Kann man Informationssicherheit & Datenschutz trennen?

Autor:

Bruno Biedermann, edcom gmbh
Ingenieur FH, EMBA-iimt, Auditor CISSP, CISA
br@edcom.ch; +41 78 748 56 89

Peut-on dissocier sécurité de l'information et protection des données ?

Auteur :

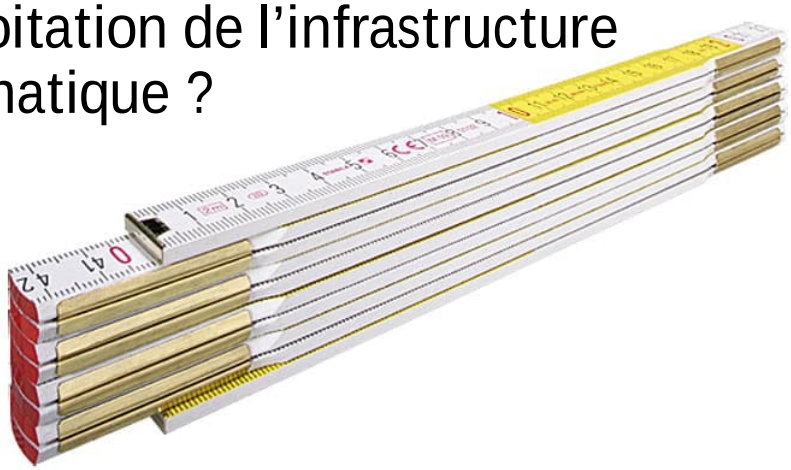
Bruno Biedermann, edcom gmbh
Ingénieur HES, EMBA-iimt, auditeur CISSP, CISA
br@edcom.ch; +41 78 748 56 89

Kernfrage:

Wie messen und beurteilen Sie einen «datenschutzkonformen Betrieb der IT-Infrastruktur»?

Question clé :

Quelle méthode utilisez-vous pour mesurer et évaluer le respect de la protection des données dans l'exploitation de l'infrastructure informatique ?



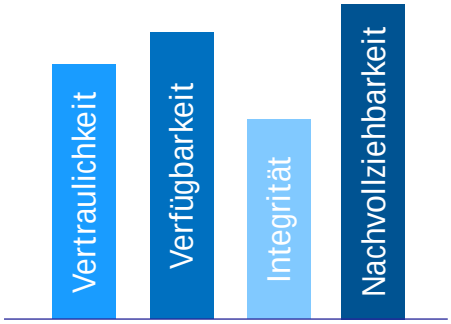
Inhaltliche Schwerpunkte

- Sicherheitsziele
- Risikoabwägung
- Beispiel Mobilität und Smartphone mit Lösungsansätzen.

Thèmes principaux

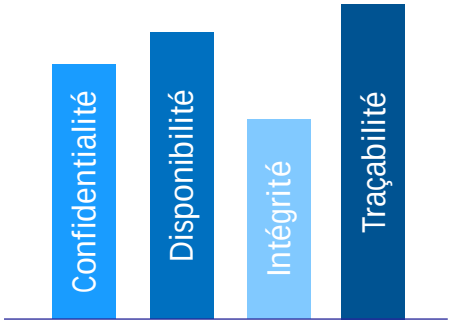
- Objectifs de sécurité
- Évaluation des risques
- Exemple de la mobilité et du smartphone avec des solutions possibles.

Bestimmen der Sicherheitsziele



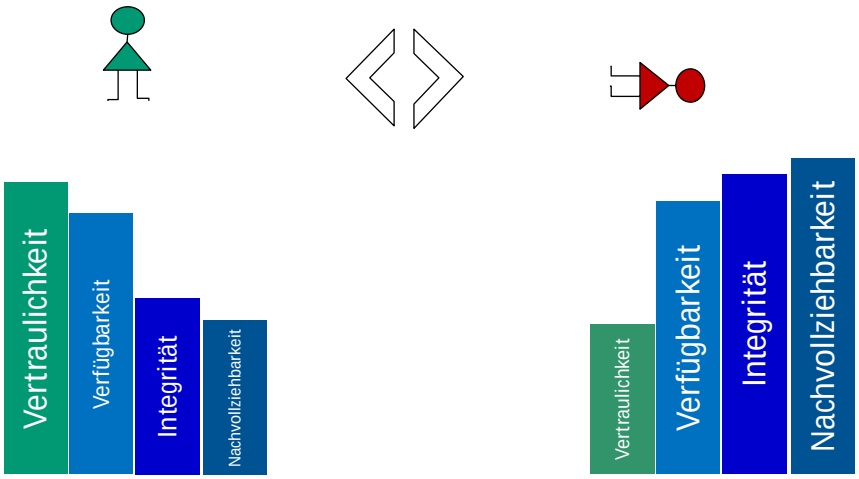
Die Gewichtung ist abhängig von den Anforderungen an die Anwendungen und Systeme, basierend auf einer *Risikobetrachtung*.

