Sicherheitskonzept Freie Netze München e.V. (FNMUC)

Stand 06/2021

"Zweck des Vereins [Freie Netze München] ist die Erforschung, Anwendung und Verbreitung von kabellosen und kabelgebundenen Netzwerken für die Allgemeinheit (freie Netze), sowie die Verbreitung und Vermittlung von Wissen über Funk- und Netzwerktechnologien, die es Menschen ermöglichen, sich untereinander und als Teil des Internets zu vernetzen." (Satzung §2)

Im Rahmen des Vereinszwecks ist FNMUC als Erbringer von öffentlich zugänglichen Telekommunikationsdiensten und / oder als Betreiber eines öffentlichen Telekommunikationsnetzes gemeldet.
Nach § 109 Abs. 4 TKG ist daher ein Sicherheitsbeauftragter zu benennen und ein Sicherheitskonzept zu erstellen.

Sicherheitsbeauftragter

Der Vorstand des Vereins FNMUC bestellt eine(n) Sicherheitsbeautragte(n).
Bestellt ist aktuell: Ole Dreessen, Sonnenbichlweg 2, 85748 Garching
Telefon 01577-5005516 Email: Mail@dreessen.de

Sicherheitskonzept

A. Infrastruktur; mögliche Gefährdungen und Störungen

1. Netzwerk und Dienste
   FNMUC betreibt Next Generation Netzwerke (NGN) sowie Server- und Netzwerktechnik. Die öffentlich zugänglichen Teile bzw. Schnittstellen der Netzwerkstruktur basieren auf Freifunk-Technologien und können sich systembedingt ständig ändern.

2. Gefährdungen
   Die nichtöffentliche, zum Betrieb des Netzes erforderliche Server- und Netzwerktechnik von FNMUC erfasst Metadaten der Benutzer und Verbindungen und wickelt teilweise den Datenverkehr ab. Mit Zugriff auf diese internen Strukturen ist daher ein Risiko in Bezug auf die Verletzung des Fernmeldegeheimnisses und des Schutzes personenbezogener Daten verbunden.

3. Betriebsstörungen
   Da das öffentlich zugängliche Freifunknetz ohne die zugrundeliegenden nichtöffentlichen internen Komponenten von FNMUC nicht vollumfänglich funktionsfähig ist, ist ein möglichst störungfreier Betrieb dieser wünschenswert.

B. Risikobewertung

1. Es bedarf einer der Nutzung angemessenen Planung, Konfiguration und Absicherung der internen Netzwerkkomponenten sowie einer kompetenten Auswahl des mit Zugriff auf diese legitimierten Personenkreises.

2. Die Beteiligung an den sowie die Nutzung der öffentlich zugänglichen Freifunkdienste erfolgt anonym und ohne Anmeldung. Personenbezogene oder anderweitig verwertbare Daten fallen daher nur in vergleichsweise geringem Umfang an, ein Einbruch/Angriff auf die internen Strukturen aus diesen Gründen ist damit weitgehend uninteressant.

3. Da das öffentliche Netz ohne Gebühren kostenfrei nutzbar ist, gilt generell ein Best-Effort-Ansatz ohne QoS-Garantie. Einschränkungen/Ausfälle haben keine direkten kommerziellen Auswirkungen.
   Das Verursachen von Störungen im Betriebsablauf, der Missbrauch von Infrastruktur und damit eine Einschränkung/Ausfall der öffentlichen Telekommunikationsdienste ist allerdings ein weitverbreitetes und teils finanziell lohnenswertes Phänomen und damit auch für FNMUC ein als relevant einzustufendes Risiko.

C. Technische Vorkehrungen / sonstige Schutzmaßnahmen

1. Organisation, Sicherheitsrollen und Verantwortlichkeiten

   1.1 FNMUC ist als eingetragener Verein organisiert; den Mitgliedern und dem Vorstand obliegen Rechte und Pflichten anhand der aktuell gültigen Satzung. Der Vorstand ist für alle laufenden Angelegenheiten des Vereins verantwortlich und kann einzelne Aufgaben ganz oder teilweise auf einzelne seiner Mitglieder übertragen. Insofern ist der Vorstand auch verantwortlich für den laufenden Betrieb der Infrastruktur und ermächtigt, eine Auswahl zugriffsprivilegierter Personen sowie eines/einer Sicherheitsbeauftragten zu treffen.

   1.2 Der interne Netzbetrieb erfolgt auf geeigneter vereinseigener oder gemieteter Hardware in Rechenzentren nach aktuellen Standards.

2. Personalmanagement

   FNMUC lebt vom Engagement und der regen Beteiligung seiner Mitglieder und der Freifunk-Community. Die Berechtigung zum Zugang zu internen Strukturen erfolgt gezielt individuell nach Vertrauenswürdigkeit und Engagement innerhalb der Community durch das Admin-Team in Rücksprache mit dem/der Sicherheitsbeauftragten und dem Vorstand.

