SOPHOS
Security made simple.

Verschlüsselungstechnologien: So meistern Sie die Implementierung erfolgreich

Guide zur Entwicklung einer erfolgreichen Verschlüsselungsstrategie

Sie haben hin- und herüberlegt, die Vor- und Nachteile abgewogen und sind zu dem Schluss gekommen: Damit Ihre Daten wirklich sicher bleiben, braucht Ihr Unternehmen eine Verschlüsselung. Aber was nun? Das Angebot an Verschlüsselungstechnologien ist groß, aber was ist die beste und sicherste Methode zur Implementierung einer Verschlüsselung, ohne die Arbeitsabläufe und Effektivität Ihrer Benutzer zu beeinträchtigen?

Kurzfassung

Auf eine Verschlüsselung kann heutzutage nicht mehr verzichtet werden. Oft ist eine Verschlüsselung sogar gesetzlich oder von Seiten bestimmter Branchen vorgeschrieben. Unternehmen, die solche Gesetze und Vorschriften ignorieren, droht der finanzielle Ruin – schließlich werden durch mangelnde Verschlüsselung verursachte Datenpannen nicht selten mit hohen Geldstrafen geahndet. Zudem sind Datendiebstähle und -verluste zurzeit eine der größten Gefahren für Unternehmen. Der Schutz Ihrer Daten ist nicht nur eine Verpflichtung gegenüber Ihren Kunden, Partnern und Mitarbeitern, sondern kann in Ihrer Branche auch einen Wettbewerbsvorteil bedeuten.

Selbst eingefleischte Sicherheitsexperten haben jedoch Respekt vor der Implementierung von Verschlüsselungsverfahren. Die Verschlüsslung von Daten gilt als schwierige Aufgabe, die kompliziert genug ist, um Workflows zu beeinträchtigen, und durch die Nutzung mobiler Geräte und die Cloud noch weiter verkompliziert wird.

In diesem Guide verraten wir Ihnen, wie Sie eine Verschlüsselungsstrategie umsetzen, mit der Sie die Daten Ihres Unternehmens in der Ära von Cloud Computing und mobilen Geräten effizient schützen, komplexe Vorgänge auf ein Minimum reduzieren und die Produktivität der Benutzer aufrechterhalten.

Im Folgenden erklären wir Ihnen Schritt für Schritt, wie Sie hierzu vorgehen müssen.

Schritt 1: Grundsätzliche Überlegungen

Jedes Unternehmen ist anders; dementsprechend wird sich auch eine Datenschutzrichtlinie von Unternehmen zu Unternehmen unterscheiden. Die Datenschutzanforderungen eines kleinen Lieferanten unterscheiden sich erheblich von denen eines multinationalen Großkonzerns. Opfer einer Datenpanne kann aber jeder werden.

Daten sind wertvoll. Kreditkartendaten, Patientenakten, Geschäftsberichte: Sie allen können gestohlen und gewinnbringend verkauft werden.

Datendieben bieten sich für ihre kriminelle Machenschaften zahlreiche Möglichkeiten: zum Beispiel Hacking, gezielte Angriffe und Malware. Gleichzeitig ist und bleibt menschliches Versagen ein Haupt-Risikofaktor für Datenpannen und lässt sich oft genauso schwer verhindern wie die Angriffe selbst.

Wir sind alle nur Menschen und wir alle machen Fehler. Wer hat nicht schon einmal einen Dateianhang an den falschen Empfänger geschickt? Täglich werden Telefone oder andere mobile Geräte an der Sicherheitskontrolle am Flughafen liegengelassen. Cyberkriminellen gelingt es mit Phishing, Zugangsdaten zu stehlen, weil nicht jeder von uns immer und überall zu 100 % wachsam sein kann. Leider kann jedoch jede noch so kleine Unachtsamkeit leicht zu einer Datenpanne führen.

Die meisten von uns wissen, dass sie eine Lösung benötigen, um diese Risiken in den Griff zu bekommen. Aber wo sollten Sie am besten ansetzen?

Schritt 2: Audit

Wissen Sie, wo sich Ihre Daten befinden?