Définition des objectifs de sécurité

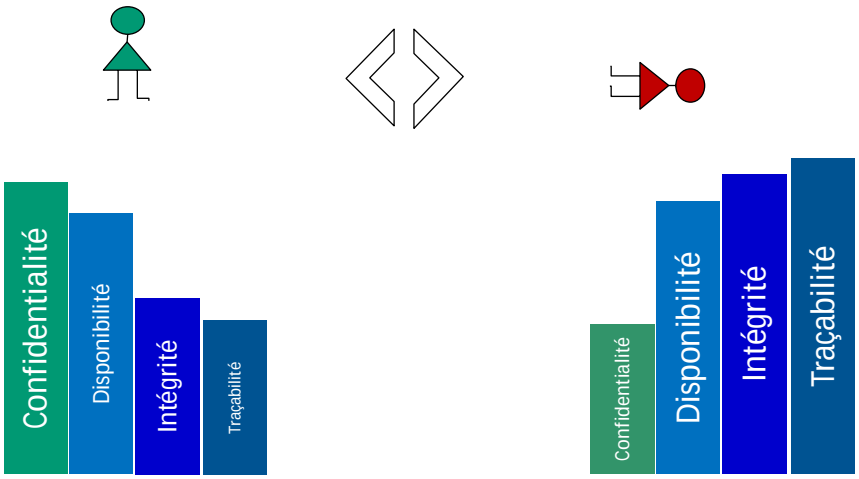


La pondération dépend des exigences posées aux applications et aux systèmes, sur la base d'une *évaluation des risques*.

Dilemma der Gewichtung



Dilemme de la pondération



Risikoabwägung

Wieviel Sicherheit ist notwendig?

Für eine erste Einschätzung helfen:

- Eine Analyse der potentiellen Risiken
- Eine Klassifizierung der Daten und Systeme
- Eine Analyse der Auswirkungen eines Zwischenfalls auf die Geschäftsprozesse

Évaluation des risques

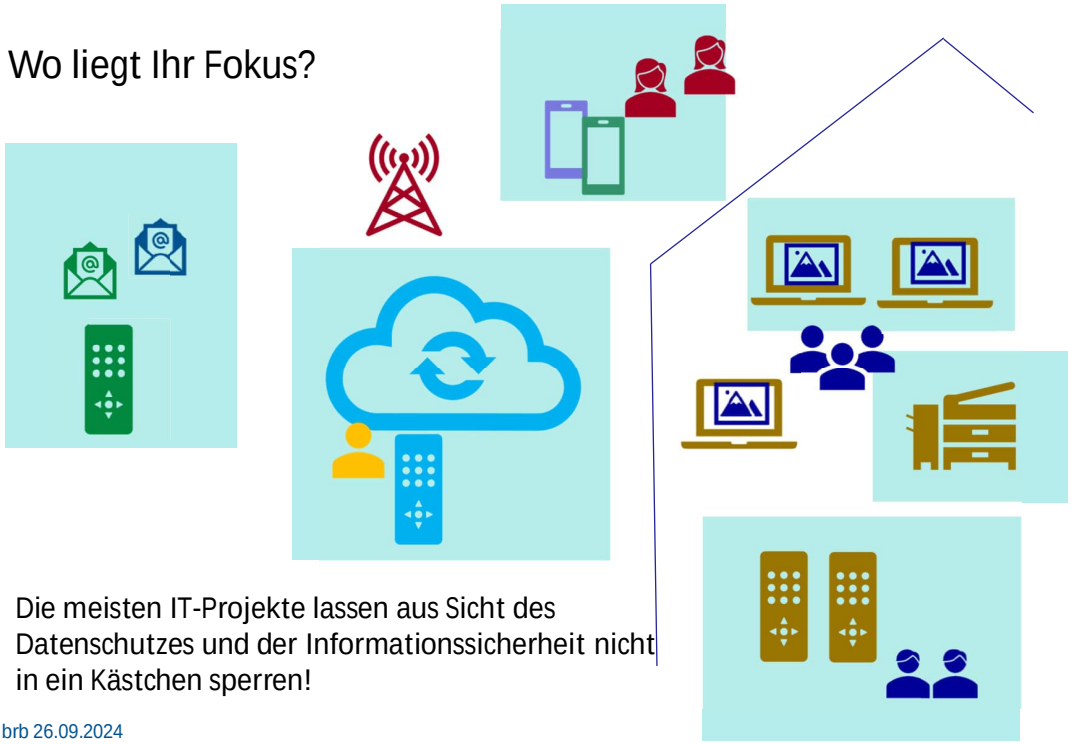
Quel est le niveau de sécurité nécessaire ?

Pour une première évaluation, il est utile de :

- réaliser une analyse des risques potentiels
- classer les données et les systèmes
- réaliser une analyse de l'impact d'un incident sur les processus d'entreprise

Risikoabwägung

Wo liegt Ihr Fokus?

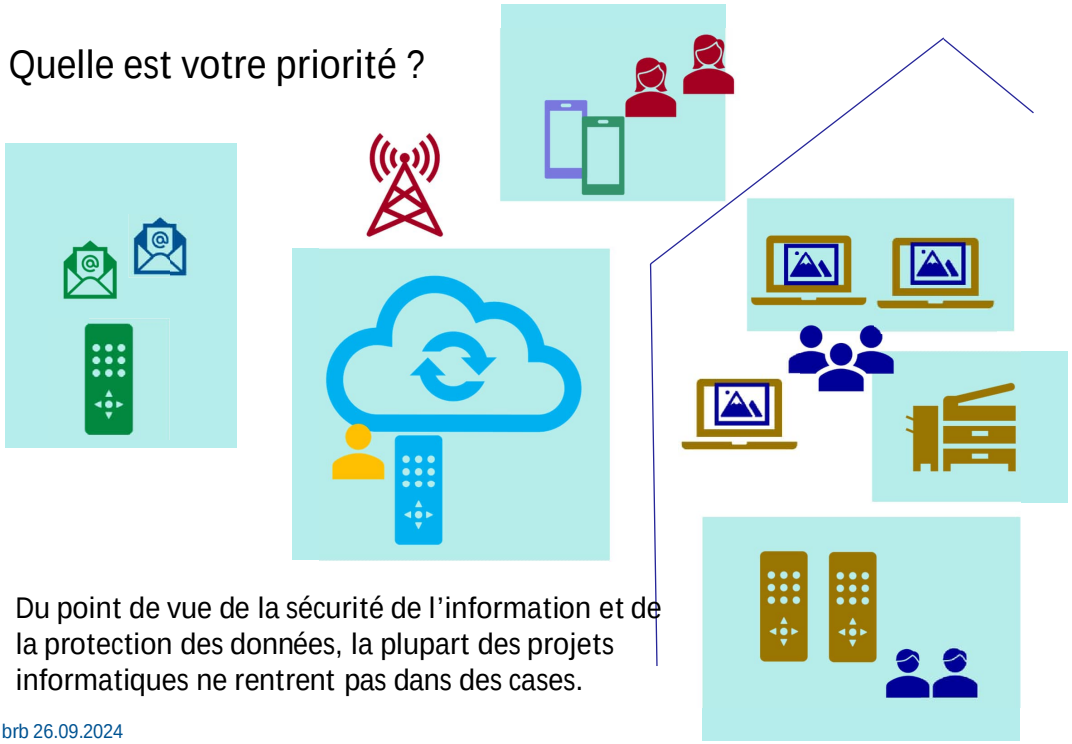


Die meisten IT-Projekte lassen aus Sicht des Datenschutzes und der Informationssicherheit nicht in ein Kästchen sperren!

brb 26.09.2024

Évaluation des risques

Quelle est votre priorité ?

