

2011



ProLog Systembeschreibung

Version 1.3i

1. Einleitung

Finanz- und Industrieunternehmen sind einer stetig wachsenden Anzahl von Angriffen oder anderen Gefährdungen Ihres sicheren IT Betriebs ausgesetzt.

Die IT Prüfungsgremien, als auch die haftenden Vorstände sowie die verantwortlichen Mitarbeiter sind aufgefordert entsprechende Maßnahmen in den Instituten um zu setzen.

2. Ansatz

Log- und Monitoringdaten werden in jedem IT-Verbund von den verschiedensten IT-Systemen und Anwendungen in großer Menge und Vielfalt generiert. Vielfach enthalten die erzeugten Meldungen Informationen, die auf mögliche Sicherheitsprobleme oder bereits eingetretene Sicherheitsvorfälle schließen lassen. Die Idee, diese Informationsquellen zur Verbesserung der IT-Sicherheit detailliert auszuwerten und Maßnahmen abzuleiten, liegt daher nahe.

3. Revisionsanforderung

IT Systeme und Anwendungen müssen nach den gängigen IT Sicherheitsstandards betrieben werden. Dies folgt aus den handelsrechtlichen Vorschriften der Belegbarkeit und Nachvollziehbarkeit (§238 Abs. 1 und 239 HGB). Ferner aus den GOBS sowie den Anforderungen an die Sicherheit und die technisch organisatorische Ausstattung von IT Systemen (Hard- und Software) gem. MaRisk sowie dem erforderlichen Schutz personenbezogener Daten gem. §9 BDSG. Aktivitäten und Fehlermeldungen der verwendeten Systeme müssen zur Aufrechterhaltung der IT Sicherheit protokolliert- und auswertbar sein. Gefordert ist eine Einheitliche, standardisierte Vorgehensweise bei der Erhebung und Auswertung von Log- und Monitoringdaten nach MaRisk (Mindestanforderung an das Risikomanagement) z. B. auf Basis der BSI Logdatenstudie für sicheren IT Betrieb.

4. Zielsetzung

Die systematische Erhebung und Nutzung von maschinell erstellten Log- und Monitoringdaten zur Erkennung von Sicherheitsproblemen oder Sicherheitsvorfällen. Dazu werden die Daten nach individuellen Kriterien ausgewertet. Die gewonnenen Informationen dienen vorbeugend als Frühwarnsystem oder nachgelagert zur Aufklärung/Rekonstruktion von IT-Sicherheitsvorfällen. Im Fokus steht dabei die Gewährleistung der IT-Sicherheit, d.h. von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen.



5. Umsetzung

Die Kernaufgabe der Applikation ist die Auswertung und unveränderte Archivierung von pseudonymisierten sicherheitsrelevanten IT-Events. ProLog bietet eine ressourcenschonende und sichere Archivierung sowie eine leicht und intuitiv zu bedienende Oberfläche gefordert.

Die hochverfügbare Clustertechnologie von ProLog, sowie die Eigenüberwachung zum Schutz vor Manipulation von ProLog unterstreichen den höchsten Sicherheitsanspruch dieser Lösung. Kurze Integrationszeiten mit Know-How Transfer an die Administratoren garantieren eine schnelle und transparente Betriebsbereitschaft von ProLog.

6. Physikalische Plattform:

ProLog läuft auf zeitgemäßen Standard Serversystemen mit Quad Core Technologie und 48 GB Hauptspeicher. Im Hintergrund befindet sich ein speziell abgeschottetes Linux Cluster System inklusive einer abgesicherten SQL basierenden Datenbank Applikation.

Es sind keine Linux Kenntnisse zur Administration von ProLog nötig, da die komplette Konfiguration in der grafischen Weboberfläche geschieht.

7. Datensicherheit:

ProLog ist als hochverfügbare Cluster Lösung vorgesehen, bei der die Daten permanent gespiegelt sind. Ist vom Kunden eine Anbindung an das interne Backupsystem vorgesehen so kann hier individuelle das verschlüsselte Backup auf Server externen Speicher (bspw. SAN) abgelegt werden.

Selbst in komplexen Installationsszenarien ist das komprimierte Monatsbackup erfahrungsgemäß nicht grösser als 20 GB. Dies variiert nach Kundenkonfiguration und Eventkaufkommen.

8. Kapazität und Performance

In der Standardvariante (ProLog ENTRY) ist ProLog für die revisionskonforme Speicherung von ca. 400 Millionen Events und einer maximalen Eventaufnahme von bis zu 35 Millionen Events pro Tag ausgelegt.

ProLog ist in komplexen Szenarien nach vorangegangener Analyse und individueller Betrachtung nahezu beliebig skalierbar.

In einem gemeinsamen Regelworkshop werden die entsprechenden Auswertungen und Überwachungen der Log Dateien, die Pseudonymisierungsregeln sowie die Benachrichtigungswege definiert und später bei der Integration umgesetzt.



9. Pseudonymisierung

Anhand von individuell definierten Pseudonymisierungsregeln werden die eingehenden sensiblen Informationen sofort durch Platzhalter (#-Zeichen) ersetzt und die Originalinformationen in einem getrennten und abgesicherten Bereich abgespeichert.

