FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Netzwerksicherheitskonzept der FAU

1 Einleitung

Das Netzwerksicherheitskonzept der FAU hat zum Ziel die Sicherheitsrisiken in Bezug auf das Datennetz mit einem Bündel an IT-Sicherheitsmaßnahmen auf ein akzeptables Maß zu reduzieren bzw. erst gar nicht entstehen zu lassen. Hierzu müssen sowohl technische als auch organisatorische Maßnahmen betrachtet werden. Im Folgenden werden die gegenwärtig vom RRZE für das gesamte Datennetz der FAU praktizierten Maßnahmen zur Erhöhung des Sicherheitsniveaus kurz umrissen.

1. Maßnahmen organisatorischer Natur

1.1 Stellenwert des Themas Netzwerksicherheit innerhalb der FAU-Organisationsstruktur

Essentiell für das Erreichen eines ausreichenden Maßes an IT-Sicherheit ist ein regelmäßiger und konstruktiver Austausch der technischen Diensterbringer mit den entsprechenden Funktionsträgern auf den organisatorischen Leitungsebenen.

An der FAU bzw. am RRZE wird die Thematik der IT-Sicherheit durch zahlreiche Maßnahmen innerhalb der Verwaltungsstrukturen transportiert, wie z. B.

- die stetige Vermittlung des Themas IT-Sicherheit in die universitäre Leitungsebene
- die enge Abstimmung mit dem CIO bzw. den CISO-Funktionsträgern
- die Kontaktpflege mit den jeweiligen IT-Sicherheitsbeauftragten an den dezentralen Einrichtungen, um Ansprechpartner für das RRZE bzgl. aller sicherheitsrelevanter Themen zu generieren
- die Freigabe personenbezogener Prozesse in Zusammenarbeit mit dem universitären Datenschutzbeauftragten
- die Bildung einer vertrauenswürdigen abteilungsübergreifenden Arbeitsgruppe zur Behandlung von IT-„Abuse“-Fällen

1.2 Definition von Regeln und Richtlinien

Die Definition und Kommunikation klarer Regeln und Richtlinien sind ein essentieller Bestandteil im Bereich der IT-Sicherheit. Das RRZE veröffentlicht in diesem Sinne als zuständige Instanz für die Konzeption, den Aufbau und den Betrieb des zentral verwalteten Datennetzes der FAU auf den entsprechenden RRZE-Webseiten die jeweils dafür geltenden Regeln und Richtlinien.

Neben den technischen Benutzungsrichtlinien werden dort auch die Zuständigkeits- und Verantwortungsbereiche zwischen Endnutzer, IT-Betreuer und Diensterbringer klar definiert und geregelt.

1.3 Regeln für die Beschaffung

Für einen stabilen und sicheren Betrieb der weit über tausend aktiven Komponenten des Datennetzes ist es unerlässlich, dass die Geräte sowohl den Anforderungen des technischen Betriebs als auch der laufenden Pflege und Wartung in jeder Hinsicht genügen.

Zu diesem Zweck stehen an der FAU regelmäßig Rahmenverträge zur Beschaffung von Datennetzkomponenten in den Bereichen Switching, Routing und WLAN zur Verfügung. Diese Verträge werden im Rahmen des Arbeitskreises Bayerisches Hochschulnetz (BHN) von den teilnehmenden Einrichtungen gemeinsam erarbeitet und ausgeschrieben. Eine Beschaffung ausschließlich über die bestehenden Rahmenverträge wird nicht zuletzt unter den Aspekten der IT-Sicherheit als verbindlich angesehen, da sie neben der Vereinfachung der Beschaffung den teilnehmenden Einrichtungen gleichzeitig ein hohes Maß an Sicherheit gewährt:

- Die technischen Komponenten werden im Vorfeld des Rahmenvertrags im Wettbewerbsverfahren auf Tauglichkeit überprüft.
- Eine ungewollte Beschaffung von „Grauware“ und im schlimmsten Fall kompromittierter Geräte wird wirksam unterbunden.
- Es wird ein langfristiger Support der angebotenen Komponenten angeboten.
- Der Zugriff auf wichtige sicherheitskritische Softwareupdates wird unkompliziert zur Verfügung gestellt.
- Schulungen und Consulting-Leistungen für die angebotenen Komponenten können in Anspruch genommen werden.

1.4 Personalmanagement

Die Leistungsfähigkeit und das angebotene Maß an Sicherheit innerhalb der Netzwerkinfrastruktur hängen unmittelbar mit den zur Betreuung beauftragten Mitarbeiterinnen und Mitarbeitern zusammen. Nicht zuletzt fällt dem Thema Personalmanagement aus diesem Grund eine Schlüsselrolle zu: Die Weiterbildung des Personals und ein offenes und konstruktives Arbeitsklima im Sinne eines „crew ressource management“ - sind an der FAU bzw. dem RRZE speziell bei sensiblen IT-sicherheitsrelevanten Themen ein ebenso wichtiger Aspekt wie die Schaffung einer ausreichenden Personaldecke.

2. Maßnahmen zum Schutz der Klienten im Netz

2.1 Netztrennung durch Netzwerksegmentierung

Der Aufbau des Netzes erfolgt nach dem Prinzip einer möglichst hohen Segmentierung lokaler Netze (LANs). Die Infrastruktur wird hierbei ggf. nach Anwendern oder Anwendungen in einzelne LAN-Segmente mit dazugehörigen individuellen Adressräumen unterteilt. Übergänge zwischen den einzelnen LAN-Segmenten sind nur an definierten Stellen angesiedelt (i.d.R. durch Gateways bzw. Router), wo bei Bedarf eine Filterung bzw. ein Firewalling des Datenverkehrs zwischen den Netzbereichen stattfinden kann. Bedrohungen und Störungen werden auf diese Weise eingedämmt und deren Ausbreitung auf andere Bereiche verhindert.

2.2 Einsatz von Firewalling und Perimeterschutz

Speziell im Hochschulumfeld, das einen traditionell eher niedrigen Regulierungsgrad mit gleichzeitig hohem Anteil an Nutzerfluktuation (Studierende, befristet Beschäftigte) aufweist, müssen zum Schutz der Ressourcen im Netz auch die Zugriffsmuster innerhalb einer Organisation eigenständig und gesondert betrachtet werden. Aus diesem Grund werden vom RRZE an der FAU in Absprache mit den IT-Beteuern vor Ort regelmäßig auch die vielen Netzsegmente innerhalb der Organisation mit zum Teil strikten Filterregeln voneinander (teil)isoliert.

Innerhalb der FAU findet zu diesem Zweck an den Grenzen der lokalen Netze mindestens eine Filterung per Access-Control-Listen (ACLs) statt. Besonders gesicherte Abschnitte wie z.B. die Netze der universitären Verwaltung, werden zudem mittels einer dedizierten Firewall geschützt.

Am Übergang zum X-WiN/Internet werden einige, als schädlich erachtete Dienste (z.B. unverschlüsselte Dienste wie „telnet“ oder nicht autorisierte Mailserver), aus Gründen der Datensicherheit in eingehender Richtung standardmäßig geblockt und können erst nach dedizierter Freigabeaufforderung betrieben werden. Rechnern ohne Registrierung im Domain-Name-Service (DNS) wird die Kommunikation ins Internet regelmäßig verwehrt.

Eine Zusammenstellung des Schutzbedarfs in den Subnetzen vor Ort bzw. das sich daraus ergebende Regelwerk wird in Absprache mit den IT-Verantwortlichen des jeweiligen Netzbereichs auf Basis von Klassifizierungen und anschließender Feinparametrierung erstellt. Dabei wird für Klassen von Netzen möglichst umfassend und nachvollziehbar definiert, welche Kommunikationsbeziehungen sie standardmäßig haben dürfen (Ausprägung per Positiv- oder Negativlisten).

Beispiele für Netzklassen an der FAU:

- Arbeitsplatzrechner (mit unterschiedlich eingestuften Sicherheitsniveaus)
- Server / „DMZ-Bereiche“ (je nach Anwendungsbereich wie z.B. Webserver, Mailserver, ...)

- VoIP-Telefone
- Bürodrucker
- Multifunktionskopiergeräte inklusive Scanner
- Gebäudeleittechnik / Schließtechnik / Überwachungstechnik
- Potentiell verwundbare Geräte ohne aktiven Herstellersupport (z.B. Labor und Messgeräte auf Basis älterer Windowsversionen)
- Sondernetzbereiche bzw. Netzwerke zu Forschungszwecken
- Management-Schnittstellen der Datennetzkomponenten (siehe „Managementnetze“)

Entsprechende Firewall- oder ACL-Mechanismen werden idealerweise beim Anlegen eines neuen Netzes auf der Basis seiner Klasse automatisch aktiv geschaltet. Alle künftigen bzw. notwendigen Änderungen in den Netzzugriffsrechten werden als genau definierte Abweichung davon erfasst und dokumentiert. Aus Gründen der Revisionssicherheit wird jede Regeländerung grundsätzlich schriftlich angefordert.

2.3 Einsatz geeigneter Adressierungsrichtlinien

Hinsichtlich der zu verwendenden IPv4/v6-Adressbereiche für die einzelnen Netzbereiche korelliert in aller Regel der Gültigkeitsraum der IP-Adressen mit dem festgelegten bzw. abzusehenden Regelwerk des Netzes bzw. der Netzklasse. So kommen z.B. global gültige IP-Adressen nur dann zum Einsatz, wenn auf die entsprechenden Systeme hauptsächlich von außerhalb der Organisation bzw. vom Internet aus zugegriffen werden muss (z.B. im Sinne eines IT-Dienstes für externe Nutzer).

Wo immer möglich, wird auf private Adressbereiche zurückgegriffen, um generelle Angriffsflächen von außen zu vermindern und die ohnehin nur spärlich vorhandenen globalen IPv4-Adressressourcen einzusparen.

Bzgl. eines potentiellen IPv4-/IPv6-Dualstackbetriebs wird regelmäßig auf einen identischen Gültigkeitsbereich der beiden Adressräume geachtet (private vs. globale Adressen).

3. Maßnahmen zum Schutz der Netzwerkinfrastruktur

Die Netzwerkinfrastruktur (d.h. passive wie aktive Komponenten) muss in ihrer Gesamtheit gegen möglichst viele Einwirkungen und Angriffe unterschiedlicher Natur geschützt werden. Dies betrifft die physikalische Absicherung ebenso wie den logischen Zugang auf die einzelnen Komponenten.

3.1 Physikalische Absicherung

Standardmäßig wird eine Reihe von Maßnahmen umgesetzt, die den physikalischen Zugriff auf die räumlichen Verteilerstrukturen betreffen. So gilt für die FAU-weit stark verteilen Netzwerkinfrastrukturen grundsätzlich, dass Zugriff auf deren Komponenten regelmäßig nur dem berechtigten Personenkreis aus dem RRZE sowie ggf. berechtigten Personen aus dem Bereich des Gebäudemanagements der FAU zugänglich ist.

Insbesondere beutet dies:

- Verteilerschächte auf dem Gelände sind regelmäßig gegen Zugriff gesichert,
- Verteilerräume in Gebäuden sind nur einem genau definierten und für die Aufrechterhaltung des Betriebs berechtigten Personenkreis zugänglich,
- ggf. werden alle im Raum befindlichen Verteilerschränke zusätzlich verschlossen,

- bei Verteilerschränken mit gemeinsam berechtigtem Zugriff durch andere Benutzergruppen (z.B.: IT-Betreuer vor Ort) kommen bevorzugt elektronische Schließsysteme mit entsprechenden elektronischen Schlüsseln (Token) zum Einsatz.

3.2 Versorgungstechnische Absicherung

Für die innerhalb der Infrastrukturverteilerräume zur Verfügung gestellten Energiezuführung sowie der daraus folgenden Wärmeableitung wird regelmäßig auf Einhaltung geltender technischer Standards geachtet. Insbesondere gilt:

- Es sollte als Minimalanforderung mindestens ein eigener Stromkreis pro Verteilerraum zur Verfügung stehen.
- Einer Einflussnahme von außerhalb des Raumes (z.B. durch das Auslösen von Leitungsschutzschaltern oder den Zugriff auf Sicherungskästen) muss in ausreichender Art und Weise entgegengetreten werden.
- Die Klimatechnik muss für die aktiven Komponenten des Raumes ausreichend dimensioniert sein. Eine Einflussnahme von außen (z.B. eine Blockade von Lüftungsgittern an der Tür) muss möglichst ausgeschlossen werden.
- Eine unterbrechungsfreie Stromversorgung per USV ist zu etablieren, wenn die IT-Versorgung vor Ort dies als notwendig erachten lässt.
- Die technische Ausprägung der Netzteile der eingesetzten Komponenten muss mit der ggf. vor Ort vorhandenen Diversität der Energieversorgung (z.B. „Stadtstrom“, USV-Strom, Ersatzstromversorgung) harmonieren und deshalb ggf. über mehrere Einspeisungen verfügen.

