

Tuesday, May 13. 2008

## Intrusion Tolerance replacing intrusion detection?

Is "Intrusion Tolerance" replacing "Intrusion Detection and Prevention"? I doubt it.

Reading an [article on DarkReading](#) today about a new project started by "Aron Sood" that he's dubbed "Intrusion Tolerance". Basically the approach is simple, his idea was to take a "clean" copy of a web, dns or other server and rotate it into 1st position on the DMZ on a regular interval roughly 1 minute. He commented that this would lower the window of opportunity for a system to become breached and limit the data loss exposure.

In my humble opinion, Intrusion Detection and Prevention is not going away any time soon and here's why:

1. Web Servers don't normally store sensitive data these days (Application Databases do).
2. This does nothing to prevent zero day application exploit via the exposed web server.
3. To infect a system only takes moments and therefore any exposure for even more than 1 second can lead to a breach. Case in point - Place an unpatched Windows XP system on the internet for about 10 minutes and whammo, you'll have several worms infecting your machine in that timeframe.

Summary:

Although this technology helps aid us security folks in our endeavour, its by no means a panacea. Honestly, this is only one small component that can be added to your overall security strategy and call it a day. Don't drop your Firewall, Intrusion Detection and Prevention and other compliance technologies on account of someone saying they will "limit" your data loss. I'll be keeping an eye on this technology as it has some promise if combined with the right complementary technologies. We'll see.

Read the Article [here](#)

Read about SCIT - Self Cleansing Intrusion Tolerance [here](#)

Posted by Lawrence Pingree in Security at 12:13