IT – Sicherheitskonzept

Freifunk Nord

Registernummer bei der Bundesnetzagentur 17/265

Freifunk Nord e.V.

IT-Sicherheitskonzept – Version 3.1 vom 8.3.2019

1. Einleitung

Gemäß §109 Telekommunikationsgesetz (TKG) sind Diensteanbieter verpflichtet, angemessene Vorkehrungen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten zu treffen, sowie die Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu schützen.

Betreiber von Telekommunikationsanlagen, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, sind darüber hinaus verpflichtet, Systeme durch angemessene technische Vorkehrungen oder Maßnahmen gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu schützen.

Dieses Dokument beschreibt das Sicherheitskonzept des Freifunk Nord e.V. Es identifiziert Sicherheitsteilsysteme beim Betrieb des Kommunikationsnetzes und bei der Bereitstellung von Kommunikationsdiensten und beschreibt teilsystemübergreifende und teilsystemspezifische Sicherheitsaspekte.

Der Verein Freifunk Nord e.V.

Aufgabe des Freifunk Nord e.V. ist die Einrichtung und Unterhaltung von Datennetzwerken, betrieb von Datendiensten und Umsetzung von Datensicherheit sowie mit diesen Tätigkeiten zusammenhängende Beratungs- und Dienstleistungshilfen.

2. Identifikation von Sicherheitsteilsystemen

Folgende Sicherheitsteilsysteme werden im Freifunk Nord e.V. unterschieden:

1. Datenverabeitungssysteme (Server)
   - Dedizierte oder Virtuelle Server bei Zertifizierten Dienstleistern
2. Telekommunikationssysteme
   - Mikrotik
   - Ubiquiti
3. Übertragunswege
   - Glasfaserkabel
   - Kupferleitungen
   - Richtfunksysteme
4. Anbindungen an das Internet
   - Transit
   - Private- und Öffentliche Peerings

3. Teilsystemübergreifende Aspekte

Aspekte, die alle Sicherheitssysteme betreffen sind

1. Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationssystemen führen.
2. Schutz der Telekommunikations- und Datenverarbeitungssysteme gegen äußere Angriffe und Einwirkungen von Katastrophen.

3.1 Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen der Telekommunikationssystemen führen

Strom und Klimatisierung sind für Sicherheits-, Telekommunikations- und Datenverarbeitungssysteme von lebenswichtiger Bedeutung. Ein Ausfall von Strom kann nicht verkraftet werden. Ein Ausfall der Klimatisierung kann nur für einen gewissen Zeitraum verkraftet werden. Ein Ausfall der Stromversorgung kann zum einen durch den Wegfall der Stromzulieferung, zum anderen durch Defekte, Wartungs- oder Erweiterungsarbeiten durch Mitarbeiter/Dienstleister verursacht werden.

3.2 Schutz der Telekommunikations- und Datenverarbeitungssysteme gegen äußere Einwirkungen und Katastrophen

Grundsätzlich müssen alle Telekommunikations- und Datenverarbeitungsanlagen gegen äußere Angriffe und Einwirkungen von Katastrophen geschützt werden.

Mögliche Gefährdungen sind insbesondere:

- Unberechtigter Zugang (externe Personen, nicht autorisierte Mitarbeiter)

- Einbruch
- Diebstahl
- Manipulation von Systemen
- Umwelteinflüsse (Feuer, Wasser, Blitz, Sturm)
  - Bei Unseren Serverhostern ist ein modernes Brandfrühesterkennungssystem eingerichtet, das direkt mit der Brandmeldezentrale der örtlichen Feuerwehr verbunden ist (siehe https://www.hetzner.de/pdf/Sicherheit.pdf)

Schutzanforderung ist der Ausschluss dieser Gefährdungen.

Um diese Anforderungen als Freifunk Nord e.V. auch in Zukunft sicherstellen zu können nutzen wir hier nur zertifizierte Rechenzentren durch externe Dienstleister.