3.3 Logische Absicherung

Um unautorisierte Zugriffe bzw. eine Manipulation der Geräte über das Netz selbst oder über drahtlose Verfahren im Nahbereich auszuschließen bzw. zu minimieren, gilt beim Aufbau neuer Netzstrukturen sowie für ihren weiteren Betrieb:

- Ein Management-Zugriff erfolgt ausschließlich über dedizierte und dafür vorgesehene und abgesicherte Management-Schnittstellen bzw. über eine Management-Infrastruktur.
- Nahbereichszugriffsmöglichkeiten der Geräte (z.B. Provisionierung per Bluetooth) werden nach erfolgter Inbetriebnahme grundsätzlich abgeschaltet.
- Zur Vermeidung einer potentiellen Ausnutzung von Sicherheitslücken der Komponenten erfolgt die Gerätepflege mit aktueller Soft-/Firmware.
- Zur Vermeidung einer Netzmanipulation durch manipulierte Protokollnachrichten (OSPF, BGP, ...), ist eine exakte und sorgfältige Konfiguration der vom Gerät bedienten Netzwerkprotokolle notwendig.
- Zur Vermeidung von Denial-of-Service-Szenarien gegen die Infrastruktur im LAN-Bereich werden grundlegende Mechanismen gegen Schleifenbildung und Flooding im LAN-Bereich aktiviert (z.B. STP/Loop-Protect/Rate-Limiting, ...).
- Damit ein Dienst in bestimmten LAN-Fehlersituationen aufrecht erhalten werden kann, werden grundlegende Mechanismen gegen Angriffe auf IP-Ebene aktiviert (Anti-Spoofing, ARP-Protection, DHCP-Snooping,…).

3.4 Absicherung durch Betrieb dedizierter Management-Netze

Die Schnittstellen zum administrativen Zugang auf die Netzwerkkomponenten sind in einem oder mehreren dediziert dafür vorgesehenen Netzbereich(en) untergebracht, die von allen anderen Netzbereichen entkoppelt sind (sog. Management-Netze). Das RRZE betreibt hierbei für die Masse aller in der Fläche installierten Komponenten sog. Inbound-Management-Netze, d.h. die einzelnen Netzkomponenten betreiben neben den normalen Betriebsnetzen auch ihr eigenes Management-Netz.

Für die wichtigsten Komponenten des Kernnetzes existiert zusätzlich ein dediziertes Outbound-Management-Netz, das über eigene Geräte und Leitungen bereitgestellt wird und komplett unabhängig von den zu verwaltenden Komponenten ist. Es ist besonders stabil gegenüber Störungen und Ausfällen, erfordert jedoch einen erheblich höheren Aufwand an Ressourcen.

3.5 Absicherung durch funktionale Redundanz

Netzkomponenten von herausragender funktionaler Bedeutung sind grundsätzlich redundant aufgebaut, um auch bei einem Ausfall den Betrieb für wesentliche Teile der Hardware weiterhin sicherzustellen.

Herausragende funktionale Bedeutung haben in diesem Sinne alle Netzkomponenten, die gemäß dem Prinzip des hierarchischen Netzwerkdesigns als Kernnetzkomponenten (sog. Core-Router) ausgelegt sind, weiterhin alle funktionstragenden Netzkomponenten des zentralen RRZE-Datacenters sowie - sofern der Anwendungszweck dies erfordert - ausgewählte Netztechnik für Netzkomponenten in der Fläche vor Ort.

Je nach räumlichen Voraussetzungen erfolgt die Etablierung dieser Redundanzen im Idealfall durch räumlich getrennte Gerätepaare (Bsp.: Gebäudekomplex RRZE), mindestens jedoch durch eine Doppelung oder Mehrfachauslegung wesentlicher Hardwarekomponenten eines modular aufgebauten Gerätes (Intra-Chassis-Redundanz): In diesem Fall sind die redundanten Komponenten grundsätzlich „hot-swap-fähig“, d.h. für einen Austausch im laufenden Betrieb ausgelegt.

