Infographie

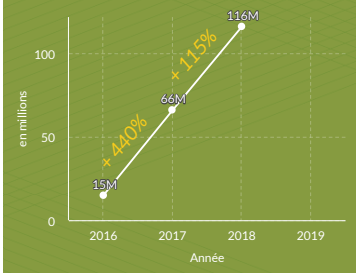
Cybersécurité des Smartphones

Constat

Grâce aux fonctionnalités intégrées, le cloud et les applications, le smartphone est devenu un outil indispensable du quotidien. On gère agenda, comptes bancaires, abonnements, réservations... d'une certaine manière, ce mini ordinateur sait plus sur nous que nous mêmes!
Il connaît notre position géographique avec exactitude, nos habitudes, trajets, photos, voyages, mots de passe... bref, il est le passeport numérique de notre vie. Aujourd'hui on se sert plus de son téléphone que de son ordinateur, pour les criminels le choix est fait!

CONSTAT

Plus de six milliards de téléphones mobiles seront actifs sur la planète d'ici 2020.



Facteurs à risque :

- Le BYOD : "Bring your own device" ou apportez votre propre appareil. Cela ouvre la porte aux réseaux de l'entreprise avec des technologies personnelles.
- Les réseaux de Wi-fi publics.
- Les applications réseaux sociaux (Facebook, Instagram, Snapchat...).

Malwares les plus actifs :

- **Lotoor** : malware Android reconditionnant des applications légitimes pour accéder aux informations du système d'exploitation.
- **Triada** : Un porte modulaire qui accorde des privilèges super-utilisateur.
- **Ztrog** : cheval de troie qui s'installe dans le répertoire du système.
- **XcodeGhost** : malware qui transforme les appareils Apple en un botnet à grande échelle.
- **Skygofree** : spyware, igéolocalise, enregistre photos, vidéos, conversations, agenda...

MESURES

Les pirates l'ont bien compris, désormais ils tirent plus d'avantages à exploiter les failles de l'humain, en attaquant les applications trop permissives.

1. Jamais installer des applications externes aux app stores officielles.
2. Faire les mises à jour régulièrement.

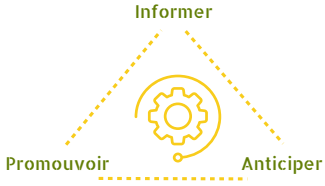
"Le danger est omniprésent pour l'individu, mais également pour l'entreprise! Documents partagés, emails, cloud..."

3. Sensibiliser les collaborateurs aux bons usages.
4. Mettre en place une gestion optimisée des mots de passe.
5. Limiter les téléchargements d'applications mobiles.
6. Séparer données personnelles et professionnelles.

7. Opter pour le Mobile Device Management, pour gérer toute la flotte mobile.

eAwareness par eCyberProtect.fr

Les pirates l'ont bien compris, désormais ils tirent plus d'avantages à **exploiter les failles de l'humain**, en attaquant les applications trop permissives.
Chez eCyberProtect nous avons mis en place un module de sensibilisation afin de protéger les collaborateurs et les organisations.
3 étapes et 3 actions concomitantes :



1. Sensibilisation des parties prenantes
2. Exploration des cas réels
3. Mesure des conséquences

eCyberProtect
4, Avenue du Général de Gaulle
92170 Vanves
01 55 95 64 65

SAS au capital de 20 000 € RCS Nanterre 840 410 690 – TVA FR24822234472– APE 6202A