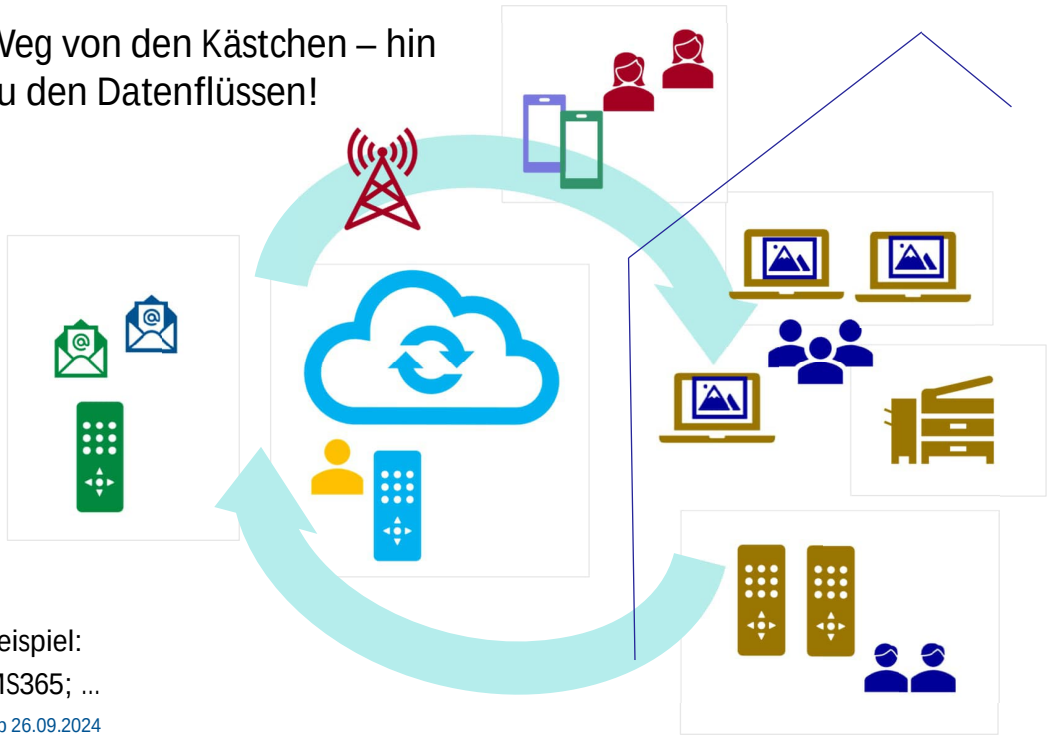


Du point de vue de la sécurité de l'information et de la protection des données, la plupart des projets informatiques ne rentrent pas dans des cases.

brb 26.09.2024

Risikoabwägung

Weg von den Kästchen – hin zu den Datenflüssen!



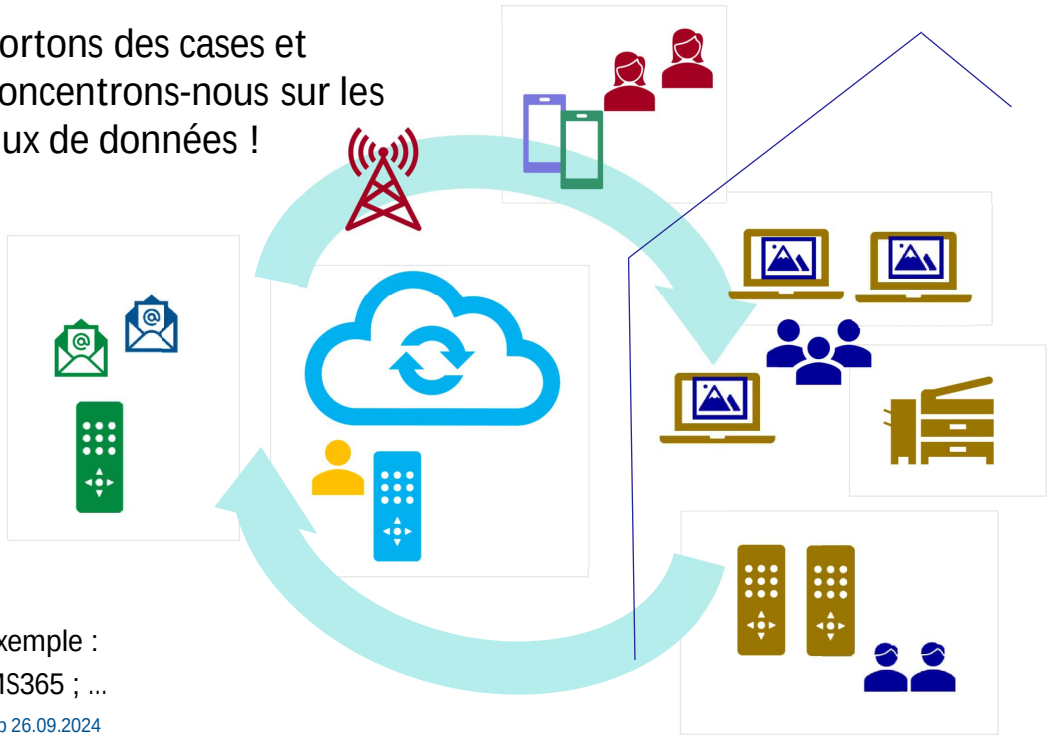
Beispiel:

MS365; ...

brb 26.09.2024

Évaluation des risques

Sortons des cases et concentrons-nous sur les flux de données !



