

Forrester mahnt: Schützt die Daten, nicht die Infrastruktur – Doch übergreifende Standards fehlen – Anbieter kochen ihr eigenes Süppchen



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Infos entlang des Lebenszyklus verschlüsseln

Die Fusion von EMC und RSA rückt das Konzept der dokumentenzentrierten Verschlüsselung ins Rampenlicht. Eine gute Idee, loben Experten, doch der Weg zur Umsetzung ist steinig.

„Schützt die Daten, nicht die Infrastruktur“ – so fordert Forrester-Analyst Paul Stamp ein Security-Umdenken: Denn mobiles und verteiltes Arbeiten durchlöchert die gut gesicherten Firmengrenzen. Zudem würden Kunden und Gesetzgeber Unternehmen verstärkt für den Schutz wichtiger Daten verantwortlich machen.

„Und wenn eine sensible Info von einem verschlüsselten Fileserver auf ein nicht kodierte Mobilgerät übertragen wird, ist sie dort ungeschützt“, verdeutlicht Stamp. Entsprechend seien künftig datenzentrierte Konzepte nötig, bei denen Security-Attribute über den Lebenszyklus hinweg mit den Informationen verbunden bleiben.

Allerdings, kritisiert Stamp, würden heute – wenn überhaupt – nur voneinander isolierte Kryptolösungen für Datenbank, Fileserver oder Netzwerk eingesetzt. „Von den Verschlüsselungsspezialisten lebt jeder in seiner eigenen Welt“, bestätigt cirosec-Chef Stefan Strobel: „Speichernetz-Anbieter haben mit Plattenverschlüsseln oder Mail-Codierern nichts am Hut.“

Doch die Branche kommt in Bewegung: So hat RSA kürzlich eine Enterprise-Data-Protection- Initiative ins Leben gerufen. Ziel ist, Daten zu verschlüsseln, egal wo sie sitzen – in der Datenbank, auf Laptops, auf Fileservern oder im Storage.

Kern der Initiative ist ein Key Manager Partner Programm, das die firmenweite Verwaltung von Krypto-Schlüsseln vorantreiben soll. Denn der reibungslose anwendungsübergreifende Austausch von Keys ist ein Grundpfeiler für umfassende Verschlüsselungslösungen.

An Gewicht gewinnt RSAs Ansatz durch die Fusion mit Storage-Primus EMC. Denn dieser ergänzt Archiv- und Speicherlösungen sowie Content- und Information Lifecycle Management zu RSAs Produkten in Sachen Benutzeridentifizierung, Zugriffskontrolle sowie Kryptografie und Key-Management.

Doch auch Content-Spezialist Stellent hat sich mit dem digitalen Rechteevalver Sealedmedia und dem Content-Filterer Bitform beim Dokumentenschutz verstärkt.

Und Netapp/Decru arbeitet mit dem Inhalteverwalter Filenet am sicheren Enterprise Content Management. Decru steuert dabei mit den Datafort-Appliances das Krypto-Know-how bei, Filenets P8 Software das Wissen, welche Dokumente oder E-Mails wichtig sind.

Decru hat zudem wie RSA die Programmierschnittstellen seiner Lifetime Key Management 3.0 Appliance (LKM Appliance) für Drittanbieter geöffnet und schon Partner wie die Backup-Softwerker Symantec/Veritas oder Quantum gewonnen.

Wettbewerb zögert eine Öffnung hinaus

Trotz aller Versprechungen der Hersteller ist Strobel skeptisch, ob das Ziel einer lebenszyklus- und anwendungsübergreifenden Verschlüsselung erreicht werden kann: „Wenn man wirklich konsequent alle Schlüssel der verschiedenen Anwendungen und Hersteller zentral verwalten möchte, ist man wieder da, wo sich die Verfechter der Public Key Infrastrukturen schon vor ein paar Jahren die Zähne ausgebissen haben.“

Insofern hält er die Idee für theoretisch überzeugend, in der Praxis aber fragwürdig. „Zumal die isolierten Lösungen gut funktionieren und sich daher für Anbieter wie Anwender die Frage stellt, warum man das Rad neu erfinden muss.“

Zudem werde die Konkurrenzsituation Anbieter davon abhalten, sich allzu sehr zu öffnen. Entsprechend dürfte es Utimaco oder Pointsec schwer fallen, sich der zentralen Key-Verwaltung von RSA unterzuordnen. Zumal dabei auch etwa die Synchronisation von Notfallmechanismen (wie Key Recovery) für Probleme sorgen dürfte.

Rechtmanagement für Dokumente

Dem stimmt Eric Zenner als Sprecher der Fachgruppe angewandte Kryptologie in der Gesellschaft für Informatik (GI) zu: „Eine dokumentbasierte Verschlüsselung ist sicher wünschenswert, wird aber in der Praxis enorm schwierig umzusetzen sein.“ Die Probleme lägen nicht so sehr in der Verschlüsselung selbst, sondern im Rechte- und Schlüsselmanagement: „Wer darf wann was, wie werden Schlüssel verteilt, was passiert bei Änderungen (Mitarbeiterwechsel, neue Gruppenstruktur), wie sind Schlüssel-Backups geregelt etcetera.“

Zenner verdeutlicht: „Im Prinzip handelt es sich bei der Idee um ein digitales Rechtmanagement für Dokumente.“ Auch Strobel sieht eine Verwandtschaft zu den Bemühungen von Microsoft oder Dokumenten- oder Content-Verwaltern in Richtung sicheres Enterprise Rights Management (ERM). Doch Strobel mahnt: „Dazu muss das Format der Dokumente geändert werden. Und gerade in heterogenen Umgebungen könnte das zu Interoperabilitätskonflikten führen.“

Entsprechend drohe bei ERM eine zu große Abhängigkeit von einem Anbieter, so Strobel weiter: „Und Microsoft war ja noch nie dafür bekannt, die offenen Standards anderer Hersteller zu unterstützen“. Dem stimmt Zenner zu: „Um die Daten auch wirklich auf allen Plattformen verwenden zu können, wären offene Standards erforderlich – daran werden viele Hersteller nicht interessiert sein.“

Darüber hinaus führt der GI-Experte noch zwei grundsätzliche Bedenken ins Feld:

- „Eine universelle Verschlüsselungslösung wird sehr viel komplizierter als die derzeitigen maßgeschneiderten Produkte“, so Zenner. „Komplexität war aber schon immer der Todfeind der Sicherheit, weil sich leicht Fehler oder Missverständnisse einschleichen.“
- Dokumentbasierte Verschlüsselung löse nach wie vor nur das Problem, dass Unbefugte die Dokumente entschlüsseln. Zenner: „In der Praxis entstehen die Probleme aber meist durch Befugte.“ Ab

Computer Zeitung 36/2006, netigator 04.09.06