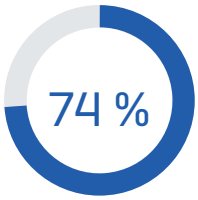
SOPHOS
Security made simple.

Dem Code auf der Spur: Verschlüsselungs-technologien einfach erklärt

Von **Anthony Merry**, Director of Product Management, Data Protection

Für den Erfolg eines Unternehmens ist zunehmend eine effektive Datennutzung und -verwaltung entscheidend. Ob es darum geht, den Umsatz oder den Gewinn zu steigern: Unternehmen benötigen Daten, um Verkäufe und Produktinnovationen voranzutreiben, Kunden gezielt anzusprechen und einen Wettbewerbsvorteil zu erlangen. Unternehmensdaten sind wertvoll – doch in den falschen Händen können sie viel Schaden anrichten.

Datenpannen machen heutzutage praktisch täglich Schlagzeilen. Tatsächlich zielt jedoch nur ein kleiner Prozentsatz aller Cyberangriffe auf Großunternehmen ab. Kleine und mittelständische Unternehmen dürfen sich nicht in Sicherheit wiegen. Mehr als 700 Mio. Datensätze wurden 2014 kompromittiert und 53 % der bestätigten Datenverluste geschahen einem Bericht von Verizon[1] zufolge in Unternehmen mit weniger als 1.000 Benutzern*. Kein Unternehmen und keine Einrichtung weltweit ist immun gegen Datenverluste – unabhängig von Standort, Größe und Branche.



aller Kleinunternehmen hatten 2015 eine Sicherheitspanne[2]

IT Security konzentriert sich größtenteils auf den Schutz materieller Gegenstände – Server, Desktops und Laptops, mobile Geräte – Unternehmen dürfen jedoch den Schutz der auf diesen Geräten gespeicherten Daten nicht außer Acht lassen. Vor dem Hintergrund des stetig wachsenden Datenvolumens und der Notwendigkeit, jederzeit und von überall auf Daten zugreifen zu können, kristallisieren sich Verschlüsselungstechnologien zunehmend als entscheidende Grundlage für eine erfolgreiche Sicherheitsstrategie heraus.

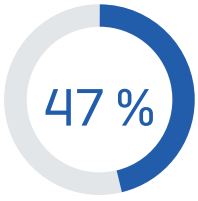
Trotz der knallharten Fakten in Form von verheerenden Datenpannen und Datenverlusten scheuen viele Unternehmen nach wie vor die Implementierung einer Verschlüsselung. Warum? Teilweise, weil das Thema Verschlüsselung seit langem von Mythen umrankt ist:

- Die Installation und Verwaltung einer Verschlüsselung ist zu kompliziert
- Eine Verschlüsselung beeinträchtigt die Performance von Laptops, Desktops, Servern und Anwendungen

Zusätzlich zu diesen gängigen Mythen sind die Anforderungen für die Implementierung eines Datenschutzplans oft alles andere als eindeutig, wie die folgenden Beispiele zeigen:

- Müssen Sie überall dort verschlüsseln, wo sich Daten befinden – auf Laufwerken, in Dateien, Ordnern, auf Wechselmedien, mobilen Geräten und in Cloud-Speichern?
- Welche Best Practices sind bei der Implementierung einer Verschlüsselung zu beachten?
- Wie können Sie alle wichtigen Daten schützen, ohne die Unternehmensproduktivität zu beeinträchtigen?

Mit diesem Whitepaper möchten wir Bedenken und Missverständnisse rund um das Thema Verschlüsselung ausräumen. Wir zeigen, wie Unternehmen eine Verschlüsselungsstrategie einfach, praktisch und realisierbar umsetzen. Zu Beginn räumen wir erst einmal mit einigen Mythen auf, die sich hartnäckig halten.



aller Datenpannen sind auf böswillige/ kriminelle Angriffe zurückzuführen – im Vorjahr lag der Anteil noch bei 42 %[3]

Mythen zum Thema Verschlüsselung

Mythos: Nur Unternehmen, die spezielle Compliance-Vorgaben erfüllen müssen und gesetzlich zur Verschlüsselung verpflichtet sind, müssen ihre Daten verschlüsseln.