Exemple :

MS365 ; ...

brb 26.09.2024

Risikoabwägung

Ohne die Datenflüsse zu verstehen, sind die Risiken für einen datenschutzkonformen Betrieb kaum abschätzbar!

Dazu sind zumindest folgende Kernfragen zu klären:

- Welche Arbeitsprozesse sollen unterstützt werden?
- Wer ist berechtigt die Daten und Systeme zu nutzen?
- Welche Daten werden benötigt und bereitgestellt?
- Welche Applikationen werden eingesetzt?
- Welche Services werden von wem erbracht?
- Welche Architektur wird von wem bereitsgestellt?

Évaluation des risques

Sans comprendre les flux de données, il est difficile d'évaluer les risques pour une exploitation conforme à la protection des données !

Il convient donc au moins de clarifier les questions clés suivantes :

- Quels sont les processus de travail qui doivent bénéficier d'un soutien ?
- Qui est autorisé à utiliser les données et les systèmes ?
- Quelles données sont nécessaires et mises à disposition ?
- Quelles applications sont utilisées ?
- Qui fournit quels services ?
- Qui fournit quelle architecture ?

Mobilität: Smartphones im beruflichen Einsatz

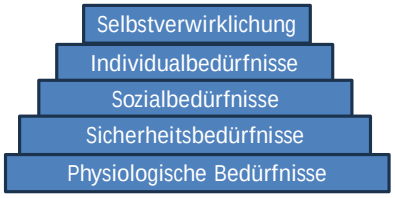
brb 26.09.2024

Mobilité : les smartphones dans le cadre professionnel

brb 26.09.2024

Mobilitätsbedürfnis

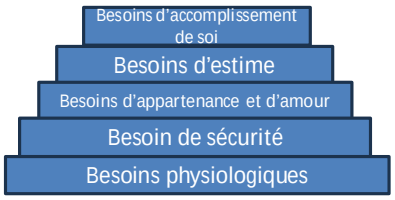
Bedürfnispyramide nach Maslow



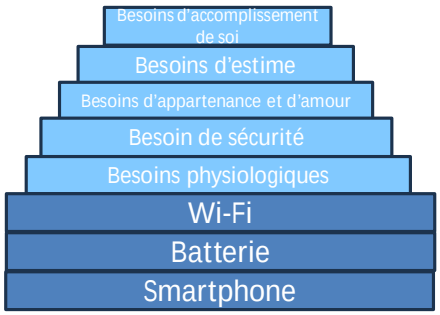
Bedürfnispyramide nach Maslow 2.0

Besoin en matière de mobilité

La pyramide des besoins de Maslow



La pyramide des besoins de Maslow



Risikoabwägung

Welche Arbeitsprozesse sollen unterstützt werden?

- Kommunikation; eMail; Dokumente lesen; Informationsbeschaffung; Datenerfassung: Bild und Tonaufzeichnungen zur Dokumentation; AI

Wer nutzt die Daten und Systeme?

- Alle Benutzer der Smartphones

Welche Daten werden dazu benötigt?

- Geschäftliche Daten, private Daten

Welche Applikationen werden eingesetzt?

- Individuell ohne Grenzen

Welche Services werden von wem erbracht?

- Unterschiedliche Hersteller, Internet-Provider und SW-Lieferanten

Welche Architektur wird von wem bereitsgestellt?

- Je nach Einsatz unterschiedliche Architekturen möglich

brb 26.09.2024

Évaluation des risques

Quels sont les processus de travail qui doivent bénéficier d'un soutien ?

- Communication ; e-mail ; lecture de documents ; collecte d'informations ; saisie de données : enregistrements audio et vidéo à des fins de documentation ; IA

Qui utilise les données et les systèmes ?

- Tous les utilisateurs de smartphones

Quelles sont les données nécessaires à cet effet ?

- Données professionnelles, données privées

Quelles applications sont utilisées ?

- Personnelles, sans limites

Qui fournit quels services ?

