dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Softwarelösungen für IKT-Verantwortliche

Dieses Merkblatt richtet sich an IKT-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 IKT-Systemen
8. Sicherer Zugriff über das Internet
9. Überprüfen auf Schwachstellen
10. Erstellen von Webstatistiken

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch

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
- Nextcloud
  Datenschutzfreundliche Alternative zu Google Workspace und Microsoft 365 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 IKT-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
- 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 heikle Daten verschlüsselt zu versenden. Dafür können die folgenden Lösungen eingesetzt werden:

- Gpg4win
  Open Source Software für die Mailverschlüsselung mit PGP, mit der 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)
- HIN Mail
  Im Gesundheitswesen verbreitete E-Mail-Verschlüsselungslösung

– Weitere Möglichkeiten zur Verschlüsselung von E-Mails finden Sie auf den DSB-Webseiten E-Mail-Sicherheit und Datenschutzfreundliche Apps

5 Verschlüsseln von Dateien

Um heikle Daten 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
– fideAS file
  Dateiverschlüsselung innerhalb eines Dateisystems
– FileVault
  Verschlüsselungslösung von Apple (Startvolume)
– SafeGuard Encryption von Sophos
  Festplatten- und Dateiverschlüsselung auch bei Datenweitergabe
– VeraCrypt (kostenlos und 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 Intune
  MDM von Microsoft
– Unified Endpoint Manager
  MDM von Ivanti
– WSO2 Enterprise Mobility Management
  Open Source MDM

7 Überwachen von IKT-Systemen

Um die Verfügbarkeit und Sicherheit von IKT-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
– PRTG
  Monitoringsystem von Paessler
– CheckMK
  Open-Source-Monitoringsystem

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.

- OpenVPN
  Open-Source-VPN-Lösung
- VPN- oder ZeroTrust-Lösungen der bekannten Firewall-Hersteller wie beispielsweise Cisco, Fortinet oder Paolo Alto.
- Citrix Gateway
  Verschlüsselte Terminalserver-Anwendungen
- Ivanti Connect Secure
  VPN-Lösung

9 Überprüfen auf Schwachstellen

Die Netzwerke und die Anwendungen enthalten oft unbekannte Schwachstellen. Sie können durch eine regelmässige Überprüfung entdeckt werden. Dafür können beispielsweise die folgenden Softwarelösungen eingesetzt werden.

9.1 Netzwerk

- GFI LanGuard
  Netzwerksicherheitsscanner
- Nessus
  Sicherheitsscanner von Tenable
- OpenVAS
  Open-Source-Schwachstellenscanner
- Nikto
  Open-Source-Schwachstellenscanner

9.2 Webanwendungen

- Acunetix
  Webschwachstellenscanner
- Burp Suite
  Open-Source-Webschwachstellenscanner
- Invicti (ehemals Netsparker)
  Webschwachstellenscanner
- Qualys SSL Server Test
  Scanner für die Überprüfung der TLS/SSL-Webserverkonfiguration
- Zed Attack Proxy (ZAP)
  Open-Source-Webschwachstellenscanner

10 Erstellen von Webstatistiken

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

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

- AWStats
  Datenschutzkonforme Open-Source-Anwendung für Webstatistiken, wenn die Daten lokal gespeichert werden
- Matomo
  Datenschutzkonforme Open-Source-Anwendung für Webstatistiken, wenn die Daten lokal gespeichert werden
- Open Web Analytics
  Datenschutzkonforme Open-Source-Anwendung für Webstatistiken mit lokaler Datenspeicherung
- Nilly
  Datenschutzkonforme Anwendung für Webstatistiken

V 1.9 / Oktober 2024