TOMs für IT

Geltungsbereich der technischen und organisatorischen Maßnahmen

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen (TOMs) sind gem. dem Datenschutzkonzept der Universität Münster sowie den Richtlinien zur IT-Sicherheit auf die vom der Universität Münster CIT bereitgestellten und verwalteten IT-Systeme anzuwenden. Die konkrete Umsetzung wird in den jeweiligen Konzepten für Dienste bzw. Systeme dokumentiert.

Pseudonymisierung

- Bei Bedarf müssen Daten abhängig vom Umfang und Zweck geeignet pseudonymisiert werden. Die Notwendigkeit hierzu muss bereits bei der Konzeption einer Verarbeitung geprüft werden. (Datenschutzkonzept)

Verschlüsselung

- Datenträger von mobilen Endgeräten für den Dienstgebrauch (z. B. Notebooks, Smartphones) sind nach Stand der Technik zu verschlüsseln (Regelung zur Verschlüsselung von mobilen Endgeräten und Datenträgern)
- Die Notwendigkeit zur Verschlüsselung einzelner Dateien, Informationen oder Übertragungswege muss im Einzelnen geprüft und falls nötig umgesetzt werden (RL01.1 Klassifizierung von Informationen)
- Zur Verschlüsselung werden stets geeignete Verfahren nach dem Stand der Technik genutzt (RL02 Sicherer IT-Betrieb)

Vertraulichkeit

Zutrittskontrolle

- Serverräume, Räume für Netz-Infrastruktur und Büroräume sind mit Schließanlagen ausgestattet. Die Vergabe von Zutrittsrechten sowie

die Ausgabe der Schlüssel erfolgt ausschließlich nach einem internen Nutzer-Rollen-Konzept und ist zu dokumentieren
- Die Berechtigung zum Betreten der Serverräume ist auf einen eingeschränkten Personenkreis zu begrenzen und zu dokumentieren (RL02 Sicherer IT-Betrieb)

Zugangskontrolle

- Netzwerkperimeter-Sicherheit (RL06 Sicherheitsrichtlinie Netz)
  - Es wird eine mehrstufige Next-Gen-Firewall mit IPS Funktionalität am Internet-Gateway eingesetzt
  - Es besteht eine Trennung von Sicherheitszonen mit unterschiedlichem Schutzbedarf durch restriktive Firewalls
  - Der externe Zugriff auf Systeme wird durch eine restriktive und jährlich geprüfte Allowliste beschränkt
- Fernzugänge (RL06 Sicherheitsrichtlinie Netz)
  - Zentral geregelter Einsatz von Client-to-Site VPN nach Stand der Technik
  - Zugang mit zentralem Benutzernamen und separatem Passwort
  - Mehrfaktorauthentifizierung für alle administrativen VPN Zugänge (zukünftig für alle VPN Zugänge)
  - Remote Desktop Zugriff beschränkt auf Remote Desktop Gateways
- WLAN (RL06 Sicherheitsrichtlinie Netz)
  - Zentral betrieben und verwaltet sowie nach Stand der Technik abgesichert
  - Zugang mit zentralem Benutzernamen und separatem Passwort
  - Zugriff auf einen eingeschränkten Netzbereich
- Arbeitsplätze (Desktops/Notebooks) (RL02 Sicherer IT-Betrieb)
  - Zugänge müssen angemessen abgesichert sein (mindestens mit Benutzername und Passwort oder gleichwertigen Authentifizierungsmethoden)
  - Administrative Zugänge müssen über Mehrfaktor-Authentifizierung abgesichert werden (z. B. per OTP, Zertifikat mit eToken, SSH Keys)
  - Einsatz von automatischen Bildschirmsperren bei Inaktivität
- Passwortrichtlinien
  - Für zentrale Zugangsdaten werden die jeweiligen Anforderungen durch die zentrale Nutzerverwaltung festgelegt und technisch beim Ändern von Passwörtern erzwungen
  - Administrative Zugangsdaten müssen nach Stand der Technik gewählt und sicher verwahrt sowie genutzt werden (RL02 Sicherer IT-Betrieb)

