Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

# IT Security from Down Under

By Paul Kenyon

While many readers will be familiar with the Department of Homeland Security in the U.S., there are similar security initiatives being planned, or already under way, elsewhere in the world. In Australia, for example, under the guidance of Prime Minister Julia Gillard and her federal team, the government is carving out something of a name for itself in the IT security arena. This development is somewhat surprising considering Australia's relative youth and the fact that the country has around 22 million citizens — big enough to make its weight felt in international terms, but small enough to be flexible in the modern world of IT matters.

A key example of this is the Defence Signals Directorate (DSD), Australia's equivalent of the Department of Homeland Security, which has analyzed some of the attack methods used by cybercriminals and come up with four main techniques for blocking them. The government, moving swiftly in response, has started rolling out these techniques across its IT infrastructure, reportedly to great effect.



The third and fourth techniques center on the idea of whitelisting — that is, forcing Australian public-sector computer users to install only approved, or whitelisted, applications, and only allowing similarly approved and risk-analyzed emails to be viewed. This means that on their office computers Australian government employees can only access their corporate email and browse a limited number of websites, which, in turn, means they have far less of a chance of infecting their PCs than "civilian" Internet users.

In addition to its controlled-software-and-Internet-usage approach to IT, the Australian government has been highly proactive in quickly patching high-risk security vulnerabilities in both the operating systems and software that its many computers run.

Based on an analysis of its Internet usage during 2010, in fact, the DSD concluded that at least 85 percent of the targeted cyber-intrusions it responded to during the year could have been prevented by using the four main mitigation techniques. All four are highlighted in a 35-point report, "Strategies to Mitigate Targeted Cyber Intrusions," which found that although resistance to the idea of patching operating systems and software was low, the costs involved on the financial and staff-training side of things were still quite high.

That's not to say that Australian public-sector staff response to the report's recommendations, which included control over both portable and data devices, was entirely positive. The report's authors found a high degree of staff resistance to the idea that their access to USB sticks and other forms of low-cost data storage was to be restricted.

Nevertheless, there are signs that public-sector employees are realizing that these data-security requirements are a normal part of doing business and will therefore be the normal IT methodology from now on.

If we contrast this methodology with that of the U.S., we can see that budget issues have started to encroach on the need to reduce the security-risk profile, as has been the norm in Australia for several years, even after the economic downturn hit the world's economies.

In fact, if we look closely at the Signals Intelligence (SIGINT) aspect of U.S. national security we can see that the shift in U.S. intelligence collection priorities since the September 11, 2001, terrorist attacks on New York and Washington has continued, largely thanks to a security commitment made by the U.S. government in the aftermath of the tragedy.

But what's interesting about the U.S. approach to national infrastructure and that seen in Australia is that Australia's public-sector workers have effectively been told which operating system and software they will be using in the workplace — i.e., what IT governance/security staff can plan and accommodate accordingly — while their U.S. counterparts are still allowed to select which software suits them best.

IT purists might argue that this makes for a more efficient IT user base in the U.S. government and its agencies when compared to their Australian colleagues, but there are real reasons behind the Australian mandate on what operating systems and software employees can and cannot use.

A clear example of this is the use of SCADA (Supervisory Control and Data Acquisition) computer control systems, seen at the heart of many industrial automation and control systems. Developed in the 1960s, SCADA-driven systems really came into their own with the arrival of the first PCs in the '80s, and are typically found in industrial systems such as power plants, chemical plants, electricity supply grids, and many others that require a high degree of computerized control as well as 100 percent systems availability.

This is Mission Critical: capital M, capital C. Many businesses claim their IT processes are mission critical, but SCADA control systems are often critical to national infrastructures. For example, if a country's electrical grid goes down it can cost industry many tens of millions of pounds per hour, and in the case of hospitals, air-traffic-control systems and the like, can actually place people's lives in jeopardy.

Despite the fact that a growing number of PC users in the private and public sector are migrating, or have migrated, to the Windows 7 platform, most SCADA-based systems use a robust and ruggedized version of Windows 98, a 16-bit version of Windows dating back to the late '90s.

The reason for this apparent Luddite approach is quite simple: by using a stable and unchanged operating system that's been fully updated and completed its life cycle, SCADA-based systems can have their operating system loaded into firmware. This means that although there is no equivalent of Microsoft's "Patch Tuesday" update program for Windows 98, cybercriminals can't easily subvert the code of SCADA-based systems since the firmware-based operating system is fixed and can't be updated.

**Australia's Defence Signals Directorate blocks 85 percent of cyber attacks with four effective methods.**

This fully embedded firmware approach is fairly unique to SCADA-based operating systems but helps one to understand why a highly controlled operating system and software environment, as mandated under the Australian DSD's diktat, has a far lower risk of subversion than the open-market approach seen in the U.S. and certain parts of Europe.

While we understand the need to maintain choice in an open-market environment, this doesn't mean that the Australian ideas enshrined in the DSD report can't be applied elsewhere in the free world.

This is because the principle on which our security offerings are built is Windows privilege management — namely, the control over who has access to specific applications running on the corporate IT platform as well as the underlying data. This means, for example, that if the admin team only runs its control and security software from within the network perimeter on known PCs, then access to those applications can be locked down to specific on-network computers.

Then, even if a set of admin account credentials is compromised by hackers, they can't use those credentials from the Internet — they would still have to gain physical access to the terminals used by the admin staff. There is a similar belt-and-braces approach being adopted by a growing number of banks for online account access: not only must users present the right credentials, they must also authenticate themselves using the appropriate hardware token.

Meanwhile, back in the land of securing Windows-based computers, it's interesting to note that in a second report from Australia, "Implementing the DSD's Top Four for Windows Environments" the conclusion is quite unequivocal:

"Minimizing administrative privileges is an exercise in the principle of least privilege. In a properly designed, administered and maintained environment there is no requirement for any user to have administrative privileges on their day-to-day account. In addition there should be no account which has both administrative

privileges and access to networks outside of the organization, such as Internet or email services."

The report adds, "When properly planned and executed, minimizing administrative privileges can have significant flow on benefits to the stability and consistency of the computing environment, simplifying administration and support of that environment."

Does this sound vaguely familiar? It should — it's effectively a summary of the reasoning and principles surrounding the use of SCADA-based computer systems that run our critical infrastructures.

And while I'm clearly not advocating the use of the inflexible embedded-operating-system approach seen on SCADA-based platforms, I think there is considerable scope for the Australian DSD's report recommendations to be deployed in corporate IT departments in the U.S. and Europe. As well as reducing the risk profile of company IT systems, they would also greatly assist in the number of support calls needed in a typical major corporation, which is something that will make the bean counters happy.

And that's not a bad thing when you think about it.

**No account should have both administrative access and access to networks outside of the organization, including the Internet and email.**