IT-Compliance mit Log-Management für die Finanzindustrie: Banken, Versicherungen und Leasinggesellschaften

IT@WORK ProLog®

6 gute Gründe für ProLog:

- maximiert Ihre IT-Sicherheit und IT-Verfügbarkeit
- Umsetzung von BAIT ab Herbst 2017 als Ergänzung zu MaRisk
- Umsetzung der Vorgaben aus den BSI-Handbüchern zum Thema „Sicherer IT-Betrieb“
- Beachtung des Mitarbeiter-datenschutzes (BDSG und EU-DSGVO)
- Standard Protokollierungs- und Auditierungskonzept mit fertigen Berichtspaketen
- keine Investitionskosten, sondern Servicepauschale in €/Monat/ Mitarbeiter

Allianz für Cyber-Sicherheit

Die anhaltende Regulierungsflut trifft Deutschlands Finanzinstitute hart. Die Umsetzung gesetzlicher Vorgaben für Revision und Compliance wird ab Ende 2017 mit BAIT (Bankaufsichtliche Anforderungen an die IT) als Ergänzung zu MaRisk und Anfang 2018 mit der neuen europäischen EU-DSGVO (Datenschutzgrundverordnung) umso wichtiger.

Eine Fülle von Regularien ergießt sich bereits heute über die Finanzlandschaft, die besonders das Risikomanagement und die IT-Systeme im Bereich Risikosteuerung treffen. Am 25. Mai 2018 tritt die neue EU-Datenschutzgrundverordnung (EU-DSGVO) mit verschärften Regeln in Kraft. Werden dann personenbezogene Daten von EU-Bürgern gestohlen, drohen dem betroffenen Finanzinstitut hohe Geldbußen. Für die Finanzindustrie heißt das: Tempo machen bei der Umstellung.

Neben den gesetzlichen gilt es aber auch eine Reihe unternehmensinterner Vorschriften zu beachten, wie zum Beispiel: Betriebs- und Handlungsanweisungen und Compliance Richtlinien. Neue Berichtspflichten werden die bisherige Praxis ablösen müssen.

Diese Anforderungen schaffen eine Fülle von organisatorischen Herausforderungen, die eine konzeptionelle Darstellung aller damit verbundenen Prozesse und Systeme zwingend erforderlich machen und klassischerweise in ein Protokollierungs- und Auditierungskonzept des Finanzinstituts einfließt.

Wichtige Inhalte des Konzeptes sind unter anderem:

- Einhaltung der Gesetze des KWG, Telemediengesetz, BDSG und DSGVO
- Umsetzung BAIT (Bankaufsichtliche Anforderungen an die IT) ab Herbst 2017 als Ergänzung zu MaRisk
- Umsetzung der Vorgaben aus den Handbüchern des BSI (Bundesamt für Sicherheit in der Informationstechnik) zum Thema „Sicherer IT-Betrieb“
- Definition von Grundsätzen zur Protokollierung
- Bestimmung der relevanten Systeme und Anwendungen
- Erstellung einer Risikobetrachtung
- Erarbeitung eines Umsetzungsleitfadens

Rechtliche Herausforderungen

Die gesetzlichen Rahmenbedingungen für die Banken, Versicherungen und Leasinggesellschaften sind im Folgenden detailliert beschrieben:

Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) fordert von Unternehmen eine Reihe regulatorischer Richtlinien sicher zu beherrschen und anzuwenden. Dies sind u.a.:

- Datenvermeidung und -Sparsamkeit
- Pseudonymisierung aller persönlichen Informationen
- Sicherstellung der Zulässigkeit der Datenerhebung
- Diverse technische und organisatorische Maßnahmen

EU-Datenschutzgrundverordnung

Im Rahmen der Einführung der **EU-DSGVO** kommen ab Mai 2018 neue Anforderungen auf den IT-Betrieb zu. Dies betrifft vor allem den Schutz von personenbezogenen Daten welche besonders geschützt werden müssen.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Im Rahmen des KonTraG kam es 1998 zu einer Reihe von Anpassungen für Unternehmen. Es fordert beispielsweise von Vorständen: *„ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“* können. Diese wichtige Anforderung an Unternehmen setzt für die IT neben Monitoring auch Protokollierung voraus.

Telemediengesetz

Die Verwendung von Kundendaten konfrontiert Unternehmen mit ähnlichen Anforderungen wie die Verwendung interner Ereignisinformationen. Das TMG fordert spezifizierte organisatorische und technische Maßnahmen im Umgang mit diesen Daten wie z.B.:

- *„Eine Maßnahme [...] ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.“*
- *„Der Diensteanbieter darf [...] Nutzungsprofile bei Verwendung von Pseudonymen erstellen [...]“*

Kreditwesengesetz

Unternehmen und Organisationen, die unter das KWG fallen, werden im Rahmen der Regelungen zu besonderen organisatorischen Pflichten angehalten. Diese sind in Bezug auf die IT und die Verwendung von Logdaten u.a.:

- *„Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen [...]“*
- *„angemessene personelle, technische und organisatorische Ausstattung des Instituts“*
- *„die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme“.*

IT-Sicherheitsgesetz

Verpflichtet deutsche Unternehmen in „infrastrukturkritischen“ Bereichen zu ausführlichem Reporting bei Angriffsfällen. Diese Bereiche umfassen:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen

MaRisk, BAIT und MaGo

MaRisk, BAIT ab Herbst 2017 und MaGo (ersetzt seit 1.1.2016 MaRisk VA) beschreiben übergreifend die aufsichtsrechtlichen Mindestanforderungen an die Geschäftsorganisation von Banken, Versicherungen und Leasinggesellschaften. Im Speziellen für das Log-Management bedeutet das:

- Referenz auf BDSG (Datensparsamkeit, -vermeidung und Pseudonymisierung)
- Protokollierung Auswertung der Protokolle, aus AT 7.2 MaRisk und §9 BDSG
- **Neu** BAIT (Bankaufsichtliche Anforderungen an die IT) als Ergänzung zu MaRisk

Fazit:

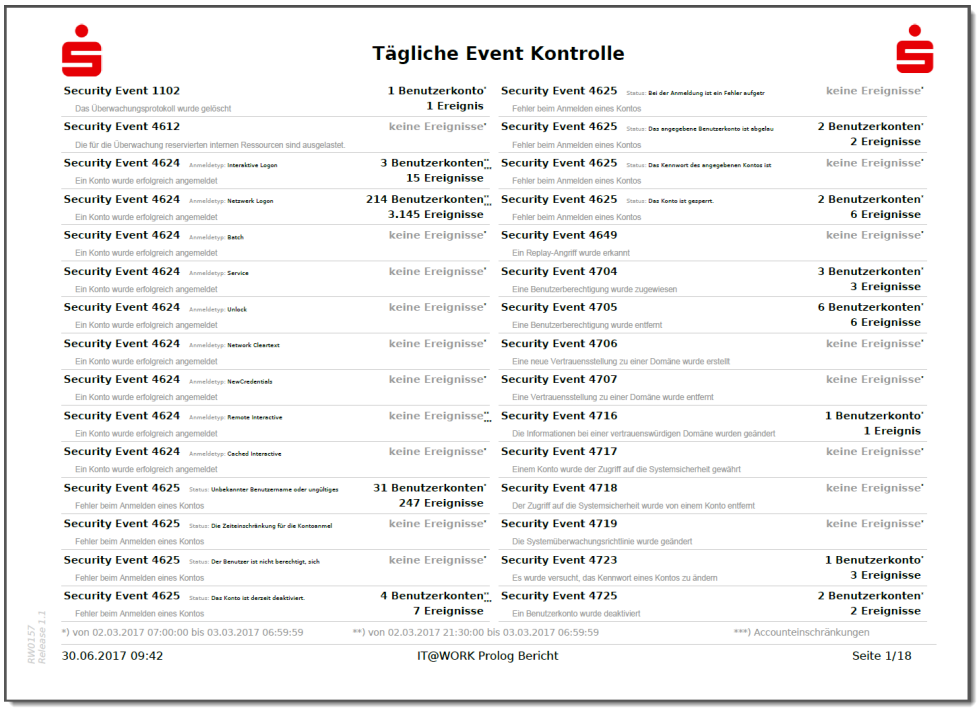
Alle diese gesetzlichen Vorgaben setzen das Vorhandensein eines Systems zum Erfassen und Auswerten von Ereignismeldungen voraus. Dies wiederum erfordert zwingend eine konzeptionelle Darstellung aller damit verbundenen Prozesse und Systeme in Form eines Protokollierungs- und Auditierungskonzeptes.

Unsere Lösung

IT@WORK ProLog® bietet für die Finanzinstitute eine etablierte und standardisierte Lösung mit fertigen Paketen für Alarmierungen, Filter und Berichte.

