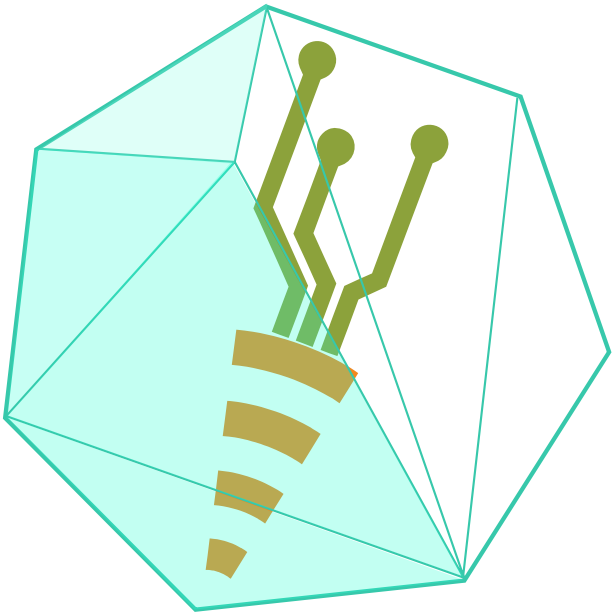
Sicherheitskonzept

Reudnetz w.V.



Reudnetz w. V.
Wurzner Straße 2
04315 Leipzig
mail@reudnetz.org
www.reudnetz.org

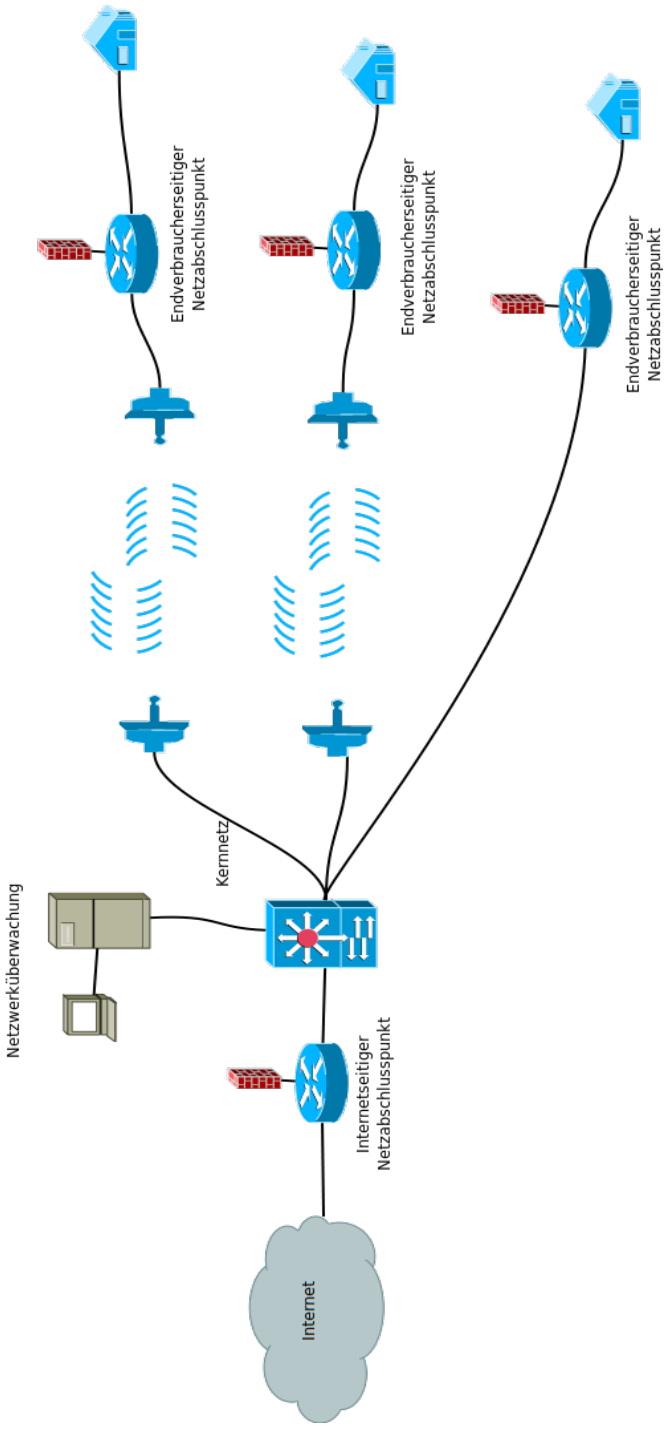
1 Einleitung

Als Infrastrukturdienstleister kommt uns die Verantwortung zu, eine zuverlässige Bereitstellung unserer Dienste sicherzustellen. Dabei müssen die übertragenen Daten im Sinne des Fernmeldegeheimnisses besonders vor Zugriffen geschützt werden und die Ausfallsicherheit der Infrastruktur gewährleistet werden.
Das folgende Sicherheitskonzept beginnt mit einer kurzen Beschreibung der Systemstruktur sowie Definitionen der einzelnen Systemkomponenten. Gefolgt von generellen Sicherheitsrichtlinien, die als grundlegendes Konzept in verschiedenen Szenarien angewendet werden.
Anschließend wird die Systemsicherheit in Bezug auf die zu erfüllenden Schutzziele ausgewertet. Dabei findet eine Bewertung des Schutzbedarfs der einzelnen Komponenten, in Verbindung mit den konkreten Gegenmaßnahmen statt.

