All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Separation of Duties and RFPs

Separation of duties is fundamental. Just as you separate purchasing from payments in a financial system to limit circumvention of financial controls by individuals, you separate performance from specification and review in information protection to prevent circumvention of information controls by individuals.

The procurement process is supposed to meet organizational standards for procurement. In particular, the same rules that apply internally should apply externally. For example, if separation of duties is required for specifying, operating, and reviewing a firewall, a perimeter control device, an access control system, or anything else, the separation of duties should extent to the vendor in a procurement as applies to anyone else.

The problem

I've been looking at lots of RFPs lately, and there is a disturbing trend. Lots of RFPs ask vendors to perform a protection analysis (review), identify what to do (specification), and then do it (performance). There are any number of problems with this from a standpoint of responding to an RFP, given that you don't know what the review will yield and therefore cannot reasonably predict what mitigation will be appropriate to perform or what the specification will involve. But lots of folks has figured out how to bid such things. The bigger problem is that such RFPs fail to recognize and address the need for separation of duties.

The people who write RFPs, or perhaps adapt existing ones for their use, typically don't understand the details of separation of duties. But procurement officials have the job of identifying what can and cannot be put together and what represents a conflict of interest, and stopping such things from going through. But usually, they don't understand enough about what is being procured in the information protection space to properly make the distinction.

Fixing the hole

This is not a hard hole to fix. A bit of awareness by procurement officers and those who write the RFPs would go along way to addressing it. But there is also often a lack of adequate specified policy within enterprises in this area of information protection. Management has failed to understand and recognize the need for separation of duties of this sort, there is no widely applied standard of practice for information protection like the generally accepted accounting principles, but the Generally Accepted System Security Principles (GASSP) in its 1994 draft states “Responsibilities and privileges should be allocated in such a way that prevents an individual or a small group of collaborating individuals from inappropriately controlling multiple key aspects of a process and causing unacceptable harm or loss.”[1] All we really need to do is follow it to solve this problem.

Summary

The principle has been around for a long time and is widely ignored. It's not hard, long, or complex, but it does require thoughtful application. Maybe that's why it is so underused.

1 http://files.all.net/books/gassp/index.html (the 1994 draft) see Principles → P-14 Separation of Duty Principle

And more...

The GASSP started out in a draft form in 1994 identifying these 17 pervasive principles:

P-1 Accountability Principle *

P-2 Awareness Principle *

P-3 Ethics Principle *

P-4 Multidisciplinary Principle *

P-5 Proportionality Principle *

P-6 Integration Principle *

P-7 Timeliness Principle *

P-8 Reassessment Principle *

P-9 Democracy Principle

P-10 Certification and Accreditation Principle

P-11 Internal Control Principle

P-12 Adversary Principle

P-13 Least Privilege Principle

P-14 Separation of Duty Principle

P-15 Continuity Principle

P-16 Simplicity Principle

P-17 Policy Centered Security Principle +

By now, this has been so watered down and changed that some of the key things that made it work are no longer included. As of 2004 in GAISP V3.0, the pervasive principles are down the ones marked with "*", adding "Equity". Policy sort of showed up under broad functional principles (+). So as of today, things like least privilege, separation of duties, and simplicity are largely gone from the hearts and minds, and the adversary and democracy principles are rarely discussed.

We need these principles, and they were there for good reasons. Many of the challenges we face today in information protection stem from failure to apply them.

Example: Separation of duties and least privilege could have stopped WikiLeaks.

Example: Simplicity ignored is much of why we have so many vulnerabilities today.

Example: Adversary ignored is why we don't match defenses to attacks very well.

Example: Democracy ignored is much of why we have so many privacy issues.

The past isn't perfect, but failing to learn the lessons it brings leads to many of the problems we face today. If we don't want to keep facing these problems in the future, we should start to embrace the principles we already know and ignore before seeking more newer ones.