Berichts– und Alarmierungspakete

Entwickelt in Zusammenarbeit mit Banken für Banken. Diese automatisierten Berichte wurden bereits in den verschiedensten Verbandsgebieten in Deutschland erfolgreich geprüft und sind sofort einsetzbar. Die Pakete werden ständig im Rahmen des Wartungsvertrages gepflegt und erweitert. Zum Umfang der Berichte gehören unter anderem die Auswertung von Ereignissen für Microsoft Server 2003-2016, Microsoft Files Server, Linux, VMware, Exchange, Lotus Notes und CISCO, ...



Tägliche Event Kontrolle

Security Event 1102 Das Überwachungsprotokoll wurde gelöscht	1 Benutzerkonto' 1 Ereignis	Security Event 4625 Status: Bei der Anmeldung ist ein Fehler aufgetr Fehler beim Anmelden eines Kontos	keine Ereignisse'
Security Event 4612 Die für die Überwachung reservierten internen Ressourcen sind ausgelastet.	keine Ereignisse'	Security Event 4625 Status: Das angegebene Benutzerkonto ist abgelau Fehler beim Anmelden eines Kontos	2 Benutzerkonten' 2 Ereignisse
Security Event 4624 Anmeldetyp: Interaktive Logon Ein Konto wurde erfolgreich angemeldet	3 Benutzerkonten'** 15 Ereignisse	Security Event 4625 Status: Das Kennwort des angegebenen Kontos ist Fehler beim Anmelden eines Kontos	keine Ereignisse'
Security Event 4624 Anmeldetyp: Netzwerk Logon Ein Konto wurde erfolgreich angemeldet	214 Benutzerkonten'** 3.145 Ereignisse	Security Event 4625 Status: Das Konto ist gesperrt. Fehler beim Anmelden eines Kontos	2 Benutzerkonten' 6 Ereignisse
Security Event 4624 Anmeldetyp: Batch Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4649 Ein Replay-Angriff wurde erkannt	keine Ereignisse'
Security Event 4624 Anmeldetyp: Service Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4704 Eine Benutzerberechtigung wurde zugewiesen	3 Benutzerkonten' 3 Ereignisse
Security Event 4624 Anmeldetyp: Unlock Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4705 Eine Benutzerberechtigung wurde entfernt	6 Benutzerkonten' 6 Ereignisse
Security Event 4624 Anmeldetyp: Network Cleartext Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4706 Eine neue Vertrauensstellung zu einer Domäne wurde erstellt	keine Ereignisse'
Security Event 4624 Anmeldetyp: NewCredentials Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4707 Eine Vertrauensstellung zu einer Domäne wurde entfernt	keine Ereignisse'
Security Event 4624 Anmeldetyp: Remote Interactive Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'**	Security Event 4716 Die Informationen bei einer vertrauenswürdigen Domäne wurden geändert	1 Benutzerkonto' 1 Ereignis
Security Event 4624 Anmeldetyp: Cached Interactive Ein Konto wurde erfolgreich angemeldet	keine Ereignisse'	Security Event 4717 Einem Konto wurde der Zugriff auf die Systemsicherheit gewährt	keine Ereignisse'
Security Event 4625 Status: Unbekannter Benutzername oder ungültiges Fehler beim Anmelden eines Kontos	31 Benutzerkonten' 247 Ereignisse	Security Event 4718 Der Zugriff auf die Systemsicherheit wurde von einem Konto entfernt	keine Ereignisse'
Security Event 4625 Status: Die Zeiteinschränkung für die Kontoanmel Fehler beim Anmelden eines Kontos	keine Ereignisse'	Security Event 4719 Die Systemüberwachungsrichtlinie wurde geändert	keine Ereignisse'
Security Event 4625 Status: Der Benutzer ist nicht berechtigt, sich Fehler beim Anmelden eines Kontos	keine Ereignisse'	Security Event 4723 Es wurde versucht, das Kennwort eines Kontos zu ändern	1 Benutzerkonto' 3 Ereignisse
Security Event 4625 Status: Das Konto ist derzeit deaktiviert. Fehler beim Anmelden eines Kontos	4 Benutzerkonten'** 7 Ereignisse	Security Event 4725 Ein Benutzerkonto wurde deaktiviert	2 Benutzerkonten' 2 Ereignisse

*) von 02.03.2017 07:00:00 bis 03.03.2017 06:59:59 **) von 02.03.2017 21:30:00 bis 03.03.2017 06:59:59 ***) Accounteinschränkungen