Inhaltsverzeichnis

2 Beschreibung der Systemstruktur

2.1 Netzwerkdiagramm



2.2 Definition der Systemkomponenten

2.2.1 Internetseitiger Netzabschlusspunkt (im Folgenden INP)

Der INP ist das System, welches zwischen dem von uns betriebenen Netz und dem restlichen Internet steht. Er wird von uns verwaltet. Er ist ein Netzwerktrennendes Datensicherheitselement, welches nur auf Schicht 3 (nach dem OSI-Modell) operiert. Zudem ist es seine Funktionalität, Datenpakete auf den richtigen Weg zu schicken, und eventuell falsch adressierte Pakete zu verwerfen, so wie sich mit der Gegenseite im Internet über verfügbare Zustellwege auszutauschen.

2.2.2 Endkundenseitiger Netzabschlusspunkt (im Folgenden ENP)

Ein ENP ist das System, welchen zwischen dem von uns und dem von einem Kunden betriebenen Netz steht. Der ENP wird vom Reudnetz w.V. verwaltet. Der ENP ist ein Netzwerktrennendes Datensicherheitselement und hat zudem die Aufgabe, Pakete, welche an das jeweilige Kundennetz adressiert sind in das Kundennetz zu leiten und andere in das Kernnetz weiterzugeben. Der ENP ist meist als ein einzelnes eingebettetes System umgesetzt.

2.2.3 Kernnetz

Das Kernnetz verbindet die anderen Komponenten miteinander und besteht
physisch aus Richtfunkstrecken, Kupferkabeln und Glasfaser.

2.2.4 Mindestspeicherfristerfüllungseinrichtung (im Folgenden MSFEE)

Die MSFEE ist die Einrichtung, welche unsere gesetzlichen Pflichten bezüglich der Speicherung von Verkehrsdaten und deren Abruf technisch erfüllt.
Noch betreiben wir keine MSFEE, da das Gesetz, welches uns dazu verpflichtet und ermächtigt noch nicht in Kraft getreten ist. Unsere Planung orientiert sich jedoch sehr eng an den Vorgaben der Bundesnetzagentur zur Umsetzung der Änderungen am TKG.

2.2.5 Netzwerktrennendes Datensicherheitselement

Ein Netzwerktrennendes Datensicherheitselement steht zwischen zwei oder mehr Netzwerken und hat die Aufgabe, Zugriffe zwischen diesen Netzen nach gesetzten Regeln einzuschränken. Es gibt zwei Varianten, welche auch parallel eingesetzt werden können und sich dadurch unterscheiden auf welcher OSI-Schicht sie operieren. Auf Schicht 3 können Pakete, welche unberechtigterweise von einem in ein anderes Netz übergeben werden sollen, aufgehalten werden. Auf Schicht 4 werden bestimmte Kommunikationsprotokolle reglementiert. In Kombination können dementsprechend auch bestimmte Kommunikationsprotokolle von bestimmten Quellen zu bestimmten Zielen selektiv erlaubt oder verboten werden.

2.2.6 Netzwerküberwachungseinheit

Die Netzwerküberwachungseinheit ist ein automatisiertes System, welches statistische Daten über den momentanen Zustand des von uns verwalteten Netzes und seiner Teilsysteme aufzeichnet und verarbeitet. Diese können von einem Netzwerkverwalter abgerufen und interpretiert werden. Des Weiteren hat sie die Funktion, einen Netzverwalter zu Benachrichtigen, wenn ein überwachter

Kennwert eine Schwelle über- oder unterschreitet, welches auf eine Fehlfunktion eines Teilsystems hinweist.

3 Sicherheitsrichtlinien

3.1.1.1 Datensparsamkeit

Es wird stets die kleinstmögliche Menge an Daten erhoben, mit denen der jeweilige Zweck erfüllbar ist.

3.1.1.2 Systemtrennung

Separat lösbare Probleme sind mithilfe von möglichst unabhängigen Systemen zu lösen, so dass eine eventuelle Beeinträchtigung eines Systems kein anderes in Mitleidenschaft zieht.

3.1.1.3 Kleinhalten der Angriffsoberfläche

Zur Lösung von Problemen und zur Bereitstellung von Funktionalität ist immer das einfachste Werkzeug, welches diese Aufgabe erfüllt, einzusetzen.

3.1.1.4 Beschränkung der menschlichen Fehlerquelle

Zugriff auf Systeme ist immer nur dem kleinstmöglichen Personenkreis, welcher in der Lage ist das System funktionsfähig zu halten, zu gewähren.

3.1.1.5 Verschlüsselung

Wo möglich ist Verschlüsselung einzusetzen, sowohl auf Transportwegen, als auch bei der Datenhaltung, um Angriffe zu erschweren. Sollten sich durch neue technische Entwicklungen oder mathematische Erkenntnisse die eingesetzten Algorithmen als überholt herausstellen sind diese unverzüglich durch modernere Alternativen zu ersetzen.

3.1.1.6 Ersetzbarkeit

Systeme sind so anzulegen, dass deren Einrichtung einfach ist und schnell umgesetzt werden kann, so dass diese bei Ausfällen schnell ersetzt werden können.

3.1.1.7 Redundanz

Zentrale Systeme sind in mehreren Instanzen zu installieren, so dass bei Ausfall des Primärsystems das Sekundäre die Funktion des Primärsystems übernehmen kann.

