THE INTERAGENCY BOARD

Training Trigger: Operational Security and Mobile Devices

May 2017

OPERATIONAL ISSUE

Emergency responders routinely carry mobile devices, both personal and department-issued. The widespread use of these devices poses challenges to operational and cyber security. Some departments permit responders to use department-issued mobile devices for personal purposes. In such cases, users may unintentionally place their departmental information technology systems at risk if their devices are compromised. Responders must also be aware that adversaries may target both their personal and professional devices to gather locational data and other information to gain situational awareness on response operations. Organizations must be prepared to implement countermeasures to these threats to protect operational security and safety of response personnel and their families.

FAST FACTS

Many responders own mobile devices that they use for both personal and professional purposes. Some agencies issue mobile devices to their personnel while others employ a "bring your own device" (BYOD) approach. Both methods present operational and cyber security issues agencies must recognize and manage.

- Adversaries may use mobile devices as an entry point into an organization's information infrastructure in order to compromise it.
- Some responders upload personal applications and data to department-issued devices; this practice presents a cyber security risk. Apps can carry malicious code, affecting both individual users and the systems to which they connect.
- Adversaries can use the online and digital presence of responders and their family members to target them both physically and virtually.
- Smartphones enable the phone to determine its own location. Apps use locational data to provide services and some also transmit that data, providing a tracking capability. Some phones allow users to restrict the delivery of locational data to trusted apps with a need to know a responder's location.
- Responders may use one social media account (Facebook, Twitter, Instagram, etc.) to post both personal and professional information, a practice with implications for operational security (OPSEC) and appropriate content.
- Some locations may be associated with professional data or status, this is called psychographic data and can be used to identify and target responders.
- Adversaries can collect location data directly from mobile devices using items such as an International Mobile Subscriber Identity (IMSI) catcher – a portable fake cell phone tower – to catch users' mobile devices, detect their presence, and spy on communications. An IMSI catcher can find or monitor devices at a particular location. There is no reliable defense against all IMSI catchers but disabling 2G support and/or roaming can be effective.
- Smartphones have other radio transmitters aside from those that interface with the mobile network. These less powerful signals are usually only short range, but sophisticated antennas can detect then from unexpectedly long distances.
- Wireless signals include a unique serial number called a MAC address chosen by the manufacturer, which can be seen by anybody who can receive the signal. MAC addresses can be detected even if a device is not connected to a wireless network or even if it is not actively transmitting data, allowing adversaries to identify and track users. Countermeasures include turning off Wi-Fi and Bluetooth to prevent this tracking. Some devices also support address-changing apps, allowing users to change the MAC address daily.
- Signs that a mobile device may have been compromised include odd behavior, lighting when not in use, random beeping/noises, shutting down, battery rundown, strange text messages with random numbers, symbols or characters, and increased data usage.

ACTIVITIES

The IAB Training & Exercises (T&E) SubGroup recommends that organizations:

1. Establish policies related to the use of department-issued mobile devices for personal purposes and the use of personal devices for departmental purposes and during a tour of duty.
2. Ensure that responders use a passcode on mobile devices, use strong passwords and avoid using the same or variations of the same password for various systems.
3. Establish policies and conduct training related to the appropriate use of social media and safeguarding locational data including removing it from social media postings.
4. Advise responders to exercise caution with respect to their online presence and manage their identity by not using their full name and taking measures to protect their privacy.
5. Employ communications apps with end-to-end encryption to protect communications.

TEMPLATES/BEST PRACTICES

FCC Cyber Security Planning Guide

NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise

Ohio Dept of Public Safety Use of Social Media

Sample Social Media Policies

OTHER RESOURCES

White House Bring Your Own Device Resource Page

As the InterAgency Board identifies new information on this topic, it will be posted at www.interagencyboard.org. Please send any comments, feedback, and questions to info@interagencyboard.us