3.2.1 Schutz vor unberechtigtem Zugang

Der physikalische Zugriff auf unserer Anlagen ist durch Zugangssysteme, Alarmanlagen, Bewegungsmelder, Wachdienste und Sicherheitstüren unserer Dienstleister in extra dafür zertifizierten Rechenzentren sichergestellt.

3.2.2 Schutz vor Einbruch

Der physikalische Zugriff auf unserer Anlagen ist durch Zugangssysteme, Alarmanlagen, Bewegungsmelder, Wachdienste und Sicherheitstüren unserer Dienstleister in extra dafür zertifizierten Rechenzentren sichergestellt.

3.2.3 Schutz vor Diebstahl

Der physikalische Zugriff auf unserer Anlagen ist durch Zugangssysteme, Alarmanlagen, Bewegungsmelder, Wachdienste und Sicherheitstüren unserer Dienstleister in extra dafür zertifizierten Rechenzentren sichergestellt.

3.2.4 Schutz vor Manipulation von Systemen

Der physikalische Zugriff auf unserer Anlagen ist durch Zugangssysteme, Alarmanlagen, Bewegungsmelder, Wachdienste und Sicherheitstüren unserer Dienstleister in extra dafür zertifizierten Rechenzentren sichergestellt.

3.2.5 Umwelteinflüsse (Feuer, Wasser, Blitz, Sturm)

Der physikalische Zugriff auf unserer Anlagen ist durch Zugangssysteme, Alarmanlagen, Bewegungsmelder, Wachdienste und Sicherheitstüren unserer Dienstleister in extra dafür zertifizierten Rechenzentren sichergestellt.

4. Sicherheitsteilsysteme

Auf die einzelnen Sicherheitsteilsysteme wird hier im folgenden detailliert eingegangen.

4.1 Datenverarbeitungssysteme

Als Datenverarbeitungssysteme oder Datenverarbeitungsanlagen werden Endgeräte („Server“) bezeichnet, die öffentliche Dienste (Web- oder Mailserver zum Beispiel) zur Verfügung stellen oder internen Zwecken dienen.

Gefährdungen dieser Systeme entstehen durch:

- Softwarefehler
- Hardwarefehler
- Zerstörung von Daten
- Unerlaubter Zugriff
- Netzwerkangriffe (z.B. „Denial-of-Service“)

4.1.1 Softwarefehler

Der Freifunk Nord e.V. nutzt größtenteils Software die bereits ausgiebig getestet wurde und testet vor dem Einsatz von neuen Versionen auf Testsystemen um Fehlfunktionen vorher zu erkennen und in produktiven Systemen zu vermeiden. Für Fehler in Produktivsystemen wird ein Monitoringsystem genutzt was direkt an die Systemadministration alarmiert.

4.1.2 Hardwarefehler

Um Ausfälle in der Hardware zu vermeiden bauen wir unsere Systeme Redundant auf und können so Ausfälle verringern. Kritische Bauteile werden von uns oder unseren Dienstleistern bevorratet und können kurzfristig getauscht werden.

4.1.3 Zerstörung von Daten

Um Zerstörung von Daten zu verhindern setzt der Freifunk Nord e.V. auf verschlüsselte dezentrale Backups.

4.1.4 Unerlaubter Zugriff

Die Systeme des Freifunk Nord e.V. sind nur von autorisierten Personen zu erreichen. Administrative Zugriffe sind grundsätzlich nur aus dem dafür angelegten Management Netzwerk möglich und verschlüsselt. Systeme, die keine eigenen ausreichenden Sicherheitsvorkehrungen in der Autorisierung oder Verschlüsselung haben, werden nur isoliert betrieben. Ein Zugriff auf diese Systeme ist nur mittels vorgeschalteter Autorisierung und Verschlüsselung möglich (z.b. via VPN Technologie).

