



A blueprint for information fidelity

Knowledge is Power. However information, no matter what its accessibility or speed of delivery, is nothing without applied understanding of its value. In this article, Finmeccanica Cyber Solutions asks how organisations can evaluate information assurance measures, when the value of information assets and the risks to their integrity, are not fully appreciated.

Introduction

It is all too easy to mock the now infamous Rumsfeld quote of known knowns, known unknowns, and unknown unknowns but in the information age where cyber-threats evolve over hours not weeks, the sentiment the US Secretary of Defense was attempting to convey is actually more pertinent than ever.

Knowing what to look for when one is trying to detect a threat remains a thankless task unless a large pile of otherwise incomprehensible data can be analysed and understood. It is only then that the information becomes valuable intelligence on which one can act and react.

Information fidelity is a term used within Finmeccanica Cyber Solutions to describe the characteristics associated with accounting and auditing information in order to detect an IT Security Incident (referred to as *breach*).

These characteristics comprise:

- The nature of the information to be appropriate.
- Timely information, i.e. the generation and receipt of the information is appropriate.
- The veracity of the information to be sufficient on which to base decisions.

Detecting a security incident within an IT estate is not a black-art, nor does it necessarily require disproportionately expensive technology. However it does require a comprehension of the necessary process, cognisance of the infrastructures / technologies in-use and a sound appreciation of attack-methods. This approach can be classified by four laws of detection.

The first law of detection is: *if you do not generate events that indicate a breach – you will not detect it.*

It is vital that organisations understand this truism and consider accounting and auditing the information generated in order to give themselves the chance of detecting a breach. Reliance upon firewalls, anti-virus and “traditional” barriers to detect a breach can never result in the detection of the sophisticated, targeted attacks.

An analysis of accounting and audit generating components must be conducted in order to understand what information an organisation is already generating, and what information an organisation *can* generate. These are often two very different things and the most hardened and well-configured firewall is

unlikely to provide sufficient verbosity of information unless it is explicitly configured to do so. Common operating systems, applications and networking components will not, by default generate the necessary information to enable detection to occur. To detect a sophisticated attack there is a need to identify attack-vectors at an architectural-level, and ensure that there are appropriate devices and software to capture information that could provide the necessary information relating to a breach.

The second law of detection is: *a sophisticated and targeted attack is unlikely to be detected through the use of signatures.*

Specialist applications and devices such as Network Intruder Detection Systems (nIDS), Home-based Intruder Detection Systems (hIDS), and anti-virus software rely on subscription signatures. A level of heuristic-detection is normally prevalent in these technologies and some are better than others. However, these technologies must be tuned for the specific environment taking into consideration the presented attack-surface. Most of the products available for hIDS and nIDS will generate a high-level of false-positives. They are also available commercially, and it must be understood by organisations that even solo-attackers will test their exploit against the top ten Anti-Virus products.

The third law of detection is: *a combination of information generation technologies is required to detect an unknown attack.*

Network-analytics provides useful information, but relies on specific-indicators being present to identify that an attack has occurred. These are network behavioural indicators or anomalies; which can normally be defeated by an attacker being patient. A complex environment with a business-need to exchange and communicate with the outside world using a wide range of formats and protocols, leaves enough tolerance within the network profile for a slow egress of information. Host-based analytics also provide useful information and under the right configuration and management can identify (almost) any payload that has been delivered by an attacker.

But there are very few green-field organisations that can implement the most effective technologies without a major overhaul in system configuration and administration. Organisations must therefore use a combination of technologies appropriate for their business use of technology.

The fourth (and final) law of detection is: *detecting a security incident is pointless if you are unable to quantify the impact of the compromise.*

Although prevention of a breach is the best solution, it is also impractical and nigh-on impossible for any complex organisation with a requirement for technology. There is *always* an attack-vector, although it is true that sometimes

the cost of exploit is too high to warrant the resources required to take advantage of it. The insertion of new technology intended to improve the security-health of IT estate: could itself be used as a staging post for attack. Security devices are prone to vulnerabilities, like any other technology, and can be taken advantage of.

Therefore all organisations should accept that a breach is inevitable, and the information that allows an organisation to detect such, is not the same as that required to quantify it. This is often a lesson only learned by organisations after a breach has been detected. After identification of a breach, it is necessary that an organisation understands the ramifications and consequences of the incident. If the right information is not being generated this is not possible. By default, most components within an IT infrastructure will not generate the correct levels of verbosity.

Although there are various technologies that assist in the detection and quantification of security incidents, these technologies cannot achieve the business objective without analysis and appropriate configuration and customisation.

Making informed Decisions to Reduce Risk

For an organisation to determine an appropriate strategy best-practice requires the following approach:

- **Valuation of the assets** – this is rarely done correctly, even in organisations that have a long-association with formal Information Security (InfoSec). It is of paramount importance that information assets are valued correctly – this needs to be undertaken at a business and not technical level. What is the true impact of an organisations' information being able to be read, modified or deleted?
- **Determine the likelihood of attack and resources of the attacker(s)** – this is difficult for a lot of organisations to be able to quantify because they do not understand the value of their information, understand the risk to their estate or appreciate the nature or velocity of potential attacks. Most nations have a technical authority that can provide guidance on this subject. The fact is that most organisations have value in being breached; either because of the information they hold / generate; the knock-on consequence to other organisations; or simply to subvert an organisation to become a staging-post from which to attack other organisations.
- **Decide how much risk is acceptable** – In most cases, it is not necessary to mitigate every form of attack for every organisation, from every attack-source, but it is necessary for the business to make the decision as to what level of compromise is acceptable. This is not a strategic business decision NOT a technical one.

By following the above procedures an organisation can take an informed approach that will enable it to determine the level of security required to protect its estate and information assets. This increased awareness of an organisation's known knowns, known unknowns, and unknown unknowns and in turn drives the information-fidelity requirements of any organisation.