Advanced Corporate Solutions

"Debugging" Specialists | Service Excellence since 1995

EAVESDROPPING DEVICES COULD BE HIDDEN IN CLEAR SIGHT

Yearly, organisations and businesses end up losing millions of Rands to eavesdropping attacks.
These attacks are typically achieved via illegal means; by means of electronic surveillance, hacking, internal employee theft, and the black-market trading of stolen insider information.

Failure to combat these attacks through proactive steps in detecting weaknesses in their overall security programs, also contribute greatly to this growing phenomenon. Individuals on the other hand are even more susceptible to eavesdropping attacks as they don't have the resources necessary to stop or detect the threat until it's too late and the harm has already been done.

The key benefits of implementing a proactive Technical Surveillance Countermeasures (TSCM) program within your organisation include:

A. Safeguarding of Intellectual Property
B. Legal and Regulatory Compliance and Responsibility (e.g., Protection of Personal Information)
C. Optimised Information Security and Security Programs
D. Peace of Mind / Reassurance

1. Water bottle with video recording and storage capability
2. USB Rubber Ducky (malicious backdoor) and Keylogger devices
3. GSM eavesdropping device hidden in wall plugs and multi-plugs
4. Network cable with eavesdropping (audio) capability
5. Wood chip (found in pot plant decorations) with eavesdropping (audio) capability
6. Wristwatch with eavesdropping (audio and video) capability
7. Body worn eavesdropping devices
8. PIR with eavesdropping (audio and video) capability
9. Calculator with eavesdropping (audio) capability