Zugriffskontrolle

- Berechtigungen müssen angemessen verwaltet und ausschließlich restriktiv vergeben werden (RL02 Sicherer IT-Betrieb)

- Relevante Ereignisse (insbesondere Zugriffsversuche) sollten geeignet protokolliert werden (RL02 Sicherer IT-Betrieb / RL14 Protokollierung und zentrales Logging)

Sicherstellung der Integrität

Weitergabekontrolle

- Vor der Weitergabe von Informationen muss stets ihr Schutzbedarf geprüft werden und ob bzw. wie sie weitergegeben werden dürfen (RL01.1 Klassifizierung von Informationen)

Schutz vor Schadsoftware

- Eingehende und ausgehende E-Mails und Anhänge werden zentral auf Schadsoftware hin untersucht
- Alle Endgeräte und Server sollten, sofern möglich bzw. sinnvoll, mit einem zentral von der Universität Münster bereitgestellten Schutzprogramm ausgestattet werden (RL02 Sicherer IT-Betrieb)

Eingabekontrolle

- Für produktive Dienste und Systeme ist ein geeignetes Logging von wichtigen Ereignissen umzusetzen (RL02 Sicherer IT-Betrieb / RL14 Protokollierung und zentrales Logging)
- Für produktive Dienste und Systeme müssen geeignete Methoden zur sicheren Authentifizierung eingesetzt werden (RL02 Sicherer IT-Betrieb)

Verfügbarkeit und Belastbarkeit

Sicherstellung

- Brandmeldung und Brandbekämpfung
  - Zentrale Serverräume sind mit geeigneten Brandmeldeanlagen mit Brandfrüherkennung ausgestattet
  - Unregelmäßigkeiten werden automatisch der dauerhaft besetzten Leitwarte des lokalen Heizkraftwerks gemeldet sowie an die Feuerwehr weitergeleitet
  - Es stehen geeignete Feuerlöscher in ausreichender Zahl zur Verfügung
- Unterbrechungsfreie Stromversorgung und Notstrom
  - Zentrale Serverräume sind mit geeigneten USVs sowie einer Netzersatzanlage ausgestattet
- Klimatisierung
  - Zentrale Serverräume sind mit geeigneten Anlagen zur Klimatisierung ausgestattet

  - Die Klimatisierung wird kontinuierlich überwacht und Unregelmäßigkeiten werden der dauerhaft besetzten Leitwarte des lokalen Heizkraftwerks gemeldet
- Ausfallsicherheit
  - Für produktive Dienste und Systeme muss bereits bei der Planung auf geeignete Dimensionierung und Redundanz geachtet werden (RL02 Sicherer IT-Betrieb)
- Datensicherung
  - Für produktive Dienste und Systeme muss bereits bei der Planung auf ein geeignetes Konzept zur Datensicherung geachtet werden (RL02 Sicherer IT-Betrieb)
- Monitoring:
  - Für produktive Dienste und Systeme muss geeignetes Logging und Monitoring eingerichtet werden (RL02 Sicherer IT-Betrieb)
- Notfallmanagement
  - Ein übergreifendes Notfallmanagement befindet sich im Aufbau
  - Für produktive Dienste und Systeme muss stets geprüft werden, ob und welche Maßnahmen für Notfälle notwendig sind (RL02 Sicherer IT-Betrieb)
- Wartungsarbeiten
  - Die Infrastruktur der zentralen Serverräume wird regelmäßig und nach Herstellervorgaben gewartet
- Intrusion Detection
  - Netzwerkseitig sind Next-Gen-Firewalls sowie Intrusion Prevention Systeme im Einsatz (RL06 Sicherheitsrichtlinie Netz)
  - Logmeldungen der Firewalls sowie kritischer Systeme werden zentral in einem Security Information and Event Management gesammelt und kontinuierlich ausgewertet (RL14 Protokollierung und zentrales Logging/RL15 Detektion und Behandlung von Sicherheitsvorfällen)
- Patches und Updates
  - Für produktive Dienste und Systeme muss ein geeignetes Konzept zur Überwachung auf und Einspielung von neuen Patches und Updates erstellt werden (RL02 Sicherer IT-Betrieb)