Spannungsversorgende Komponenten (Netzteile) werden, neben der modularen und redundanten Bauweise, - soweit verfügbar - grundsätzlich auch mit mehreren Einspeisungen pro Netzteil ausgestattet. Hierbei erfolgt regelmäßig eine Aufteilung über Energiezuleitungen von „Stadtstrom“, USV-gepufferter Energieversorgung sowie Ersatzstromversorgung (soweit jeweils vorhanden).

Alle zu Redundanzzwecken doppelt aufgebauten Netzkomponenten bzw. deren CPU-Module oder Linecards werden, soweit netztechnisch realisierbar, grundsätzlich über eine möglichst disjunkte Leitungsführung an die übergeordneten Komponenten des Kernnetzes angeschlossen.

Datenleitungen im Weitverkehrsnetz zwischen den Kernnetzkomponenten werden grundsätzlich redundant ausgelegt. Dabei wird im Verlauf der weiteren Entwicklung des Netzes darauf hingewirkt, durch strategische Baumaßnahmen, wo immer möglich, zusätzliche Leitungsredundanzen und damit Disjunktheit in der Trassenführung herzustellen, um gegenüber Beschädigungen von Leitungswegen im Feld weitestgehend abgesichert zu sein.

Innerhalb des RRZE-Datacenters wird grundsätzlich eine maximale Redundanz über durchgängig getrennte Gerätepaare mit doppelter Anbindung aller bis an das angeschlossene Endgerät (i.d.R. Server) realisiert, um netzseitig eine maximale Verfügbarkeit der dort verorteten Dienste zu gewährleisten.

4. Maßnahmen zum Schutz vor unberechtigter Nutzung

Ein wesentlicher Faktor für die Bewertung der IT-Sicherheit besteht in einer Bestandsaufnahme aller möglichen Zugangspunkte, über die Benutzer bzw. Geräte an das Datennetz der Organisation gelangen.

4.1 Absicherung von LAN-Zugängen

Sofern Netzzugangspunkte (Netzwerkdosen) in öffentlich zugänglichen Räumen installiert sind, werden diese, soweit wie möglich, gegen missbräuchliche Nutzung abgesichert. Dies betrifft nicht nur freie und gegenwärtig nicht verwendete Anschlussdosen, sondern auch die Anschlussdosen von Geräten wie z.B. Kopiermaschinen, Verkaufsautomaten oder Kartenterminals, die oftmals in öffentlichen Räumen betrieben werden. Aufgrund der hoch verteilten und nur zum Teil homogenen Infrastruktur kommen hierbei, je nach Einsatzort, unterschiedliche Methoden zum Einsatz, wie z.B.:

- Festverdrahtungen
- Schlüsseldosen
- IEEE 802.1x
- „NAC“-Mechanismen
- Portsecurity
- Script/Eventbasierte (De-)Aktivierung von Ports

4.2 Absicherung von WLAN-Zugängen

Der Betrieb des flächendeckenden WLANs wird in Hinblick auf den Sicherheitsstandard (d.h. Verschlüsselung und Authentifizierung) grundsätzlich mindestens nach dem „Stand der Technik“ betrieben, um unbefugte Nutzung und Mithören des Datenverkehrs wirksam zu unterbinden.

In der Praxis wird dies u. a. durch die Etablierung folgender Maßnahmen erreicht:

- Aktuelle Standards für große WLAN-Netze (z.B. WPA „Enterprise“-Standards),
- individuelle Benutzerkennungen oder zertifikatsbasierte Authentifizierung,
- Abkündigung alter Standards (WPA, WEP),
- Vermeidung von Preshared-Keys WLANs.

Speziell für die Bereitstellung eines einheitlichen Sicherheitsniveaus gilt hierbei analog zum LAN-Bereich, dass WLAN-Installationen an der FAU standardmäßig vom RRZE konzipiert, installiert und betrieben werden.

