

Patching Things Up at Home

November 2010



There is hardly a piece of software in use today that does not have some level of interactivity that allows communications with the Internet and other software packages. While this feature allows for significantly expanded capability and productivity, it also carries the potential for software and systems to be compromised by malware and cyber attacks. Like your house, there are many ways to get in to the inner workings of software -- front doors, back doors, basement windows. Even when you have taken every precaution in securing you house and software from the obvious intruders, there are still successful infiltrations all the time. If not how do you explain the crickets, ants and occasional fly. When they get in, the results range from annoying chirping (adware) to infestations of your food storage (data loss and compromise). There are ways into everything and the bad guys – and bugs – make a real effort to find and exploit every vulnerability in your defenses.

Defending against these vulnerabilities is a group of cyber security and programming experts who try to discover these vulnerabilities before the bad guys and develop fixes or patches to close or protect the point of access. Under the Army's Computer Network Defense System Provider (CNDSP) Program these experts, often working with the software developers, create Information Assurance Vulnerability Alerts (IAVAs) and provides the patches that will eliminate or lessen the potential threats. While many of the patches are installed on Army networks automatically, some require the hands-on attention of system administrators and managers. This work is often time consuming and detailed oriented and because of this it is not always performed in a timely manner.

There are a number of technological solutions to this. Some are currently implemented and some are still in the works. Until that time, everyone who has any level of network or data responsibility must ensure that these IAVA's are implemented correctly and on time. How to go about this is well documented and should be every Information Assurance (IA) soldier's bed time reading (insert cure for insomnia joke here). The point is we are not where we need to be with the implementation of IAVAs and need to step it up because the consequences of military network intrusions are for more serious than a few chirping crickets.

If your Army network is airtight and well monitored, congratulations! Spread the word on how you got it done. There are those out there that could use the guidance. Before the smug smiles and back-patting get out of hand, ask yourself what is the status of another critical, and likely more vulnerable, network at risk. That network is made up of your home computers – the ones used by your spouses, kids and loved ones. Are your patches up to date there? If not your personally identifying information (PII) and personal financial resources could be at risk. Not to mention the personal safety of your family members. Most of the major software providers include automatic update functions. Microsoft for example is famous for its Patch Tuesday when it releases it version of IAVAs and other functionality fixes. But these functions can be turned off or ignored. The vulnerabilities that challenge military systems go after home networks as well. Anything that connects to the internet can be at risk, including game systems and mobile devices. Use your Army knowledge to protect the cyber home front as well. It might take a little work and you'll need to pass along some of your training to your family and friends. Given the consequences, it is worth the effort. That way you can ensure that any breach of your home defenses is just a cricket and not a trojan horse.