T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

Handout zum Vortrag

Wie funktioniert Informationsschutz in gemischten und öffentlichen Infrastrukturen?

Verschlüsselung zum Schutz sensibler Informationen

Praktischen Schutz der Vertraulichkeit von Informationen bieten Anwendungen seit Jahren durch integrierte Verschlüsselungsverfahren. Bei kommerzieller Standardsoftware meist durch ein - Stand heute - bis zu 255 Zeichen langes Kennwort für AES Verschlüsselung. Alternative Open Source Software bietet einen Kennwortschutz mit Blowfish Anstelle von AES. Je nach Software lässt sich die Schlüsselstärke fein-justieren und die eine oder andere Option zur Dateiverschlüsselung optimieren.

Zentrales Schlüsselmanagement

Steigt der Bedarf an Informationsschutz - steigt damit auch die Anzahl des zu verwaltenden Schlüsselmaterials. Die Anzahl berechtigter Personen, auch die schiere Menge an zu schützenden Daten und Dateien spielen bei dieser Entwicklung eine Rolle. Datenaustausch unterstützt ein zentraler Speicher.

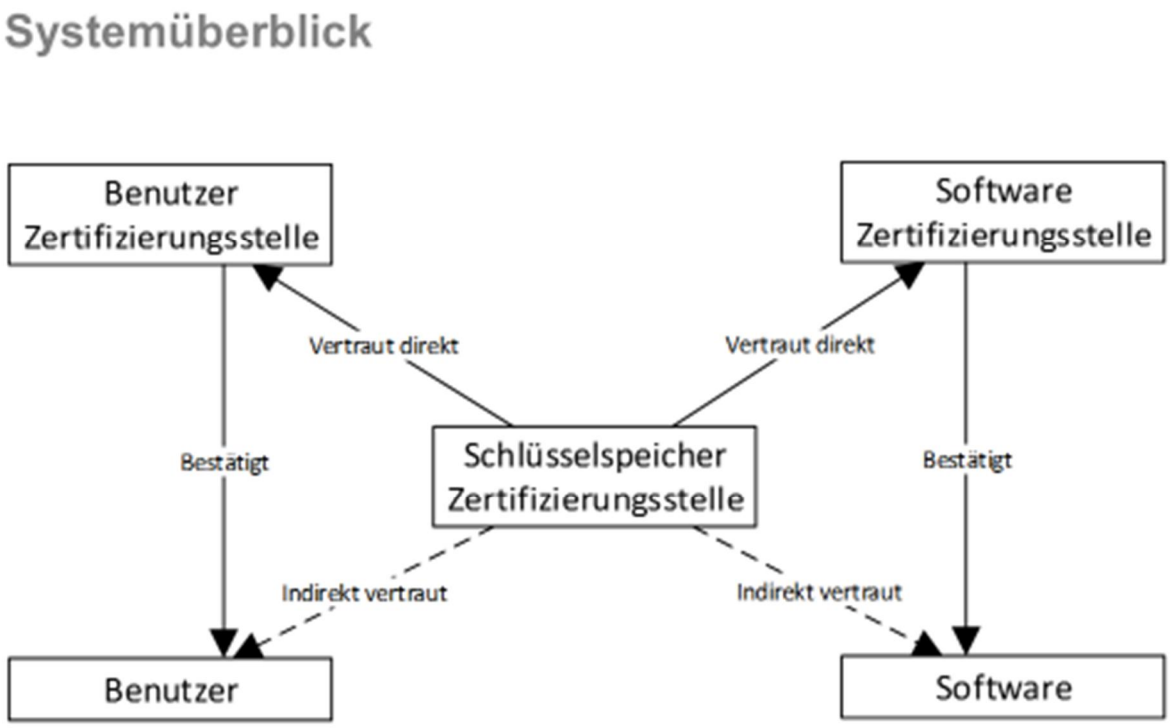
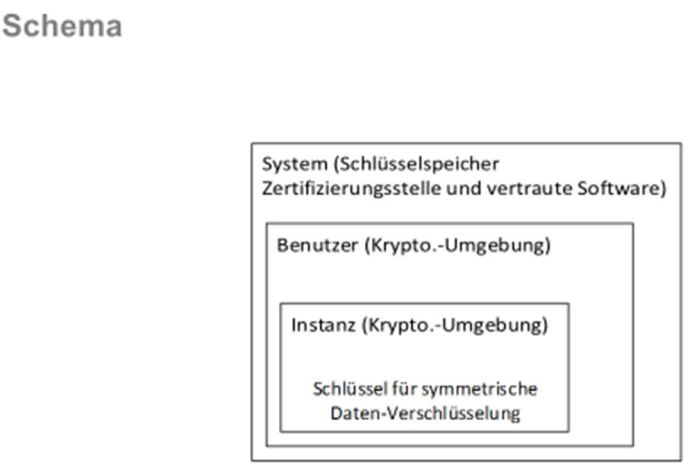