4.3 Definierte Bereitstellung von Remote-Zugängen (Client-VPN)

Für die Remote-Einwahl in das Intranet der FAU über das öffentliche Internet per VPN-Technologien gilt:

- Zugänge werden ausschließlich über die offizielle Einwahltechnik der FAU bzw. des RRZE bereitgestellt.
- Jeder Benutzer erhält während des VPN-Zugangs eine eindeutige und individuelle IP-Adresse.
- Für besonders schutzwürdige Nutzungsszenarien kommt eine 2-Faktor-Authentifizierung zum Einsatz.
- Die angebotene Technik bietet mindestens einen Grad an Verschlüsselung nach dem „Stand der Technik“ unter Berücksichtigung der Empfehlungen des BSI, LSI und des DFN Certs.

4.4 Definiertes Verfahren bzgl. Netzkopplungen (Site-2-Site VPN)

Bzgl. Netzkopplungen zwischen Netzbereichen der FAU bzw. zwischen FAU-Netzen und externen Netzen (z.B. von Firmen und externen Instituten) gilt:

- Netzkopplungen werden für die FAU ausschließlich vom RRZE konzeptioniert und betrieben.
- Auf strikte Einhaltung der Vorgaben bzgl. Sicherheitsrichtlinie (s. Klassifizierung und Filterung) der zu koppelnden Netze wird geachtet.
- Es wird auf Beibehaltung eines einheitlichen Adressraums innerhalb des gesamten Intranets der FAU geachtet.

5. Maßnahmen zum Schutz der Daten auf externen Leitungswegen

Die Qualität und die Sicherheit der verwendeten Techniken zur Standortvernetzung spielt speziell im Hochschulumfeld, das in den letzten Jahren von einer starken räumlichen Expansion geprägt war, eine wesentliche Rolle. Speziell im Weitverkehrsumfeld sind die Einhaltung der Vertraulichkeit und Integrität der übertragenen Daten sowie die angebotene Performance unter Berücksichtigung der Kosten die wesentlichen Bewertungsmerkmale.

Während an fest umrissenen Campusarealen in aller Regel auf eigene Kabelinfrastrukturen und LWL-Trassen zurückgegriffen werden kann, muss beim Thema Standortvernetzung für Anmietungen von Liegenschaften in Streulagen oftmals auf die Dienste kommerzieller Provider/Carrier zurückgegriffen werden. In einigen Fällen kann hierbei auch auf drahtlose Weitverkehrsvernetzungen (Richtfunkstrecken, „Laserlinks“, ...) ausgewichen werden.

5.1 Gewährleistung von Datenschutz- und sicherheit

Vertraulichkeit und Abhörsicherheit innerhalb des gesamten Intranets muss grundsätzlich flächendeckend gegeben sein, d.h. innerhalb eines Gebäudes ebenso wie zwischen Gebäuden und im Bereich der Weitverkehrsvernetzung. Erfordert es der Schutzbedarf der zu versorgenden Netzbereiche bzw. der zu übertragenden Daten unter Bewertung der vorliegenden Anbindungstechnik, müssen ggf. zusätzliche Sicherheitsebenen auf der Übertragungsschicht eingesetzt werden, wie z.B.

- 802.1AE MACsec,
- IP-Sec,
- Sonstige VPN-Techniken.

Dies gilt grundsätzlich und in jedem Fall bei Anbindungen über Funk und über einen öffentlichen Internetzugang. Darüber hinaus (z.B. bei der Anmietung von dedizierten Standleitungen) erfolgt eine Prüfung des Einzelfalls unter Einbeziehung der vorliegenden Anbindungstechnik und darauf verlaufenden Datenverbindungen. Unerheblich ist hierbei, ob die übertragenen Daten auf höherer Protokollebene (z.B. durch SSL/TLS) selbst verschlüsselt sind, da bei potentieller Einsichtnahme in den Kommunikationsdatenstrom, die nach wie vor sichtbaren Informationen (z.B. Quell- und Zieladresse) schon für sich schutzwürdige Daten darstellen.

5.2 Gewährleistung ausreichender Performance

Speziell bei der Anbindung neuer Liegenschaften in Streulagen muss im Hinblick auf Aufrechterhaltung eines hohen Maßes an IT-Sicherheit deren Datenanbindung ausreichend dimensioniert und für einen professionellen Mehrbenutzer ausgelegt sein. Auf diese Weise sind die vom RRZE zentral bereitgestellten Dienste jederzeit erreichbar und die Nutzung von „Seitenkanälen“ (z.B. der Datenkonnektivität von Smartphones in Verbindung mit Private Clouds) wird minimiert.

