe GUEGUEN, Responsable Practice Data & Cyber Security, Harmonie Technologie

Les équipes « digital marketing » ont généralement un triple objectif : proposer une solution simple, un service en adéquation avec les usages et les changements comportementaux des clients et fluidifier les parcours et les interactions entre les canaux.

Pour Christophe Guéguen, cela induit une complexification de gestion. Les cycles de développement sont désormais très courts (entre 10 et 20 jours). Il s'écoule généralement deux mois seulement entre l'idée et la publication de l'application. Cette évolution conduit également à une exposition croissante de données et de services métiers. Enfin, les contextes mobiles ne sont pas propices à un cadre de sécurité solide. Les coûts et les délais non négligeables liés à une exigence de sécurité sont inadaptés et il existe peu de solutions de sécurité centrale répondant aux besoins des applications.

Pour autant, il ne faut pas renoncer aux aspects liés à la sécurité. Un double défi se pose : parvenir à ce que le RSSI soit identifié comme un partenaire à part entière des équipes digitales et non pas comme un frein, et qu'il soit à même de s'adapter aux cycles courts tout en maintenant un niveau de sécurité adapté aux enjeux.

Pour y parvenir, il convient de disposer, au niveau de l'entreprise, d'un socle de sécurité pouvant répondre aux usages. Quant aux projets, il faut adapter l'intégration de la sécurité dans les méthodes agiles.

L'identification pose souvent problème aux métiers qui ne veulent pas que l'utilisateur ait à utiliser des mots de passe ou des mécanismes complexes pour pouvoir utiliser les Apps. Il faut donc avancer vers un IAM (Identity and Access Management) étendu où, par exemple, OAuth entre en jeu.

Il faut, en définitive, s'orienter vers un pilotage par les risques prenant en compte l'analyse du comportement utilisateur, la revue des contenus des stores et l'utilisation d'un référentiel des données sensibles.

Retour d'expérience : s'agit-il de protéger le mobile ou le SI

Par Jean-Paul JOANANY, RSSI, Generali

En tant qu'assureur de premier plan, Generali compte un parc très important. Parmi environ 600 applications, 170 sont des applications métier. « Nous gérons 11 millions de lignes de code Java et 40 millions de lignes de code Cobol », a précisé Jean-Paul Joanany. Si l'assureur compte plus de 200 développeurs dans ses rangs, de plus en plus d'applications sont développées off-shore ou near-shore. La multiplication des langages et des frameworks pas toujours matures, ni très pérennes complexifie encore un peu plus la situation. Les applications mobiles permettent aux clients de suivre leur situation financière. La responsabilité de Generali est donc accrue et les éventuelles failles de sécurité sont porteuses d'un risque important pour la réputation de l'entreprise.

En ce qui concerne les terminaux mobiles, leur multiplication modifie profondément l'écosystème du système d'information. Generali a opté à la fois pour le BOYD (Bring Your Own Device) et le COPE (Corporate Owned, Personally Enabled).

Pour ses développements d'applications mobiles, Generali a choisi d'intégrer le facteur sécurité tout au long du cycle de vie.

Dans la phase de développement, la méthodologie tient compte des exigences fortes de sécurité et des normes et bonnes pratiques du marché (OWASP). Il convient, par exemple, de s'assurer que l'application ne pourra pas être clonée et détournée de son usage.

Dans la phase d'exploitation, Generali opère une surveillance constante des vulnérabilités des composants de l'application, réalise régulièrement des analyses de vulnérabilités, investigue les incidents impliquant les applications, surveille les signaux faibles, la réputation de l'application et le périmètre de déploiement des mises à jour.

Bien entendu, des pistes d'amélioration sont toujours explorées et notamment une plus forte formation et sensibilisation à la sécurité des équipes de développement, ainsi qu'une sophistication des tests pratiqués tout au long du cycle de production des applications et après leur déploiement.