



dsb

datenschutzbeauftragte
des kantons zürich

Merkblatt

Softwarelösungen für IT-Verantwortliche

Dieses Merkblatt richtet sich an IT-Verantwortliche öffentlicher Organe. Es enthält eine Auswahl von Softwarelösungen, die das datenschutzkonforme Bearbeiten von Personendaten unterstützen.

Die vorgestellten Tools sind Beispiele. Die Entscheidung zur Nutzung muss den unterschiedlichen Anforderungen und Bedürfnisse entsprechend individuell und risikobasiert getroffen werden.

Folgende Themen werden berücksichtigt:

1. Lokale Cloud-Lösungen
2. Management von Informationssicherheitsmassnahmen
3. Erstellen eines Inventars
4. Verschlüsseln von E-Mails
5. Verschlüsseln von Dateien
6. Verwalten von Smartphones
7. Überwachen von IT-Systemen
8. Sicherer Zugriff über das Internet
9. Überprüfen auf Schwachstellen
10. Erstellen von Webstatistiken

1 Lokale Cloud-Lösungen

Das verantwortliche öffentliche Organ hat über Daten, die in die Cloud ausgelagert sind, nur noch eine beschränkte Kontrolle. Die Kontrolle bleibt erhalten, wenn lokal installierte Cloud-Lösungen genutzt werden, beispielsweise:

- [EtherPad](#)
Datenschutzfreundliche Alternative zu Google Docs und Microsoft 365 mit lokaler Datenablage
- [OwnCloud](#)
Datenschutzfreundliche Alternative zu Dropbox (Online-Speicher) mit lokaler Datenablage

2 Management von Informationssicherheitsmassnahmen

Das Management vieler Informationssicherheitsmassnahmen ist komplex. Diverse Tools helfen, den Aufwand zu reduzieren und die Systematik zu verbessern.

- [i-doit](#)
Open-Source-CMDB- und IT-Dokumentation
- [GRC Tool Box Pro](#)
Integrierte Softwarelösung für Governance, Risk und Compliance
- [Verinice](#)
Open-Source-ISMS-Tool, IT-Grundschutz

Auf der Website des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine umfassende Liste [Alternative IT-Grundschutz-Tools](#) verfügbar.

3 Erstellen eines Inventars

Das Erstellen eines Inventars bedeutet einen grossen Aufwand. Zudem besteht das Risiko, dass bestimmte Geräte nicht inventarisiert werden. Mit Softwareunterstützung können der Aufwand reduziert und die Qualität erhöht werden.

- [DocuSnap](#)
Automatische Inventarisierung des Netzwerks
- [José AD Dokumentation](#)
Inventarisierung des Windows Active Directory (Berechtigungen)
- [Lansweeper](#)
Automatische Inventarisierung des Netzwerks, inklusive Möglichkeit zur Analyse

4 Verschlüsseln von E-Mails

Unverschlüsselte E-Mails können abgefangen, mitgelesen oder verändert werden. Aus diesem Grund sind sensitive Daten verschlüsselt zu versenden. Dafür können die folgenden Lösungen eingesetzt werden:

- [Gpg4win](#)
Open Source Software für die Mailverschlüsselung mit PGP, bietet die Möglichkeit zur Dateiverschlüsselung
- [IncaMail](#)
Mailverschlüsselungslösung der Schweizerischen Post AG
- [PrivaSphere](#)
Lösung für den sicheren Informationsaustausch über das Internet
- [ProtonMail](#)
Lösung für eine sichere Kommunikation über das Internet
- [SEPPmail](#)
Interne Lösung zur Mailverschlüsselung (Secure E-Mail Gateway erforderlich)

5 Verschlüsseln von Dateien

Um sensitive Daten im Netzwerk zusätzlich zu schützen, sind sie zu verschlüsseln. Folgende Softwarelösungen verschlüsseln die Daten auf einfache und transparente Weise. Die genannten Softwarelösungen unterstützen eine starke Authentifizierung.

