SEPAGO 360° INFORMATION PROTECTION IMPLEMENTATION

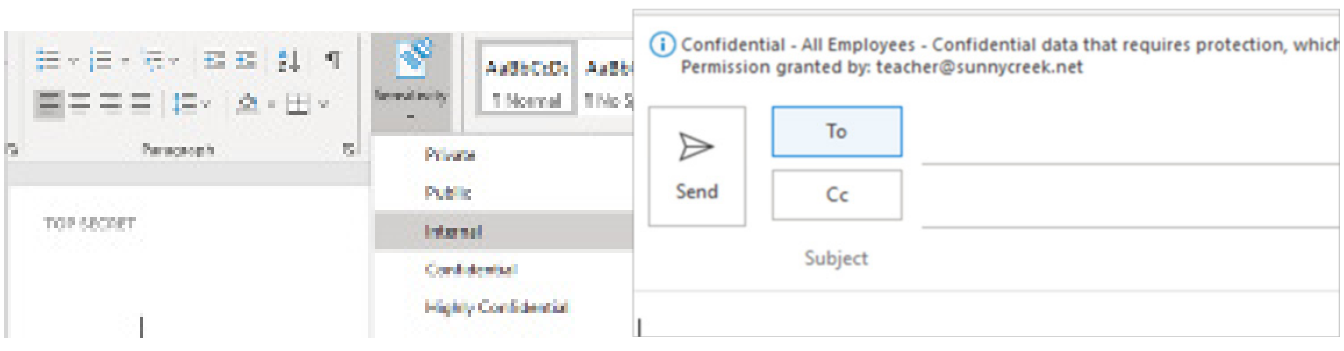
sepago. making people love it.

Compliant Cloud Services

Daten werden mehr als je zuvor zwischen Benutzern, Geräten, Anwendungen und Diensten ausgetauscht. Unternehmen arbeiten mit Kunden, Partnern und Mitarbeitenden zusammen und teilen sensible Informationen innerhalb und außerhalb der Unternehmensgrenzen.

Microsoft Azure Information Protection (AIP) kontrolliert und schützt E-Mails, Dokumente und sensible Daten, die Sie außerhalb Ihres Unternehmens freigeben. Von der einfachen Klassifizierung bis hin zu eingebetteten Kennzeichnungen und Berechtigungen können Sie den Datenschutz jederzeit verbessern - unabhängig davon, wo die Daten gespeichert sind oder mit wem sie geteilt werden.

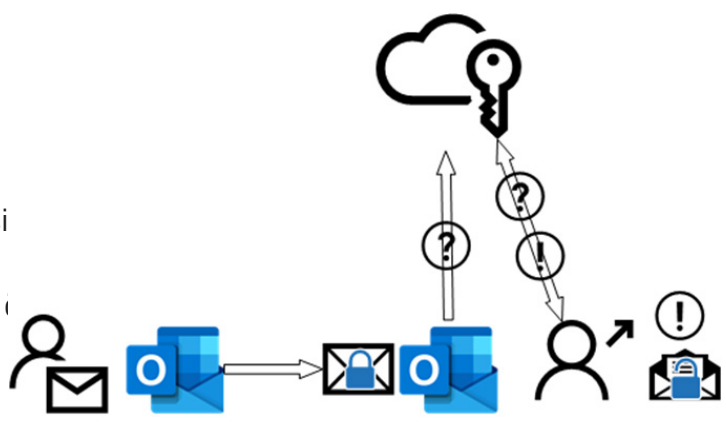
Für viele Unternehmen kann der Startpunkt für die Implementierung von Azure Information Protection eine Herausforderung sein. Wie viele Labels brauchen Unternehmen wirklich und wie stellen sie sicher, dass ihre Mitarbeiter die Labels übernehmen? Mit bewährten Blueprints und Erfahrungen aus verschiedenen Kundenprojekten wird sepago Sie auf dieser Implementierungsreise begleiten.



AIP - Wie es funktioniert

Azure Information Protection oder AIP ist ein wichtiger Bestandteil des ganzheitlichen Information Protection Framework. AIP verwendet eine Reihe von Kennzeichnungen, die die Klassifizierung der Daten Ihres Unternehmens darstellen, z. B.: "Intern" oder "Streng vertraulich". Die Kennzeichnung kann vom Benutzer mit nur einem Mausklick angebracht werden und setzt die zugrunde liegenden Richtlinien durch. Diese können von der rein visuellen Kennzeichnung bis hin zur Verschlüsselung und Nicht-Weiterleitung von E-Mails reichen. Nur Empfänger, die sich gegenüber Ihrem Rights Management Service authentifizieren können, dürfen und können die geschützten Inhalte öffnen und konsumieren. Dies alles funktioniert automatisch und entlastet Ihre Benutzer von der versehentlichen Weitergabe von Informationen, die sie nicht weitergeben wollen. Um die Sicherheit Ihrer Daten weiter zu erhöhen, kann AIP automatisch Kennzeichnungen auf der Grundlage von Identifikatoren (PII, Kreditkartennummern...) zu kennzeichnen, was Ihnen dabei hilft, z.B. mit der GDPR konform zu bleiben.
Die Schutzrichtlinien sind in die Metadaten der Dateien eingebettet und begleiten sie, wo immer sie auch gespeichert werden. Ob verschlüsselt oder unverschlüsselt, Sie haben immer noch die Kontrolle über Ihre Daten, auch außerhalb Ihrer klassischen Umgebungsgrenzen.

