Information Rights Management

Anbietervergleich

GreenLab IRM (Sommer 2017)

Autor: Bastian Kammann
Tom Pasternak
Michael Riedel

GreenLab: IRM Anbieter Vergleich

	Aus-wertung	Anbieter	**secunet Security Networks AG Kurfürstenstraße 58 45138 Essen**	**Microsoft Microsoft Deutschland GmbH Niederlassung Berlin Unter den Linden 17 10117 Berlin**	**Adobe Georg-Brauchle-Ring 56/58 80992 München**
		Produktname	**Secunet secure Workflow**	**Azure Information Protection**	**AEM Document Security**
		Termin	07.08.2017	21.08.2017	24.08.2017
Gewichtung					
7%	**Referenzen (Fokus Deutschland)**		0,21	0,42	0,42
		Für eine bessere Beurteilung der Marktreife sind Referenzen zum Produkt ein wichtiges Merkmal			
		Bewertung (1- keine ... 10 - vielfältige Referenzen)	3	6	6
		Kommentar	Bisher nur BKA keine Referenzen in der Privatwirtschaft	z.B. Siemens, Bundesdruckerei, Credit Suiss, Conti, Microsoft Keine Referenzen in der ÖV	z.B. Bombardier (Kanada), Siemens via Brainloop (SaaS) (Deutschland), ABB(Schweiz), Deutscher Sparkassenverlag, Nedbank (Südafrika), Amkor Technologies (USA), Verizon Wireless(USA), Toyota, Standford University, Adobe, Flour Corporation und als Teil von Lösungen bei Canon, Intel/McAfee und Parametric Technology. Referenzen in der ÖV: United States Army Corps of Engineering, COMMONWEALTH OF AUSTRALIA REPRESENTED BY THE DEPT. OF DEFENCE (Australien + Neuseeland).
5%	**Backend / Server**		0,15	0,35	0,5
		Sind zur Implementierung der Lösung zentrale oder dedizierte Systeme erforderlich? Wenn ja, welche Betriebssysteme werden unterstützt?			
		Server erforderlich	ja	ja / nein (nein bei reiner Cloud Umgebung)	ja
		keine Appliance erforderlich	nein	ja	ja
		Server OS Windows möglich	nein	ja	ja
		Server OS Linux möglich	ja	nein	ja
		Server OS Unix möglich	nein	nein	ja
		Bewertung (1 - Geringe Variabilität ... 10 Hohe Variabilität)	3	7	10
		Kommentar	NAS erforderlich, Sicherheit der Daten zugelassene Kryptografie in Anwendung		Auch als SaaS-Lösung verfügbar.
15%	**Frontend / Client**		0,27	1,26	0,93
		Auf welchen Clients ist die Lösung abbildbar? Welche Betriebssysteme und welche Arten von Clients werden unterstützt?			
6%	**Fat Clients**		0,18	0,48	0,3
		Windows	ja	ja	ja
		Linux	nein	ja, implementierbar mittels API	ja für PDFs bis Adobe Reader 9.
		Unix	nein	nein	ja für PDFs mit Adobe Reader 9.
		Mac OS	nein	ja, implementierbar mittels API	ja für PDFs mit Adobe Reader / Adobe Acrobat (identische Versionenen wie auf Windows)
		Bewertung (1 - Geringe Variabilität ... 10 Hohe Variabilität)	3	8	5
		Kommentar	SINA Workstation erforderlich, Windows oder Ubuntu Nutzerarbeitsplatz		
6%	**Client über Terminalserver**		0,06	0,48	0,48
		Windows - RDS	nein	ja	ja
		Windows - Citrix	nein	ja (Unbekannt)	ja
		Unix	nein	nein	nein
		Bewertung (1 - Geringe Variabilität ... 10 Hohe Variabilität)	1	8	8
		Kommentar	Aufgrund Sicherheitskonzept und -mechanismen ausschließlich auf SINA Workstation nutzbar		
3%	**Mobile Client**		0,03	0,3	0,15
		Android	nein	ja	ja für PDFs mit Adobe Reader Mobile für Android
		iOS	nein	ja	ja für PDFs mit Adobe Reader Mobile für iOS
		BlackBerry	nein	ja (Unbekannt)	Schutz von PDFs auf BlackBerry möglich, es wird jedoch eine anderen Technologie von Adobe dafür verwendet. Im Fokus dabei sind e-Books (PDF und EPUB)
		Windows Phone	nein	ja (Unbekannt)	ja für PDFs mit Adobe Reader for Windows Mobile
		Bewertung (1 - Geringe Variabilität ... 10 Hohe Variabilität)	1	10	5
		Kommentar	Ausschließlich auf SINA Workstation nutzbar	Auf mobilen Geräten, ggf. nur consumption, keine protection	Läuft auf gängiger Hardware Schutz von PDFs und EPUB auf Basis von Adobe Content Server für alle genannten mobilen Endgeräte möglich. Es existieren somit zwei unabhängige Technologien von Adobe um PDFs zu schützen.
3%	**Georedundanz**		0,3	0,3	0,3
		Ist der Betrieb als georedundante Installation möglich? Sind hierfür besondere Voraussetzungen zu schaffen?			
		Bewertung (1- nicht Abbildbar ... 10 - Vollständig Umsetzbar)	10	10	10
		Kommentar	Ist möglich (HA-Cluster)	Ist möglich (HA-Cluster) bzw. HA in Azure Cloud	Ist möglich (HA-Cluster)
4%	**Besondere Anforderungen an Netze / Infrastruktur**		0,4	0,4	0,4
[Hier eingeben]		*Sind besondere Anforderungen an die Netze / Infrastruktur erforderlich, um das System hinreichend zu betreiben?*			
		Bewertung (1- besondere Anforderungen ... 10 - Standard Netze)	10	10	10
		Kommentar	Keine besondere Anforderungen	Keine besondere Anforderungen	Keine besondere Anforderungen