In den meisten Unternehmen, ob groß oder klein, lautet die Antwort: im Prinzip überall. Auf den Laptops und Desktop-PCs Ihrer Mitarbeiter und immer häufiger auch auf deren Smartphones und Tablets. Mitarbeiter nutzen zur internen und externen Zusammenarbeit cloudbasierte Lösungen wie Dropbox und Box. Für sie ist es praktisch, überall auf Daten zugreifen zu können. Das bedeutet aber auch, dass Ihre Daten sich überall befinden können – nämlich auf jedem Gerät Ihrer Mitarbeiter. Hierbei haben wir noch nicht einmal die Daten miteinbezogen, die sich auf Ihren Unternehmensservern vor Ort und in Ihren Cloud-Rechenzentren befinden.

Berücksichtigen Sie bei der Planung Ihrer Verschlüsselungsstrategie alle Arbeitssituationen. Überlegen Sie, wie sich die Verschlüsselung auf die Speicherung, den Zugriff und den Austausch Ihrer Daten über alle Geräte und Plattformen hinweg auswirken würde.

Prüfen Sie außerdem, welche regulatorischen Vorgaben Sie beachten müssen. Gelten in Ihrer Branche spezielle Datenschutzgesetze? Gibt es spezielle Gesetze auf Bundes- und Landesebene? Außerdem müssen alle Unternehmen, die Daten über Bürger der Europäischen Union vorhalten, die Datenschutz-Grundverordnung der Europäischen Union befolgen. Je besser Sie sich mit den geltenden Gesetzen und Vorschriften vertraut machen, desto leichter wird es Ihnen fallen, Ihren eigenen Datenschutzplan zu entwickeln.

Was, wenn das Undenkbare passiert? Wie reagieren Sie, wenn Sie eine Datenpanne entdecken oder unverschlüsselte Daten massenhaft aus Ihrem Unternehmen gelangt sind? Sie benötigen eine Lösung, die den „Übeltäter" nicht nur schnell findet, sondern auch Informationen dazu liefert, welche Daten verloren gegangen sind.

Fünf wichtige Fragen

Sie fühlen sich überfordert? Das ist verständlich. Einige Berater empfehlen vor der Einführung einer Verschlüsselung eine Umstrukturierung der Workflows und ausführliche Implementierungspläne: Es gibt jedoch Möglichkeiten, eine Verschlüsselung auch ohne weitere, oft unnötige Änderungen der Workflows zu implementieren. Stellen Sie sich zunächst die folgenden fünf Fragen zur Verarbeitung sensibler Daten in Ihrem Unternehmen:

1. Wie fließen Daten ins Unternehmen? (Werden sie intern erstellt?)
2. Wie fließen Daten aus dem Unternehmen?
3. Wo werden die Daten gespeichert?
4. Wer hat Zugriff auf die Daten?
5. Wie nutzen Mitarbeiter Daten in ihrem Arbeitsalltag?
   a. Welche Anwendungen nutzen sie, um Inhalte zu erstellen oder zu bearbeiten?
   b. Auf welchen Geräten erstellen oder bearbeiten sie Inhalte?

Berücksichtigen Sie außerdem Folgendes:

Viele Unternehmen schützen Daten wie Bestellungen und Rechnungen nicht.

- Viele Unternehmen räumen ein, dass sie proprietäre und oft unstrukturierte Daten wie Bestellungen, Rechnungen oder – im Falle von Gesundheitseinrichtungen – Labortestergebnisse nicht immer ausreichend schützen.
- Unternehmen sind zudem verpflichtet, sich darüber zu informieren, wer aus welchem Grund Zugriff auf welche Daten hat, und zu entscheiden, ob bestimmte Personen Zugriff auf sensible Daten erhalten sollten oder nicht. Hier ein Beispiel: Die IT-Abteilung benötigt Zugriff auf das Netzlaufwerk der Personalabteilung, um dessen störungsfreien Betrieb, Back-up und Sicherheit zu gewährleisten. Aber sollte die IT-Abteilung Einsicht in Dokumente der Personalabteilung (z. B. Gehaltslisten und Leistungsdaten) erhalten? Höchstwahrscheinlich nicht. Stattdessen sollten unterschiedliche Zugriffsebenen ermöglicht werden.
- Wussten Sie, dass mehr als 72 % der IT-Administratoren nicht wissen, wie viele Schatten-IT-Anwendungen ihre Mitarbeiter ausführen [Cloud Security Alliance, 2015]? Diese Statistik ist alarmierend. Mitarbeiter müssen jedoch nicht auf ihre geliebten Cloud-Anwendungen verzichten, wenn eine geeignete Verschlüsselung vorhanden ist.

