PRESS RELEASE

msg systems Provides Tips for the Secure Development of Mobile Apps

The IT consulting company has put together a checklist of key safety requirements.

Munich, April 16, 2013. Nowadays mobile software applications for smartphones and tablets play a key role in everyday business. To prevent smart applications from becoming a gateway for hackers and malware, software developers must address threatening scenarios very early on and must take the issue of application security into consideration even during requirement analysis. This is the conclusion that the Information Security Center of Competence (CoC) at the IT consulting and system integration company, msg systems, has come to. The CoC, which has extensive experience from numerous customer projects, is taking an in-depth look at the security of mobile applications. Based on their experience and based on OWASP, the IT experts have put together a checklist of 10 key security requirements for the development of mobile apps:

1. **Protecting Sensitive Data**
   Sensitive data should never end up in public areas such as address books or media libraries when used on mobile end devices. The data must be encoded to ensure it can only be accessed once a user has been successfully authenticated using a PIN or password.

2. **Storing Passwords Securely**
   To fulfill a variety of requirements, passwords can only be stored as hash values.

3. **Transferring Data Securely**
   When transferring sensitive data, the data must be encoded with secure

algorithms from end point to end point, such as SSL/TLS encoding, for example. It should not be possible to transfer confidential or personal data by text message or MMS.

4. **Correct User Authentication and Authorization**
   The guidelines for company passwords should include specific requirements for password length and complexity as well as modification frequency, and those requirements should be strictly observed. Identification should not be based on device features such as an IMEI, but on the identity of the specific user instead.

5. **Safeguarding the Back End**
   Data must be protected against unauthorized access both in the back end and when being transferred from client to back end.

6. **Securely Integrating Third Parties**
   To prevent the integration of third parties from becoming a security risk, only source codes and or libraries from reliable sources should be used. Either way, data from third party apps should always be reviewed in detail before further processing.

7. **Handling User Data**
   Guidelines on data security, especially the German Federal Data Protection Act, must be followed fastidiously when collecting, processing, or storing user and personal data.

8. **Secure Distribution of the App**
   In the interest of sustainable application safety, Apps should only be distributed by official app stores. Regular security patches are an absolute must.

9. **Using Secure Coding**
   Programming must observe the guidelines for secure coding and the principles of secure application development. Any platform-specific features such as jailbreak or rootkit detections must be considered.

10. Performing Safety Checks

Before being released, apps that process sensitive or personal data must undergo penetration tests by independent experts.

"These are just a few of the key aspects that must be considered when developing mobile apps," explains Florian Stahl, Lead Consultant in msg systems' Information Security Center of Competence. "Our extensive guide contains a comprehensive collection of all safety requirements that need to be taken into consideration."

msg systems

msg systems is an independent, internationally-active company group with more than 4,000 employees around the world. The company offers a holistic service spectrum of creative, strategic consulting and intelligent, sustainable and value-added IT solutions for the following industries: automotive, financial services, food, insurance, life science & healthcare, public sector, telecommunications & media, travel & logistics, as well as utilities and has acquired an excellent reputation as an industry specialist over the past 30 years.

Within the group independent companies cover the wide variety of industry and issue-based competence: msg systems ag forms the core of the company group and works in close cooperation with the subsidiaries, both on a business and organizational level. This allows the competence, experience and know-how of all the members to be bundled into a holistic solution portfolio with measurable added value for its customers.

msg systems holds 6th place in the ranking of IT consulting and system integration companies in Germany.

Please feel free to contact us for additional information:
msg systems ag, Susanne Koerber-Wilhelm, Robert-Bürkle-Str. 1, 85737 Ismaning/Munich
Tel. +49 89/ 961 01 1538, Fax +49 89/ 961 01 1113,
E-mail: susanne.koerber-wilhelm@msg-systems.com

rheinfaktor – Agentur für Kommunikation GmbH, Birgit Steinbock, Zollstockgürtel 57, 50969 Cologne
Tel. +49 221/ 880 46 150, Fax +49 221/ 880 46 200, E-mail: steinbock@rheinfaktor.de

Images and additional press releases can be found at www.msg-systems.com and at www.rheinfaktor.de in the press section under "msg systems".