4 Evaluierung der Systemsicherheit

Die Evaluierung der Systemsicherheit wird anhand der Schutzziele gegliedert. Zu Beginn werden die nicht betroffenen Einheiten genannt. Danach folgt eine detaillierte Beschreibung der Sicherheitsrisiken und -vorkehrungen der betroffenen Einheiten.

4.1 Schutz des Fernmeldegeheimnisses

Über die Netzwerküberwachung und die MSFEE laufen keine Internetverbindungen, eine Verletzung des Fernmeldegeheimnisses ist also nicht möglich.

4.1.1 INP

Erlangt ein Angreifer Kontrolle über einen INP, so kann er den gesamten unverschlüsselten Internetverkehr aller Nutzenden mitlesen und manipulieren. Es besteht erhöhter Schutzbedarf

4.1.1.1 Sabotage von Außen

Um Sabotage von Außen auf die Infrastruktur erfolgreich durchzuführen, muss der Angreifer direkten physischen Zugriff auf den INP erlangen.

Gegenmaßnahmen

Der INP befindet sich innerhalb eines abschließbaren Technikschrankes.
Der Technikschrank befindet sich innerhalb eines abgeschlossenen Raumes.
Der Raum befindet sich innerhalb eines Wohnhauses.
Um physischen Zugriff auf den INP zu erlangen, muss zunächst in den Raum eingedrungen werden. Dies kann geschehen, indem die Tür aufgebrochen wird oder der Angreifer Zugriff auf den Schlüssel erhält.
Das Aufbrechen der Tür ist hinreichend erschwert, da das Wohnhaus, in dem sich der Raum befindet ganzjährig bewohnt ist und sich somit schweres Gerät, wie es zum Aufbrechen der Tür notwendig wäre, nicht unbemerkt an transportieren lässt. Auch die Geräuschentwicklung erschwert ein unbemerktes Eindringen.
Das Erlangen eines Schlüssels wird erschwert, indem alle Schlüssel bei Vorstandsmitgliedern verbleiben und nur für konkrete Arbeiten an die Ausführenden vergeben werden.
Ein Angreifer, der in den Raum eingedrungen ist, muss zusätzlich in den Technikschrank einbrechen. Die Ausführungsmöglichkeiten und Gegenmaßnahmen sind die Gleichen wie zur Verhinderung eines Eindringens in den Raum.
Zusätzlich verfügt der Technikschrank über einen elektronischen Eindringlingsalarm, der über Vorfälle alarmiert.

4.1.1.2 Installation eines Abhörgerätes

Sollte ein Angreifer erfolgreich eindringen, könnte dieser ein Abhörgerät auf dem internetseitigen Kabel installieren um den Datenstrom mitzulesen.

Gegenmaßnahmen

Die Installation eines Abhörgerätes würde aufgrund des dadurch erzeugten Verbindungsverlust auffallen, und deshalb kurzfristig entfernt werden.

4.1.1.3 Offensichtliche Manipulation des INP

Der Angreifer könnte auch den INP selbst, beispielsweise durch Installation eines alternativen Betriebssystems manipulieren und den Datenstrom oder Teile dessen mitlesen.

Gegenmaßnahmen

Sicherheitsrichtlinie: 5
Das Betriebssystem des INP ist verschlüsselt, eine gezielte Manipulation des Betriebssystems in abgeschalteten Zustand ist also unmöglich. In angeschaltetem Zustand ist sie durch restriktive Benutzerrechte und starke Passwörter unterbunden.

4.1.1.4 Subtile Manipulation des INP

Der Angreifer könnte statt das gesamte Betriebssystem zu ersetzen, den Teil ersetzen, welcher beim Start das Entschlüsselungspasswort entgegen nimmt, und zwar in einer Weise, dass dieses das Entschlüsselungspasswort unverschlüsselt speichert oder ein alternatives Betriebssystem lädt.

Gegenmaßnahmen

Aufgrund der großen physischen Hürden ist eine unbemerkt durchgeführte Manipulation sehr schwierig und dieses Restrisiko in Kauf zu nehmen.
Eine mögliche Gegenmaßnahme wäre allerdings, das Abtrennen des Entschlüsselungsprogrammes vom Restsystem, um ihn sicher zu verwahren. Das Problem der sicheren Verwahrung ist damit aber nicht gelöst.

4.1.1.5 Ausnutzen einer Sicherheitslücke

Ein Angreifer nutzt eine Sicherheitslücke in der auf dem INP installierten Software aus.

Gegenmaßnahmen

Sicherheitsrichtlinien: 2, 3
Auf dem INP läuft eine auf die Anwendung zugeschnittene Softwareauswahl, die über Signaturen eindeutig für Sicherheitsaudits verfügbarem Quellcode zugeordnet werden kann. Durch einen großen Umfang an Software ist auch die Anzahl an möglichen Fehlerquellen und Angriffsvektoren groß. Eine Gegenmaßnahme stellt die Beschränkung auf notwendige Programme dar, die stets mit aktuellen Sicherheitsaktualisierungen versorgt werden. Durch ein Netzwerktrennendes Datensicherheitselement werden mögliche Zugriffe auf den INP gesteuert und reglementiert. Des Weiteren werden einzelne Anwendungen, soweit dies möglich ist, in unabhängige Virtuelle Server ausgelagert um manipulierter Software keinen Zugriff auf weitere Anwendungen zu geben.

4.1.1.6 Manipulative Kommunikation

Einem Angreifer gelingt es, den Zugangsschlüssel zum INP durch manipulative Kommunikation mit zugangsberechtigten Menschen zu erhalten.