4.1.5 Netzwerkangriffe (z.B. Denial of Service)

Um Angriffe auf unsere Systeme zu vermeiden, nutzen wir Monitoringsysteme mit einer Alarmierung an die Systemadministration. In Zusammenarbeit mit unseren Dienstleistern und Peeringpartnern beteiligen wir uns aktiv an der Angriffsabwehr über entsprechende Systeme wie z.B. Blackholing und Blacklisting. Zur Vermeidung von Schäden sind unsere Systeme Redundant und dezentral aufgebaut. Ein Zugriff auf die System ist auch während Fehlfunktionen über das getrennte Management Netzwerk möglich.

4.2 Datenverarbeitungsysteme für Rechnungstellung

Der Freifunk Nord e.V. verarbeitet keine IP-Verbindungsdaten zu Abrechnungszwecken.

Der Freifunk Nord e.V. verarbeitet keine Kundendaten und betreibt keine Kundendatenbanken.

Die im TK-Netz verwendete IP-Adresse, die einem Router zugeordnet ist, kann keinem zugehörigen Standort bzw. Adresse zugeordnet werden.

4.3 Kommunikationsysteme

Der Transport von Daten zwischen Datenverarbeitungssystemen wird von Kommunikationssystemen übernommen. Der Freifunk Nord e.V. nutzt dafür größtenteils Hardware im OSI-Modell Schicht 2 und 3.

Kommunikationswege in der OSI-Modell-Schicht 2:

- Switche
- Bridges
- Medienkonverter
- VPN-Technologie (Software)

Kommunikationswege in der OSI-Modell-Schicht 3:

- Router
- Antennen

Für diese Geräte sind folgende Gefährdungen möglich:

- Unerlaubter Zugriff
- Softwarefehler
- Hardwarefehler
- Konfigurationsfehler

Der Freifunk Nord e.V. hat folgende Schutzmaßnahmen gegen diese Gefahren unternommen:

Kommunikationssysteme die administrative Schnittstellen zur Verfügung stellen, sind mit diesen nur in einem extra getrennten Management Netzwerk erreichbar. Ein Zugriff ist nur für individuell autorisierte Administratoren über das Management Netzwerk möglich und wird

mittels Zugriffskontrollisten zugewiesen. Wir verwenden keine unverschlüsselten Protokolle für Administration und sperren unverschlüsselte Protokolle aktiv bzw. rüsten verschlüsselte Verfahren über Updates nach. Wir sperren ungenutzte Administrationsmöglichkeiten aktiv. Ein Zugriff eingehend sowie ausgehend in das Internet und/oder unautorisierte IP-Netzwerke ist nicht möglich. Alle Zugriffe und Zugriffsversuche werden protokolliert.

Alle Änderungen an diesen Systemen werden dokumentiert und über ein Revisionskontrollsystem nachverfolgbar und zurücksetzbar. Die Vermeidung von Konfigurationsfehlern wird auch durch die Testsysteme reduziert.

4.4 Übertragungswege

Die vom Freifunk Nord e.V. genutzten Übertragungswege bestehen hauptsächlich aus Glasfaser- oder Kupferkabeln und Richtfunkstrecken. Diese werden von uns oder unseren Dienstleistern oder anderen Providern für uns bereitgestellt.

Gefährdungen für den Betrieb dieser Übertragungswege sind

- Konfigurationsfehler auf Abnehmerseite
- Defekt beim Carrier (Konfiguration / Hardware)
- Defekte Medien (Kabelbruch z.B. durch Bauarbeiten, Sabotage)

Als Schutzanforderung ergibt sich der fehlerfreie Betrieb der Übertragungswege.

Der Freifunk Nord e.V. setzt daher an allen Übertragungswegen (außerhalb des eigenen Sicherheitsbereichs) auf verschlüsselte und via Monitoringsystemen überwachte Verbindungen. Durch Redundante Verbindungen und Systeme werden Ausfälle oder Störungen verringert. Alle Verbindungen (auch über externe Dienstleister) verfügen über eine 24/7/365 Bereitschaftdienst.