- Différents fabricants, fournisseurs d'accès à Internet et fournisseurs de logiciels

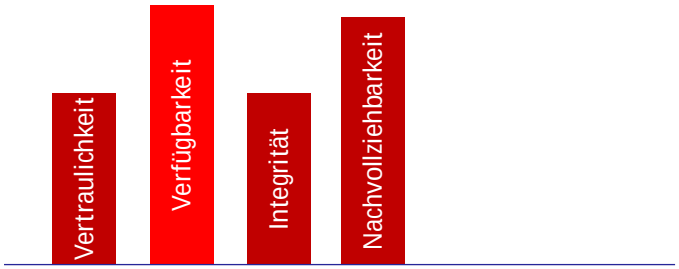
Qui fournit quelle architecture ?

- Différentes architectures possibles en fonction de l'utilisation

brb 26.09.2024

Risikoabwägung

Eine Risikoabwägung in bezug auf die Sicherheitsziele :



Fazit: Die Nutzung von Smartphones birgt grosse Risiken in Bezug auf alle Sicherheitsziele.

Lösung:

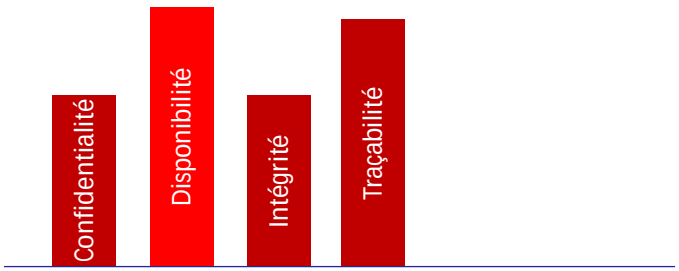
Es braucht zwingend eine Datenschutzfolgeabschätzung (ISDS-Konzept, Risikoanalyse, Massnahmenkatalog) für den Einsatz von Smartphones.

Anm: Die Massnahmen sind in einschlägigen Normen (Bsp: ISO 2700x) dokumentiert

brb 26.09.2024

Évaluation des risques

Évaluation des risques par rapport aux objectifs de sécurité :



Conclusion : l'utilisation des smartphones comporte des risques importants au regard de tous les objectifs de sécurité.

Solution :

Il est impératif de procéder à une analyse d'impact relative à la protection des données personnelles (concept SIPD, analyse des risques, catalogue de mesures) pour l'utilisation de smartphones.

N.B. : les mesures sont documentées dans les normes pertinentes (p. ex. : ISO 2700x).

brb 26.09.2024

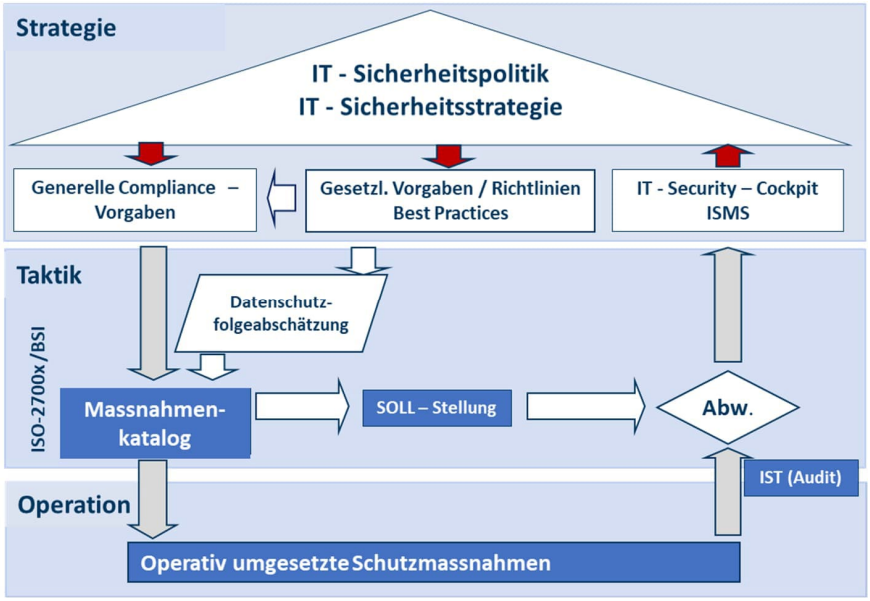
Risikoanalyse (Auszug)