Das Audit muss nicht kompliziert sein. Nutzen Sie die nachfolgende Tabelle als Ausgangspunkt für ein Audit der Datenbewegungen in Ihrem Unternehmen. Überlegen Sie auch, ob es in Ihrem Unternehmen weitere Arten sensibler Daten gibt, und fügen Sie diese zur Liste hinzu.

Sensible Daten	Wie gelangen sie ins Unternehmen? Mit welchen Anwendungen werden sie erstellt?	Wie gelangen sie aus dem Unternehmen?	Wo werden sie gespeichert?	Wer hat auf sie Zugriff?	Wie werden sie genutzt?
Private Mitarbeiterdaten (z. B. Lebensläufe, Bankdaten)					
Informationen über Kunden und Partner					
Geistiges Unternehmenseigentum					
Strategische Dokumente					
Finanzanalysen/-berichte					
Dokumente über die Einhaltung von Gesetzen/ Vorschriften					
Vertriebs- und Verkaufsinformationen (Rechnungen usw.)					

Schritt 3: Festplattenverschlüsselung

Stellen Sie sich zunächst grundlegende Fragen: Was passiert, wenn ein Gerät verloren geht oder gestohlen wird? Eine Festplattenverschlüsselung, manchmal auch Geräteverschlüsselung genannt, gewinnt vor allem durch den zunehmenden Einsatz mobiler Geräte im Unternehmensumfeld an Bedeutung. Die meisten Geräte haben bereits eine betriebssystemeigene Verschlüsselung (Microsoft BitLocker bei Windows und Apple FileVault 2 bei macOS).

In den meisten Unternehmen werden jedoch zwei verschiedene Betriebssysteme (Windows und Mac) genutzt – und sogar vier, wenn man iOS und Android für mobile und Tablet-Geräte mitzählt. Sie benötigen daher eine plattformübergreifende Lösung, mit der Sie Schlüssel und Wiederherstellungsfunktionen für verschiedene Plattformen zentral verwalten können. Gleichzeitig muss diese Lösung leistungsstarken Schutz und eine effiziente Zugriffskontrolle für Ihre Schlüssel bieten.

Sie benötigen eine plattformübergreifende Lösung, mit der Sie Schlüssel und Wiederherstellungsfunktionen für verschiedene Plattformen zentral verwalten können. Gleichzeitig muss diese Lösung leistungsstarken Schutz und eine effiziente Zugriffskontrolle für Ihre Schlüssel bieten.

Eine Festplattenverschlüsselung ist wichtig, aber kein Allheilmittel – sie schützt Geräte nur, wenn sie verloren gehen oder gestohlen werden. Wichtiger ist, was sie nicht tut: Eine Festplattenverschlüsselung bietet keinerlei Schutz für Geräte, die gerade benutzt werden. Sie schützt nicht vor gezielten Angriffen, Hacking, datenstehlender Malware oder anderen menschlichen Fehlern oder Bedrohungen.

Warum ist dieser Punkt wichtig? Datenverluste verursachen heute andere Probleme als früher. Studien belegen: Die häufigste Ursache für Datenpannen sind Hacking und Malware. Deshalb benötigen Unternehmen neben einer Festplattenverschlüsselung unbedingt auch eine Dateiverschlüsselung.

Die häufigste Ursache für Datenpannen sind Hacking und Malware.