Gegenmaßnahmen

Sicherheitsrichtlinie: 4
Nur einer kleinen Personengruppe sind die Zugangsschlüssel bekannt.
Zusätzlich wird über die Gefahren von Angriffen solcher Art aufgeklärt.

4.1.1.7 Zugangsschlüssel aus anderen Geräten extrahieren

Ein Angreifer erlangt den Zugangsschlüssel durch das Eindringen in ein Gerät, auf dem der Schlüssel hinterlegt ist.

Gegenmaßnahmen

Sicherheitsrichtlinien: 2,3,4,5
Die Zugangskennung wird nicht auf weiteren Systemkomponenten verwendet. Hauptrisiko stellt hier der Umgang der Personen mit dem Zugangsschlüssel dar, dieses lässt sich durch Informieren der Personen und zuverlässiges Personal reduzieren.

4.1.1.8 Internetseitiges Abhören

Ein Angreifer greift den Netzwerkverkehr an der internetseitigen Anschlussschnittstelle des INP ab.

Gegenmaßnahmen

Fällt in den Zuständigkeitsbereich, des mit uns verbundenen Internetserviceproviders.

4.1.1.9 Kernnetzseitiges Abhören

Ein Angreifer greift den Netzwerkverkehr an der kernnetzseitigen Anschlussschnittstelle des INP ab.

Gegenmaßnahmen

Fällt unter "Schutz des Kernnetzes".

4.1.2 Kernnetz

Der Schutz des Fernmeldegeheimnisses ist für das Kernnetz relevant, da alle Endnutzerdatenverbindungen durch dieses laufen. Es besteht erhöhter Schutzbedarf

4.1.2.1 Sabotage von Außen

Um das Fernmeldegeheimnis zu verletzen muss der Saboteur physischen Zugriff auf das Kernnetz haben, um ein Abhörgerät anzubringen, welches dann Datenströme (eventuell selektiv) ausleitet.

Gegenmaßnahmen

Sicherheitsrichtlinie: 4
Das Kernnetz befindet sich hinter mehreren physischen Schutzschichten; von Außen nach Innen: Ein Wohnhaus, abgeschlossene Räumlichkeiten, abgeschlossene Technikschränke oder ein Wohnhaus, gemauerte Kabelschächte.
Ein unbemerkter Einbruch in das Wohnhaus wird erschwert, da es ganzjährig bewohnt ist. Dasselbe gilt für Räume, Schränke und Mauerwerk.
Die Alternativmöglichkeit ist die Beschaffung sämtlicher elektronischer Zugangskarten und Schlüssel um gewaltfrei einzudringen.
Dies wird erschwert, indem die Schlüssel nur bei Vorständen liegen und nur für konkrete Arbeitsvorgänge an autorisiertes Personal ausgegeben werden.
Der Saboteur müsste ein Abhörgerät an einem Kabel anbringen. Entweder in der Mitte eines Kabels, wo statt eines Eindringens in die Technikschränke und Räumlichkeiten ein Eindringen in Kabelschächte notwendig wäre oder zwischen eine Buchse und ein Kabel.

Beide Eingriffe würden jedoch in der Netzwerküberwachung aufgrund der kurzzeitigen Verbindungsunterbrechung auffallen, was eine Untersuchung des Kernnetzes und eine Entfernung des Abhörgerätes nach sich ziehen würde.
Für eine weitere Erhöhung der Sicherheit wurde eine Transportwegverschlüsselung im gesamten Kernnetz evaluiert, aufgrund der geringen Wahrscheinlichkeit eines erfolgreichen Angriffs und dem hohen technischen Aufwand jedoch verworfen.

4.1.2.2 Ausnutzen einer Sicherheitslücke

Ein Angreifer nutzt eine Sicherheitslücke, einer der im Kernnetz verwendeten Komponenten, aus.

Gegenmaßnahmen

Sicherheitsrichtlinien: 2, 3
Durch einen großen Umfang an Programmen ist auch die Anzahl an möglichen Fehlerquellen und die Angriffsfläche groß. Eine Gegenmaßnahme stellt die Beschränkung auf notwendige Programme dar, die stets mit aktuellen Sicherheitsaktualisierungen versorgt werden. Durch ein Netzwerktrennendes Datensicherheitselement werden mögliche Zugriffe auf das Kernnetz und die darin enthaltenen Geräte gesteuert und reglementiert.

4.1.2.3 Mitlesen an einem Knoten

Ein Angreifer greift den Netzwerkverkehr an einem Knoten des Kernnetzes ab.
Entweder muss er dazu über eine ausnutzbare Sicherheitslücke einer Komponente oder über einen physikalischen Zugang zu einem Teil des Kernnetzes verfügen.

Gegenmaßnahmen

Siehe Sabotage.

4.1.3 ENP

Erlangt ein Angreifer Kontrolle über einen ENP so kann er den gesamten unverschlüsselten Internetverkehr eines Nutzenden mitlesen und manipulieren. Es besteht Schutzbedarf

4.1.3.1 Sabotage von Außen

Um das Fernmeldegeheimnis zu verletzen muss der Saboteur physischen Zugriff auf den ENP erhalten. Da dessen Software aufgrund von technischen Beschränkungen nicht verschlüsselt ist, könnte er das installierte Betriebssystem manipulieren und/oder Transportwegsverschlüsselungsschlüssel austauschen.

