

Timing is Everything

May 2008



Cyber threats are like rust – they never sleep. Somewhere, whether here at home or in some far-flung corner of the world, people ranging from thrill seeking hackers to state sponsored terrorists are cooking up new, more powerful more insidious attacks. Some – far too many – of these will be successful. A typical reaction to such frightening news is..... a yawn.

Ok then, let's look at some statistics. According to a 2007 report by Gen. James (Hoss) Cartwright, vice chairman of the Joint Chiefs of Staff, there were 37,000 reported breaches of government and private systems in FY 2007 (ending September '07). That averages to approximately 101 successful attacks a day or around four every hour. There were nearly 13,000 direct assaults on federal agencies, and 80,000 attempted computer network attacks on Defense Department (DoD) systems. That averages to approximately 219 attempted assaults on DoD every day or around nine every hour. According to that report, some of those assaults "reduced the U.S., military operational capabilities."

In a top ten list of cyber threats published by the SANS Institute, an industry leader in cyber security, the first two items were "Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites" and "Increasing Sophistication And Effectiveness In Botnets."

One of the most effective security tools against these attacks is the successful and timely implementation of IAVAs (Information Assurance Vulnerability Alerts). If you're reading this, you most likely know all about these. The question is: are you implementing them in time? The fact that a cyber attack requires only nanoseconds to take hold, means that every minute an IAVA goes unimplemented a potentially critical network is at risk.

It is a fact that many of the personnel who are responsible for implementing IAVAs are overworked, perhaps not fully trained, and often lacking the needed resources to meet critical security responsibilities. It is also a fact that a single IAVA whose implementation is postponed or ignored could result in a successful attack. That successful attack could have far-reaching consequences.

The point is that the timely implementation of IAVAs is as much of a necessity as looking your door at night or not losing your CAC. It is not a foolproof defense, but it goes a long way to ensuring that the critical data in your system and the system itself is safer and more secure.

That is why the yawn reaction hopefully is not a sign of boredom or indifference. It may be the confident reaction of someone who spends many hours making sure that all IAVAs are implemented as they come in. If you have that responsibility, you may be thousands of miles from any firefight. However, you are on the front line of cyber defense and your enemy never sleeps.