Schritt 4: Dateiverschlüsselung

Bei der Einrichtung einer Dateiverschlüsselung besteht die Gefahr, Dinge unnötig zu verkomplizieren – z. B. wenn Sie versuchen, präzise festzulegen, welche Daten verschlüsselt werden sollen und wer auf welche Daten zugreifen darf. Einige sind der Meinung, dass man nur die „wichtigen" Daten verschlüsseln sollte. Aber genau hier liegt das Problem: Wenn Sie nur die wichtigen Daten verschlüsseln wollen, müssen Sie zunächst entscheiden, welche Daten wichtig sind. Und was tun Sie, wenn Ihre Regeln, die vorgeben, welche Daten als wichtig einzustufen sind, versagen und Sie doch Opfer einer Datenpanne werden? Wir empfehlen daher, auf ein Konzept zu setzen, bei dem Daten standardmäßig verschlüsselt werden. Sie sollten grundsätzlich davon ausgehen, dass alle von Ihren Mitarbeitern erstellten Daten wertvoll und schützenswert sind – das ist nicht nur die einfachste, sondern auch die sicherste Methode. Der Trick besteht darin, sich für eine Verschlüsselungsmethode zu entscheiden, die transparent ist und die täglichen Arbeitsabläufe der Mitarbeiter nicht behindert.

Transparent bedeutet in diesem Zusammenhang, dass Ihre Benutzer ihre Arbeitsweise in den meisten Fällen nicht ändern müssen. Es bedeutet auch, dass die Benutzer auf allen Geräten, die sie zur Erledigung ihrer Arbeit nutzen, auf verschlüsselte Inhalte zugreifen können. Denn eine Verschlüsselung funktioniert am besten, wenn die Benutzer überhaupt nichts von ihr bemerken. HTTPS ist ein gutes Beispiel für eine sichere Verschlüsselungsmethode, die kaum wahrnehmbar im Hintergrund abläuft. Millionen von Benutzern merken nicht einmal, dass ihr Browser von HTTP auf HTTPS umgeschaltet hat, um ihre Bestellung oder Transaktion zu schützen – es funktioniert einfach.

Bei der Implementierung einer Dateiverschlüsselung müssen Sie zu Beginn einige wichtige Grundsatzentscheidungen treffen:

- Speicherortbasierte oder anwendungsbewusste Verschlüsselung?
- Schlüsselverwaltung: mehrere Schlüssel oder ein Unternehmensschlüssel?
- Was wird am Anfang verschlüsselt?

Speicherortbasiert vs. anwendungsbewusst

Eine speicherortbasierte Verschlüsselung, häufig auch Datei- oder Ordnerverschlüsselung genannt, verschlüsselt die Ordner, in denen die Enduser ihre wichtigen Dokumente aller Wahrscheinlichkeit nach speichern. Das Problem bei einer speicherortbasierten Verschlüsselung ist Folgendes:

1. Ihre Benutzer müssen strukturierte Unternehmensverfahren strikt befolgen
2. Ihre Benutzer müssen wissen und ermitteln können, welche Dateien wichtig sind
3. Ihre Benutzer müssen wissen, wo wichtige Daten gespeichert werden müssen, um ihre Verschlüsselung sicherzustellen

Die Gefahr für menschliches Versagen ist groß. Es ist ein hohes Maß an Mitarbeiteraufklärung/-compliance erforderlich. Früher oder später wird einem Benutzer ein Fehler unterlaufen und sensible Dokumente könnten in die falschen Hände gelangen.

Bei einer anwendungsbewussten Verschlüsselung dagegen – auch bekannt als „immer aktive Verschlüsselung" – können Administratoren eine Liste vertrauenswürdiger Anwendungen definieren, die von den Mitarbeitern zum Erstellen von Materialien genutzt werden. Nur diese Anwendungen erhalten Zugang zu dem/den Schlüssel(n), die erforderlich sind, um verschlüsselte Dateien zu erstellen und auf verschlüsselte Inhalte zuzugreifen. Dateien sind verschlüsselt – egal, wo die vertrauenswürdigen Anwendungen sie speichern. Der Speicherort wird an diesem Punkt irrelevant und das Problem der speicherbasierten Verschlüsselung beseitigt. Im Idealfall bekommt der Benutzer von diesem Vorgang überhaupt nichts mit – die Dateien sind verschlüsselt. Da sie jedoch über die vertrauenswürdige Anwendung genutzt werden, können sie problemlos geöffnet und verschlüsselt werden. Eine anwendungsbewusste Verschlüsselung ist weniger anfällig für menschliches Versagen und die Gefahr, dass Daten versehentlich offengelegt werden, ist weit geringer.