Gegenmaßnahme

Jeder ENP steht in Räumlichkeiten des entsprechenden Endnutzers, im Besonderen nicht im öffentlichen Raum. Die konkreten Sicherungen liegen somit auch im Einflussbereich des Nutzers.
Um die Auswirkungen eines potentiellen Zugriffs zu minimieren, wird die Erreichbarkeit aller ENPs permanent überwacht und Eindringlingserkennungssysteme eingesetzt.
Außerdem werden alle eingesetzten symmetrischen, und damit auch auf den ENP gespeicherten, Transportwegsverschlüsselungsschlüssel zwischen den ENPs und dem Kernnetz regelmäßig ausgetauscht.

4.1.3.2 Ausnutzen einer Sicherheitslücke

Ein Angreifer nutzt eine Sicherheitslücke in der auf dem ENP installierten Software aus.

Gegenmaßnahme

Sicherheitsrichtlinien: 2, 3
Auf den ENP werden stets die aktuellen Sicherheitsaktualisierungen des Herstellers eingespielt. Durch ein Netzwerktrennendes Datensicherheitselement werden mögliche Zugriffe auf den ENP gesteuert und reglementiert. Dadurch wird ein Ausnutzen von Sicherheitslücken weiter erschwert.

4.1.3.3 Manipulative Kommunikation

Einem Angreifer gelingt es, den Zugangsschlüssel zum ENP, durch manipulative Kommunikation mit zugangsberechtigten Menschen, zu erhalten.

Gegenmaßnahme

Sicherheitsrichtlinie: 4
Nur einer kleinen Personengruppe sind die Zugangsschlüssel bekannt.
Zusätzlich wird über die Gefahren von Angriffen solcher Art aufgeklärt.

4.1.3.4 Zugangsschlüssel aus anderen Geräten extrahieren

Ein Angreifer erlangt den Zugangsschlüssel durch das Eindringen in ein Gerät, auf dem der Schlüssel hinterlegt ist.

Gegenmaßnahme

Sicherheitsrichtlinie: 2, 3, 4, 5
Die Zugangskennung wird nicht auf weiteren Systemkomponenten verwendet. Hauptrisiko stellt hier der Umgang der Personen mit dem Zugangsschlüssel dar, dieses lässt sich durch Informieren der Personen reduzieren.

4.1.3.5 Kernnetzseitiges Abhören

Ein Angreifer greift den Netzwerkverkehr an der kernnetzseitigen Anschlussschnittstelle des INP ab.

Gegenmaßname

Fällt unter "Schutz des Kernnetzes". (siehe)

4.2 Schutz personenbezogener Daten

Der INP, das Kernnetz, die ENP und die Netzwerküberwachung verarbeiten keine personenbezogenen Daten.

4.2.1 MSFEE

Die MSFEE verarbeitet personenbezogene Daten, damit muss sie besonders vor unautorisiertem Zugriff geschützt werden.

4.2.1.1 Sabotage von Innen

Ein Saboteur könnte versuchen zur zugangsberechtigten Person erklärt zu werden und so Daten zu extrahieren.

Gegenmaßnahmen

Sicherheitsrichtlinien: 4, 5
Das vorgeschriebene Vier-Augen-Prinzip wird eingesetzt, somit könnte ein unberechtigter Zugriff durch einen einzelnen Saboteur von der weiteren zugangsberechtigten Person verhindert werden.
Unsere Sicherheitsprotokolle verbieten weiterhin die Mitnahme von elektronischen oder elektrischen Geräten in die MSFEE-Räume, so dass die Extraktion der Daten stark erschwert wird.

4.2.1.2 Sicherung gegen Sabotage von Außen

Ein Saboteur könnte auch als Unberechtigter versuchen in die MSFEE einzudringen.

Gegenmaßnahmen

Sicherheitsrichtlinie: 5
Die Überwachungsdaten werden nur vollverschlüsselt vorliegen. Im laufenden Betrieb werden die Daten durch ein Authentifikationssystem mit starken Passwörtern geschützt.
Heiße und kalte Angriffe werden dadurch stark erschwert. Der Raum wird schall- und funkisoliert, so dass unberechtigtes Abgreifen der Überwachungsdaten während eines autorisierten Vorganges erschwert wird.

4.3 Schutz gegen Störungen

Störungen der Komponentenverfügbarkeit können aufgrund verschiedener Ursachen auftreten. Störungen aus böswilliger Absicht sind oft vergleichbar mit den Methoden, mit denen beispielsweise das Fernmeldegeheimnis angegriffen wird.
Zusätzlich gibt es Störungen, die sich aus Unfällen und Naturkatastrophen ergeben. Diese werden gesondert am Ende des jeweiligen Abschnitts behandelt.

4.3.1 INP

Bei Störung des INP ist die Netzwerkanbindung aller Nutzenden beeinträchtigt. Dies ist ein kritisches Szenario, das besonderer Schutzmaßnahmen bedarf.

4.3.1.1 Physische/terroristische Angriffe

Die Angriffsszenarien und Gegenmaßnahmen sind identisch mit denen, die unter „Schutz des Fernmeldegeheimnisses gegen Sabotage von Außen“ genannt werden.

4.3.1.2 Zugriff erlangen

Um den INP dauerhaft zu stören, abzuschalten oder fremdgesteuert zu verwenden, muss ein Angreifer Zugang zu den Funktionen des Gerätes erhalten.