4.5 Anbindung an das Internet

Der Freifunk Nord e.V. ist über einen oder mehrere Zwischenprovider (Transit oder Upstream) oder über direkte Netzkopplungen mit dem Internet verbunden. Um Ausfälle zu vermeiden sind Redundanten Verbindungen zu verschiedenen Partnern über unterschiedliche Wege genutzt und mit entsprechenden Reserven ausgestattet.

4.6 **Funknetz der Freifunk Nord e.V.**

Das Funknetzwerk des Freifunk Nord e.V. wird innerhalb von Schleswig-Holstein betrieben. Hierfür werden Frequenzen im 2,4 GHz und 5 GHz Bereich genutzt (BWFA und lizenzierte Frequenzen möglich). Alle Systeme im Funknetz des Backbone Netzwerkes setzen verschlüsselte Verbindungen ein. Der physikalische Zugriff ist über Schlüssel nur autorisierten Personen möglich. Die Backboneverbindungen wie auch die Technikschränke werden aktiv im Montoring überwacht und melden Alarme direkt an die Bereitschaft. Die Backbonetechnik ist mit einer Unterbrechungsfreien Stromversorgung gegen Netzausfall gesichert.

5. Restrisikobewertung

Auch wenn jedes Sicherheitsteilsystem einzeln die Sicherheitsanforderungen erfüllt, kann das Gesamtsystem noch Sicherheitsmängel aufweisen. Aus diesem Grund ist zusätzlich eine Bewertung des Gesamtsystems erforderlich, d.h. das Zusammenwirken der Sicherheits-Teilsysteme, wie auch die Wirkung der angewendeten Schutzmaßnahmen, ist hinsichtlich der Erreichung einer angemessenen Standardsicherheit für das Gesamtsystem zu untersuchen. Daraus ergibt sich gegebenenfalls die Notwendigkeit für weitere zusätzliche Schutzmaß-nahmen, welche über die eines Teilsystems hinausgehen. Denkbar sind Schutzmaßnahmen, die über mehrere, an verschiedenen Orten installierte Sicherheitsteilsysteme wirken oder die erst beim Zusammenwirken von Sicherheitsteilsystemen erforderlich werden. In der abschließenden Risikobewertung soll das bestehende Restrisiko erkannt und bewertet werden. Ziel ist es, dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

Im folgenden Bewerten wir das Gesammtsystem unter den folgenden Schutzzielen:

1. Schutz des Fernmeldegeheimnisses
2. Schutz personenbezogener Daten
3. Schutz vor Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen

5.1. Schutz des Fernmeldegeheimnisses

Eine Kompromittierung eines der sog "Gateways" (siehe Anhang 2) würde die Sicherheit des Fernmeldegeheimnisses der von uns transportierten Datenströme gefärden. Dabei ist es möglich, dass das System ("Gateway") nachhaltig zum mitlesen dieser Daten angepasst wird und ein externer oder ein interner Angreifer Kenntnis von Datenströmen erlangt und/oder eine sog. Man-In-The-Middle Angriff auf Datenströme anwenden. Dieses Risiko ist gleichzusetzen mit dem Risiko, dass ein Angreifer die Infrastruktur an einem beliebigen Punkt innerhalb des Pfads des Datenstroms Kompromittiert. Ein Effektiver Schutz gegen diese Art von Angriffen obliegt der Beschaffenheit des Datenstroms und Schutzmaßnahmen beim Betrieb des Datenstroms durch die Kommunikationspartner. Einwirken auf die Kommunikationspartner solche Schutzmaßnahmen zu ergreifen liegt außerhalb unserer Wirkungskraft. Gegen die Kompromittierung des Systems (Gateway) können sog. Intrusion-Detection-Mechanismen, wie Sie im Teilen von unseren Monitoring Systemen umgesetzt werden, eingesetzt werden.