Abbildung 1 Systemüberblick

Vertraute Umgebung für den Austausch von Schlüsselmaterial



Eine Analyse entsprechender Software zeigte den Einsatz symmetrischer Verfahren für die Datenverschlüsselung. Asymmetrische Kryptografie - wohl auf Grund des höheren Bedarfs an Ressourcen - kommt zum Einsatz um einen sicheren Austausch des Materials für die symmetrische Ver-/Entschlüsselung zu ermöglichen. Der im Vortrag in Diagrammen aufgezeigte, teils komplexe Ablauf bietet eine hinreichend sichere Umgebung für den Schlüsselaustausch.

Abbildung 2 Schema Krypto.-Umgebung

Bislang eingesetzte Alternativen und Prognose

Heute wird ein Großteil der digitalen Informationen wohl an sicheren Speicherorten gespeichert (Laufwerksverschlüsselung, Datenträgerverschlüsselung) und bei Bedarf auf sicheren Netzwerkverbindungen transportiert (TLS für TCP/IP-Netzwerke, VPN, etc.). In Fachkreisen wird wegen der vermeintlichen Lücken und damit einhergehenden Risiken immer wieder die Ende-zu-Ende-Verschlüsselung diskutiert. Die als Grundlage für den Vortrag analysierten Informationsverwaltungs-Softwaren bieten bei der zu erwartenden Anzahl von Dateneinheiten (Dateien) eine zentrale Schlüsselverwaltung und mehr noch.

Auswirkungen auf Sicherheitseinschätzungen bei der Anwendung

Die Risikobild für Informationen ändert sich beim Einsatz einer Informationsmanagement-Software.

- Schutzziel ‚Vertraulichkeit' erhöht
- Schutzziel ‚Verfügbarkeit' verringert

Die Anwendung einer Schlüsselung macht den Zugriff auf Daten von der Verfügbarkeit u. A. des Schlüsselmaterials abhängig - verbleibende Angriffsmöglichkeiten skizierte der Vortrag. Auch verschiedene Maßnahmen wie bspw. die *Ad-hoc Entschlüsselung* oder die *Integration eines Speichersystems für RAW-Kopien* wurden im Vortrag ebenfalls aufgezeigt.

Vergleiche DLP als Fazit

Die aufgezeigten Verfahren aus der analysierten Software bieten durchgängige Ende-zu-Ende-Verschlüsselung und eine Lösung für steigende Flut des Schlüsselmaterials. Es stellt eine Alternative dar zu etablierten Technologien wie Datenträger- und Transportverschlüsselung, die aktuell mit Software zum Sperre der Lücken in diesen Ketten eingesetzt wird (Loss/Leak/Leakage Prevention). Mangelnde Standards bzw. Kompatibilität der analysierten Software stellen derzeit ein Problem dar.

Autor/Sprecher

Herr Dennis Scherrer, BLUESITE Beratungsgesellschaft für die Informationstechnologie mbH

Quellen, weiterführende Informationen

'Datenkontrolle mit Software für Informationsrechteverwaltung' (S. 170ff) von D. Scherrer im Tagungsband der D-A-CH Security 2014, einem Kooperationspartner der TeleTrusT.

Schlüsselwörter

DRM,IRM,Informationsrechte,Richtlinie,Rechtemanagement,Schnittstellen,Vertrauen,Trust,Verschlüsseln,Entschlüsseln