Mehrere Schlüssel oder ein Unternehmensschlüssel?

Die Schlüsselverwaltung gehört bei der Verwaltung von Verschlüsselungslösungen zu einer der kompliziertesten Aufgaben. Wie komplex Sie die Schlüsselverwaltung jedoch tatsächlich gestalten, liegt ganz bei Ihnen. Auch hier lautet unsere Empfehlung: Beginnen Sie zunächst einfach und fügen Sie bei Bedarf komplexere Strukturen hinzu. Beginnen Sie beispielsweise mit einem gemeinsam genutzten Unternehmensschlüssel und gestalten Sie Ihren Verschlüsselungsprozess damit von Anfang an transparent. Die interne Zusammenarbeit ist einfach und die externe Zusammenarbeit lässt sich leicht kontrollieren.

Wie kompliziert Sie Ihre Schlüsselverwaltung gestalten, liegt ganz bei Ihnen.

Zu einem späteren Zeitpunkt kann es jedoch definitiv gute Gründe geben, warum Sie ausgewählten Gruppen ggf. Spezialschlüssel (oder Gruppenschlüssel) zuweisen möchten. Branchenspezifische Vorschriften schreiben eine Zugriffsbeschränkung auf Basis von Benutzerrollen und -verantwortungsbereichen vor (z. B. für Finanz- oder Personalabteilungen, die Zugriff auf vertrauliche private und Unternehmensdaten benötigen). Ein passender Vergleich: Heißen Sie jeden in Ihrem Haus willkommen, aber teilen Sie die Kombination für den Safe nur Ihren Familienmitgliedern mit.

Bei zu vielen Gruppenschlüsseln können IT-Administratoren schnell den Überblick verlieren – beschränken Sie die Schlüsselanzahl also auf das Nötigste. Denken Sie daran: Sie können mit einer „immer aktiven Verschlüsselung" und einem Unternehmensschlüssel beginnen und das Modell später überarbeiten und um weitere Schichten ergänzen.

Was wird am Anfang verschlüsselt?

Wie bereits erwähnt, ist eine „Ab heute"-Verschlüsselung am einfachsten. Hier werden alle neu erstellten Dateien sowie alle bestehenden Dateien, die aktualisiert werden, automatisch verschlüsselt. In den meisten Unternehmen besteht keine Notwendigkeit, ältere Dokumente zu verschlüsseln. Falls ein Benutzer ein älteres Dokument aktualisiert, wird die neue Version automatisch verschlüsselt.

Das einfachste Konzept zur Verschlüsselung von Dateien: „ab heute"-Verschlüsselung

Eine gute Verschlüsselungslösung sollte Ihnen jedoch bei Bedarf ermöglichen, auch ältere Dateien und Dokumente zu verschlüsseln – z. B. Verschlüsselung aller Dateien mit einer bestimmten Dateierweiterung (.doc, .xls etc.).

Schritt 5: Mitarbeiteraufklärung

Mit einer immer aktiven Verschlüsselung wird die Verschlüsselung für die Enduser einfach. Trotzdem sollten Sie Ihre Mitarbeiter über Ihren Verschlüsselungsprozess, die Bedeutung von Datensicherheit und ihre Rolle beim Schutz sensibler Daten aufklären. In einigen Fällen ist dies sogar gesetzlich oder anderweitig vorgeschrieben. Sie müssen insbesondere sicherstellen, dass Ihre Mitarbeiter verstehen, welche Pflichten und Erwartungen an die Verarbeitung persönlicher und Unternehmensdaten geknüpft sind. Ihre Mitarbeiter müssen auch verstehen, welche Ausnahmen für Ihre Verschlüsselungsrichtlinien gelten – insbesondere was externe Kontakte betrifft.

Klären Sie Mitarbeiter über Ihren Verschlüsselungsprozess, die Bedeutung von Datensicherheit und ihre Rolle beim Schutz sensibler Daten auf.