5.2. Schutz von personenbezogener Daten

Wir erfassen wie oben aufgezeigt keinerlei Daten unserer Nutzer, damit ist eine mögliche Gefärdung ausgeschlossen.

5.3. Schutz vor Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikations-netzen und -diensten führen

Es besteht das Risiko, dass durch nicht erkanntes Fehlverhalten ein Deny-Of-Service ähnliches Verhalten von unserer Infrastruktur ausgeht, was ebenfalls eine Störung unseres Betriebs darstellen würde. Ein durch solche Verhalten erzeugte Menge von Datenströmen sind nur schwerlich von regulären Lastszenarien unterscheidbar, könnten aber anhand ihrer gerichteten Eigenschaften statistisch Erkannt werden. Was wiederum durch Monitoring Systemen aufbereitet von der Bereitschaft ausgewertet und durch oben beschrieben Schutzmaßnahmen unterbunden werden kann.

Anlagen:

1. Begriffsbestimmung
2. Kernnetz und Zugangsnetz
3. Grundsätzliche Struktur des Freifunknetzes
4. Beispiel FF-Router

Anlage 1

Begriffsbestimmung

1. Freifunkrouter (kurz FF-Router) sind Wlan-Router mit einer speziellen Software sogenannt die Freifunkfirmware.

2. Eigentümer des FF-Router ist derjenige, dem der FF-Router (Hardware) gehört.

3. Besitzer des FF-Routers ist derjenige, in dessen Besitz sich der FF-Router (Hardware) befindet.

4. Betreiber des FF-Routers ist derjenige, der Standort und Energie für den Freifunk Router zur Verfügung stellt.

5. Verwalter des FF-Routers ist derjenige der passwortgeschützten oder key basierten Zugang zum FFRouter hat und Einstellungen am FF-Router ändern kann.

6. Eigentümer: Der Eigentümer verfügt über das Recht, seine Netzwerkinfrastruktur zu betreiben und einen Teil ihrer Funktionalität für das freie Netzwerk (FreeNetwork) bereitzustellen (zu stiften, zu spenden).

7. Transit: Transit ist der Austausch von Daten in ein Netzwerk hinein, heraus oder durch ein Netzwerk hindurch.

8. Freier Transit: Freier Transit bedeutet, dass der Eigentümer weder Gebühren für den Transit von Daten erhebt, noch die Daten verändert.

9. Freies Netzwerk: Das Freie Netzwerk ist die Summe der miteinander verbundenen Hard- und Software, dessen Anteil für den freien Transit vom Eigentümer dieser Ressourcen zu Verfügung gestellt wird.

10. Der Dienst: Der Dienst (Betrieb, Service) besteht aus freiem Transit und zusätzlichen Diensten.

11. Zusätzliche Dienste: Im Sinne des PPA ist ein zusätzlicher Dienst alles was über freien Transit hinaus geht. Zum Beispiel die Bereitstellung eines DHCP-Servers, WEB-Servers oder Mail-Servers.

