Parasol Island

Arbeitsanweisung zur Aufzeichnung der Benutzertätigkeit

Dateiname:	03_08_PSL_ISMS_Benutzerlogs_v01.00_jH
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	13.11.2017 | Justus Heinser
Exportiert am:	13.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	13.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	12.5 | 12.6

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	21.09.2017	Justus Heinser	Anpassungen
00.03	17.10.2017	Peter Norenkemper	Ergänzungen
01.00	13.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Zielsetzung

Zu Diagnosezwecken ist es wichtig, das Arbeitsverhalten auf den Systemen zu überwachen und auszuwerten. Einerseits sollen so Fehlverhalten der Benutzer entdeckt werden und damit zur Einhaltung der Sicherheitsrichtlinien beitragen. Andererseits können die Logfiles Aufschluss über mögliche Systemfehler oder bisher unentdeckte Schadsoftware Infizierungen geben.

2. Zu loggende Systeme

Auflistung der Systeme mit Benutzerzugriffen:

- pslsrv10 / pslsrv17
- psldc01 / psldc02 / psldc03
- pslsrv05
- Licenser (pslsrv24 / pslsrv25 / pslsrv09 / pslsrv11)

3. Zu loggende Ereignisse

Einstellungen der Überwachungsrichtlinien

Für normale Nutzer

- Anmeldeversuche (Fehler)
- Objektzugriffsversuche (Fehler)
- Systemereignisse (Erfolg/Fehler)
- Verzeichnisdienstzugriff (Fehler)

Zusätzliche Events Admin

- Kontenverwaltung (Erfolg/Fehler)
- Richtlinienänderung (Erfolg/Fehler)

Zusätzlich bei sehr hohem Schutzbedarf:

- Objektzugriffsversuche (Erfolg/Fehler)

Kurzbeschreibungen

Anmeldeversuche überwachen

Kontoanmeldungsereignisse werden generiert, wenn die Anmeldeinformationen eines Kontos geprüft werden.

Objektzugriffsversuche überwachen

Mit dieser Sicherheitseinstellung wird festgelegt, ob Benutzerzugriffe auf Nicht-Active-Directory-Objekte überwacht werden. Überwachung wird nur für Objekte generiert, für die eine eigene SACL (System Access Control List, Zugriffssteuerungsliste für das System) angegeben ist, und nur dann, falls der angeforderte Zugriffstyp (beispielsweise Schreiben, Lesen oder Ändern) und das Konto, von dem die Anforderung stammt, den Einstellungen in der SACL entspreche.

Systemereignisse überwachen

- Versuchte Änderung der Systemzeit
- Versuchtes Starten oder Herunterfahren des Sicherheitssystems
- Versuch, erweiterbare Authentifizierungskomponenten zu laden
- Verlust von überwachten Ereignissen aufgrund eines Fehlers im Überwachungssystem
- Größe des Sicherheitsprotokolls überschreitet einen konfigurierbaren Warnungsschwellenwert

Verzeichnisdienstzugriff

Mit dieser Sicherheitseinstellung wird bestimmt, ob Benutzerzugriffe auf Active-Directory-Objekte überwacht werden. Überwachung findet nur bei Objekten statt, für die die Systemzugriff-Steuerungsliste (SACL) angegeben wurde, und nur dann, wenn der angeforderte Zugriffstyp (beispielsweise Schreiben, Lesen oder Ändern) und das Konto, von dem die Anforderung stammt, den Einstellungen in der Systemzugriff-Steuerungsliste entsprechen.

Kontenverwaltung überwachen

- Ein Benutzerkonto oder eine Benutzergruppe wird erstellt, geändert oder gelöscht.
- Ein Benutzerkonto wird umbenannt, deaktiviert oder aktiviert.
- Ein Kennwort wird festgelegt oder geändert.