Wahrheit: Daten sind für alle Unternehmen wertvoll und müssen geschützt werden. Gute Beispiele sind Kundendaten (Namen, E-Mails, Kreditkartendaten), interne Finanz- und Wettbewerbsdaten, Mitarbeiterdaten oder geistiges Eigentum. Oder einfach gesagt: Daten sind Ihr Kapital und müssen daher unbedingt geschützt werden. Unternehmen sollten sensible Daten grundsätzlich verschlüsseln – unabhängig davon, ob sie rechtlich dazu verpflichtet sind oder nicht.

*Falls Unternehmensgröße bekannt

Mythos: Eine Verschlüsselung ist zu kompliziert und erfordert zu viele Ressourcen.

Wahrheit: Die Implementierung und Verwaltung einer Datenverschlüsselung kann ganz einfach sein. Sie müssen im Grunde nur verstehen, welche Arten von Daten Sie verschlüsseln müssen, wo diese sich befinden und wer Zugriff haben sollte. Und wenn Sie sich für eine Next-Gen-Verschlüsselungslösung entscheiden, die alle Dateien standardmäßig verschlüsselt, wird es für alle Beteiligten noch einfacher.

Mythos: Eine Verschlüsselung ist Gift für die Performance von Datenbanken und Anwendungen.

Wahrheit: Die Performance von Anwendungen, Datenbanken, Servern und Netzwerken hat für die IT-Abteilung und die Enduser höchste Priorität. Bei einer ordnungsgemäßen Konzeption und Implementierung kann eine Verschlüsselung nicht nur kritische Daten auf diesen Systemen schützen, sondern auch nahezu unbemerkt von den Benutzern und ohne Beeinträchtigung der Produktivität im Hintergrund ausgeführt werden.

Mythos: Eine Verschlüsselung macht in der Cloud gespeicherte Daten nicht sicherer.

Wahrheit: Verschlüsselte Daten in der Cloud zu speichern, ist sicherer, als nicht verschlüsselte Daten in der Cloud zu speichern. Wissen Sie, wo Cloud-Daten gespeichert werden? Wer hat wirklich Zugriff? Die Antworten auf diese Fragen unterstreichen die Tatsache, dass alle an die Cloud gesendeten Dateien verschlüsselt und Sie die Kontrolle über die Schlüssel haben sollten.

Mythos: Die Verschlüsselung von Daten ist wichtiger als die Schlüsselverwaltung.

Wahrheit: Eine Verschlüsselung ohne sorgfältige Schlüsselverwaltung ist sinnlos. Zu viele Unternehmen versagen bei der Verwaltung ihrer Schlüssel. Entweder speichern sie die Schlüssel auf demselben Server wie die verschlüsselten Daten oder sie betrauen einen Cloud-Anbieter mit der Verwaltung. Das ist in etwa so, als würden Sie Ihre Haustür abschließen und dann den Schlüssel im Schloss stecken lassen.

Mythos: Verschlüsselte Daten können nicht gestohlen werden.

Wahrheit: Eine Verschlüsselung verhindert keinen Datenverlust oder -diebstahl. Aber sie schützt Daten, indem sie diese unleserlich und unbrauchbar macht. Entscheiden Sie sich für eine Verschlüsselungslösung, mit der Sie nachweisen können, dass Ihre Daten tatsächlich verschlüsselt wurden.

Verschlüsselung – das Funktionsprinzip

Unter Verschlüsselung versteht man eine Methode, mit der Daten in ein für unbefugte Benutzer unleserliches Format umgewandelt werden. Kryptografie – die Wissenschaft, die sich hinter der Verschlüsselung verbirgt – nutzt Algorithmen, die lesbare Daten (Klartext) in einen Geheimtext (auch: „Chiffrat") umwandelt.

Ohne zu sehr ins Detail zu gehen, ist es hilfreich, sich den Verschlüsselungsvorgang folgendermaßen vorzustellen: Wenn Sie Daten verschlüsseln, ist das in etwa so, als würden Sie Ihr Erspartes in einem Safe verwahren – Sie benötigen einen Schlüssel, um den Safe zu öffnen und an das Geld zu gelangen.