Wiederherstellung

- IT-Hardware
  - Für produktive Dienste und Systeme muss geeignete Hardware mit entsprechenden Wartungsverträgen beschafft werden, um Ersatzsysteme im Rahmen der angestrebten Wiederherstellungszeit zu erhalten (RL02 Sicherer IT-Betrieb)
- Wiederherstellung von IT-Systemen
  - Für produktive Dienste und Systeme muss ein geeignetes Konzept zur Wiederherstellung entwickelt werden (RL02 Sicherer IT-Betrieb)
- Dokumentation
  - Entsprechende Maßnahmen und Anweisungen sind in den jeweiligen

Betriebskonzepten zu dokumentieren (RL02 Sicherer IT-Betrieb)

Wirksamkeitskontrolle

- Dienste werden nach und nach in das ISMS aufgenommen und anhand der BSI IT-Grundschutz-Methodik überwacht (RL13 Überprüfung und Verbesserung der Informationssicherheit)
- Nach Bedarf werden externe oder interne Auditierungen von Diensten/Systemen durchgeführt (RL13 Überprüfung und Verbesserung der Informationssicherheit)
- Automatisierte Schwachstellenscans werden eingesetzt, um grundlegende technische und organisatorische Maßnahmen zu kontrollieren (RL13 Überprüfung und Verbesserung der Informationssicherheit)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Informationssicherheits-Management (ISMS)

- Es wird ein ISMS nach der BSI IT-Grundschutz-Methodik betrieben (RL13 Überprüfung und Verbesserung der Informationssicherheit)
- Nach Bedarf werden externe oder interne Auditierungen von Diensten/Systemen durchgeführt (RL13 Überprüfung und Verbesserung der Informationssicherheit)

Datenschutz-Management

- Eine zentrale Stelle zum Datenschutz-Management wurde eingerichtet (Datenschutzkonzept)
- Mitarbeitende werden für datenschutzrechtliche Anforderungen sensibilisiert und zur Einhaltung dieser verpflichtet (Datenschutzkonzept)
- Datenschutzrelevante Verarbeitungstätigkeiten werden durch einen geregelten Prozess vor der Etablierung geprüft. Bei entsprechender Notwendigkeit werden Datenschutzfolgeabschätzungen durchgeführt (Datenschutzkonzept)
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach (Datenschutzkonzept)

Sicherheitsvorfall-Management

- Als zentrale Stelle zum Management von Sicherheitsvorfällen wurde das CERT der Universität Münster eingerichtet (RL15 Detektion und Behandlung von Sicherheitsvorfällen)

- Prozesse zur zentralen Meldung und Dokumentation von Sicherheitsvorfällen wurden definiert (RL15 Detektion und Behandlung von Sicherheitsvorfällen)
- Sicherheitsvorfälle werden untersucht und ausführlich dokumentiert (RL15 Detektion und Behandlung von Sicherheitsvorfällen)
- Eine Einbindung der Stabsstelle Datenschutz erfolgt bei entsprechender Notwendigkeit (RL15 Detektion und Behandlung von Sicherheitsvorfällen)

Auftragskontrolle / Weisungskontrolle

- Formalisierte Auftragserteilung erfolgt in schriftlicher Form
- Es werden Vereinbarungen zur Auftragsverarbeitung abgeschlossen, wenn Daten bei externen Anbietern verarbeitet werden
- Es werden, soweit möglich, Standardvertragsklauseln der EU verwendet
- Mitarbeitende werden auf die Einhaltung datenschutzrechtlicher Anforderungen sowie auf Geheimhaltung verpflichtet

Autoren

- Dustin Gawron
- Sophie Rydzik
- Dr. Markus Blank-Burian