

Counterpane Professional Services Case Study: Penetration Testing

Description of Client: Large electronics manufacturing company

Description of Problem: The client contacted Counterpane to audit the security of their DMZ networks, perform social engineering attacks, and war dial their phone blocks to check for unauthorized modems. They were concerned that through organic growth they had lost control of their networks and needed a third party to verify their controls, or lack thereof.

Details of SOW:

Scope: Counterpane was contracted to perform:

- External network penetration test
- Social engineering attack
- War dialing assessment
- Verification testing – retest of identified vulnerabilities

The outcome of the assessment activities was a formal report that:

- Identified vulnerabilities and weaknesses of the external environment through data gathering, controls testing, and information analysis, and then ranked the vulnerabilities and weaknesses in order of business impact, ability to be exploited, and effort to resolve.
- Developed security recommendations and solutions that were both technically- and process-oriented.
- Presented a final list of findings and recommendations based on the assessment activities and the technical environments tested.
- Identified actions that will mitigate risk to an acceptable level

Service types: The general professional services types used in this engagement were from the following categories:

- Threat Assurance Services
- Due Diligence Services

Number of assigned personnel: Two

Timeline to Delivery: The customer worked with Counterpane to develop a timeline after the kickoff meeting. Milestones were agreed on and a timeline that fit the customer's change control scheduled was put in place. The engagement required three weeks of testing, two weeks of re-testing, and one week to prepare the final deliverable.

Findings: Counterpane discovered that the customer's networks were vulnerable to:

- Social engineering attacks
- Patch management vulnerabilities
- Configuration management vulnerabilities

Recommendations: Counterpane provided detailed remediation recommendations for all of the security exposures we discovered. Counterpane also took a look at the root cause of the application security flaws by asking the question, "How could have this been avoided to begin with?" Our root cause analysis explores the operational circumstances that lead to unsafe application deployment. In this customer's case it was a lack of enforced IT operational procedures and lack of a corporate security policy that lead to ad hoc deployment of IT resources in an unsafe manner.