Microsoft Exchange 2003 Mailbox Auditing CorreLog Use Case

The CorreLog Server contains specific features and functions to support auditing of Microsoft Exchange, with special emphasis on tracking access to mailboxes by administrative users.

One of the security issues with regard to Exchange is that individuals with administrative logins can read the Inbox and other private folders of individuals. This poses a security risk of malicious snooping by Administrators of top executives and managers within an organization.

In particular, Microsoft Exchange 2003 poses a particular difficulty because no explicit auditing exists to distinguish whether an administrator is reading Calendar information of an individual (which may be a normal part of operations), or whether a malicious administrator is snooping the private Inbox and other folders of an individual (which would constitute an obvious abuse of administrative power.)

To correct for this deficiency, CorreLog Server can create a "pattern of usage" for administrators, and alert security officers if administrator accesses a mailbox outside of expected usage patterns, as described herein.

CorreLog Use Case Description

CorreLog provides specific controls that track mailbox access for administrators, to reduce operational risk posed by Exchange 2003. These controls are added to a standard version of CorreLog Server, as follows.

1. CorreLog provides a "mailbox usage auto-learn" function, which gathers an information baseline on how administrators normally access mailboxes of users and associates. This creates a "pattern of usage" that shows the mailboxes an administrator may access as part of normal activities (such as viewing a user's calendar to make a meeting appointment.)

2. Once this baseline is established and reviewed, CorreLog will alert personnel if an administrator accesses any mailbox outside of this usage baseline. This indicates suspicious behavior, especially if this occurs frequently, or an administrator is already suspected of other malicious activities.

3. The security officer can take appropriate action when such an alert is generated, including adding the administrator to the usage baseline, to prevent further alerts of this type from being generated.

Using the above controls, security officers can be immediately alerted when an administrator accesses a mailbox outside of normal usage patterns. In this case, the strong presumption can be made that the administrator is snooping on the mailbox (because the administrator has no reason to look at the mailbox of that user for any reason, including accessing the user's calendar.)

For example, CorreLog can alert security officers that administrator X has accessed the CFO's mailbox. Because administrator X has no reason to make appointments with the CFO, the strong suspicion exists that the administrator is snooping on the CFO's Inbox.

Use Case Setup

Configuration of the use case is as follows:

1. The CorreLog Operator configures Microsoft Exchange 2003 to send a 1016 message to CorreLog (via the Windows Agent) whenever any login attempts to access a mailbox that is not the mailbox of the primary user. (See Appendix, Setup Detail #1.)

2. The CorreLog Operator configures the "LOG_EXCHANGE_BASELINE" correlation action, and allows this program to run for a period of time, such as for a week. This establishes a "pattern of usage" for administrators, describing which mailboxes they normally access. (See Appendix, Setup Detail #2.)

3. After a period of time (such as after one week) the CorreLog Operator disables the above action program, and configures the CHECK_EXCHANGE_BASELINE correlation action. This checks 1016 messages against the baseline, and sends a message back to CorreLog when some mailbox outside the baseline is accessed. (See Appendix, Setup Detail #3)

4. The CorreLog Operator configures a thread, alert, and ticket for the message generated by the CHECK_EXCHANGE_BASELINE action. This provides notification that a particular Windows administrator has accessed a mailbox outside of normal operations. The ticket is sent to a special security officer. (See Appendix, Setup Detail #4)

5. The security officer evaluates all tickets, and takes necessary corrective action such as further investigation, or adding the administrator to the traffic baseline. If the security officer elects to add the user to the baseline (through direct edits of the Exchange Baseline, or via some custom tool provided by CorreLog professional services) then no further alerts will be generated for that administrator / mailbox combination.

The above technique furnishes a clear way of managing Exchange 2003 access given the limitations of Exchange 2003 to track mailbox usage.

Additional Notes

1. The CorreLog Exchange 2003 baseline is normally stored in a special Microsoft Access database, which is updated by the LOG_EXCHANGE_BASELINE correlation action. The database can be substituted for some other database by specifying a different ODBC connection for the program.

2. The "pattern of usage" baseline contains information as to mailbox access times, and frequencies, and can be reported on using standard Microsoft Access reporting tools. The contents of the database can also be viewed at the CorreLog site by configuring a database query screen within CorreLog using standard framework components.

3. Once the baseline is created, a security officer can update the database manually, or can use a utility program provided by CorreLog professional services. This provides a way to slowly adjust the baseline over time (as opposed to periodically establishing a new baseline.)

4. In addition to monitoring 1016 errors, CorreLog can also monitor a variety of other Exchange application auditing events, including invalid access errors, and alerts associated with performance. The standard CorreLog threading and alerting capabilities for Active Directory events can further augment this information, such as tracking of all administrator activity on the system.

5. The monitoring described herein should be made available only to special security officers, and not to CorreLog administrators. This is recommended in order to insure that a malicious administrator, with access to Correlog, does not modify the usage baseline. Standard CorreLog controls can notify the security officer if unauthorized changes to the baseline are made.

References

How To Monitor Mailbox Access, Microsoft Application Notes:
http://support.microsoft.com/kb/867640

Auditing Mailbox Access Using Exchange System Manager and Event Viewer
http://www.msexchange.org/tutorials/Auditing-Mailbox-Access-Exchange-System-Manager-Event-Viewer.html

Mailbox Access Auditing in Exchange 2007
http://www.howexchangeworks.com/2009/09/mailbox-access-auditing-in-exchange.html

CorreLog, Inc.
http://www.correlog.com
mailto:support@correlog.com