This article is the second in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). The first article looked at fundamental concepts and terminology; this one reviews basic advice on deployment of IDS and some aspects of data analysis.

* * *

IDS sensors can be located anywhere that is interesting to attackers and to defenders. Thus one can install IDS outside the main perimeter firewall, in the demilitarized zone (DMZ) between the outer firewall and internal firewalls (the typical location of Web servers), behind internal firewalls, and inside critical subnets in a complex topology that segregates sections of the intranet from each other for security reasons.

The most important rule when installing an IDS is that you must _not_ rush the installation. You should let the system accumulate knowledge of normal usage patterns so that you can keep false alarms to a minimum. Now, defining normal behavior is not as easy as it sounds – a problem that I’m sure parents of teenagers have discovered for themselves. IDS use statistical or artificial intelligence techniques (these are not equivalent, by the way) to spot deviations from the norm; therefore, definition of the norm – what is expected, repeatable, authorized, unexceptional, and unexceptionable – becomes a critical phase in the deployment of these tools. Put another way, it is important _not_ to allow the baseline to include unexpected, rare, unauthorized, exceptional and exceptionable events into the standard data set.

Ah, but here comes a very serious problem indeed: just how are we to prevent such inclusion of nasty data if there is already criminal activity going on inside the network or if there are attacks in progress while the data are being collected? How would one know that these data were being included in the baseline? This is not a trivial problem: we’re talking about a fundamental difficulty here. If we have no particular expertise in detecting attacks and that’s why we are installing an IDS, then how do we tell if the baseline data are contaminated by attacks and internal shenanigans?

I think that one approach to resolving what could become an impasse – a double bind – is to hire outside experts if necessary. Use the services of a managed-security company to establish that the baseline data are in fact acceptable and safe so that the IDS is initialized with clean data. These experts will work with you to verify that you aren’t setting yourselves up with the equivalent of unnoticed back doors through the IDS.

Whether you have external experts involved or handle the initialization (training) phase yourselves, expert this part of the deployment to take weeks or even months to work out the bugs. You’ll not only have to let the system accumulate baseline data as explained above, but
also to refine the alarm settings to minimize both false alarms and false negatives (that is, missing real anomalies or attacks). It is appropriate during this wearing-in phase to suspend alarms so that your staff are not constantly kept on edge by erratic reports from the new system. A continuous series of false alarms could not only be disruptive to productivity but could also densitize your crew so that they simply ignore real alarms later. Finally, this period of adjustment can serve for development and refinement of the computer-emergency response team, of which more in a later column.

* * *

In the next short contribution on this subject, I’ll look at some of the factors contributing to effective responses once your IDS notifies you of real attacks or security violations.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.