Es gibt verschiedenste Anwendungsfälle für Verschlüsselungstechnologien. Für Unternehmen, die sich vor Datenverlusten schützen möchten, sind im Wesentlichen jedoch zwei Formen relevant: Festplattenverschlüsselung und Dateiverschlüsselung.

Festplattenverschlüsselung
Unter Festplattenverschlüsselung versteht man die Verschlüsselung einer gesamten Festplatte (nicht nur bestimmter Dateien) auf Sektorebene unter dem Dateisystem. Mit anderen Worten: Alle Daten der physischen Festplatte Ihres Geräts werden verschlüsselt.

Eine Festplattenverschlüsselung bietet den besten Schutz, wenn das Gerät ausgeschaltet ist (nicht eingeschaltet oder im Energiesparmodus). Man spricht auch von „Data at Rest"-Schutz. Eine Festplattenverschlüsselung gilt im Rahmen Ihrer Datenschutzstrategie als erste Verteidigungslinie und soll hauptsächlich sicherstellen, dass Ihre Daten sicher bleiben, wenn ein Gerät verloren geht oder gestohlen wird.

Bei einer Festplattenverschlüsselung werden alle Dateien, die Sie auf einem Computer oder digitalen Gerät speichern, automatisch verschlüsselt (geschützt). Sobald eine Datei jedoch die Festplatte verlässt (z. B. durch Versenden per E-Mail oder Kopieren auf Wechselmedien/in die Cloud), greift der Schutz der Festplattenverschlüsselung nicht mehr.

Dateiverschlüsselung
Bei einer Dateiverschlüsselung werden nur bestimmte Dateien verschlüsselt. Stellen Sie sich vor, Sie haben zwei Dokumente auf Ihrem Computer. Sie können sich entscheiden, nur eine dieser Dateien zu verschlüsseln. Im Gegensatz zu einer Festplattenverschlüsselung, die automatisch alle auf die Festplatte geschriebenen Daten verschlüsselt, müssen Sie bei einer Dateiverschlüsselung Regeln und Richtlinien erstellen, die festzulegen, welche Arten von Dateien verschlüsselt werden sollen.

Im Gegensatz zur Festplattenverschlüsselung bleiben die Dateien auch dann verschlüsselt, wenn sie die Festplatte oder das Gerät verlassen. Sie können eine verschlüsselte Datei also per E-Mail versenden, ohne deren Sicherheit zu gefährden. Dasselbe gilt, wenn Sie eine verschlüsselte Datei auf Wechselmedien oder in die Cloud übertragen. Man spricht in diesem Fall auch manchmal von „Data in Use" oder „Data in Transit".

Bei einer Dateiverschlüsselung sollten Sie zur Vereinfachung Regeln erstellen – beispielsweise könnten Sie vorschreiben, dass alle Word-Dokumente, nicht jedoch Bilder, standardmäßig verschlüsselt werden sollen.

Moderne Next-Gen-Verschlüsselungslösungen propagieren das Prinzip der immer aktiven Verschlüsselung. Im Klartext bedeutet das, dass alle Dateien automatisch und standardmäßig verschlüsselt werden. Benutzer werden damit von der Last befreit, selbst entscheiden zu müssen, welche Daten eine Verschlüsselung benötigen. D. h. standardmäßig sind alle Dateien sicher verschlüsselt und können bei Bedarf manuell entschlüsselt werden.