Gegenmaßnahmen

Hier gilt dasselbe wie für Angriffe auf den INP zur Erlangung der Fernmeldedaten. (siehe 4.1.1)

4.3.1.3 Angriffe durch extrem zahlreiche Anfragen (AdezA)

Aus dem Internet kann der INP Ziel von Angriffen durch extrem zahlreiche Anfragen (AdezA) werden. Die so angegriffene Systemkomponente, kann bei ausreichend hoher Anzahl von Anfragen überlastet werden und so an Funktionalität verlieren.

Gegenmaßnahmen

Gegen diese können wir uns nur bedingt schützen. Durch redundante Anbindungen und große Bandbreite lässt sich der Aufwand für eine derartige Störung stark erhöhen. Gleichzeitig ist das Risiko, eines solchen Angriffes eher gering und hinterlässt über die Dauer des Angriffes hinaus keine nachhaltigen Schäden. Um die Einschränkung der Verbindungsqualität während eines solchen Angriffes auf ein Minimum zu reduzieren, lassen sich, auch in Absprache mit weiteren Dienstleistern, Verbindungen von bestimmten Adressbereichen unterbinden.

4.3.1.4 Hochwasser

Da der INP aktuell in einem Kellerraum untergebracht ist, könnte er von Hochwassern betroffen sein.

Gegenmaßnahmen

Der INP und die gesamte zu seinem Betrieb notwendige Technik sind in mehr als einem Meter Höhe über dem Boden angebracht. Damit befindet sie sich außerhalb der bisher aufgetretenen Wasserhöchststände für dieses Gebiet. Darüber hinaus ist der Keller mit einer automatischen Pumpe mit ausreichender Fördermenge ausgestattet.

4.3.1.5 Gebäudebrand

Das Gebäude, in dem der INP untergebracht ist, kann abbrennen.

Gegenmaßnahmen

Dem normalen Schutz des Gebäudes ist Nichts hinzugefügt. Als weitere Sicherheit ist eine komplett redundante Netzstruktur in Form eines Kreises als Fernziel angestrebt.

4.3.1.6 Stromausfall

Erfahrungsgemäß kann es geschehen, dass die Stromversorgung für kurze Zeit aus den verschiedensten Ursachen unterbrochen wird.

Gegenmaßnahmen

Der INP ist mit einer Notstromversorgung ausgestattet, die den Betrieb für mindestens zwei Stunden sicherstellt. Dieser Zeitraum liegt deutlich über der üblichen Ausfalldauer.
Im Falle eines Stromausfalles verschickt der INP Warnmeldungen. Ausrüstung zur manuellen Sicherung der Stromversorgung über einen längeren Zeitraum ist vorhanden.

4.3.1.7 Unbeabsichtigte Zerstörung durch Dritte (Baumaßnahmen)

Der INP ist in einem abgetrennten Raum untergebracht, der nur von zugangsberechtigten Personen betreten werden kann.

4.3.2 Kernnetz

Da ein größerer Ausfall des Kernnetzes auch einen größeren Ausfall, der zur Verfügung gestellten Dienstleistung nach sich ziehen würde, ist ein Schutz gegen Störungen relevant.

4.3.2.1 Physische/terroristische Angriffe

Ein Angreifer erlangt gewaltsam physischen Zugang zum Kernnetz.

Gegenmaßnahme

Das Kernnetz ist, mit Ausnahme der Richtfunkstrecken, in Kabelschächten in abschließbaren Räumlichkeiten verlegt. Ein physischer Angriff auf dieses ist mit ähnlich hohem Aufwand verbunden, wie ein Angriff auf den INP.

4.3.2.2 Zugriff erlangen

Um das Kernnetz dauerhaft zu stören, abzuschalten oder Komponenten fremdgesteuert zu verwenden, muss ein Angreifer Zugang zu den Funktionen der Geräte erhalten.

Gegenmaßnahmen

Hier gilt dasselbe wie für Angriffe auf das Kernnetz zur Erlangung der Fernmeldedaten. (siehe 4.1.2)

4.3.2.3 Angriffe durch extrem zahlreiche Anfragen (AdezA)

Um eine vorübergehende Störung des Kernnetzes zu erreichen, wäre ein Angriff durch extrem zahlreiche Anfragen denkbar, bei dem die Geräte durch zu viele Anfragen überlastet werden und vorübergehend nicht reagieren.

Gegenmaßnahmen

Netzwerktrennende Datensicherheitselemente an den Außenseiten des Kernnetzes verhindern Verbindungen zu Komponenten des Kernnetzes aus dem Internet und dem kundenseitigen Netz. Dadurch kann ein derartiger Angriff nur von internen Netzwerkkomponenten aus erfolgen. Diese sind durch die jeweiligen Sicherheitsvorkehrungen geschützt.

4.3.2.4 Gebäudebrand

Das Gebäude, in dem Komponenten des Kernnetzes untergebracht sind, kann abbrennen.

Gegenmaßnahmen

Dem normalen Schutz des Gebäudes ist Nichts hinzugefügt. Als weitere Sicherheit ist eine komplett redundante Netzstruktur in Form eines Kreises als Fernziel angestrebt.

4.3.2.5 Stromausfall

Erfahrungsgemäß kann es geschehen, dass die Stromversorgung für kurze Zeit aus den verschiedensten Ursachen unterbrochen wird.

Gegenmaßnahmen

Alle kritischen Komponenten des Kernnetzes sind mit einer Notstromversorgung ausgestattet, die den Betrieb für mindestens zwei Stunden sicherstellt. Dieser Zeitraum liegt deutlich über der üblichen Ausfalldauer.

