SAND2011-4723C

Risks associated with Foreign Travel

Securing our Resources

6/16/2011 10:30am

Catherine Smith
CSUCAL Operations Lead

Nichole Kenton
Technologist

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Risks while on Foreign Travel

Corporations today are presented with many challenges that were not prevalent a few years ago. Quickly emerging technologies continually change cyber security challenges.

Recommendations from top security analyst include ways to address heightened risks associated with use of computing resources/network access while on foreign travel.

Risk Mitigation to be Addressed

- Managing mobile devices must address the issue of compromise of proprietary data on computing devices while on foreign travel

- Compromise of computing and/or network resources due to loss, confiscation, theft, unauthorized access and/or introduction of malware or malicious code by foreign entities

Cyber Recommendations

Cyber security analyst recommend use of encrypted mobile devices while on Foreign Travel - specifically having dedicated and managed assets for proper Risk Mitigation

- **Mobile devices used exclusively for international travel**
- **Mobile devices are controlled by a corporation's IT department (managed, secured, tracked)**
- **Laptops should be isolated from the corporations primary network**
- **Full Disk Encrypted Hard Drives**
- **Devices should be thoroughly inspected and possibly re-imaged/secured prior to next trip**

New technology, new challenges

- Mobile devices broadcast Wi-Fi, Bluetooth and GPS information, which pose unique challenges
  - Meta data is contained within pictures allowing GPS information to be tracked via social net working sites once they have been posted
  - Travelers should be aware of information being broadcast/transmitted in general, not limited to the "data" stored/placed on the mobile device
- It is recommended to turn off phones and remove batteries until they are needed

Upon return

- When returning from traveling abroad, it is important to consider all of the accompanying equipment to be “compromised” until it is examined
- Travelers should avoid connecting equipment to a work or home network, as it could have picked up malware that could propagate upon connection
- All equipment should be submitted for scanning, examination and/or replacement
- Once back at a secure and trusted facility, it is recommended to change all passwords and dispose of any removable media acquired or used during the course of travel

In Conclusion

- **Physical security measures alone are not sufficient. Due to ever changing technological advances, IT professionals must continually evaluate and improve their processes. Most importantly, travelers must maintain awareness that anything they transmit may be intercepted and it is ultimately up to them to think proactively before they send.**

Reference

- Note: Content in this presentation was obtained primarily from three sources:“Tips from the National Counterintelligence Executive: Traveling Overseas with Mobile Phones, Laptops, PDA's and Other Electronic Devices” “How to manage cybersecurity risks of international travel” and the State Department’s“International Travel Information, Country Reports.”
- http://gcn.com/Articles/2010/09/15/ISC2-risks-of-international-travel.aspx?sc_lang=en&Page=2