- Mitarbeitende sendet E-Mail
- Der/ die Empfänger:in authentifiziert si
  Ihrem Schlüssel in Azure
- Der/ die Empfänger:in kann die E-Mail



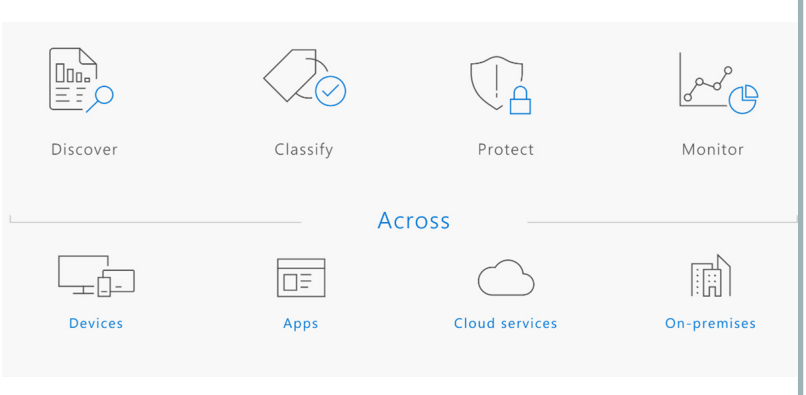
Technische Umsetzung

1. AIP PoC Kick-Off Workshop mit Showcases
2. Anforderungsphase
3. Definitionsphase
4. Pilotprojekt zur technischen Konzeption
5. Implementierung/ Roll-out des technischen Konzepts in der Pilotumgebung
6. Nachbereitung/Anpassungsphase
7. Technisches Roll-out

Adoption & Awareness campaign

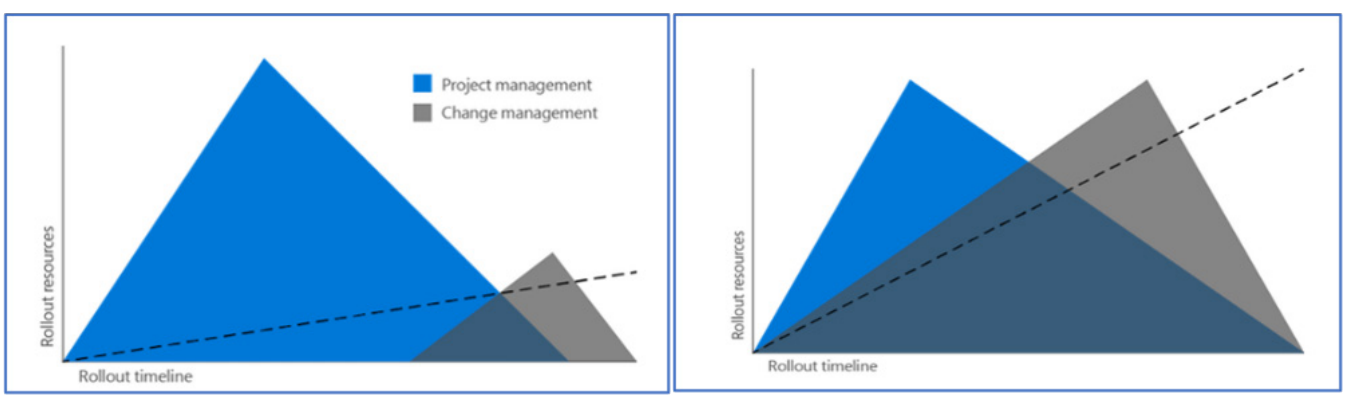
1. Organisatorische Bewertung Proof-of-concept
2. Identifizieren von verschiedenen Bezeichnungen, Rollen, Szenarien & stakeholder
3. Tailor-made roll-out management: Kommunikationsplan & Material
4. Aktivierung der Mitarbeitenden: Ausbildung
5. Feedback messen und geeignete Maßnahmen ergreifen: UX Measurement plan

Mit AIP können Sie feststellen, welche Daten Sie vor Ort oder in der Cloud haben. Sie können dann automatisch oder durch die Benutzer manuell die richtige Kennzeichnung vornehmen gemäß Ihrer bestehenden Klassifizierung. Mit Hilfe der Kennzeichnung werden die Daten dann geschützt. Ein leistungsfähiger Überwachungsdienst hilft Ihnen dann, die Speicherung und Übertragung von klassifizierten Daten zu überwachen.

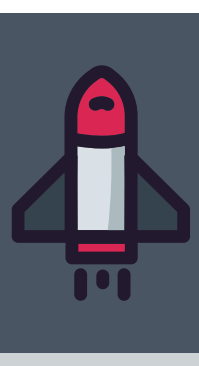


Implementation und Roll-out

Oft wird neue Software wie AIP ohne eine ganzheitliche organisatorische Betrachtung eingeführt. Dies wirkt sich auf die Akzeptanz durch die Endbenutzer und damit auf die Sicherheit und die Einhaltung der Vorschriften aus. Der Zeitpunkt und Umfang des organisatorischen Anderungsmanagements beeinflussen den Erfolg der Software-Implementierung.



"IT ist wichtig, um den Veränderungsprozess kontinuierlich und prozessual strukturiert zu unterstützen. Eine ganzheitliche Betrachtung mit Mitarbeitern aus allen betroffenen Abteilungen und Hierarchieebenen sorgt für eine höhere Akzeptanz und Verständnis bei der Einführung von Microsoft-Sicherheitslösungen."



KONTAKTIEREN SIE UNS

TILMANN SIES
Lead Consultant Technology & Organization

tilmann.sies@sepago.de

sepago. making people love it.