International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6,September 2015
ISSN: 2395-3470
www.ijseas.com

Security and management of applications and mobile Data protections

AMMAR ES-SAID[1], LABRIJI EL HOUSSINE[2]
HANOUNE MOSTAFA[3] , GHANIMI FADWA[4]

[1] University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco
Hay lamia block 06 N° 07 Hay Mohammadi Casablanca Morocco
Department of Mathematics and Computer,

[2] University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco
Department of Mathematics and Computer,

Abstract

The mobile data security permits keeping control over the use of the device by integrating a management system and data protection functions on the centralization of the safety regulations with endpoints and other solutions to form a global security strategy.

- Neutralizes malevolent programs and blocks Webs with malevolent anti-program points
- Detects attacks that manage to infiltrate via ports and services.
- Supervises, blocks and records calls, SMS and MMS sent forward and from devices according to the policy of use.
- Improves the visibility and the control of the Android and iOS devices. With a function of inventory management and generation of rapports allowing a better visibility of applications used on the device.
- Protects device data lost or stolen thanks to remote function, selective and localization of the device.
- Applies the strategies of data preventions, ensures the coding of conformity by blocking unbridled or unencrypted devices.

After having put to pomposity on the vulnerabilities of the platforms of the mobile applications, the devices management ***represents a major need within the framework of numerous opportunities more importantly it permits activating a security service of the devices equally flexible and stable this principal is in the center of our philosophy.***

Keywords: *Selective, Mobile Devices, Sensitive Data, BYOD, RESTFUL, SOAP, Sandbox*

I. Introduction

The organizations developing strategies in order to explore new opportunities by constantly evolving on mobile development, the challenges of the applications and data security prevent certain organizations from attending their objectives to the mobile customer's commitment .Now the search for solutions that allows to easily extend the environment of Web applications to the new models of mobile supply and at the same time keeping the significant data transmitted between devices safe.

Organizations rather need a universal approach which resolves the problem in a global manner into two axes: by allowing on the one hand the commitment by the means of management of the

applications and on the other hand the security focusing on the data.

II . The challenges of commitment and mobiles protection

New mobiles peripherals, equipped with a high-speed access and mobile applications are innovating commercial opportunities emergent to a measure that the entire world adopts however these devices the number of users possessing many peripherals and the appearance of the application BYOD (Bring your own device), which supposes that each brings his own materiel, the innovating speed in the field of mobiles equipments exceeds the adaption capacity of organizations.

2.1 Implications of the frowth of the applications onthe

Mobility brings solutions and additional means to enrich their ranges by means of new channels of development .It sets up innovating approaches making it possible for teams to reduce the deadline to the point of new programs, however, the proliferation of type of peripherals had consequences on the standardization and created an environment of heterogeneous application that organizations must from now on put up with to reach more quickly.

Rich mobiles applications allow users a rapid access to the content and to carry out commercial transactions, since the organizations seek to expand their presence near mobile users by means of mobiles application development, It is interesting to begin with applications, but this also comprises challenges.

For example, most of mobiles applications are developed using RESTFUL protocols, whereas the existing applications environment relies on SOAP. This difference sometimes blocks the compatibility of mobiles applications on the market, but the existing management access possibilities can allow their launching.

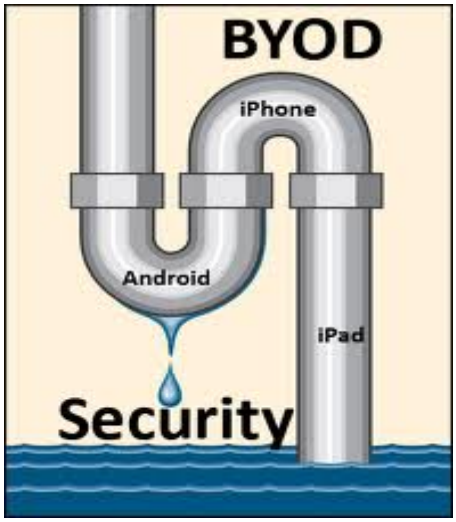
2.2 Intelligent and composite applications
The development of innovating applications multiplied the commercial opportunities and enriched the way organizations can make deals with clients, so that the content distributing strategies and the installation of the organizations transactional mobile applications progresses, these last study the option related with intelligent application or composite for mobile peripherals

2.3. The important is the data not the peripheral

The organizations must implement solutions of unified security applications, and they also must make data protections measures, even though they always had little control on the peripherals and data of their clients, they also start losing control over peripherals of their employees.

2.4. Phenomenon BYOD

This rising growth rate of the number of peripherals and the use of numerous peripherals by one person influences directly the BYOD Phenomenon.
According to Forrester « many information professionals in North America and Europe declared that they chose their peripherals themselves (rather than having it imposed by the computer department or being limited to a determined list by this later)
This percentage reaches 73% for smart phones, 53% for the laptops, and at even 22% for desktops ».this proves that employees directly gain control, which has consequences on the future data information planning.
However, even if the organizations begin losing control of peripherals by admitting devices under the responsibility of employees, they cannot afford to lose control of data : they must continue keep control of the data in order to reduce the risk loss of intellectual property.

