PRESS RELEASE

Data security abroad - msg explains what travelers need to know

The data security risk in foreign countries is high, but can be significantly reduced by taking a few simple steps / Tips for employees

Munich, September 22, 2015. When traveling for business your data is exposed to numerous risks: Loss or manipulation of end devices, unsecured W-LAN connections or inattentive employees are just a few examples. However, taking the right precautions can help you control these risks.

Data security tends to take a back seat when in the midst of planning a trip abroad. Yet, there are so many risk scenarios that special security measures simply have to be taken. Not just when traveling to a high-risk country where data espionage is an everyday event either. Even brief lapses in attentiveness or simply using a device in the manner you are accustomed to "back home" can unintentionally expose data to risks. Thus, it is not only companies that need to take preventative measures, but employees themselves can also minimize risks considerably by being mindful of their actions.

What Employees Can Do

A company's best intentions are of no avail if employees do not follow certain rules of conduct. Taking the following measures to heart can help ensure that the next trip abroad does not end in disaster.

- **Concealed Entry of Passwords.** The same rule that applies to entering a pin at an ATM also applies for passwords: Their entry should always be concealed. Otherwise, other people or hidden cameras may be able to track or record their entry.
- **Never Lend End Devices or Leave them Unattended**. An end device containing sensitive data should never leave your possession - not even in alleged cases of emergency. Hotel rooms or hotel room safes should not be considered secure either. Doing so poses the risk of someone else accessing the device and manipulating it or tapping into its data.

- **Never Use Unencrypted or Unfamiliar WLANs**. Anyone who uses an inadequately secured WLAN when traveling runs the risk of having their data stolen. Larger chain hotels can be considered somewhat trustworthy, as their WLAN infrastructures tend to be operated by well-known, reliable providers - however, care should be taken in smaller hotels or in coffee houses and restaurants. When in doubt, the general rule of thumb is to assume that the unknown WLAN is transmitting its data unencrypted or is not adequately secured.
- **Caution when Using External USB Devices**. USB sticks or devices that can be connected to one's own end device may be compromised or may contain malware. This applies for both devices that are assumed safe, such as keyboards or chargers that are made available to travelers, as well as so-called USB gadgets such as ventilators, coffee cup warmers, etc.
- **Only Use Your Own End Devices**. A colleague's kind offer to let you use their end device to access important websites, content or services should be politely refused. A keylogger might be recording the login data or the device might be contaminated with malware.

"Time and again we see business people and managers taking a haphazard approach to data security when heading abroad, even if they access critical data on a regular basis or are heading to a country where data security is questionable," Mark-W. Schmidt, Head of msg Information Security, has come to realize. "Furthermore, the loss potential is often underestimated. To ensure business travelers take these tips to heart and avoid dangerous usage behavior when abroad, we recommend companies offer training courses to create awareness among their employees as to which risks they are exposed to and how best to avoid them."

msg
msg is an independent, international group of companies with more than 5,000 employees around the world. The group of companies 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 during its more than 30 years in business.

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 holds sixth place in the ranking of IT consulting and system integration companies in Germany.

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

Hotwire PR, Daniel Hardt, Franziska-Bilek-Weg 9, 80339 Munich

Tel. +49 89/ 210 932 81, E-Mail: Daniel.hardt@hotwirepr.com

Images and other press-related releases are available at www.msg-systems.com
Reprint free of charge. Sample copies on request.