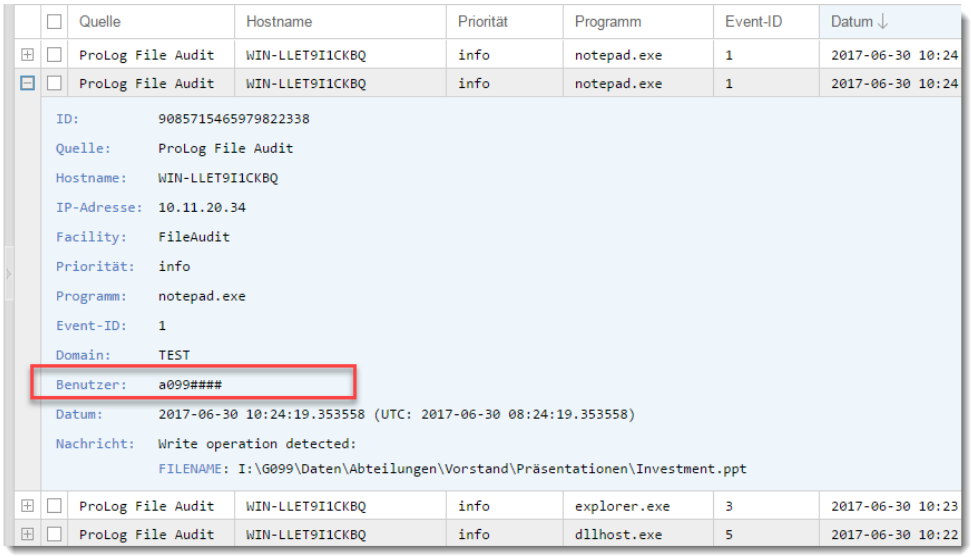
RW01.57 Release 1.1

30.06.2017 09:42 IT@WORK Prolog Bericht Seite 1/18

Abb. 1 zeigt einen Ausschnitt aus dem Management-Report der täglich vom SIEM-Administrator kontrolliert wird

Pseudonymisierung

ProLog pseudonymisiert nach diversen Kriterien den Benutzerbezug in einer Ereignismeldung. Hierbei werden die sensiblen Informationen technisch von der Ereignismeldung getrennt. Pro-Log bietet auch die Möglichkeit einen LDAP konformen Server (z.B. OpenLDAP, MS AD...) für die Pseudonymisierung anzubinden. Mit der logischen Trennung des Benutzerbezug vom Ereignis, kann man unterschiedliche Speicherfristen definieren.



Quelle	Hostname	Priorität	Programm	Event-ID	Datum ↓
ProLog File Audit	WIN-LLET9I1CKBQ	info	notepad.exe	1	2017-06-30 10:24
ProLog File Audit	WIN-LLET9I1CKBQ	info	notepad.exe	1	2017-06-30 10:24

```
ID:          9085715465979822338
Quelle:      ProLog File Audit
Hostname:    WIN-LLET9I1CKBQ
IP-Adresse:  10.11.20.34
Facility:    FileAudit
Priorität:   info
Programm:    notepad.exe
Event-ID:    1
Domain:      TEST
Benutzer:    a099####
Datum:       2017-06-30 10:24:19.353558 (UTC: 2017-06-30 08:24:19.353558)
Nachricht:   Write operation detected:
             FILENAME: I:\G099\Daten\Abteilungen\Vorstand\Präsentationen\Investment.ppt
```

ProLog File Audit	WIN-LLET9I1CKBQ	info	explorer.exe	3	2017-06-30 10:23
ProLog File Audit	WIN-LLET9I1CKBQ	info	dllhost.exe	5	2017-06-30 10:22

Abb. 2 zeigt eine „Write Operation" im Dashboard von ProLog FileAudit. Rot umrandet ist der pseudonymisierte Benutzername.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Lizensierung

Aufgrund der intelligenten Angebotsform als Servicepauschale in €/ Monat/MA (Anzahl Mitarbeiter) ist die Lösung für kleine und große Institute höchst interessant. Mit der Kündigungsfrist von drei Monaten auf Quartalsende ist die Lösung ad hoc und temporär auch für Institute anwendbar, die bereits planen selektives Outsourcing umzusetzen oder darüber nachdenken.

Über uns

Seit 2012 wird **IT@WORK ProLog®** stetig weiterentwickelt und an die neuen Herausforderungen im Bereich der IT-Sicherheit und IT-Compliance angepasst. Die NETZWERK Software GmbH ist ein Deutsches Softwarehaus mit Sitz im Raum München. Wir entwickeln nur in Deutschland und dank dem Einsatz von C++ und quellcode-offenen Programmbibliotheken stellen wir sicher, dass unsere Software frei von Hintertüren ist. Dies ist für die eine oder andere Behörde oder einem Mittelständler mit Mitbewerbern im Ausland von großer Bedeutung.