Implementierung einer Verschlüsselungsstrategie

Einem Bericht des Ponemon Institute[4] zufolge gaben Befragte als größte Herausforderungen bei der Planung und Ausführung einer Datenverschlüsselungsstrategie Folgende an:

56 %	Ermittlung der Speicherorte sensibler Daten innerhalb des Unternehmens
34 %	Klassifizierung der zu verschlüsselnden Daten
15 %	Aufklärung der Benutzer über die richtige Nutzung der Verschlüsselung

Eine Verschlüsselung bildet das Fundament einer jeden Datenschutzstrategie. Bevor Sie Ihre Strategie in die Tat umsetzen können, müssen Sie jedoch die folgenden Fragen beantworten:

1. **Wie sieht der Datenfluss in und aus meinem Unternehmen aus?** Erhalten Sie E-Mails mit Dateianhängen oder schicken Sie solche E-Mails? Erhalten Sie Daten auf USB-Sticks oder anderen Wechselmedien? Wie speichert und tauscht Ihr Unternehmen große Datenmengen intern und extern aus? Nutzen Sie cloudbasierte Speicher wie Dropbox, Box oder OneDrive? Kommen mobile Geräte und Tablets zum Einsatz? Einer Umfrage von Sophos zufolge besitzt der durchschnittliche Technologie-Nutzer 2,9 Geräte. Wie behalten Sie die Kontrolle über die Vielzahl von Geräten, die Zugriff auf Unternehmensdaten haben? Sie sollten nach einer Verschlüsselungslösung suchen, die sich auf die Datennutzung und Datenbewegeungen in Ihrem Unternehmen anpassen lässt.

   Anwendungsfall: Immer mehr KMUs speichern Daten in der Cloud. Deshalb benötigen Sie eine Lösung, die den cloudbasierten Datenaustausch sicher gestaltet und ermöglicht, dass Sie Ihre Schlüssel selbst verwalten.

   Sie brauchen eine Datenverschlüsselungslösung, die Ihre Daten überall dort schützt, wo Benutzer auf diese zugreifen müssen – ohne den Vorgang für die Enduser unnötig kompliziert zu gestalten. Die Lösung muss als eine Art „Schutzengel" fungieren, der vom Benutzer unbemerkt im Hintergrund agiert.

2. **Wie nutzen mein Unternehmen und meine Mitarbeiter Daten?** Wie sehen die Arbeitsabläufe aus und wie werden alltägliche Aufgaben produktiver gestaltet? Welche Hilfsmittel, Geräte und Anwendungen werden verwendet und stellen diese möglicherweise eine Quelle für Datenverluste dar?

3. **Wer hat Zugriff auf meine Daten?** Dieser Punkt ist sowohl aus ethischer als auch aus regulatorischer Sicht entscheidend. In manchen Fällen sollten Benutzer aus ethischen Gründen keinen Zugang zu bestimmten Daten (z. B.Personal- und Gehaltsdaten) erhalten. Zudem gibt es Datenschutzrechte, die vorschreiben, dass nur diejenigen Personen Zugriff auf Daten erhalten sollten, die diese Daten zur Erledigung ihrer Arbeit benötigen. Allen anderen Personen sollte der Zugriff verwehrt werden.

Haben Ihre Mitarbeiter lediglich Zugriff auf die Daten, die sie für ihre Arbeit benötigen, oder haben sie auch Zugriff auf nicht benötigte Daten?

Anwendungsfall: IT-Administratoren haben in der Regel unbeschränkten Zugriff auf Daten und die IT-Infrastruktur. Benötigt der IT-Administrator jedoch Zugriff auf die Personaldaten aller Mitarbeiter oder auf Dokumente der Rechtsabteilung zu aktuellen Gerichtsverfahren? Sollten Mitarbeiter einer Aktiengesellschaft, die nicht der Finanzabteilung angehören, Zugriff auf aktuelle Geschäftszahlen haben?

4. **Wo befinden sich meine Daten?** An zentraler Stelle und überwiegend in einem Rechenzentrum? Komplett in der Cloud gehostet? Gespeichert auf Laptops und mobilen Geräten Ihrer Mitarbeiter? Einer Umfrage von Tech Pro Research zufolge erlauben 74 % aller Unternehmen ihren Mitarbeitern, private Geräte zur beruflichen Nutzung mit ins Büro zu bringen (BYOD), oder planen dies für die Zukunft. Außerdem nehmen die Mitarbeiter oft auch ihre Arbeit mit nach Hause oder arbeiten von unterwegs. Sie führen sensible Unternehmensdaten auf ihren Geräten mit sich und erhöhen damit das Risiko von Datenlecks und Compliance-Verstößen. Stellen Sie sich vor, wie einfach es wäre, auf vertrauliche Daten über Ihr Unternehmen zuzugreifen, wenn das Smartphone eines Mitarbeiters verloren ginge oder gestohlen würde.

