aconet

Austrian Academic Computer Network

2016

JAHRESBERICHT

ACOnet Jahresbericht

2016

Inhalt

Vorwort

Christian Panigl

Abteilungsleiter ACOnet & VIX

Das Motto für 2016 könnte man unter „Vorbereitende Maßnahmen“ zusammenfassen: Einige Veränderungen, die in den nächsten zwei Jahren ihre Umsetzung finden, haben sich 2015 geschärft und wurden schließlich 2016 auf den Weg gebracht. Unter anderem konnte die Vertragsverlängerung für den ACOnet-Backbone nach mehreren Abstimmungsrunden mit der A1 Telekom Austria AG (A1TA) abgeschlossen werden.

Backbone-Erneuerung

Die Verlängerung des Rahmenvertrages mit der A1TA bis Mitte 2022 wurde vom Rektorat der Universität Wien im November 2016 unterzeichnet. Bei gleichzeitiger Senkung der laufenden Kosten ergab sich durch einige Änderungen der Topologie und zusätzliche Standorte die Möglichkeit, innerhalb Österreichs „kurze Verbindungen“ herzustellen (siehe Seite 14). Diese Topologie-Anpassung soll bis Herbst 2017 abgeschlossen werden.

EU-Datenschutz-Grundverordnung

Im Mai 2016 wurde die neue EU-Datenschutz-Grundverordnung verabschiedet. Sie bringt ab Mai 2018 zahlreiche Neuerungen zum Umgang mit personenbezogenen Daten mit sich, die sich auch bei unseren ACOnet-Teilnehmern auswirken werden. Unsere Gastautorinnen Ingrid Schaumüller-Bichl und Andrea Kolberger geben ab Seite 52 einen Überblick mit konkreten Anweisungen, wo überall Handlungsbedarf für Organisationen besteht.

Neue ACOnet-Teilnehmer

Der erfreuliche Aufwärtstrend bei den ACOnet-Teilnehmerzahlen konnte fortgesetzt werden: 12 neue Teilnehmerorganisationen sind im Jahr 2016 dem ACOnet beigetreten (siehe Seite 48). Diese Zahl schließt an den Erfolg vom letzten Jahr an und ist für uns ein Zeichen, dass sich die ACOnet-Community anhaltend großer Beliebtheit erfreut. Die fortwährenden Bestrebungen, unser Service-Portfolio zu verbessern, finden offenbar großen Anklang, und wir freuen uns sehr über das in uns gesetzte Vertrauen.

You say goodbye and I say hello

Auch der Kindersegen im ACOnet-Team hält weiter an: Monika Schneider und Christine Dworak waren 2016 nach wie vor in Elternkarenz und wir wünschen ihnen weiterhin alles Gute. Seit September 2016 verstärkt Erwin Rennert unser ACOnet & VIX-Betriebsteam, formal als Nachfolger von Wilfried Wöber, der mit Ende Juni in Pension gegangen ist. Unser langjähriger Experte im Bereich Security und unser Link zu internationalen Organisationen wie RIPE NCC und GÉANT ist nicht 1:1 ersetzbar, daher wurden Wilfrieds Aufgaben vorsorglich auf andere Mitarbeiterinnen und Mitarbeiter aufgeteilt. Weiters steht uns Wilfried erfreulicher- und dankenswerterweise noch in geringem Ausmaß als freier Mitarbeiter und Consultant, speziell in Secu-

aconet
Austrian Academic Computer Network

rityfragen, zur Seite. Markus Raditsch verstärkt bereits seit Jänner 2016 erfolgreich und tatkräftig unser ACOnet-CERT-Team.

40 Jahre Netzwerken im Rückspiegel

Als technikaffiner Mensch und Netzwerker der ersten Stunde kann Wilfried Wöber auf einen reichen Erfahrungsschatz zurückblicken. Im Artikel ab Seite 18 gewährt er uns einen Einblick, welche komplizierten Arbeitsschritte in den 1970ern nötig waren, um Computersysteme miteinander zu verbinden. Aber auch die Entstehungsgeschichte von Ethernet oder TCP/IP bis zur heutigen Selbstverständlichkeit einer „Totalvernetzung" ist in jedem Fall einen Blick wert.