Im Falle eines Stromausfalles verschicken der INP und die Netzwerküberwachung Warnmeldungen. Ausrüstung zur manuellen Sicherung der Stromversorgung über einen längeren Zeitraum ist vorhanden.

4.3.2.6 Unbeabsichtigte Zerstörung durch Dritte (Baumaßnahmen)

Teile des Kernnetzes sind trotz räumlicher Trennung im Rahmen von Baumaßnahmen zu erreichen. Dadurch könnten sie von unachtsamen Personen zerstört werden.

Gegenmaßnahmen

Wo immer möglich sind die Komponenten des Kernnetzes außerhalb des Einflussbereiches Dritter aufgestellt. Für Einige lässt sich das jedoch nicht umsetzen.
Die betroffenen Komponenten des Kernnetzes sind deutlich gekennzeichnet und weisen auf die Rechtsverletzung hin, die mit ihrer Störung oder Zerstörung einhergeht. Die Netzwerküberwachung registriert Ausfälle von Komponenten. Diese werden unverzüglich ersetzt.

4.3.3 ENP

Bei Störung des ENP ist die Netzwerkanbindung eines einzelnen Nutzenden beeinträchtigt. Dies ist zu vermeiden, bedeutet aber nur geringen Schutzbedarf.

4.3.4 Physische/terroristische Angriffe

Um den ENP funktionsunfähig zu machen sind viele Angriffsszenarien denkbar, vom einfachen Eindringen und gezielt Zerstören bis zu einem vollständigen Angriff, bei welchem Brandsätze und/oder Explosivstoffe zur Zerstörung des Standpunktes eingesetzt werden.

Gegenmaßnahme

Sicherheitsrichtlinie: 6
Es wird nicht versucht die Zerstörung zu verhindern, sondern eine schnelle Wiederherstellung der Funktionalität sichergestellt, indem ein ständiger Vorrat an Ersatzgeräten gehalten wird, aus dem zerstörte ENP innerhalb eines Werktages ersetzt werden können.

4.3.4.1 Zugriff erlangen

Um den ENP dauerhaft zu stören, abzuschalten oder fremdgesteuert zu verwenden, muss ein Angreifer Zugang zu den Funktionen des Gerätes erhalten.

Gegenmaßnahmen

Hier gilt dasselbe wie für Angriffe auf den ENP zur Erlangung der Fernmeldedaten. (siehe 4.1.3)

4.3.4.2 Angriffe durch extrem zahlreiche Anfragen (AdezA)

Um eine vorübergehende Störung des ENP zu erreichen wäre ein Angriff durch extrem zahlreiche Anfragen denkbar, bei dem die Geräte durch zu viele Anfragen überlastet werden und vorübergehend nicht reagieren.

Gegenmaßnahmen

Als Gegenmaßnahme verhindert das Netzwerkstrennende Datensicherheitselement Verbindungen zum ENP aus dem Internet. Dadurch kann ein derartiger Angriff nur von internen Netzwerkkomponenten aus und aus dem Netz des jeweiligen Nutzenden erfolgen. Diese sind durch die jeweiligen Sicherheitsvorkehrungen geschützt.

4.3.4.3 Gebäudebrand

Das Gebäude, in dem der ENP untergebracht ist kann abbrennen.

4.3.4.4 Gegenmaßnahmen

Dem normalen Schutz des Gebäudes ist Nichts hinzugefügt. Wie bei Schutz gegen Sabotage/ Zerstörung wird der ENP zeitnah ersetzt.

4.3.4.5 Stromausfall

Erfahrungsgemäß kann es geschehen, dass die Stromversorgung für kurze Zeit aus verschiedenen Ursachen unterbrochen wird. Bei Ausfall ist jedoch nur ein Anschluss betroffen.

Gegenmaßnahmen

Auf besonderen Wunsch der Nutzenden kann eine Notstromversorgung eingerichtet werden.

4.3.4.6 Unbeabsichtigte Zerstörung durch Dritte (Baumaßnahmen)

Da die ENP stets in Räumen der Nutzenden untergebracht sind, können sie von unachtsamen Personen gestört oder zerstört werden.

Gegenmaßnahmen

Die ENP sind deutlich gekennzeichnet und weisen auf die Rechtsverletzung hin, die mit ihrer Störung oder Zerstörung einhergeht. Die Netzwerküberwachung registriert Ausfälle.

4.3.5 MSFEE

Auch wenn der Betrieb einer MSFEE für den Netzbetrieb vollkommen unbedeutend ist, ist der Nichtbetrieb mit hohen Geldstrafen belegt, wir sind also gezwungen die MSFEE gegen Störungen zu sichern.

4.3.5.1 Physische/terroristische Angriffe

Ein Angreifer könnte versuchen durch physische Gewalt, Brand- oder Sprengsätze die MSFEE zu beschädigen oder zu zerstören.
Da die MSFEE von Behörden der Kriminalitätsbekämpfung genutzt wird und gegen die Erhebung der Daten von verschiedenen Gruppierungen, welche im Leipziger Raum aktiv sind, Einspruch geäußert wurde, halten wir dieses Angriffsszenario für möglich.