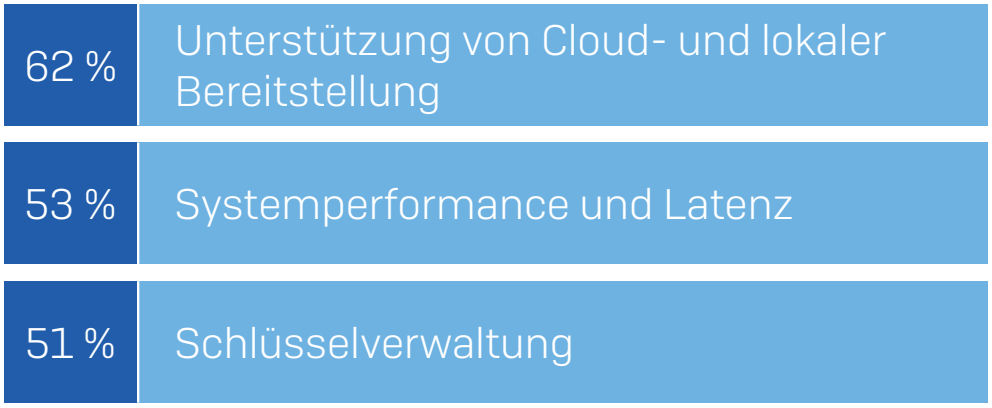
Jedes Unternehmen ist anders. Daher gibt es auch nicht DIE EINE Datenschutzstrategie, die für jedes Unternehmen geeignet ist. Ihr Datenschutzplan muss auf Ihr Unternehmen, die Beschaffenheit der in Ihrem Unternehmen generierten und verwendeten Daten, lokale bzw. branchenspezifische Vorschriften und die Größe Ihres Unternehmens ausgelegt sein.

Sie müssen also viele Entscheidungen speziell für Ihr Unternehmen treffen. Nur eines gilt für alle Unternehmen gleichermaßen – Sie müssen Ihre Mitarbeiter aufklären.

Mitarbeiter müssen verstehen, wie sie einen klar definierten Datenschutzplan einhalten und die Verschlüsselung anwenden. Sie müssen explizit darüber aufgeklärt werden, auf welche Daten sie Zugriff haben, wie sie auf diese Daten zugreifen dürfen und wie sie die Daten schützen können. Und am wichtigsten: Sie müssen die Verschlüsselung so gestalten und verwalten, dass sie die betrieblichen Arbeitsabläufe nicht beeinträchtigt. Viele Personen tun sich von Natur aus schwer mit Veränderungen. Ihr Datenschutzplan sollte daher Aufklärung und Training vorsehen.

Wahl einer Lösung

In einer Studie des Ponemon Institute wurden als wichtigste Features von Verschlüsselungstechnologielösungen folgende genannt[5]:



Im Folgenden finden Sie eine Reihe wichtiger Punkte, die Sie bei der Wahl einer Verschlüsselungslösung für Ihr Unternehmen beachten sollten:

Benutzerfreundlichkeit: Eine Verschlüsselung muss einfach und gleichzeitig umfassend sein. Ihr Verschlüsselungsprodukt sollte sich einfach einrichten und bereitstellen lassen und über eine intuitive Management-Konsole verfügen.

Plattformunabhängigkeit: Suchen Sie nach einer Lösung, die alle Verschlüsselungsformen, einschließlich Festplatten- und Dateiverschlüsselung, auf verschiedensten Betriebssystemen wie Windows, Mac, Android und iOS ermöglicht.

Anpassungsfähigkeit: Ideal wäre eine Lösung, die Ihre Daten ohne Beeinträchtigung der Unternehmens-Workflows und Produktivität schützt. Ihre Verschlüsselungslösung sollte sich an den Workflow Ihres Unternehmens anpassen und nicht umgekehrt.