Wilfried macht in seinem Artikel noch einmal unser jahrelanges gemeinsames Ziel deutlich: Es geht nicht nur darum die Organisationen der Wissenschaft und Forschung mit einer gemeinsamen Infrastruktur zu versorgen, sondern gleichzeitig einen möglichst breiten internationalen Kooperations- und branchenübergreifenden Vernetzungsansatz zu pflegen.

Update der Website

Der ACOnet-Webserver wurde 2016 auf eine neue TYPO3-Version umgestellt und im Zuge dessen wurde die Webseite gleich einem Redesign unterzogen. Es wurde ein neues, responsives Webdesign eingeführt und die Anmeldung beim Webportal über die ACOnet Identity Federation förderiert ermöglicht.

Wie immer an dieser Stelle ein großes Dankeschön an alle Gastautorinnen und -autoren, die sich dazu bereit erklärt haben, einen Beitrag für diesen Jahresbericht zu verfassen.

Abschließend möchte ich mich auch wieder bei meinem Team und bei der gesamten ACOnet Community für die gemeinsame gut funktionierende und fruchtbare Zusammenarbeit bedanken.

Und nun wünsche ich eine interessante Lektüre.

Christian Panigl
Abteilungsleiter ACOnet und Vienna Internet eXchange am Zentralen Informatikdienst der Universität Wien

www.aco.net | www.vix.at

Leitbild & Ziele

ACOnet-Leitbild

ACOnet bietet seinen Teilnehmern eine Kombination aus **leistungsfähigem Backbone und zielgruppenorientierten Services** an. Dadurch werden Anreize und Möglichkeiten zur wissenschaftlichen und innovativen Kommunikation, Kooperation und Weiterentwicklung auf nationaler und internationaler Ebene geboten.

ACOnet unterstützt – aufbauend auf der Größe und der unterschiedlichen Zusammensetzung der Teilnehmer – die Bildung von „**Communities**". Dies trifft sowohl auf die gesamte Gemeinschaft zu als auch auf Gruppen mit ähnlichen Interessen oder Zielen. Dieses Community-Building ist die Basis für gegenseitiges Vertrauen und somit eine wesentliche Voraussetzung für sichere und effiziente Kommunikation sowie die Implementierung sicherheitsrelevanter Services.

ACOnet stellt sein **Know-How** und seine nicht-kommerzielle, neutrale Expertise in den Dienst der Informationsgesellschaft und kooperiert mit relevanten Organisationen und Institutionen im In- und Ausland.

Strategische Ziele

ACOnet unterstützt vorrangig die teilnehmenden österreichischen Universitäten sowie Forschungs- und Bildungseinrichtungen gemäß ihren Anforderungen an nationale und internationale Datennetze und Services.

ACOnet richtet die **Weiterentwicklung** seiner Infrastruktur und Services regelmäßig an den Entwicklungen im internationalen Wissenschaftsnetzverbund aus.

ACOnet verbessert laufend das Kosten-Nutzen-Verhältnis für seine Teilnehmerorganisationen. Die Schwerpunkte liegen hierbei auf der Beibehaltung der **Betriebsstabilität** bei gleichzeitiger **Erweiterung des Service-Angebots**.

ACOnet ist interessiert, neben der betriebssicheren „Internet-Versorgung" für seine Teilnehmer auch spezifische Anforderungen von **Forschungsprojekten** und Benutzergruppen mit besonders hohen **Qualitätsansprüchen** bedienen zu können.