GreenLab: IRM Anbieter Vergleich					
5%	**Aufwand Administration / Wartung**		0,15	0,35	0,35
		Wie hoch ist der administrative Aufwand für Konfiguration und Betrieb? Welche Zertifizierungen und Kenntnisse sind erforderlich?			
		Bewertung (1- hoher Aufwand ... 10 - geringer Aufwand)	3	7	7
		Kommentar	Window, SecunetWorkflow und SINA Administratoren	Windows, Azure Administratoren	Je nach verwendeter Plattform (JEE Application Server auf Windows/Unix/Linux), Adobe AEM Administratoren
15%	**Implementierte / Mögliche Sicherheit**		1,2	1,2	1,35
		Welche Sicherheitsmechanismen sind implementiert oder können nachträglich konfiguriert oder nachgerüstet werden?			
		Bestehen für die Lösung Sicherheitszertifizierungen oder Zulassungen	BSI-Zulassung bis GEHEIM (Im Zulassungsprozess)	Federal Information Processing Standard 140-2 (FIPS), ISO/IEC 27001:2013, SOC 2 SSAE, HIPAA BAA	Federal Information Processing Standard 140-2 (FIPS), SOC2, ISO 27001, HIPPA, GBLA
		Verschlüsselung (Algorithmen)	ja (BSI zugelassen + AES 256 CBC Betriebsart)	ja (AES 128 / AES 256)	ja (AES 128 / AES 256)
		PKI / IAM	ja	Nicht im Standard bei On Premise. Für On Premise gibt es weitere Lösungsansätze	ja
		SSO möglich	nein	ja	ja
		2 FA möglich	ja	ja	ja
		OTP möglich	nein	nein	ja
		Bewertung (1- stark beschränkt ... 10 - vielfältig)	8	8	9
		Kommentar	SINA Smartcards als lokaler Sicherheitsanker Nutzerauthentifizierung (SC und PIN), Digitale Signatur für Nachweisführung		
9%	**UX / UI - Usability**		0,18	0,72	0,72
		Kann der Benutzer auf vertraute oder intuitive Oberflächen und Steuerelemente zurückgreifen? Welcher Aufwand ist für Administration und Anwendung erforderlich? Welcher Schulungsaufwand ist überlichweise notwendig?			
		Bewertung (1- Aufwendige Nutzung ... 10 - Nahtlose Integration in die Arbeitswelt)	2	8	8
		Kommentar	Der Nutzer muss zwischen 2 Betriebsystemen wechseln (Arbeits-Session) und (VS -Session), Properitäre Menüführung	Vertrautes Microsoft Look&Feel	Vertrautes Microsoft Look&Feel
9%	**Audit & Compliance Fähigkeit**		0,72	0,54	0,81
		Ist die Lösung zur Sicherstellung von Compliance Anforderungen auditierbar?			
		Bewertung (1- trifft nicht zu ... 10 - trifft vollständig zu)	8	6	9
		Kommentar	Auswertung möglich, sichert eine VSA-konforme Bestands- und Nachweisführung Compliance in Bezug auf Formen der Zusammenarbeit (Workflows) nach Organisationskonzept elektronische Verwaltungsarbeit (Baustein: e-Zusammenarbeit.	Umfangreiche Auswertung (z.B. Geodaten, Nutzer, ...) möglich, regionale Schlüsselhinterlegung,	Umfangreiche Auswertung (z.B. Geodaten, Nutzer, ...) möglich, Webinformation, Continus Monitoring for Anomalies, Funktionslimitierung, Expiration & Revocation, Administrator Warning, Überwachung versuchter Zugriffe
3%	**Backup & Recovery**		0,27	0,3	0,3
		Welche Backup und Wiederherstellungsfunktionen sind implementiert? Ist die Einbindung in bestehende Systeme möglich?			