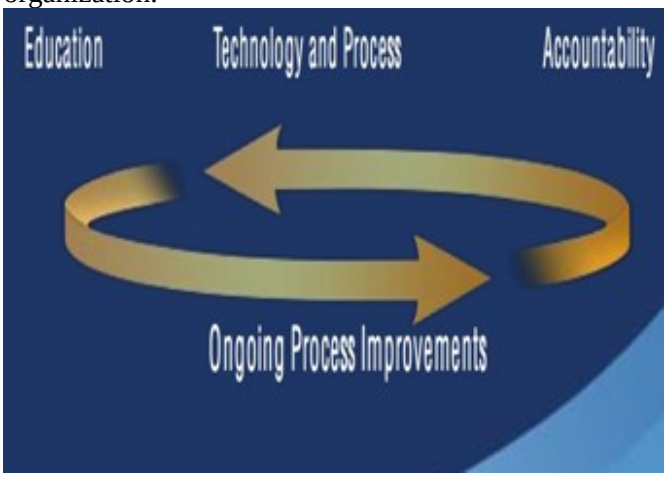


III.The selection of mobile security solution

The opportunity of developing your activities is often slowed down by challenges related to the applications and data security. It is necessary to adopt a pragmatic approach to meet these challenges, by simplifying decision making and by satisfying two principle criteria: the client's commitment and the security centered on the data

3.1 Solutions to mobiles data security?

The solutions to mobile data security are currently available on the market and enable you to give priority to capacities based on the client's engagement security centered on the data , This system provides general advices for the selection of mobile solutions, but must also be evaluated compared to the specific objectives of the organization.



The organization type, cases of mobile use, applications strategies …….
The axis of commitment is defined by several features which allow mobile clients a better implication in the activity, among these features, we mention, the authentication, authorization, unique authentication, sessions management, the translation of protocols and secured management of the API, data protections solutions are also included, because they also remove obstacles to the data security which prevents the commitment to clients, all the features cover diverse technologies and must be chosen by specific project criteria.

The management of the identities and the access : This solution is appropriate to organizations that seeks to extend their access managing feature and authorization up to the organizations applications * at the same time for their mobile clients and their employees.
API management : This solution effectively allows community developers to write in a secured way in the API and at the same time translate protocols for new complex applications.

Mobiles applications management: This feature makes it possible to include different application which assures authentication features and local data protection

3.2 *Security centered on the data*

The axis of the security centered on the data gathers solutions to mobility according to security solutions that protects indirectly the data in different ways, then, the solutions which focuses more and more on the protection of the data itself.
Malevolent codes: A protection against harmful codes and anti-viruses is useful to protect
The organization in case of connection to a compromised application, but the applications and the personal data are then protected in an indirect way. The protection Is not exclusive to the data
Virtualization : with the principle of the 'sandbox', it constitutes an approach of segmentation aiming to isolate the organization's applications from the personal application on the peripheral, the information are separated, which allows the control of the professional data, but* flees to the facility of using.
Classification: This option Is essential to understand the data localization and their degree of sensitivity to the organization and the client, although the classification by itself does not protect data, it facilitates a lot the management of identity and the access as well as the other security controls centered on the data such as the coding ,in order to control in a selective way the sensitive information ,whatever the site of the data is.
Preventing data lost: this function applies data rules by combining the classification with the control, for example the blocking or the sending to the quarantine

when the data is being accessed, used, moved, or at rest.

IV. Conclusions

The opportunity of benefiting from mobile market is at reach, but the obstacles must be surmounted if the organizations are willing to present high chances of success.
Many solution options are available in order to help them in their path. Several factors also influence their decision, It is favor of adopting a unified solution, the technologies propose two axis to help choosing a mobile solution that makes the organization progress: the commitment to client and to the security centered on the data.

References

[1]Florian Maleki, Concerned about security issues related to BYOD and mobility 03 November 2014

[2] Nicolas Caproni ,Web application security Vol. 37 - July, 2013.

[3] Bertrand Lemaire ,Security and Application Management ,25 April 2000.

[4] Piotr Kijewski ,The reference data underlying the entire information system (Vol.234 N° 67 – October,2011

5: Chadi Hantouche ,mobile security and application management are IT priorities,07 December ,2001.

[6] Steeve BARBEAU ,Management of Operational security and application industry ,15 February 2014

[7] Scott Kennedy ,Hosted security management of mobile applications, (479 N° 150- October, 2011).

[8] Jerome Saiz , security risks of your web and mobile applications through a cloud-based solution, N ° 690 , 30 August 2003.

[9] Mikko Hypponen , The mobile operational safety management elements for the technology. mobility now at the heart of debates, 17 May 2015.

[10] David Bisson , Mobile oversight audit process for critical systems analysis for safety,27 January 2000.

[11] Francesca Bosco , organizational structures, responsibilities, and procedures necessary applications for mobile data security, N° 347 ,23 July 2007.