Gegenmaßnahmen

Sicherheitsrichtlinien: 6, 7
Als Gegenmaßnahme werden besonders verstärkte Türen, sowohl für die Räume, als auch für die Technikschränke und ein stilles bewegungsaktiviertes Alarmsystem eingesetzt.
Des Weiteren werden die Daten dreifach redundant gespeichert und es werden die technischen Geräte für eine vollständige MSFEE auf Vorrat gehalten, um zerstörte Komponenten ohne Verzögerung durch Lieferzeiten ersetzen zu können.

4.3.5.2 Angriffe ohne physischen Zugang zu den Komponenten (Hackerangriff)

Zwischen der MSFEE und dem Kernnetz oder dem Internet existiert eine Luftlücke. Störungen ohne physischen Zugang sind somit ausgeschlossen.

4.3.5.3 Gebäudebrand

Das Gebäude, in dem die MSFEE untergebracht ist, kann abbrennen.

Gegenmaßnahmen

Dem normalen Schutz des Gebäudes ist Nichts hinzugefügt.

4.3.5.4 Stromausfall

Erfahrungsgemäß kann es geschehen, dass die Stromversorgung für kurze Zeit aus verschiedenen Ursachen unterbrochen wird.

Gegenmaßnahmen

Durch einen Stromausfall kommt es lediglich zu einer Verzögerung des Einspielens neuer Daten oder der Datenabfrage.

4.3.5.5 Unbeabsichtigte Zerstörung durch Dritte (Baumaßnahmen)

Die MSFEE ist in einem abgetrennten Raum untergebracht, der nur von zugangsberechtigten Personen betreten wird.

5 Gesamtsystematische Analyse

5.1 Sabotage von Innen

Für eine Sabotage von Innen muss ein Saboteur in die Organisation eingeführt werden.
Dieser könnte zwei Ziele verfolgen, direkte Sabotage der operativen Systeme oder Lähmung der Organisation.
Reudnetz w.V. ist in seiner Organisationsstruktur als Verein mit offenen Anmeldungen gegenüber der Einführung von Saboteuren besonders gefährdet.
Zur direkten Sabotage muss der Saboteur Zugang zu Zugangsdaten zu den Operativen Systemen erlangen. Dies wird verhindert, indem diese Zugangsdaten nur einer sehr begrenzten Personengruppe zugänglich gemacht werden, diese nur erweitert wird, wenn es aufgrund des Arbeitsaufwandes unabdingbar notwendig ist und alle Zugangsdaten ausgetauscht werden, sobald eine der berechtigten Personen ausgetauscht wird.
Im April 2016 beträgt die Größe der berechtigten Personengruppe zwei Personen.
Zur indirekten Sabotage durch Lähmung der Organisation ist es für den Saboteur ausreichend an Organisationstreffen und Mitgliederversammlungen teilzunehmen, wozu er bereits durch eine simple Mitgliedschaft berechtigt ist.
Die Gegenmaßnahme setzt an der Tatsache an, dass das Verhalten des Saboteurs sich zumindest subtil von dem eines konstruktiven Mitgliedes unterscheiden muss. Sollte irgend einem Teilnehmer während

einer Mitgliederversammlung oder eines Organisationstreffens ein solches Verhalten auffallen, wird dieses einem Vorstandsmitglied gemeldet, welches dann Ermittlungen einleitet. Dieses Verfahren ist in der Geschäftsordnung geregelt.
Die Mitglieder werden regelmäßig über sabotierende Verhaltensmuster aufgeklärt.

5.2 Angriffe ohne physischen Zugang zu den Komponenten

Zur allgemeinen Verbesserung des Schutzes gegen Angriffe, die auf Fehlern in den von uns eingesetzten Komponenten, entweder durch Sicherheitslücken oder durch Fehlkonfiguration, basieren, fordern wir aktiv dazu auf uns auf gemachte Fehler hinzuweisen.
Vergangene Fälle, in denen Unternehmen nach Bekanntwerden von Sicherheitsdefiziten ihrerseits, durch Ignoranz und Strafandrohung, Ausnutzung oder Veröffentlichung des Sicherheitsdefizits provoziert haben, legen nahe, ein Kommunikationsorgan für solche Fälle anzulegen.
Als einfache strukturelle Maßnahme, Sicherheitsrisiken zu minimieren, richten wir eine Kommunikationsschnittstelle ein, an die sich Personen wenden können, die einen Sicherheitsmangel entdeckt haben und fordern explizit dazu auf, uns über derartige Vorfälle zu informieren.
Wir kümmern uns um öffentliche Dokumentation der von uns eingesetzten Technik, da sich in der Vergangenheit bei verschiedenen Unternehmen Versuche Sicherheit durch Verschleierung zu erreichen als grobe Fehlgriffe erwiesen. Des Weiteren fördert dieses Verhalten die Vereinsstruktur, da es mündige Mitglieder ermöglicht, die ein vollständiges Verständnis der Infrastruktur besitzen, über die sie entscheiden.

5.3 Abschlussbemerkung

Wir sind überzeugt, durch diese Maßnahmen das verbleibende Restrisiko auf ein akzeptables Maß zu reduzieren. Besonders hohe Anforderungen stellen wir an ein ausgeprägtes Fehlerbewusstsein aller bei uns tätigen Technikerinnen und Technikern, da gerade Fehleinschätzungen und Fahrlässigkeit eines der am schwierigsten zu bewertenden Sicherheitsrisiken darstellen. Durch Aufklärung bezüglich der auftretenden strukturellen Risiken und Probleme wirken wir diesem Problem entgegen. Austausch mit anderen Internetdienstleistern und Weiterbildung der an der Technik arbeitenden Personen tragen des Weiteren dazu bei.