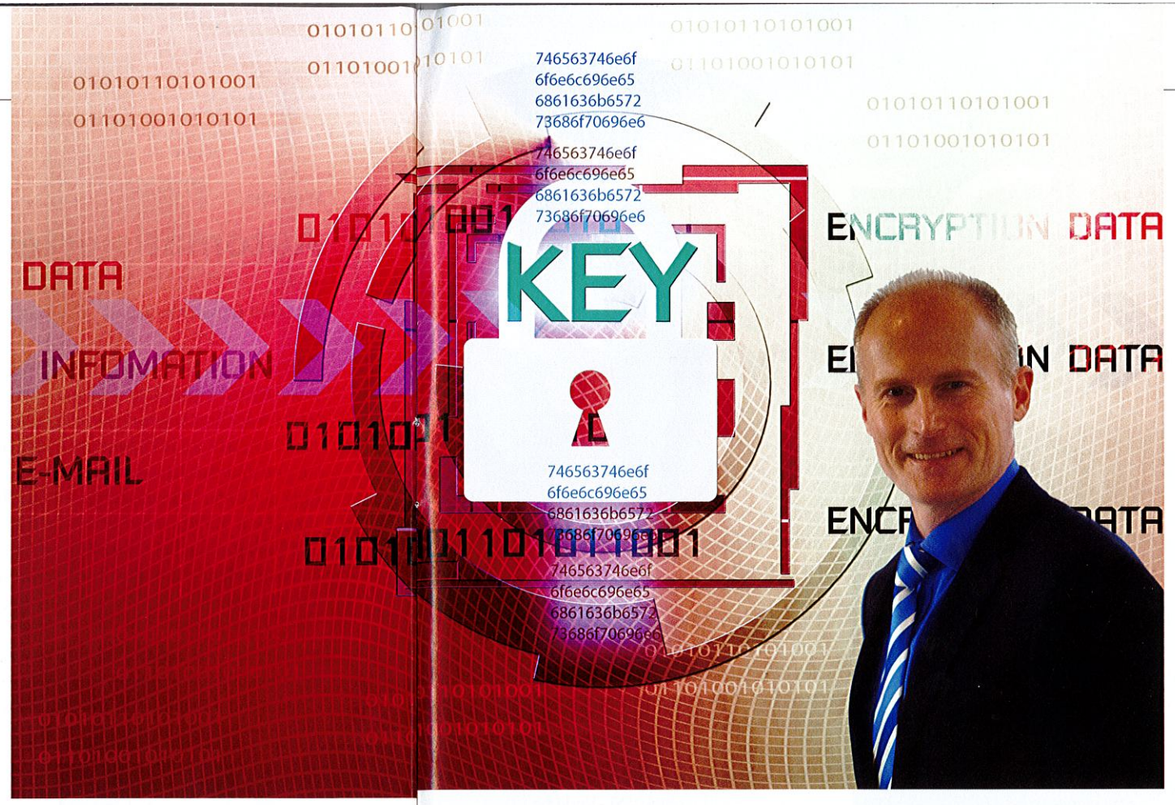
Sensible Daten auch außerhalb der SAP-Umgebung sichern

Klassifizieren, **schützen,** auditieren

Halocore for SAP Netweaver ist eine Software, die sensible Unternehmensdaten schützt, sobald sie die sichere SAP-Umgebung verlassen. Mit Hilfe von Microsofts Active Directory Rights Management Services kann das System so konfiguriert werden, dass die Daten automatisch verschlüsselt sind und nur von befugten Mitarbeitern bearbeitet, gedruckt oder weitergeleitet werden können. Ulrich Parthier sprach darüber mit Holger Hinzmann, Geschäftsführer von SECUDE.



Ulrich Parthier: *Herr Hinzmann, SECUDE hat eine Sicherheitstechnologie entwickelt, um SAP-Daten zu schützen. Sind die Daten in der SAP-Umgebung denn nicht sicher?*

Holger Hinzmann: In der SAP-Umgebung selbst sind die Daten umfangreich geschützt. Das führt aber zu einem trügerischen Sicherheitsgefühl, denn sobald ein Nutzer die Daten von SAP auf seinen Computer exportiert, verlassen sie ja die sichere SAP-Umgebung. Wenn sensible Daten wie Finanzkennzahlen, Personaldaten oder Kunden- und Verkaufsinformationen aus SAP heruntergeladen werden, liegen sie vollkommen ungeschützt auf dem Rechner und werden zum Beispiel per E-Mail an Kollegen in anderen Abteilungen oder sogar anderen Unternehmen geschickt. Sie werden ohne jegliche Sicherung auf Endgeräten gespeichert oder auf USB-Sticks transportiert.

Halocore for SAP NetWeaver verschlüsselt exportierte Daten automatisch und versieht sie mittels MS AD RMS mit einem Zugriffsschutz.

Ulrich Parthier: *Wodurch unterscheidet Halocore sich von anderen Sicherheitsprodukten?*

Holger Hinzmann: Halocore ist eine revolutionäre Technologie, weil es sich direkt in die wichtigsten Anwendungen des Benutzers einfügt. Somit schützt es sensible Daten direkt am Ort ihrer Entstehung, bei geringer Interaktion des Anwenders. Bereits beim Download von SAP zum Gerät des Nutzers greift die Software auf die Daten zu und schützt sie umfassend. Das bedeutet: Sicherheit von Anfang an und Schutz, wo auch immer sie gespeichert sind.

Ulrich Parthier: *Aber es ist doch naheliegend, die Daten von Anfang an zu schützen.*

Holger Hinzmann: Die meisten der heutzutage angebotenen Sicherheitstechnologien erkennen und sichern Daten erst am Zielpfad. Das ist gefährlich, da Informationen auf ungeschützten File-Server-Bereichen verbleiben oder über unsichere Kommunikationswege verbreitet werden können.

Ulrich Parthier: *Was passiert denn mit den Dateien, wenn sie auf mobile Geräte gezogen werden?*

Holger Hinzmann: Einmal heruntergeladene Dateien bleiben geschützt, unabhängig davon, ob sie innerhalb oder außerhalb des Unternehmens sind. Halocore schützt die Inhalte dauerhaft. Auf diese Weise ist das Risiko minimal, selbst wenn sie per E-Mail, durch Netzwerkfreigabe oder Cloud Services wie Dropbox auf die Reise gehen.

Ulrich Parthier: *Ist es für den Anwender nicht zu mühselig, jedes Mal den Schutz zu aktivieren?*

Holger Hinzmann: Wir sind zum Schluss gekommen, dass der Schutz am wirksamsten ist, wenn er automatisch und transparent für den Anwender funktioniert. Deshalb kann Halocore so konfiguriert werden, dass es den Endnutzer in seiner Arbeit nicht beeinträchtigt, sondern der Schutz automatisch greift. Nur autorisierte Mitarbeiter können darauf zugreifen und die Einstellungen ändern.

Ulrich Parthier: *Wie viel Aufwand bedeutet es für den Administrator, das Schutzprogramm zu konfigurieren?*

Holger Hinzmann: Halocore ist für die gängigsten Anwendungen vorkonfigurierbar, abhängig von Benutzerrollen, der Art der Anwendung oder dem Inhalt der herunterzuladenden Daten. Wir sind überzeugt, dass einfache Lösungen die besten sind und eine hohe Benutzerfreundlichkeit mit hoher Akzeptanz und damit einen hohen Schutz bieten.

Ulrich Parthier: *Schränkt der Schutz die Flexibilität der Benutzer ein?*

Holger Hinzmann: Der Anwender wird in seiner Arbeit nicht beeinträchtigt, da die Lösung nahezu völlig transparent arbeitet. Außerdem wird der Schutz auf jeden Dokumententyp angewendet und bietet eine genaue Kontrolle darüber, welcher Anwender die Informationen sehen, bearbeiten, drucken oder weitergeben darf.

Ulrich Parthier: *Für welche Art von Datenverkehr eignet sich der Schutz?*

Holger Hinzmann: Halocore schützt die Daten unabhängig von der Art des Datenverkehrs. Das schließt auch mobile und Cloud-Plattformen ein.