Richtlinienänderungen überwachen

Mit dieser Sicherheitseinstellung wird festgelegt, ob jede Instanz von Versuchen zur Änderung der Richtlinien für Benutzerrechtezuweisung, Überwachung, Konten oder Vertrauensstellung überwacht wird.

Zusätzliche Aufzeichnungen

Unabhängig von den generell zu erfassenden Benutzerlogs, welche permanent gesammelt werden, sind temporär zusätzliche Aufzeichnungen der Benutzeraktivität möglich. Dies ist zum Beispiel der Fall bei kundenspezifischen Wünschen, welche vertraglich beschlossen wurden, oder aber obligatorisch bei besonders sensiblen Projekten.
Bei Informationen mit sehr hohem Schutzbedarf sind die „Objektzugriffsversuche“ in den Überwachungsrichtlinien für Administratoren nicht nur bei Fehlern, sondern auch bei Erfolg aufzuzeichnen. Dadurch wird jeder Dateizugriff eines Benutzers aufgezeichnet.
Die Projektleitung hat den Administrator über die Anforderung zu informieren und den zeitlichen Rahmen für die Erweiterung der Aufzeichnungen festzusetzen. Der ISB ist ebenfalls zu informieren, da eine Richtlinienänderung andernfalls bei der Auswertung als Auffälligkeit gewertet werden würde. Aus Gründen der Übersicht empfiehlt es sich, vor Änderung der Richtlinie die Benutzerlogs zu exportieren und dies zu Protokoll zu nehmen. Ebenso bei der Änderung zurück auf den Normalzustand.

- ➢ Exportprozess im Kapitel **Auswertung** beschrieben

4. Auswertung

Die ausgewählten Computer werden so im Betriebssystem konfiguriert, dass die systemeigenen Überwachungsrichtlinien die erforderlichen Ereignisse aufzeichnen.
Die Logfiles können anschließend im *.evtx Format gespeichert werden. Dieser Vorgang wird vom Administrator unter Aufsicht des Informationssicherheitsbeauftragten durchgeführt. Der Informationssicherheitsbeauftragte legt umgehend eine Roh-Kopie der Logfiles an, um diese vor Veränderung abzusichern. Ein Löschen der Files ist vom Informationssicherheitsbeauftragten im Protokoll zu vermerken. Eine Löschung außerhalb der protokollierten Zeit ist als schwere Auffälligkeit umgehend der Geschäftsführung zu melden, da dies den Verdacht auf Missbrauch durch den Administrator hindeuten kann.
Die Auswertung erfolgt stichprobenartig und manuell unter vier Augen von Systemadministrator und Informationssicherheitsbeauftragten und sollte mindestens einmal jährlich durchgeführt werden. Auffälligkeiten sind in einem Protokoll zu erfassen und auszuwerten. Bei größeren Auffälligkeiten oder möglichen Verstößen gegen die Sicherheitsrichtlinien ist die Geschäftsführung zu informieren.
Nach dem Export der Eventfiles können die Protokolle auf dem System unter vier Augen gelöscht werden, um Datenmüll zu vermeiden. Eine Löschung ist in dem Protokoll zu vermerken, um eine Lückenlosigkeit zu kontrollieren.

5. Automatische Auswertung (SIEM)

Ein Security Information and Event Management sammelt Eventlogs automatisch und wertet diese aus.
Die Einrichtung eines solchen Systems ist bis jetzt noch nicht umgesetzt. Pläne zur Einrichtung eines solchen Systems sind allerdings in Arbeit.

Ziele und konkrete Pläne:

- Finden einer geeigneten Software für unsere Bedürfnisse:
    - Geeignet für Firmengröße
    - Überwachung von mehreren Systemen gleichzeitig und zentrale Sammlung
    - Sicherung vor Veränderung oder Verlust
    - Sicherung vor unbefugten Zugriffen
- Besonderer Schutz der Files vor Veränderung, insbesondere durch den Administrator.
- Automatische Auswertung der Logs in übersichtlicher Form.