dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

# Softwarelösungen für IT-Verantwortliche

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

Über Daten, die in die Cloud ausgelagert sind, hat das verantwortliche öffentliche Organ nur noch eine beschränkte Kontrolle. Um die Kontrolle zu behalten, bieten sich lokal installierte Cloud-Lösungen an.

- EtherPad
  Datenschutzfreundliche Alternative zu Google Docs und Office 365 mit lokaler Datenablage
- OwnCloud
  Datenschutzfreundliche Alternative zu Dropbox (Online-Speicher) mit lokaler Datenablage

# 2 Management von Informationssicherheitsmassnahmen

Das Management vieler Informationssicherheitsmassnahmen ist komplex. Um den Aufwand zu reduzieren und die Systematik zu verbessern, können diverse Tools eingesetzt werden.

- i-doit
  Open-Source-CMDB- & IT-Dokumentation
- GRC Tool Box Pro
  Integrierte Softwarelösung für Governance, Risk & Compliance
- verinice
  Open-Source-ISMS-Tool

Auf der Website des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine umfassende Liste von IT-Grundschutztools verfügbar.

# 3 Erstellen eines Inventars

Das Erstellen eines Inventars ist mit grossem Aufwand verbunden. Darüber hinaus besteht das Risiko, dass bestimmte Geräte nicht inventarisiert werden. Um den Aufwand zu reduzieren und die Qualität zu erhöhen, kann auf Softwareunterstützung zurückgegriffen werden.

- Docusnap
  Automatische Inventarisierung des Netzwerks
- José AD Dokumentation
  Inventarisierung des Windows Active Directory (Berechtigungen)
- Lansweeper
  Automatische Inventarisierung des Netzwerks

## 4 Verschlüsseln von E-Mails

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

- Gpg4win
  Open Source Software für die Mailverschlüsselung mit PGP. Bietet zusätzlich 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

## 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. Alle genannten Softwarelösungen unterstützen eine starke Authentifizierung.

- Bitlocker
  Verschlüsselungslösung von Microsoft
- fideAS file
  Dateiverschlüsselung
- FileVault
  Verschlüsselungslösung von Apple
- SafeGuard Encryption
  Festplatten- und Dateiverschlüsselung
- VeraCrypt
  Festplattenverschlüsselung und Containerlösung für die verschlüsselte Dateiablage

## 6 Verwalten von Smartphones

Auf Smartphones befinden sich oft sensitive Daten. Um diese angemessen zu schützen, sollte ein Mobile Device Management (MDM) eingesetzt werden.

- AirWatch EMM Suite
  MDM von VMWare
- Citrix XenMobile
  MDM von Citrix
- Microsoft Intune
  MDM von Microsoft
- MobileIron
  MDM von MobileIron
- Mobility Manager
  MDM von Ivanti
- Unified Endpoint Management
  MDM von Blackberry
- WSO2 Enterprise Mobility Manager
  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 die folgenden Softwarelösungen eingesetzt werden.

- Icinga
  Open-Source-Monitoringsystem
- OpenNMS
  Open-Source-Netzwerkmanagementsystem
- WhatsUp
  Netzwerkmonitoring von Ipswitch

# 8 Sicherer Zugriff über das Internet

Ein externer Zugriff auf interne Daten ist mit erheblichen Risiken verbunden. Insbesondere wenn der Zugriff mit fremden 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. Um diese zu entdecken, empfiehlt sich eine regelmässige Überprüfung auf Schwachstellen. 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 den folgenden Anwendungen lassen sich 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, da die Daten lokal gespeichert werden

V 1.2 / Juli 2018

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh