Advanced Corporate Solutions

“Debugging” Specialists | Service Excellence since 1995

INFORMATION & CYBER SECURITY – TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) SCOPING ASSESSMENT

ACS / DYNAMDRE

dynamdre

INNOVATIVE SOLUTIONS

INTRODUCTION TO TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) SCOPING ASSESSMENT

There is a common misconception that South-African businesses are rarely a target for hackers because of our geographical location on the world threat map, as well as what we as South-African business owners would like to believe “lack of valuable data”. However, any information stored on our systems might be, and could have already been of interest to criminals. According to the Institute of Risk Management, “Cyber risk” means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

All types and sizes of organisations are at risk, not only the financial services firms, government organisations and high-profile names which make the headline news. Anyone and everyone could be affected by this plague of attacks. Advanced Corporate Solutions now offer and incorporate TSCM into our arsenal of Intellectual Property Protection Services. Our clients now have access to state-of-the-art technology and industry leading skills to give them a glimpse of what cyber risks their organisations might be facing.

This is achieved by incorporating a segmented vulnerability assessment (TSCM Scoping Assessment) into our Debugging assessments. TSCM Scoping Assessment will focus on specific segments of the business environment namely;

- Wireless Access
- Physical Network Access (Cabled LAN Environment)
- Voice / Telephony Systems
- CCTV Environment

The purpose of the TSCM Scoping Assessment is to do a focused vulnerability assessment on a small (yet important) segment of the network. This in turn will allow our clients to get a glimpse of vulnerabilities that these network segments might be exposed to, and based on the information at hand, allow them the opportunity to consider a full-fledged penetration test and vulnerability assessment across the entire network and business environment.

When we know that 50 new vulnerabilities are discovered every day, the area of exposure to cyber-attacks for companies has never been so important. It is also time to act because currently, a company corrects a vulnerability on approximately 200 days after its detection.