		Kein dediziertes Backup erforderlich	ja, Backup des zentralen NAS-Storage	ja	ja
		Einbindung in bestehende Backup Infrastruktur möglich	ja , Das Backupkonzept folgt bestehenden operationellen Backup-Strategien	ja	ja
		Granulare Wiederherstellung von Berechtigungen aus Backup möglich	ja - Datenbestand ist komplett kryptiert, Berechtigungen werden getrennt verwaltet, Kryptographische Berechtigungen können übertragen werden.	ja, IRM Berechtigungen sind in der Datei selber gespeichert	Ja, Wiederherstellung des Zustands zum Zeitpunkt des Backups mit anschließender granularer Modifikation von Berechtigungen möglich.
		Bewertung (1- hoher Integrationsaufwand / nicht möglich ... 10 - geringer Integrationsaufwand)	9	10	10
		Kommentar	obliegt dem Nutzer / Betreiber Es besteht ein Konzept für ein Recovery nach Komplettausfall aller Serversysteme)	IRM ist stateless, da Informationen jeweils in der Datei selber gespeichert sind. Datenbank ist nur für AD RMS und kann regulär gesichert und wiederhergestellt werden	Restore über DB Transaktionslogs auf DB-Ebene möglich, aber nicht durch den technischen Support unterstützt. Die Verwendung wird nicht empfohlen.
10%	**Berücksichtigte Geheimschutz Anforderungen**		0,9	0,4	0,4
		Inwiefern werden die in der VSA definierten Schutzkategorien abgebildet?			
		VS - NUR FÜR DEN DIENSTGEBRAUCH	ja	nein - keine offizielle BSI Freigabe	nein - Schutzkategorie durch Richtlinien abbildbar
		VS - VERTRAULICH	ja	nein - keine offizielle BSI Freigabe	nein - Schutzkategorie durch Richtlinien abbildbar
		GEHEIM	ja	nein - keine offizielle BSI Freigabe	nein - Schutzkategorie durch Richtlinien abbildbar
		STRENG GEHEIM	nein	nein - keine offizielle BSI Freigabe	nein - Schutzkategorie durch Richtlinien abbildbar
		Bewertung (1- stark beschränkt ... 10 - vielfältig)	9	4	4
		Kommentar	Schutzkategorien gemäß VSA Anforderungen abgebildet	Individuelle Definition von Schutzkategorien möglich. Keine direkte Entsprechung zur VSA	Individuelle Definition von Schutzkategorien möglich. Keine direkte Entsprechung zur VSA
15%	**Abbildbare Dateitypen**		1,5	1,35	0,9
		Welche Dateitypen werden mit welchem Funktionsumfang durch die Lösung unterstützt? Gibt es die Möglichkeit, weitere Dateitypen in die Lösung einzubinden?			
		Bewertung (1- stark beschränkt ... 10 - vielfältig)	10	9	6
		Kommentar	Dateityp Unabhängig	Unterteilung in Native und Generic. Native: Hohes implementiertes Schutzniveau (Kryptierung + Rights Enforcement) Generic: Fokus auf Kryptierung, jedoch kein Rights Enforcement Wenige Dateitypen z.T. ausgeschlossen (Systemdateien, Executables, ...). Über SDK ist Rights Enforcement nachimplementierbar.	Geringe Anzahl Dateitypen (PDF, Word, Excel, PowerPoint). Über SDK ist Rights Enforcement nachimplementierbar
100%	**Auswertung**		6,25	7,59	7,38