Eine standardmäßige Verschlüsselung bedeutet, dass externe Kontakte von Ihren Benutzern erstellte Dokumente zunächst entschlüsseln müssen, um sie lesen zu können. Mit der richtigen Lösung sollte die Entschlüsselung jedoch kein Problem sein. Falls ein Dokument für den öffentlichen Gebrauch bestimmt ist – z. B. eine Marketing-Broschüre, ein Whitepaper oder eine Pressemeldung – sollte der Benutzer in der Lage sein, es mit einem Klick zu entschlüsseln. Dies stellt eine bewusste Handlung auf Seiten des Benutzers dar, die protokolliert wird und ein Audit-Trail für den IT-Administrator hinterlässt.

Es gibt eine weitere Schutzschicht, die Sie berücksichtigen sollten: den sicheren Austausch vertraulicher Daten mit externen Parteien, unabhängig davon, ob auf beiden Seiten eine Verschlüsselungssoftware vorhanden ist. Hier bietet sich meist eine passwortgeschützte Datei an. Sie sollten die Möglichkeit haben, passwortgeschützte Dateien zu erstellen, die Sie mit externen Kontakten austauschen können. So bleiben Ihre Daten geschützt und Sie zeigen den externen Parteien, dass Sie das Thema Sicherheit ernst nehmen.

Schritt 6: Wahl der richtigen Lösung

Das Angebot an Verschlüsselungslösungen ist groß. Sie sollten sich daher genau überlegen, was Ihre Verschlüsselungslösung jetzt und in Zukunft können sollte, bevor Sie eine Kaufentscheidung treffen.

Berücksichtigen Sie Folgendes:

- Funktioniert die Lösung auf verschiedenen Plattformen und Geräten wie Windows, macOS, iOS und Android?
- Lässt sich die Software zentral verwalten und kontrollieren?
- Ist eine „anwendungsbewusste" und „immer aktive" Verschlüsselung möglich?
- Wo schützt die Lösung Daten? In der Cloud, lokal und auf allen Geräten?
- Wie einfach lassen sich verschlüsselte Inhalte mit externen Benutzern austauschen?
- Welche Auswirkung hat die Software auf das Verhalten und die Arbeitsweise der Benutzer?
- Verfügt die Lösung über eine leistungsstarke Schlüsselverwaltung?
- Wie ist der Backup- und Wiederherstellungsmechanismus für Schlüssel gestaltet, um zu verhindern, dass Sie den Zugriff auf verschlüsselte Daten verlieren?

Sophos SafeGuard Encryption

Sophos SafeGuard ist die vielfach prämierte Next-Gen-Encryption-Software von Sophos. Sophos SafeGuard bietet eine immer aktive Verschlüsselung, die Ihre Daten intelligent verschlüsselt, sodass diese vor Diebstahl geschützt bleiben und unbrauchbar sind, falls sie in die falschen Hände gelangen.

Sophos SafeGuard kommuniziert direkt mit dem Sophos-Endpoint-Agenten und ermöglicht so proaktiven Schutz und eine sofortige Reaktion. Darüber hinaus synchronisiert Sophos SafeGuard Schlüssel mit Sophos Mobile Control und ermöglicht damit unabhängig vom genutzten Gerät einen nahtlosen Zugriff auf verschlüsselte Dateien. Dabei laufen alle Vorgänge für die Benutzer transparent ab.

Zusammenfassung

Sobald Sie sich für den Kauf einer Verschlüsselungslösung entschieden haben, beginnt die wirkliche Arbeit. Sie müssen eine Lösung finden, die Ihre Sicherheitsanforderungen erfüllt, ohne den Workflow Ihrer Benutzer zu beeinträchtigen. Sie sollten sich darüber informieren, wie Ihre Daten erstellt und verwaltet werden, und eine Lösung wählen, die nicht nur die Geräte Ihrer Benutzer, sondern auch Ihre Dateien und Daten vor Angriffen und Malware schützt. Beginnen Sie mit einfachen Maßnahmen: Verschlüsseln Sie zunächst grundsätzlich alle Dateien und nutzen Sie einen unternehmensweiten Schlüssel – Sie können die Verschlüsselung später spezifischer gestalten. Und vergessen Sie nicht, bei der Entwicklung Ihrer Richtlinien die Compliance zu berücksichtigen. Entscheiden Sie sich für eine Lösung, die Ihre Compliance mit Datenschutzgesetzen und -vorschriften sicherstellt.

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

21.10.2016 WP-DE (NP)

SOPHOS