Unabhängige Empfehlung: Stellen Sie in jedem Fall sicher, dass der von Ihnen gewählte Verschlüsselungsanbieter umfangreichen Support bietet und von Branchenanalysten, Testern und Kunden empfohlen wird.

Skalierbarkeit: Sie möchten höchstwahrscheinlich, dass Ihr Unternehmen in Zukunft weiter wächst. Sie benötigen deshalb eine Lösung, die sich parallel zu Ihrem Unternehmen skalieren lässt. Außerdem sollte die Lösung eine einfache Schlüsselverwaltung und Durchsetzung Ihrer Datenschutzrichtlinie ermöglichen.

Compliance-Nachweis: Im Ernstfall müssen Sie nachweisen können, dass Ihre Daten geschützt waren. Wenn Sie in einer Branche oder Region tätig sind, in der besondere Datenschutzgesetze oder -vorschriften gelten, müssen Sie gegenüber Auditoren nachweisen können, dass die Daten verschlüsselt waren.

Sophos SafeGuard Encryption

Sophos SafeGuard ist die vielfach ausgezeichnete Next-Gen-Encryption-Lösung von Sophos. Sophos SafeGuard ist **immer aktiv** und verschlüsselt Daten sofort bei deren Erstellung. Ihre Ausgangsposition ist also in jedem Fall sicher. **Synchronized Encryption** schützt Ihre Daten proaktiv, indem kontinuierlich die Benutzer-, Anwendungs- und Sicherheitsintegrität eines Geräts geprüft wird, bevor auf verschlüsselte Daten zugegriffen werden darf. All dies geschieht **transparent** für die Benutzer, damit eine nahtlose und sichere Zusammenarbeit gewährleistet ist. Mit Sophos SafeGuard wird es auch einfach, die Einhaltung von Datenschutzvorschriften sicherzustellen, ohne die Produktivität zu gefährden.

Sophos SafeGuard ist die derzeit beste Verschlüsselungslösung auf dem Markt:

- Gartner Magic Quadrant Leader seit 7 Jahren[6]
- Unabhängige Tests zeigen, dass Sophos Encryption schneller ist und die Performance am wenigsten beeinträchtigt

Weitere Informationen unter www.sophos.de/encryption

Fazit

Viele Unternehmen entscheiden sich gegen eine flächendeckende Verschlüsselung, weil sie denken, diese sei zu kompliziert. Dabei lässt sich eine Verschlüsselung recht einfach implementieren, und sie lohnt sich: Wenn Ihre Daten verschlüsselt sind, bleiben sie bei Verlust oder Diebstahl für Unbefugte unleserlich und damit unbrauchbar.

Verschlüsselungslösungen waren noch nie so wichtig wie heute. Mobile Mitarbeiter, immer perfidere Cyberkriminalität und der wachsende Schwarzmarkt für Daten sorgen dafür, dass sensible Daten gefährdeter sind denn je.

Für die Implementierung einer verschlüsselungsbasierten Datenschutzstrategie müssen Sie zunächst verstehen, warum Sie eine Verschlüsselung benötigen und welche Vorteile Sie Ihnen bringt. Durch die Implementierung einer einfachen Verschlüsselungslösung können Sie sicher sein, dass Ihre Daten immer zuverlässig geschützt sind.

Disclaimer

Gartner befürwortet in seinen Forschungsbeiträgen keine bestimmten Hersteller, Produkte oder Dienstleistungen und rät Technologie-Nutzern nicht ausschließlich zu Anbietern mit besten Bewertungen. Forschungsbeiträge von Gartner sind als Meinungsäußerungen des Gartner Forschungsinstituts einzustufen und in keinem Fall als Tatsachenfeststellung zu werten. Gartner übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

1. Verizon. (2015). 2015 Data Breach Investigations Report
2. PwC. (2015). 2015 Information Security Breaches Survey
3. Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis
4. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
5. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
6. Gartner Magic Quadrant for Mobile Data Protection, John Girard, 8. Oktober 2015

Mehr erfahren

Weitere Informationen über Sophos SafeGuard unter www.sophos.de/encryption

Preisanfrage

Unverbindliches Angebot anfordern

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

16-10-21 WPDE (DD-2467)

SOPHOS