Anlage 2: Kernnetz und Zugangsnetz

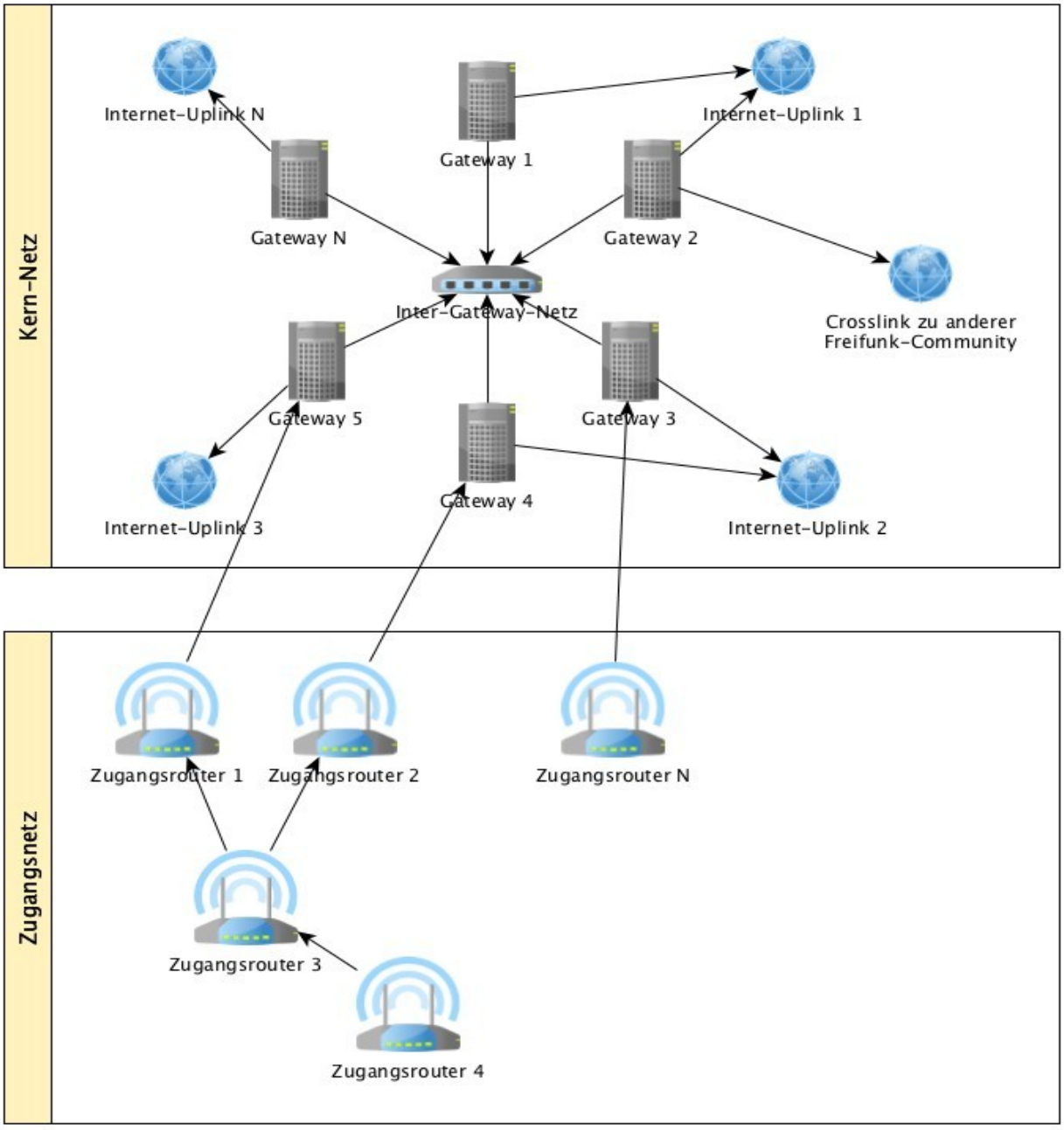

Illustration 1: Schematische Darstellung des Systemverbunds

Bestandteil des Systemverbunds ist das Kern-Netz sowie die Übergänge zu anderen Netzwerken. Nicht Bestandteil des Systemverbunds sind die durch Bürgerinnen oder Bürger verwalteten WLAN-Endgeräte im Zugangsnetz.

Anlage 3: Datenfluss im Systemverbund

Anlage 4:

Beispiel FF-Router

Freifunk Nord e.V.

Ernennung zum Sicherheitsbeauftragten (§ 109 Abs. 4 TKG)

wird für den Freifunk Nord e.V. zum Sicherheitsbeauftragten ernannt.

Kiel, den 7.3.2019

Der Vorstand

Im Auftrag

Erklärung zum IT-Sicherheitskonzept

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

Kiel, den 7.3.2019

Der Vorstand

Im Auftrag