Christian Panigl


Abideen Bamgbala


Kurt Bauer


Romana Cravos

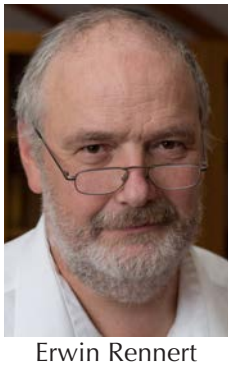

Christine Dworak


Christoph Genser


Harald Michl


Michael Perzi


Liviu-Radu Radulescu


Erwin Rennert


Monika Schneider


Peter Schober


Tina Stadlmann


Robert Wein


Wilfried Wöber

Team ACOnet & VIX

Panigl	Christian	Abteilungsleiter
Bamgbala	Abideen	Netzwerk-Betrieb
Bauer	Kurt	Netzwerk- & Server-Betrieb, Identity Federation, Zertifikatsservice
Cravos	Romana	Projektmanagement, Veranstaltungen, Öffentlichkeitsarbeit
Dworak	Christine	Webentwicklung, Öffentlichkeitsarbeit (in Karenz)
Genser	Christoph	Webentwicklung
Michl	Harald	Netzwerk-Betrieb, Betriebskoordination
Perzi	Michael	Netzwerk- & Server-Betrieb, LIR, Teilnehmeradministration
Radulescu	Liviu-Radu	Softwareentwicklung
Rennert	Erwin	Netzwerk-Betrieb (seit September)
Schneider	Monika	Netzwerk-Betrieb (in Karenz)
Schober	Peter	Server-Betrieb, Identity Federation
Stadlmann	Tina	Administratives, Veranstaltungen
Wein	Robert	Netzwerk- & Server-Betrieb, Monitoring
Wöber	Wilfried	Internationale Kontakte, Security, Consulting (bis Juni)


Alexander Talos-Zens


Patrick Pichler


Markus Raditsch


Gerhard Winkler


Arsen Stasic


Renate Kreil


Wilfried Wöber


Elisabeth Zoppoth

Computer Emergency Response Team (CERT)

Talos-Zens	Alexander	Teamleiter CERT
Pichler	Patrick	CERT-Betrieb
Raditsch	Markus	CERT-Betrieb (seit Februar)

Internet Domain Administration

Winkler	Gerhard	Team- und Referatsleiter
Adam	Achim	Software- und Systementwicklung
Dorner	Clemens	Software-Qualitätssicherung
Englisch	Holger	ac.at-Domains, Kundensupport
Fischer-Mitoiu	Valentin-Adrian	Monitoring und Datenvisualisierung
Grünauer	Marcel	Software- und Systementwicklung
Heimhilcher	Markus	DNS-Administration
Hofstetter	Mark	Software- und Systementwicklung
Ogrisegg	Thomas	Systemadministration
Papst	Andreas	Projektmanagement
Reutner-Fischer	Bernhard	Software- und Systementwicklung
Schmidt	David	Software- und Systementwicklung
Stasic	Arsen	ACOnet-Services, GovIX

Freie Mitarbeiterinnen und Mitarbeiter

Kreil	Renate	Kunst- und Kulturkommunikation
Wöber	Wilfried	Security, Training & Consulting (seit Juli)
Zoppoth	Elisabeth	TNC17-Eventmanagement (seit Juli)

Netzwerk

Status quo der Backbone-Erneuerung

Die Vertragsverlängerung für den ACOnet-Backbone konnte 2016 abgeschlossen werden. Ab 2017 erfolgt die Umsetzung, die eine Änderung der Topologie und eine Senkung der Kosten als Ziel hat. Eine Service-Router-Plattform von Nokia und die Rahmenvertragsverlängerung mit der A1 Telekom Austria AG bilden die Eckpunkte für die Backbone-Erneuerung.

Im Juli 2007 wurde nach einem europaweiten Ausschreibungsverfahren für ein österreichweites Glasfaser-Backbone-Netzwerk mit der A1 Telekom Austria AG (A1TA) ein Rahmenvertrag für initial 10 Jahre abgeschlossen. A1TA ging in dem Bieterverfahren als technisch und ökonomisch bester von drei Anbietern hervor. Der damals abgeschlossene Vertrag beinhaltete eine Verlängerungsoption für maximal weitere 5 Jahre.