Im Rahmen der Verwendung kommerzieller Produkte zur Standortvernetzung bedeutet dies, dass standardmäßig professionelle Datendirektverbindungen („Festverbindungen“) gegenüber kostengünstigeren „consumer“-Produkten (z.B. auf A/V-DSL-Basis), insbesondere im Hinblick auf die Einhaltung der IT-Sicherheitsvorgaben, bevorzugt werden.

Sie zeichnen sich u. a. durch die Merkmale

- ausreichend hohe Datenrate,
- symmetrische Datenrate,
- niedriges Latenz- und Jitterverhalten,
- Übergabe auf Layer 2, Terminierung durch eigene Router,
- hohe Jahresverfügbarkeit und
- zeitnahe Entstörung

aus. Nur unter Berücksichtigung dieser Parameter kann das gesamte Spektrum an IT-Dienstleistungen zuverlässig und zukunftssicher bereitgestellt werden.

5.3 Vorrang eigenerbrachter Technik vor Inanspruchnahme Dienste Dritter

Abhängigkeiten und Datenaus- bzw. -durchleitungen an externe Firmen werden auf das notwendige Maß reduziert. Es erfolgt grundsätzlich eine Prüfung alternativer Möglichkeiten im Hinblick auf die Nutzung von Ressourcen „vertrauter“ Einrichtungen und Partner des öffentlichen Sektors (z.B. Stadtwerke, Kommunalbetriebe, Feuerwehren). Diese kommen bevorzugt zum Einsatz.

Das RRZE folgt bei der Anfrage von Vernetzungsprodukten deshalb grundsätzlich der Reihenfolge:

1. Prüfung der Möglichkeiten bzgl. Erweiterung eigener Leitungsressourcen (LWL, Richtfunk, …)
2. Anfrage bzgl. Leitungsressourcen bei öffentlichen/kommunalen Einrichtungen der Region (Stadtwerke, Feuerwehr, benachbarte Hochschulen/Forschungseinrichtungen, DFN, …)
3. Anfrage bzgl. Leitungsressourcen bei kommerziellen Providern.

6. Maßnahmen zum Schutz der Dienstqualität

Laufende Überwachung des Betriebszustands des Datennetzes mit vor- und frühzeitigem Erkennen potentieller Störungen durch Komponentenfehler, Anwendungsfehler oder Angriffe, sind ein essentieller Bestandteil eines professionellen Netzwerkmanagements. Das RRZE betreibt zu diesem Zweck umfangreiche Systeme zur Verwaltung und Überwachung des Netzwerkbetriebs.

6.1 Betrieb eines zentralen Network Management System (NMS)

Die gesamte Netzwerkinfrastruktur der FAU wird grundsätzlich zentral vom RRZE aus betrieben und verwaltet. Das RRZE betreibt zu diesem Zweck ein zentrales Netzwerkmanagementsystem, um den stabilen, zuverlässigen und sicheren Betrieb des gesamten Datennetzes der FAU sicherzustellen.

Umfasst werden dabei u. a. die Punkte

- „Device health state“,
- Konfigurationsmanagement (Archivierung „running“/“startup“-Konfiguration),
- Firmware Management,
- Device-Typ / Asset-Management,
- Netzwerkdokumentation (Trassen- und Gebäudeverkabelung, Anschlussdosen, Switchports).

Je nach Gewichtung der potentiellen Störung, kann eine Alarmierung bzw. Störungsmeldung visuell, per E-Mail oder auch per SMS erfolgen.

6.2 Proaktives Sicherheitsmanagement

Um Anomalien im Datennetz und somit potentielle Sicherheitsrisiken frühzeitig erkennen und abfangen zu können, unterhält das RRZE entsprechende Systeme zur Erkennung von Schwachstellen in unterschiedlicher Abstufung, wie z.B.

- nicht-Intrusives Netzwerkscanning / Portscanning,
- passive Angriffserkennung (z.B. Logauswertungen, Bruteforce-Loginversuche),
- Erkennung von Flow-Anomalien auf den Routern (z.B. ddos-Angriffe),
- Erkennung von LAN-Anomalien (z.B. Schleifen, „Flooding“-Situationen),
- Auswertung von Statistikdaten: Differenzanalysen, Trenderkennungen.