Insider Threats: **Why behaviour is the key to early detection** OVERVIEW

Huntsman®
Defence-Grade Security Platform

The recent cases of whistleblowers Bradley Manning and Edward Snowden highlighted the challenges many organisations face in protecting data from determined insiders.

A recent Ponemon study found that the organisations surveyed had seen an average of 55 employee-related incidents of fraud in the past 12 months.[1] At the same time, the UK's Fraud Prevention Service (CIFAS) reported a 43% increase in employee fraud, largely driven by a harsher economic climate.[2]

SPOTLIGHT ON TRUST

It is well-known that insider breaches are under-reported; many organisations do not report them for fear of damage to reputation or company value. Don Bailey in Dark READING cites 'a recent report by firewall management firm AlgoSec (that) showed that almost two thirds of information security and IT professionals rated insiders as their greatest security risk.'[3]

The most common kinds of insider threat are not headline material; they are low-key, opportunistic actions over long periods that largely go unnoticed. The crucial difference is that insiders already have access and they can compromise sensitive data even without intending to - through ignorance, negligence and just plain carelessness. It is a common belief that most deliberate insider data breaches are the work of technical staff. In the case of fraud though, a study conducted in the financial sector backed up the link between non-technical staff and fraud with a sobering figure: 'nearly 93% of fraud incidents were carried out by someone who did not hold a technical position within the organisation or have privileged access to organisational systems.'[4]

There is also an affiliate risk closer to home: the friends, relatives or clients who can use your employee's credentials to gain access. The culprits have access to your system and you have little knowledge or control of them.

ANOMALOUS BEHAVIOUR: ONE OF THE FBI'S KEY FIVE

To prevent and detect insider crimes, an organisation must control both the technical and behavioural sides of the issue.

> *'Almost two thirds of information security and IT professionals rated insiders as their greatest security risk'.*
>
> **The State of Network Security 2013, AlgoSec in Dark Reading, April 17, 2013**

The FBI seems to agree and has moved to a behavioural baselining methodology to detect anomalous insider activity. As Patrick Reidy, the FBI's CISO, reported in Dark READING: 'We look at how people operate on the system, how they look contextually, and try to build baselines and look for those anomalies.'[5] Patrick Reidy's recommendations were summarised by Forbes as follows:

1. **Focus on deterrence not detection** to create a culture that deters any aberrant behaviour, by ensuring that it stands out.
2. **Know your people.** Know who your weak links are and who are most likely to be a threat.
3. **Identify information that is most likely to be valuable** to someone else and protect it accordingly.
4. **Monitor ingress and egress** points for information.
5. **Baseline normal activity** and look for anomalies.[6]

Technical staff are most often the culprits when it comes to IT sabotage and IP theft.

In the case of fraud though, the culprits are more likely to be non-technical.

Carnegie Mellon Study, October 2012

EFFECTIVE CONTROLS

New technologies have enabled more business data to move from behind the corporate firewall, ending up on cloud computing platforms and smart mobile devices, which further increases its exposure to data leakage, theft or fraud.

The most useful controls are those that provide evidence to support their operation, which is generated continuously through normal use – such as real time log collection and intelligent analysis of event logs. Since their inception, Verizon's Data Breach Investigations Reports have backed up this proposition: between 70% and 90% of victims would have found evidence of data breaches in their log files, if only they had looked.[7]

WHAT ABOUT GENUINE WHISTLEBLOWERS?

One question remains: how do you handle a genuine commercial, moral or legal need for an individual to highlight malpractice in a function, level of management or whole organisation?

IT security monitoring systems should not make it more difficult for ethical whistle-blowers. Instead, these systems should enable proper escalation and investigation, by allowing transparent access to the data by specialist teams and prompt action by senior management.

The role of an advanced behavioural technology like BAD is clear: it enables early detection and investigation, verification of the risk to the enterprise and the taking of appropriate action, regardless of insider motive.

REFERENCES

1 THE RISK OF INSIDER FRAUD SECOND ANNUAL STUDY, Ponemon Institute, February 2013

2 CIFAS Staff Fraudscape report 2012

3 Insider Threats And BYOD Greatest Risks In State of Network Security 2013 Survey, dark READING, April 17, 2013

4 Study Probes Insider Threat in Financial Services Sector, Software Engineering Institute, Carnegie Melon, July 31, 2012

5 5 Lessons From The FBI Insider Threat Program, dark READING, March 1, 2013

6 FBI 5 Best Practices For Combatting The Insider Threat In Your Business, Forbes, August 7, 2013

7 2013 Data Breach Investigations Report, Verizon Business

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman