## All-in-One-Sicherheit

# Rundumschutz

von Michael Krause


Quelle: savanno – 123RF

Wer sich die Masse der in den letzten Monaten installierten IT-Sicherheitslösungen ansieht, könnte meinen, die Verantwortlichen hätten das Motto "Viel hilft viel" ausgegeben. Das bedeutet aber keineswegs, dass die Daten dieser Unternehmen auch alle sicher sind. Tatsächlich kann die Vielfalt und -zahl der Produkten einen immensen Verwaltungsaufwand verursachen und neue Schwachstellen mit sich bringen – wichtig ist also ein ganzheitlicher Ansatz.
Wir zeigen, auf was Sie bei der Auswahl eines All-in-One-Sicherheitssystems achten sollten.

Datensicherheit ist zwar ein fester Bestandteil moderner IT-Konzepte, aber die valide Steuerung der verschiedenen Datenschutzlösungen ist aufwendig, teuer und fehleranfällig. Die zunehmende Komplexität des Datenschutzes ist eine nur schwer einzuschätzende Herausforderung. Schon heute kämpfen viele Unternehmen damit, dass ihnen die Mitarbeiter, das Know-how oder schlimmstenfalls beides fehlt. In Deutschland kommt zu dieser Problematik ein besonderer Umstand hinzu: Nach wie vor ist es üblich, dass Unternehmen Software gerne erwerben und nicht, wie in anderen Ländern üblich, mieten.

Auf den ersten Blick mag das oft unter wirtschaftlichen Aspekten sinnvoll erscheinen, weil es durchaus sein kann, dass die einmalige Investition günstiger und der ROI besser ist als das Mieten einer entsprechenden Software-as-a-Service. Wer aber genau hinschaut, wird feststellen, dass die Flexibilität dadurch massiv eingeschränkt ist. Unter Umständen liefert der Hersteller nicht mehr oder zumindest nicht schnell genug den notwendigen Schutz vor den aktuellen Bedrohungen.

### Unternehmensleitung einbeziehen

Um die Datensicherheit herzustellen, ist es vor allem wichtig, das Management mit einzubinden. Die Risiken von Cyberangriffen scheinen oft noch nicht in den Köpfen der Führungsriege verankert zu sein. Da hilft auch der aktuelle Risk Value Report von NTT nicht weiter, der besagt, dass 72 Prozent der befragten Sicherheitsbeauftragten der Meinung sind, Cybersecurity sei ein Vorstandsthema. Gleichzeitig sagen 45 Prozent, Cybersicherheit sei ein Problem der IT-Abteilung und dass diese die Herausforderung lösen müsse.

Es ist also überfällig, konkrete Ansätze zu realisieren – beispielsweise mit einem SIEM-System (Security Information and Event Management). Dieses sammelt automatisch alle in einer IT-Umgebung anfallenden Daten, analysiert sie und löst darauf basierend Aktionen aus. Das ist zwar eine Lösung des Problems – aber meist scheitert die Einführung eines solchen Systems am großen Konfigurationsaufwand. Ein derartiges Produkt könnte einem Unternehmen zwar einen Vorsprung und vor allem eine Effizienzsteigerung bieten; ist es aber lediglich vorhanden und nicht in Betrieb, hilft es auch nicht. Es besteht sogar die Gefahr, dass auf den CSO oder CIO eine Anzeige, eine Unternehmensstrafe oder Regressforderungen zukommen, weil "wider besseren Wissens" nichts unternommen wurde, um das Unternehmen besser zu schützen.

### Sicherheitsansätze hinterfragen

Immer wieder zeigt sich, dass Endgerätesicherheit nur mit einem ganzheitlichen Ansatz praktikabel und erfolgreich umgesetzt werden kann. Im Zentrum derartiger Konzepte steht die Konsolidierung der bestehenden Sicherheitssysteme. Nur wer so mutig ist, vorhandene Sicherheitswerkzeuge ernsthaft zu hinterfragen, wird problematische Überschneidungen oder versteckte Lücken zwischen den Systemen entdecken.

Der Grund, warum an dieser Stelle so viele Projekte scheitern ist, dass sich die Verantwortlichen nicht genügend Zeit nehmen, bestehende Security-Systeme zu analysieren und gegebenenfalls Neue zu implementieren. Das Problem ist, dass die Aufgaben, die sie bewältigen müssen, immer mehr und schwieriger werden und die Zeit knapper. Da die Bedrohungen weiter zunehmen, muss aber dringend gehandelt werden.

### Mehr Sicherheit mit dem CAFE-Prinzip

Grundsätzlich sind diese Bereiche gefährdet: klassische Computer, Mobilgeräte sowie Cloudservices. Die Bedrohungen, denen sie ausgesetzt sind, kommen sowohl von innen als auch von außen. Eine moderne Endpoint-Security kann helfen,

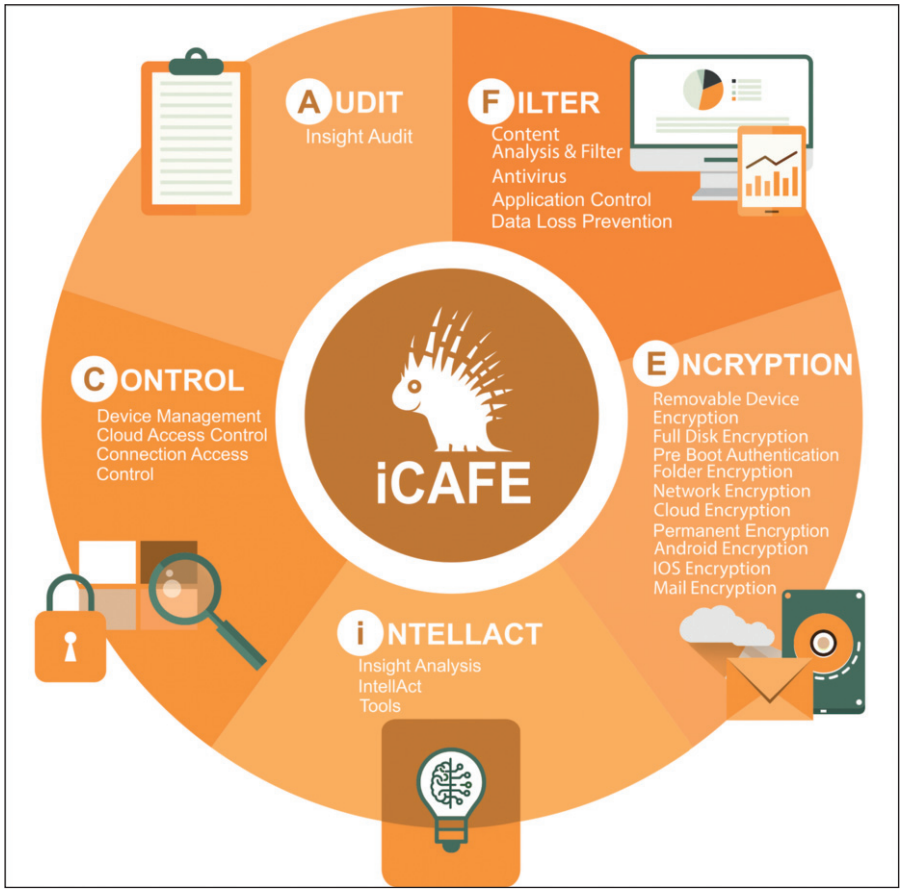


Bild 1: Wer bei der Absicherung heterogener Landschaften erfolgreich sein will, der sollte nach dem CAFE-Prinzip agieren: Control – Audit – Filter – Encryption.

diesen Teufelskreis zu durchbrechen und das große Ganze zu schützen. Solche All-in-One-Produkte funktionieren nach den vier Konzepten des CAFE-Prinzips:

- Control: Es wird definiert und kontrolliert, welche Datenwege jemand benutzen darf und wer auf sensible Daten Zugriff hat.
- Audit: Durch das Protokollieren von Verstößen erfolgt eine konsequente Sensibilisierung und der Grundstein für einen zunehmend bewussten Umgang mit den Daten wird gelegt – eine wichtige Voraussetzung für IT-Compliance.
- Filter: Ein Filter separiert kritische Datentypen, blockiert diese und sorgt so für mehr Schutz.
- Encryption: Wird durch die ersten drei Punkte sichergestellt, dass ausschließlich berechtigte Mitarbeiter auf Daten und Applikationen zugreifen können, die für ihre Arbeit wirklich relevant sind, werden diese Daten dann auch noch verschlüsselt, sodass ein Rundumschutz – auch gegenüber vorsätzlichem Datendiebstahl oder fahrlässigem Datenverlust – entsteht.

So entsteht ein Gesamtkonzept, dass sich einfach und ohne etablierte Arbeitsabläufe zu verändern, implementieren lässt. Mit einer solchen Endpoint-Security lassen sich Attacken, Schwachstellen oder Bedrohungen besser identifizieren und rechtzeitig Schutzmaßnahmen ergreifen.

Bei der Auswahl der passenden Security-Angebote sollten die Verantwortlichen auf folgende Aspekte besonders achten:

- Schutz vor Datenverlust: Datenverlust kann nur gelingen, indem Dateien auf Endgeräten nach vorgegebenen Inhalten und Schlagworten durchsucht werden und deren Weitergabe blockiert wird.
- Sicherheitsprüfung: Mit der richtigen Sicherheitsprüfung lassen sich Datenflüsse visualisieren und potenzielle Schwachstellen identifizieren, um gefährliche Entwicklungen rechtzeitig abzuwenden.
- Verschlüsselung: Die Verschlüsselung sorgt dafür, dass nur berechtigte Personen Zugriff auf Speichermedien, Verzeichnisse, Clouds, Festplatten oder Dateien haben.
- Usability: Nichts ist schlimmer als eine Software, die keiner bedienen will oder kann. Aus diesem Grund spielt bei der Auswahl auch die Bedienungsfreundlichkeit des Security-Produkts eine wichtige Rolle.

Auf diese Features sollte der IT-Verantwortliche bei der Auswahl des passenden Angebots achten:

- Access Control: Die Zugangskontrolle verwaltet die Nutzung von Geräten an Schnittstellen von Endpoints. Sie sorgt für eine getrennte Zugriffsverwaltung für den Online- und Offline-Betrieb, unterstützt merkmalbasierte Freigaben, kontrolliert Tastatur, Maus und Netzwerkverbindungen und verfügt über Filterfunktionen, mit denen sich bestimmte Datenformate blockieren lassen.
- Application Control: Moderne Endpoint-Security verfügt über eine Applikationskontrolle, die verhindert, dass Schadsoftware durch unkontrollierte Installationen ins Netzwerk gelangt. Dieser Filter sorgt außerdem dafür, dass keine unlizenzierten Softwareprodukte genutzt werden können.
- Analytics: Der Kontrollmechanismus überprüft die Datenflüsse innerhalb eines Netzwerks und leitet im Bedarfsfall automatisch passende Schutzmaßnahmen ein. Relevante Vorgänge werden grafisch und tabellarisch aufbereitet, sodass entsprechende Analysen erfolgen können.
- Antivirenscanner und mehr: Ein Antivirus-Management gehört ebenso zur Basisausstattung einer Endpoint-Security wie auch ein Passwortmanager und -container, ein BitLocker-Management sowie eine Funktion zum sicheren Löschen von Daten.

## Fazit

Schwachstellen und neuralgische Sicherheitspunkte lassen sich zwar mit modernen Endpoint-Security-Produkten schützen, aber Voraussetzung für ein jedes Sicherheitskonzept ist und bleibt die Einbindung der Menschen – von der Chefetage über den Administrator bis hin zum Anwender. Nur wenn parallel zur Einführung des CAFE-Prinzips auch intensive und nachhaltige Aufklärungsarbeit betrieben wird, lässt sich eine solide Basis für ein sicheres Business legen. *(jm)*