Bitlocker

Verschlüsselungslösung von Microsoft, Laufwerksverschlüsselung

fileAS file

Dateiverschlüsselung innerhalb eines Dateisystems

FileVault

Verschlüsselungslösung von Apple (Startvolume)

SafeGuard Encryption von Sophos

Festplatten- und Dateiverschlüsselung auch bei Datenweitergabe

VeraCrypt (free OpenSource)

Festplattenverschlüsselung und Containerlösung für die verschlüsselte Dateiablage

6 Verwalten von Smartphones / Enterprise

Auf Smartphones befinden sich oft sensitive Daten. Mit einem Mobile Device Management (MDM) können die Daten angemessen geschützt und die Geräte bestmöglich verwaltet werden.

– Workspace ONE Unified Endpoint Management (UEM)

MDM von VMWare

– Citrix Endpoint Management

MDM von Citrix

– Microsoft Endpoint Manager

MDM von Microsoft

– Mobileiron

MDM von Mobileiron

– Unified Endpoint Manager

MDM von Ivanti

– Unified Endpoint Management

MDM von Blackberry

– WSO2 Enterprise Mobility Management

Open Source MDM

7 Überwachen von IT-Systemen

Um die Verfügbarkeit und Sicherheit von IT-Systemen zu gewährleisten, sind diese zu überwachen und die Protokolle regelmässig auszuwerten. Dafür können beispielweise die folgenden Softwarelösungen eingesetzt werden.

Icinga

Open-Source-Monitoringsystem

OpenNMS

Open-Source-Netzwerkmanagementsystem

WhatsUp

Netzwerkmonitoring von Progress

8 Sicherer Zugriff über das Internet

Der externe Zugriff auf interne Daten ist mit erheblichen Risiken verbunden, besonders wenn er mit privaten Geräten oder über öffentliche Netzwerke erfolgt. Mit entsprechender Software lassen sich die Risiken reduzieren.

- [G/On](#)
Starke Authentifizierung für den externen Zugriff
- [OpenVPN](#)
Open-Source-VPN-Lösung

9 Überprüfen auf Schwachstellen

Netzwerke und Anwendungen enthalten oft unbekannte Schwachstellen. Sie können durch eine regelmäßige Überprüfung auf Schwachstellen entdeckt werden. Dafür können folgende Softwarelösungen eingesetzt werden.

9.1 Netzwerk

- [GFI LanGuard](#)
Netzwerksicherheitsscanner
- [Nessus](#)
Sicherheitsscanner von Tenable
- [OpenVAS](#)
Open-Source-Schwachstellenscanner

9.2 Webanwendungen

- [Acunetix](#)
Webschwachstellenscanner
- [Arachni](#)
Open-Source-Webschwachstellenscanner
- [Netsparker](#)
Webschwachstellenscanner
- [PrivacyScore](#)
Websites auf Datenschutz- und Sicherheitsaspekte untersuchen
- [Qualys SSL Server Test](#)
Scanner für die Überprüfung der TLS/SSL-Webserverkonfiguration

10 Erstellen von Webstatistiken

Daten von Webseitenbesucherinnen und -besuchern sind Personendaten und dürfen entsprechend den datenschutzrechtlichen Anforderungen nur mit Einwilligung der Betroffenen zur Auswertung an Dritte bekannt gegeben werden.

Mit der entsprechenden Konfiguration lassen sich mit folgenden Anwendungen datenschutzkonforme Webstatistiken erstellen.

- [Matomo \(ehemals PIWIK\)](#)
Datenschutzkonforme Open-Source-Anwendung für Webstatistiken, wenn die Daten lokal gespeichert werden
- [Open Web Analytics](#)
Datenschutzkonforme Open-Source-Anwendung für Webstatistiken. Die Daten werden lokal gespeichert.