



Client

Non-Departmental Public Body

Project Background

With high-profile data losses over recent years, public sector organisations are expending more effort than ever on securing networks and protecting data. Unfortunately, despite this attention to security the insider threat has not diminished and external attacks are still succeeding in breaching networks.

This client had a very proactive view to security, with a dedicated security team outsourcing traditional penetration testing and social engineering exercises on a quarterly basis. Security was paramount to the operation of the organisation, and whilst a good understanding had been gained of the vulnerabilities and risks associated with the infrastructure, the client had very little knowledge of the day-to-day activities of staff, attacks from outside, nor the operation of the network. This was primarily down to the outsourcing of all IT to a third-party provider, and ineffective incident detection at the network boundary.

IRM was originally approached by the client requesting a review of all traffic leaving their network – an egress traffic assessment. Whilst perfectly feasible, IRM suggested this would only illustrate part of the overall picture, and suggested a full NetFACTS assessment more appropriate given the risk involved.

IRM's Approach

NetFACTS is a combined network-based assurance and assessment service, designed to measure the collective efficacy of deployed security controls across IT systems, infrastructure or an entire estate. In this case, the client was specifically concerned about data leakage via email and file upload sites – essentially the insider threat. Whilst an IDS (Intrusion Detection System) or DLP (Data Leakage Prevention) solution may provide some insight into this specific risk, without skilled network analysts high false positive rates and missed incidents is an almost certainty. NetFACTS analysts counters this issue by only reporting confirmed incidents and targeted attacks, allowing the client to focus directly on the true impact without requiring specialist technical knowledge.

Additionally, traditional solutions would also require input from the third-party IT provider; far from ideal as it was perceived that the highest risk of insider threat actually may actually be within this subcontracting organisation. IRM's NetFACTS service is completely passive, the use of specialist network TAPs allowing installation without any network reconfiguration or input required from the third party.

As with all NetFACTS engagements, an in-depth scoping meeting was arranged with key personnel within the organisation to understand the exact data that was at risk to facilitate targeted detection. Key projects and codewords were identified, along with individuals and teams with access to sensitive information. Existing controls and network architecture was reviewed to select an appropriate probe location, and to identify potential weaknesses or 'blind spots' that may be an area of focus.

IRM recommended that the employees of the organisation would not be directly informed of the additional NetFACTS monitoring – existing SYOPS documentation clearly stated that monitoring was taking place. A more realistic snapshot of users' behaviours would be gained if only key senior staff were aware of the operation.

Custom IDS signatures were developed to accompany the heuristic techniques and manual review conducted by NetFACTS analysts. As standard for a first engagement, the probe was deployed for a one week period – allowing IRM and the client to understand the current state of the network and perform any potential remedial work before deploying a permanent NetFACTS solution.

FAST FACTS

Geography

- ▶ UK

Challenges

- ▶ Very little knowledge of the day-to-day activities of staff
- ▶ Very little knowledge about perimeter attacks
- ▶ No process to identify if policies were enforced

Solutions

- ▶ NetFACTS

Results

- ▶ Identified Infiltration and Exfiltration incidents
- ▶ Identified risk areas not considered previously
- ▶ Identified violations to corporate security policies
- ▶ Snapshot of the network showing points of security failure

Information Assurance
Risk Mitigation
Business Resilience
Compliance





What IRM delivered

IRM delivered a structured risk assessment report detailing evidence of real events and actual incidents; covering sophisticated attack detection – including infiltration and exfiltration incidents, corporate or third party security policy violations, and specific compliance non-conformities. This included forensically sound evidence in the form of PCAP traffic, suggested remedial actions, and in some cases, immediate incident response and forensic investigations on-site.

In terms of target audience, information was presented in an actionable intelligent form that enabled various stake holders ranging from business managers to specific teams that could make informed decisions. Whenever a serious issue was identified, IRM's incident response procedures would be initiated immediately, allowing the client to work with IRM's technical network forensic specialists to immediately respond to the threat without having to wait for a final draft of the report.

Benefits to the Client

Within minutes of the probe being deployed on-site - during the signature tuning process – a serious issue was identified as taking place in real-time; this particular event involved potentially illegal material being viewed on the Internet by an employee. Similar serious issues were identified throughout the capture, many of which were deemed very high risk.

The NetFACTS assessment highlighted many risks that the client had not considered, these included data leakage through network misconfiguration, lack of security education (company credit card details were found leaving the organisation via unsecured email) and concerning employee character traits; searches for knives, weapons and pornographic material are some examples.

Of most benefit to the client was the identification of a successful targeted attack, and also multiple malware installations within the organisation, actively exfiltrating sensitive corporate data to foreign countries.

What the Client did next

The seriousness of a large number of events prompted immediate incident response procedures, with IRM's forensic team and penetration testers being engaged to perform some remedial work as a result of the findings.

The success of the project immediately prompted the client to purchase IRM's NetFACTS probe for permanent deployment on-site, allowing non-technical security staff within the organisation to monitor all web and email traffic without any assistance from IRM. Due to the high risk nature of the network in question, and lack of an effective IDS, the client decided to also purchase a NetFACTS analysis subscription – in essence a managed network forensic and intrusion detection service – to mitigate the requirement for a large internal team of network specialists and ensure first class detection of incidents in near real time.

Information Assurance
Risk Mitigation
Business Resilience
Compliance