N-Augen-Prinzip

Die Mitarbeiter eines mittelgroßen Finanzinstituts (zirka 1.000 Benutzer) erzeugen im Schnitt vier Millionen Ereignismeldungen pro Tag. Dies ist de jure eine Massendatenerhebung mit personenbezogenen Daten und damit ein harter Verstoß gegen das BDSG und die kommende EU-DSGVO.

Das N-Augen Prinzip ist eine organisatorische Lösung, die prozesstechnisch in ProLog fest verankert ist. Ohne die Zustimmung Dritter kann kein IT-Administrator einen Personenbezug in der Darstellung der Ereignismeldungen im Dashboard oder in einem Bericht herstellen.

Dieses Prinzip stellt jeden Datenschutzbeauftragten, Betriebs– und Personalrat zufrieden.

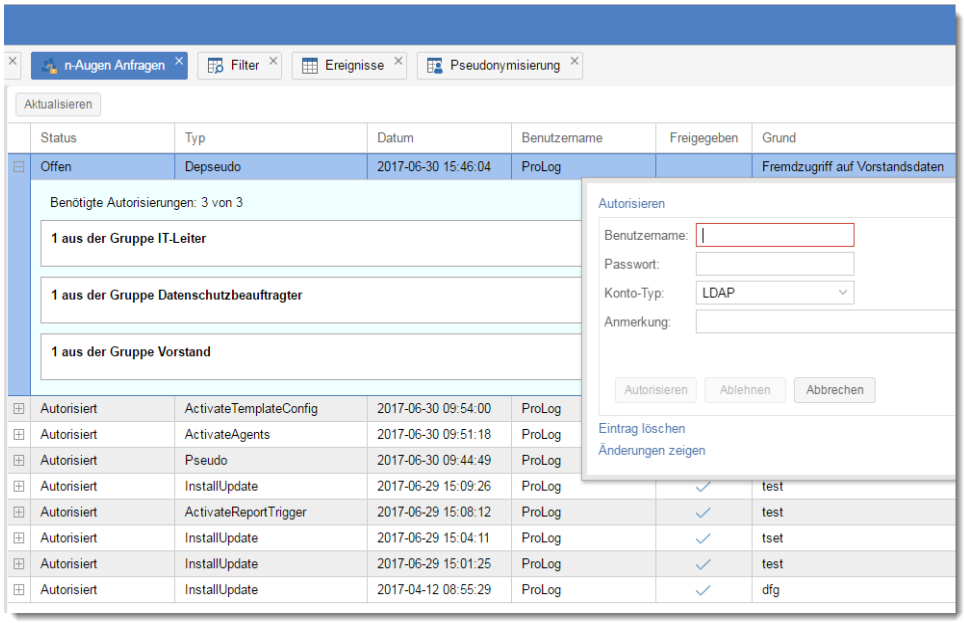


Abb. 3 zeigt den jeweils zu definierenden N-Augen Prozess des Finanzinstituts

FileAudit

Unser FileAudit liefert mehr Sicherheitsinformationen als die Auditfunktion des Microsoft File Server. Mit FileAudit kann man gezielt einzelne wichtige Dateien und/oder Dateiverzeichnisse schützen.

IT-Monitoring und IT-Verfügbarkeit

Viele unserer Sparkassenkunden nutzen unsere Lösung nicht nur für die Umsetzung und Überwachung der IT-Compliance sondern zusätzlich für das IT-Monitoring und IT-Verfügbarkeit.

Protokollierungs– und Auditierungskonzept

Aus der Erfahrung von vielen externen Audits ist ein Rahmen für ein Protokollierungs– und Auditierungskonzept entstanden, welcher im Zusammenspiel unserer Consultants und den Fachabteilungen des Kunden kundenspezifisch angepasst und gepflegt werden kann.

Services

Zusammen mit unseren Partnern bieten wir Ihnen **IT@WORK ProLog®** als „on Premise“ oder Cloud-Lösung an. Der Trend bei unseren Kunden geht eindeutig hin zur „Managed Security Service“ Lösung.

Unsere Mitarbeiter und Partner stehen Ihnen gerne persönlich zur Verfügung um mehr über die Lösungsmöglichkeiten mit **IT@WORK ProLog®** zu erfahren. Nutzen Sie unsere Informationsveranstaltungen, Webinare oder kontaktieren Sie uns einfach über Telefon oder E-Mail.

NETZWERK
IT-SICHERHEITSSOFTWARE

NETZWERK Software GmbH
Adalperostraße 80
85737 Ismaning

Telefon: **+49 (0)89 452 452 0**
eMail: **info@netzwerk.de**
Web: **http://netzwerk.de**