Ulrich Parthier: *Wäre es nicht am einfachsten, die Daten in der sicheren SAP-Umgebung zu belassen und eine Weitergabe oder Speicherung zu verbieten?*

Holger Hinzmann: Das ist richtig, aber hier kommen Sie in einen Konflikt zwischen Sicherheit und Produktivität. Auf der einen Seite verlangen gesetzliche und interne Anforderungen ein Höchstmaß an Datensicherheit. Auf der anderen Seite wollen Entscheidungsträger den Datenaustausch und die Zusammenarbeit zwischen Abteilungen, aber auch mit Partnern und Lieferanten ausbauen, um die Produktivität zu steigern. Die IT-Verantwortlichen sitzen zwischen beiden Stühlen und müssen eine Lösungsarchitektur entwickeln, die allen Anforderungen gerecht wird.

> „Die meisten der heutzutage angebotenen Sicherheitstechnologien erkennen und sichern Daten erst am Zielpfad. Das ist gefährlich, da Informationen auf ungeschützten File-Server-Bereichen verbleiben oder über unsichere Kommunikationswege verbreitet werden können."

Ulrich Parthier: *Müssen denn wirklich alle Daten in gleicher Weise geschützt werden?*

Holger Hinzmann: Generell sollten Unternehmensdaten geschützt werden. Die Technologien müssen jedoch intelligent sein und in die jeweilige Umgebung passen, sonst besteht das Risiko, dass Arbeitsabläufe ausgebremst oder blockiert werden. Aus diesem Grund ist Halocore for SAP NetWeaver sehr flexibel, benutzerfreundlich und durch intelligente Berechtigungsvorlagen (Security Templates) höchst sicher. Diese werden automatisch generiert und enthalten Informationen über den Nutzerkreis und dessen Rechte.

Ulrich Parthier: *Warum hat SECUDE sich für die Microsoft-Technologie entschieden?*

Holger Hinzmann: Active Directory Rights Management Services (AD RMS) von Microsoft ist der Marktführer im Bereich Dokumenten-Sicherheit. AD RMS gewährleistet, dass nur autorisierte Personen Zugriff auf bestimmte Informationen erhalten. Diese Lösung existiert zwar schon seit etwa zehn Jahren, allerdings sind Analysten überzeugt, dass diese Technologie mit MS Office 365 und dem Cloud-Ansatz in Unternehmen in Zukunft eine wichtige Rolle spielen wird, gerade mit Blick auf die aktuellen Enthüllungen im Fall Snowden.

Ulrich Parthier: *Wie funktioniert das?*

Holger Hinzmann: MS AD RMS nutzt Genehmigungen und Autorisierungen, um unbefugte Personen daran zu hindern, sensible Informationen zu bearbeiten, auszudrucken, weiterzuleiten oder zu kopieren. Der Schutz umfasst plattformübergreifend sämtliche Dateitypen: Microsoft-Office, PDF-, Bild- und Textdateien. Vor allem können Nutzer sicher innerhalb des Unternehmens wie auch mit Partnern zusammenarbeiten und Daten austauschen.

Ulrich Parthier: *Woher hat SECUDE das Know-how für SAP NetWeaver?*

Holger Hinzmann: SECUDE entwickelt seit Gründung 1996 SAP-Sicherheitslösungen. So etwa Single Sign-On, das heutige „SAP Netweaver Single Sign-On". SECUDE ist seit 2012 SAP-Partner und wurde bereits im ersten Jahr mit dem Award „SAP Innovation Partner of the Year" in der Schweiz ausgezeichnet. Damit honorierte SAP uns als innovativsten SI Value-added-Reseller Partner.

Ulrich Parthier: *Herr Hinzmann, wir danken Ihnen für das Gespräch.*

WEB-TIPP:
www.secude.de

Weiterführende Informationen:
www.it-daily.net

Whitepaper

Video

Die Buttons führen Sie in der ePaper-Version direkt zum Ziel. In der Printversion nutzen Sie bitte den QR Code.