Beispiel Nr. 1: Entspricht eine Information dem Format $x + 5 \text{ Zahlen}$ so ist dies eine sensible Information – hier ein Benutzername

Beispiel Nr. 2: Ist eine Information im Format $\text{Zahl } 4 + 15 \text{ weitere Zahlen}$ – hier eine Visa Kreditkartennummer, so ist diese Information zu pseudonymisieren

Der Benutzer hat immer eine pseudonymisierte Sicht und kann nur depseudonymisieren, indem er die Freigabe im n-Augenprinzip beantragt.

ProLog seitig kann die Anzahl der Personen bestimmt werden, die der Depseudonymisierung zustimmen müssen.

Beispiel: 1 Personalreferent, 1 Betriebsrat und 2 Teamleiter oder aber 3 Vorgesetzte und ein Revisor etc.



10. ProLog Features

- Benutzerfreundliche und intuitive Bedienung (Drag & Drop, Kontextmenüs)
- Performante, leicht anpassbare, schlanke Webanwendung ohne Installationsaufwand auf den Clients
- Einfache und hocheffiziente Filterung der automatisch eingesammelten Events
- Automatische Kategorisierung der empfangenen Events nach Schweregrad durch visueller Hervorhebung (Highlighting)
- Frühwarnung und Erkennung von Netzwerkangriffen (Intrusion Detection) / Richtlinienverstößen / Problemen
- **ProLog** Eigenüberwachung zum Schutz vor Manipulationen (HW, SW Monitoring sowie Logging aller Adminaktionen)
- Nahtlose Integration von Lotus Notes Eventhandlern sowie Weiterverarbeitung durch **ProLog**
- Überwachung von vielen unterschiedlichen Systemen und Komponenten (Windows, Linux, Cisco, HP, IBM, FSC, ...)
- Manipulationssicher durch speziell abgesichertes Linux Basissystem
- Schnelle und einfache Berichterstellung sowie Export (PDF, CSV, HTML, PNG, ...)
- Flexible Benachrichtigungs- und Eskalationswege (Z.B. SMS*, E-Mail, Twitter*, VoIP*, RSS*, XML* ...)
- Berechtigungssystem und Authentifizierung über verschiedene Systeme möglich (Active Directory, Lotus Notes, HTTP Auth, Kerberos)
- Zugriff auf vielfältige Filter- und Berichtsvorlagen für gängige Filterevents ab Werk (z.B. IBM Lotus Notes, Cisco Port Security, Windows Security Events)
- (De-)Pseudonymisierung durch beliebig viele Verantwortliche (z.B. Freigabe nur durch zwei Revisoren und zwei Entscheider)
- Zentrale Speicherung der ungefilterten aber pseudonymisierten Ereignisse mit individueller Speicherdauer und effizienter Komprimierung
- Import und Korrelation verschiedenster Log-/Dateiformate (SYSLOG, SNMP, CSV, SQL, TXT, RRD, ...)
- Leicht zugängliche, deutsche Dokumentation durch Supportportal (Dokumentation, Bugreporting, Supportforum, Download von Updates)

* optional



11. ProLog Mindestanforderungen / Standardsystem:**Hardware Mindestanforderungen:**

Hersteller	Fujitsu Technology Solutions
Modell	RX300 Sx (ab S5)
CPU:	2 x QuadCore CPU
RAM:	48 GB
RAID:	SAS 6G RAID 5/6 512MB + BBU
Festplatte:	6 x 450GB SAS 15K Hot Plug (2 x 450 im RAID 1; 4 x 450GB im RAID 10)
Netzwerk :	4 x 1Gbit Intel Ethernet

ProLog Facts*

IT@WORK ProLog ist in der angebotenen Standard Version auf 35.000.000 Events/Tag, d.h. 25.000 Events/Minute ausgelegt. (Die maximale Speicherdauer bei kurzfristiger Spitzenauslastung ist vom verfügbaren Festplattenspeicher abhängig)

Maximale Speicherkapazität: ca. 400 Millionen Events
(bei empfohlener Mindestanforderung)

Definition der Plattform und der Redundanzstufe

ProLog kann auf physikalischen Systemen jeweils als Single- oder Clusterlösung eingesetzt werden. Eine nachträgliche Clustermigration von einem Singlesystem ist möglich, jedoch mit Aufwand verbunden. Wir empfehlen als höchste Sicherheitsstufe einen physikalischen Aktiv-/Passiv Cluster, bestehend aus zwei Knoten.

Maximaler theoretischer Datendurchsatz zwischen den einzelnen Clusterknoten: 2,3 Gbit

* Angegebene Daten basieren auf den Mindestanforderungen und einer Durchschnittseventgröße von 1,25KB pro Event. Genaue Anzahl der Events, benötigter Plattenplatz sowie Performance des Eventhandlings und Berichtswesens sind Anforderungs-, Umgebungs- und Hardwareabhängig und können variieren. Durch fremd Soft- und Hardware bedingte Limitierungen vorbehalten.

