Have you been paying enough attention to your mainframe lately? According to an article by Benjamin Pimentel from April 2004 (<http://tinyurl.com/2vmfb>), IBM mainframes are still serving many organizations 40 years after the first ones were introduced. Indeed, Big Blue is still selling the big machines: “IBM sold $4.2 billion worth of mainframes in 2003, up 6 percent from the previous year, according to International Data Corp.” Even more startling, “Doug Balog, an IBM vice president, noted that 70 percent of the world's data are still housed in mainframe computers. And Josselyn said they are bound to stay there for a long time.”

My old friend Jerry Harding, Managing Director of Type80 Security Software, Inc. (<http://www.type80.com>) (the name is derived from the IBM log file record for security events) was chatting with me recently about some of the work his company has been doing with mainframes and I think readers will be interested in his perspective as a mainframe-security vendor.

Jerry says that mainframe computers are generally good, secure systems but they are being overlooked as security managers implement centralized security-monitoring systems. You can’t ignore mainframes when planning for enterprise-wide security. He finds that some security products have surfaced in the market in which mainframe operating-system logs, including console logs, are piped into the security incident monitor (SIM) repository using batch-mode FTP. The problems with this approach are that
* The data transfer is not in real time;
* The logs are sent without much configurability to filter out useless records such as tape-mount messages and other innocuous events;
* The excess data contribute to data overload and excessive false-positives on the analysis side.

Type80 based its product (<http://tinyurl.com/af8wq>) on a network-centric approach instead of sticking to the traditional mainframe model. The goal was to interoperate with other security products and to share alert data with existing security-monitoring software so that network and security administrators could see an integrated picture of the whole network that included the mainframes. They made the mainframe look like a UNIX box sitting on a network delivering security-event data via standard TCP/IP connections. These data and connection protocols are understood by all the SIM vendors in the market. Once the data are available and analyzed, they can be used for forensic analyses such as tracking intruders through a network. Did the intruder attack the mainframe? Was (s)he successful in penetrating the mainframe defenses?

Making mainframes part of the overall security architecture is particularly important for organizations working through the audit process to satisfy due-diligence requirements that demonstrate compliance with demands from laws such as Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability (HIPAA) and Sarbanes-Oxley (SOX).
If you’d like to learn more about Jerry’s background and his perspectives on mainframes, you can read one of my articles from 2004 in the ACM _Ubiquity_ online magazine <http://tinyurl.com/7c4zz>.


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management 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 © 2006 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.