

An annual muse by Secerno

The State of Data Security 2007/8

Contents

- 2 The whistle will blow for signatures
- 2 Data consolidation behind the move to close the door *before* the horse has bolted
- 3 Better reporting for compliance
- 3 Shift to securing data at source



1. The whistle will blow for signatures

We have seen, throughout 2007 that we are in a time of an incredibly rapid expansion in the threats to networks that IT solutions seek to combat. The scale of malware variants has grown to the point where it now threatens to overwhelm attempts to protect against each rapidly-evolving specific exploit.

Put simply, defences based on signatures for each new attack cannot possibly hope to keep pace with the tide of new threats – the signature-based block list concept is creaking and must soon crumble. The cracks have started to show and will become all the more evident in 2008.

But what of the alternative approach – defining what is good and allowed (a.k.a. the whitelist)? Surely here we have the obvious resolution to the problem, if defining all that is bad is proving impractical.

Well, no. Firewalls in complex environments can run to tens of thousands of rules. The hope that any human can understand and manage the complete picture is becoming fanciful, leaving many configurations calcified – a mystery to those charged with maintaining them.

We may not have seen the end of the signature list, or the rules-based network security device, in 2007, but we will surely look back to this point and accept that in 2007 all the evidence was there that these simplistic approaches were in terminal decline.

We are still a way off the point where companies will dispense with their AV protection or switch off their firewalls, but it is clear that a change is needed, and that a radical change is coming, to the way that security is approached in the twenty-first century.

1.1 Prediction for 2008:

The chaos will drive security attention up the stack from the network towards the applications, and specifically to data sources – the real point of value in the infrastructure. We will see the emergence of more intelligent behavioural analysis solutions, to understand the context of requested data transfer as data flows into and out of organisations.

2. Data consolidation behind the move to close the door *before* the horse has bolted

The year has been 'topped and tailed' by two colossal security breaches. TJX lost 46 million credit card records to hackers. Quite to what extent this will eventually damage TJX has yet to become clear, but the breach has certainly affected the political landscape in the industry. Consumers and credit card companies alike will no longer tolerate the routine loss of data, especially now breach notification is required in many States in the US. TJX is far from out of the woods on this one, and their discomfort will certainly have caused hurried security assessments and even new investments in retail organisations across the world.

Here at the other end of the year, Her Majesty's Revenue and Customs, at the time of writing, still has yet to find the two CDs they sent by post, even though they contained sensitive data on every family in the realm. The direct effect will be less measurable commercially, but the political effect threatens to be profound. If UK government departments can be seen to flaunt so readily data protection rules, then what is to become of the public sector's drive to establish fewer, larger consolidated data systems?

Data consolidation was one of the most powerful trends in 2007. The business drivers make perfect sense, but the security implications, especially in the public sector, seem ill thought-through in so many cases. Each project brings together vast amounts of sensitive data to a single source, which is scary enough from a security standpoint. But it also inevitably creates systems with orders of magnitude of more authorised users. It is all very well monitoring staff behaviour in a local office – but when users are spread across the country, how can this best be achieved?

Simple authentication cannot suffice – with so many users, statistically a few of them are very likely to be abusing their access rights. Is monitoring and auditing their behaviour of any use beyond understanding exactly how they abused the data – when the damage has likely already been done? It won't stop them.

2.1 Prediction for 2008:

Monitoring and Auditing will start to become accepted as just the simple first steps towards achieving true control of data access through the adoption of more intelligent blocking approaches to protect enterprise scale environments. Prevention will start to become accepted as less risky than huge data losses.

3. Better reporting for compliance

Which brings us to compliance. The legal responses to escalating threats to consumers' data have driven security spending around the world in 2007. Companies are required to comply and so have to invest in technologies to satisfy auditors. The best organisations embrace the spirit of the legislation and seek to improve their operations in the process; the rest merely seeking to tick the boxes at minimum cost. Once the required technologies are in place, then all that remains revolves around reporting processes, few of which represent a great intellectual or technical challenge. In such circumstances, IT purchasers will avoid point solutions, preferring approaches integrated into their existing platforms.

3.1 Prediction for 2008:

Reporting capabilities will become strengthened in the platforms. This will force the point solution providers to deliver added value beyond audit and reporting if they are to thrive. Those without the required IP will begin to fade away.

4. Shift to securing data at source

The slow adoption of new forms of enterprise computing, such as Web Services, has been disappointing for some in 2008, but change is still happening. These new complex environments may offer huge benefits in business flexibility, but again increased flexibility brings security risk. As these new business systems take shape, the data sources become accepted as the key IT asset, on which all else is built. The focus in IT security continues to move away from the relative chaos of the network to the more precise, uncluttered world of the applications and their associated data.

4.1 Prediction for 2008:

Security will increasingly become an issue of tracking and securing data in its many forms, rather than seeking the footprints of intruders on the network. Approaches which follow the data across the enterprise, and model the behaviour of those using it, will start to make headway, as traditional approaches buckle under the strain of new threats and increasing numbers of authorised users.

