

the DIGITAL INVESTIGATOR

JANUARY/FEBRUARY 2011

The 'Broken Window' Theory of Network Security



Identify, investigate and respond to minor security infractions in order to uncover and even prevent major security breaches.

They say that small crimes lead to big crimes, and the same appears to be true of insider security breaches. According to the 2010 Data Breach Investigations Report, a study conducted by the Verizon RISK Team in cooperation with the U.S. Secret Service, insiders were involved in 48 percent of security breaches and exclusively responsible for 27 percent. The researchers concluded that 90 percent of

internal security breaches involved deliberate and malicious activity.

That said, the study acknowledges that inappropriate behavior such as security policy violations and other activities that are not overtly malicious can contribute to security breaches. More significantly, researchers found that many of the employ-

Continued on page 2

The 'Broken Window' Theory of Network Security

ees who committed serious insider cybercrimes had been guilty of “minor” infractions in the past.

The researchers also found that inappropriate behavior provides a reasonable probability that the employee will commit a serious security breach in the future. As a result, the study recommends that organizations police security policy violations in order to prevent more serious abuse.

“Pursuing apparently minor infractions has the effect of deterring more major problems later. Also, by pursuing minor infractions, you may uncover evidence of major infractions committed by the same user,” said Kurt Aubuchon, Forensic Investigator, Ispirian Computer Forensics. “If a user has pornography or other illegal content on his computer, or has engaged in illegal file sharing, he clearly does not respect the organization’s security policies. Organizations should promptly respond to such security violations or, better yet, actively look for such indicators to prevent a future breach. It’s like the ‘broken window’ theory in law enforcement. If you clean up the petty crime in a neighborhood you’re also likely to prevent major crimes.”

Forget the Needle – Find the Haystack

Finding security violations does not take in-depth investigative skills. According to the report, 86 percent of victims had clear evidence of the security breach in their network or server log files. Yet many organizations struggle to detect and respond to security breach incidents. In fact, most security breaches are uncovered by third parties long after the breach occurs.

“Organizations often have the audit logs necessary to identify inappropriate use but resource constraints make it difficult to conduct proactive monitoring. According to the report, log files were available in 90 percent of incidents, but only 5 percent of incidents were actually discovered through log analysis,” Aubuchon said. “These statistics reinforce something that we’ve known in security for a while. You should be paying attention to your logs because if someone is doing something bad, you’re probably capturing a record of it someplace.”

The problem is that IT teams are so busy handling day-to-day activities that no one takes the time to look at log files proactively. Organizations also complain that the logs contain so much information that it’s virtually impossible to sort through it all.

“That’s true, but when you’re looking at logs you’re usually not looking for minutiae. You’re looking for a big noisy thing, and you can parse through your logs in such a way that finding it is not that much of a chore,” Aubuchon said. “You’re looking for abuse of system access privileges, use of unapproved hardware, and other indications that an employee is siphoning off sensitive data. Odds are you will find that

the employee is stealing data little by little over a long period of time. And odds are the employee has engaged in other security violations.”

When to Call for Help

While finding insider threats is within the skills of any network administrator with the patience to pore over log files, investigating security incidents should generally be left to professionals. An experienced digital forensic investigator can better determine the scope of an employee’s malicious activities and preserve the evidence needed for dismissal or further legal action as appropriate.

“If evidence of inappropriate activity turns up in log files, a more detailed investigation may bear fruit. Organizations should thus engage qualified investigators to conduct the more detailed investigation — particularly smaller organizations that do not have those skills in-house,” Aubuchon said. “At Ispirian Computer Forensics, we have the tools and experience to chase down those minor infractions and make sure they are not an indication of a bigger problem. And if we do find serious wrongdoing we will conduct a thorough investigation and arm you with the tools you need to take action. This is particularly important if the case goes to trial.”

While we tend to hear about sophisticated attacks compromising millions of records, the fact is that a significant number of security breaches involve smaller amounts of data and relatively simple techniques. The study found that 85 percent of the attacks were not that sophisticated, and insiders in particular tend to move slowly so that their activities aren’t detected. Insiders are also prone to start with relatively minor infractions and “move up” to more malicious activities.

“The insiders involved in embezzlement, fraud and other serious crimes typically have done smaller things in the past,” Aubuchon said. “So don’t just shrug off petty security breaches. Keep an eye on your log files, and call a qualified digital forensic investigator to help investigate any suspicious activities.”

The Digital Investigator

Copyright © 2011 CMS Special Interest Publications.

All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave., Tulsa, OK 74145

Phone (800) 726-7667

Fax (918) 270-7134

Change of Address:

Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

The Digital Investigator is published by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.