3. Sicherheit von Daten, Systemen und Einrichtungen

   3.1 Sicherer Umgang mit sensiblen Daten und Informationen

   Da die Beteiligung am öffentlichen Teil des Netzwerks sowie die Nutzung der Dienste ohne Anmeldung möglich ist, fallen Bestands-/Stammdaten idR nicht an. FNMUC speichert grundsätzlich nur ein Minimum der zum Betrieb des Netzes und zum Erkennen, Eingrenzen oder Beseitigen von Störungen unbedingt notwendigen Verkehrs- und Steuerdaten. Inhaltsdaten werden übertragen, aber nicht gespeichert.

   3.2 Physische und elementare Schutzanforderungen

   Der Betrieb der internen Infrastruktur erfolgt ausschließlich in Rechenzentren mit ISO/IEC 27001 - Zertifizierung.

   3.3 Versorgungssicherheit

   FNMUC betreibt ein Best-Effort-Netz. Dennoch ist die interne Infrastruktur in mehreren Rechenzentren redundant aufgebaut.

   3.4 Zugriffs- und Zugangskontrolle auf Netzwerk- und Informationssystemen

   Die Zugangskontrolle liegt bei den Betreibern der entsprechend zertifizierten Rechenzentren. Administrative Zugriffe von außen sind ausschließlich durch gesicherte verschlüsselte Zugänge möglich.

   3.5 Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen

   Zusätzlich zu kontinuierlicher Netzwerkanomalieerkennung (Stand 06/2021: sFlow), wird die Infrastruktur von FNMUC regelmäßig durch externe Audits (Stand 06/2021: Shadowserver) überprüft.

   3.6 Vertraulichkeit der Kommunikation

   Von FNMUC bereitgestellte Hypertext-Dienste werden nach aktuellen Standards SSL-verschlüsselt. Die Kommunikation zwischen Freifunk-Geräten (Router, Offloader; allg.: Knoten, Nodes) und der internen FNMUC-Infrastruktur erfolgt grundsätzlich verschlüsselt (Stand 06/2021: Wireguard). Systemlogs können nur von Administration eingesehen werden; allgemeine Kennzahlen sind öffentlich einsehbar.

4. Betriebsführung

   4.1 Betriebsverfahren

   Die Betriebsabläufe und -Ressourcen werden im Community-Chat ständig kommuniziert, überprüft und diskutiert.

4.2 Änderungsmanagement
Da der Vereinszweck des FNMUC Erforschung, Anwendung und Verbreitung auch experimenteller Netzwerke beinhaltet, ist die Infrastruktur einem ständigen Wandel unterzogen. Die potentiellen direkten und indirekten Auswirkungen von Änderungen werden vorab abgewogen, in der Praxis bewertet und überprüft.

5. Störungen und Sicherheitsvorfälle
   5.1 Erkennen von Sicherheitsvorfällen und Störungen
   Die Metadaten von FNMUC werden in Echtzeit erfasst und aufbereitet. Anhand der Metadaten werden automatisiert Benachrichtigungen in entsprechende Kanäle der Community-Kommunikationsmedien gemeldet. Allgemein gehaltene Statistiken und Metriken werden auch öffentlich zur Verfügung gestellt, um eine aktive Mitarbeit der Community zu ermöglichen, potentielle Unregelmäßigkeiten zu erkennen und ggf. das Admin-Team zu benachrichtigen.

   5.2 Umgang mit Sicherheitsvorfällen und Störungen
   Störungen werden nach dem Best-Effort-Prinzip ohne Garantien möglichst zeitnah behoben. Da Dienste ohne Ankündigung eingeschränkt oder eingestellt werden können, ist dies auch bei Sicherheitsvorfällen oder Störungen der Fall.

   5.3 Kommunikation und Meldung von Sicherheitsvorfällen
   Da das Netz anonym zu Verfügung gestellt wird, erfolgt eine Information der Teilnehmer und Nutzer über die öffentlichen Kommunikationsmittel von FNMUC.

6. Not- oder Ausfallmanagement
   6.1 Aufrechterhaltung von Telekommunikationsinfrastrukturen und Diensten
   Die Kerninfrastruktur von FNMUC ist redundant ausgelegt, so dass das Netz auch bei Ausfall eines einzelnen Rechenzentrums weiter funktioniert.

   6.2 Wiederanlauf nach Ausfällen
   Es bestehen verschlüsselte Off-Site-Backups der Systeme sowie Automatismen, um den Betrieb auch an anderen Standorten wieder aufnehmen zu können.

7. Überwachungs- und Testverfahren
   Der gesamte Netzbetrieb wird durch kontinuierliches Monitoring evaluiert und weitestgehend öffentlich protokolliert. Störungen werden automatisiert gemeldet. Administrative Tätigkeiten an betriebsrelevanten Systemen werden zeitlich beschränkt protokolliert.

8. Einhaltung gesetzlicher Anforderungen
   Der Vorstand des FNMUC stellt die Einhaltung gesetzlicher, vertraglicher oder freiwilliger Regeln sicher und beobachtet die Rechtsentwicklung.

Verweise:
- Satzung Freie Netze München e.V.
- Aktuelle Verantwortlichkeiten und Ansprechpartner
- Plan Infrastruktur
- öffentlich einsehbare Kennzahlen

Erklärung zur Umsetzung des IT-Sicherheitskonzepts

Hiermit erklärt der Vorstand, dass das IT-Sicherheitskonzept umgesetzt ist.

Gauting, den 21.09.2021

Tobias McFadden