Risiken beim Einsatz mobiler Geräte	
• Die Bearbeitung von Geschäftsdaten mit Smartphones ist nicht geregelt (Upload, Download, Versand, Speicherung)	
• Vermischung privater / geschäftlicher Daten	
• Synchronisation auf private Geräte / Clouddrive	
• Nutzung durch nicht berechtigte Benutzende	
• Download von unerwünschten Inhalten	
• Die Zuständigkeiten sind nicht klar geregelt	
• Wartung und Support der Geräte nicht gewährleistet	
• Überwachung der (Privatsphäre) via Geräteortung	
• Geräteverlust führt zu Bekanntgabe vertraulicher Daten	
• Download und Installation von Software (Apps) führt zu Gerätefehlern, Viren, unerwünschten Funktionen	
• Wahl der Provider ist nicht an ISDS-Kriterien gebunden	
• Konfiguration ist individuell veränderbar, keine Kontrolle möglich	
• Zugriffsrestriktionen nicht kontrollierbar	

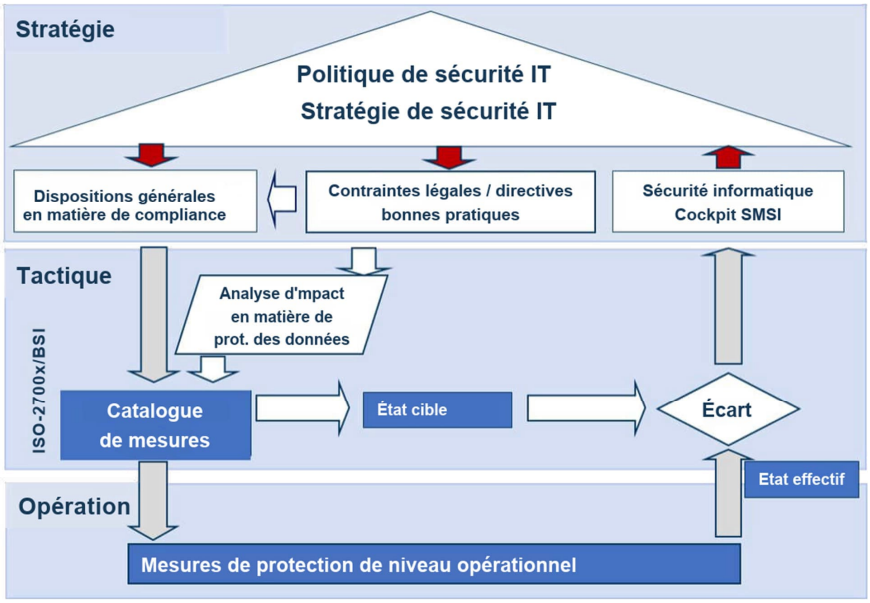
Analyse des risques (extrait)

Risques liés à l'utilisation d'appareils mobiles	
• Le traitement des données commerciales à l'aide de smartphones n'est pas réglementé (chargement, téléchargement, envoi, stockage)	
• Confusion entre données personnelles et professionnelles	
• Synchronisation sur des appareils privés / sur Cloud Drive	
• Utilisation par des utilisateurs non autorisés	
• Téléchargement de contenus indésirables	
• Responsabilités pas clairement définies	
• Maintenance et assistance des appareils non garanties	
• Surveillance (de la sphère privée) via la localisation de l'appareil	
• Perte de l'appareil entraînant la divulgation de données confidentielles	
• Téléchargement et installation de logiciels (applis) entraînant des dysfonctionnements de l'appareil, des virus, des fonctions indésirables	
• Choix du fournisseur d'accès non lié aux critères SIPD	
• Configuration pouvant être modifiée individuellement, aucun contrôle n'est possible	
• Restrictions d'accès non contrôlables	

Lösungsansatz: Grundlage



Solution possible : approche de base



Praktische Lösungsansätze

1. Management der Geräte, Applikationen und Daten

Zur Bewältigung dieser Herausforderungen helfen verschiedene Mobility Management-Lösungen. Diese dienen unter anderem folgenden Zielen:

- Sichere Bereitstellung von mobilen Geräten, auf denen sich der User authentifiziert
- Technische Durchsetzung der Richtlinien (Konfiguration der Geräte)
- Unternehmens-Applikationen laufen nur auf autorisierten Geräten
- Löschung von Daten und Apps bei Verlust oder Diebstahl
- Trennung von privaten und geschäftlichen Daten
- Sicheres Tunneling ins Netzwerk des Unternehmens

Praktische Lösungsansätze

2. Containerlösungen

Durch das Managen der Applikationen und Geräte werden diese nicht vorbehaltlos sicher.
Die Containerlösung stellt sicher, dass Anwendungen und ihre Daten in einem abgeschotteten Umfeld (Container) laufen.
Die korrekte Konfiguration vorausgesetzt, kann damit verhindert werden, dass z. Bsp. Firmeninformationen per Copy & Paste auf sozialen Medien landen (X, Facebook etc.) oder unerwünschte Daten in die Organisationsumgebung eingeschleust werden.
Die Firmenanwendungen und die privaten Apps sind deutlich getrennt, so dass der Benutzer weiss, in welchem Kontext er sich befindet.

Pro: Klare Trennung von privaten und geschäftlichen Daten und Applikationen.

Kontra: Aufwendig

Solutions pratiques

1. Gestion des appareils, des applications et des données

Différentes solutions de gestion de la mobilité permettent de relever ces défis. Elles visent notamment les objectifs suivants :

- Mise à disposition sécurisée d'appareils mobiles permettant l'authentification de l'utilisateur
- Application technique des directives (configuration des appareils)
- Exécution des applications d'entreprise uniquement sur les appareils autorisés
- Suppression des données et des applications en cas de perte ou de vol
- Séparation des données privées et professionnelles
- Tunneling sécurisé vers le réseau de l'entreprise

Solutions pratiques

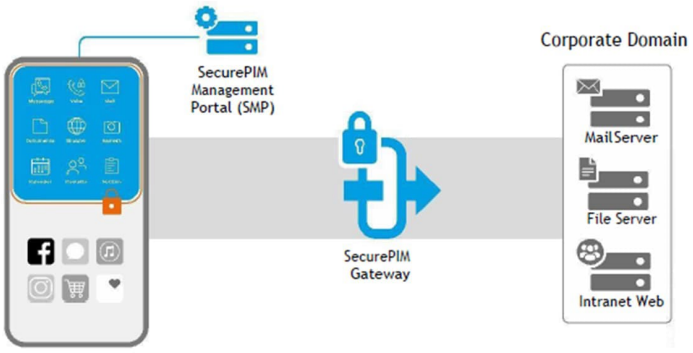
2. Solutions « conteneur »

La gestion des applications et des appareils ne garantit pas une sécurité totale.
La solution « conteneur » garantit que les applications et leurs données fonctionnent dans un environnement cloisonné (conteneur).
Sous réserve d'une configuration correcte, il est ainsi possible d'éviter que des informations d'entreprise ne soient copiées-collées sur des réseaux sociaux (X, Facebook, etc.) ou que des données indésirables ne soient introduites dans l'environnement organisationnel.
Les applications d'entreprise et les applications privées sont clairement séparées, de sorte que l'utilisateur sait dans quel contexte il se trouve.

Avantage : séparation claire entre les données et les applications privées et professionnelles

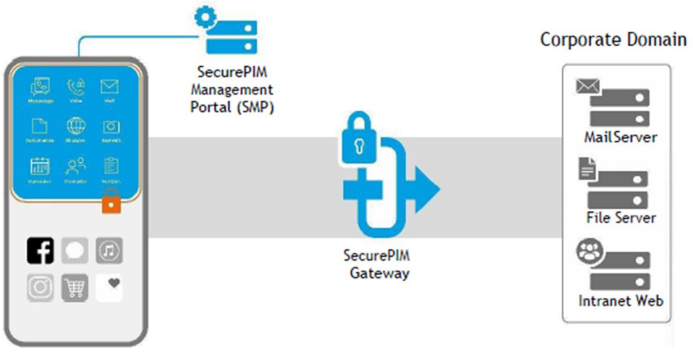
Inconvénient : coûteux

Lösungsansätze



Quelle: https://www.secure-pim.ch/

Solutions possibles



Source : https://www.secure-pim.ch/

Kann man Informationssicherheit & Datenschutz trennen?

Nein - bei der Komplexität heutiger IT-Systeme, sind die Auswirkungen auf Informationssicherheit und Datenschutz oft nicht auf den ersten Blick zu erkennen.
Es bedarf einer Kooperation aller Beteiligten mit dem gemeinsamen Ziel datenschutzkonforme Systeme zu bauen und zu betreiben und damit Lösungen bereitzustellen, die die Privatsphäre der BürgerInnen respektieren.

Peut-on dissocier sécurité de l'information et protection des données ?

Non. Vu la complexité des systèmes informatiques actuels, les conséquences sur la sécurité de l'information et la protection des données ne sont souvent pas visibles de prime abord.
Il est nécessaire que toutes les parties concernées coopèrent dans le but commun de construire et d'exploiter des systèmes conformes à la protection des données et de fournir ainsi des solutions qui respectent la vie privée de la population.