Das ACOnet-Team begann bereits 2015 in Abstimmung mit dem ACOnet-Lenkungsausschuss und den ACOnet-Teilnehmerorganisationen die möglichen Optionen für den ACOnet-Backbone ab Mitte 2017 abzuwägen. Im Wesentlichen standen zur Auswahl:

- sofortige Neuausschreibung
- Teilverlängerung (z. B. um weitere 1–5 Jahre)
- Verlängerung des Rahmenvertrages um die vollen fünf Jahre

Aufgrund der guten Betriebsstabilität lag die Präferenz auf der dritten Option, also der Verlängerung des Rahmenvertrages um fünf Jahre – allerdings unter zwei Bedingungen: Die laufenden Kosten sollten gesenkt werden, und die Topologie des Backbones musste an neue Anforderungen angepasst werden. Insbesondere sollte es möglich werden, innerhalb Österreichs „kurze Verbindungen" herzustellen, also z. B. direkt zwischen Innsbruck und Salzburg, ohne Umweg über Wien.

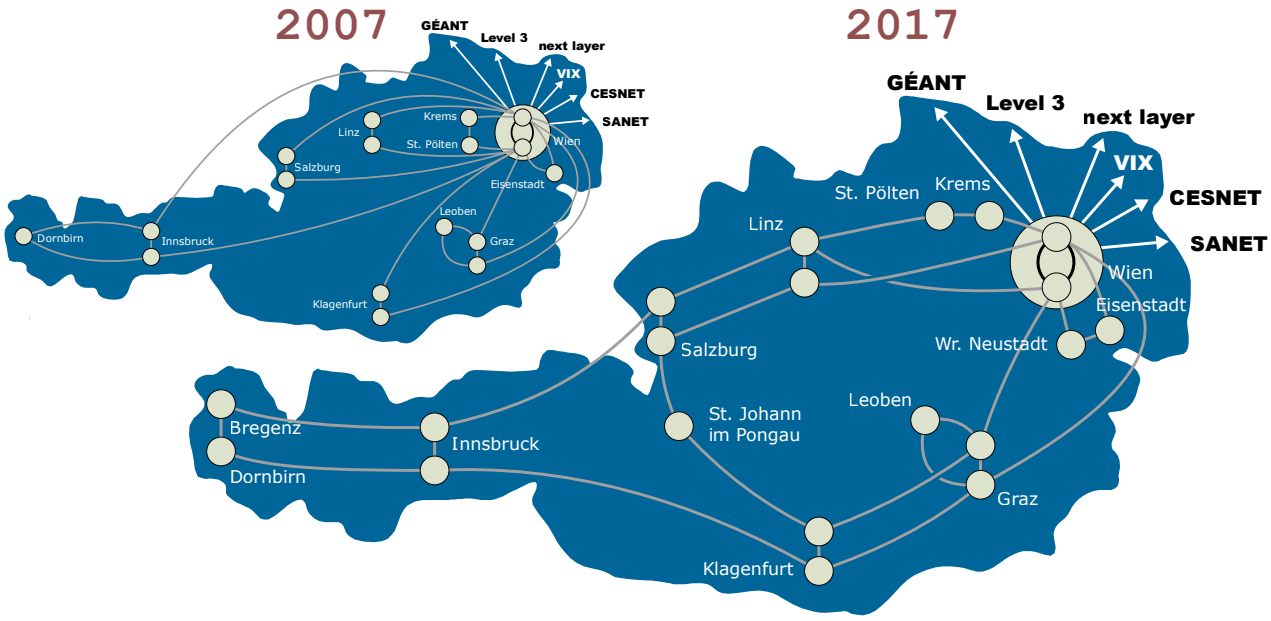
Mit diesen Vorgaben im Gepäck trat das ACOnet-Team in technische und kaufmännische Verhandlungen mit A1TA. Die technische Abklärung zeigte rasch, dass unseren topologischen Änderungswünschen mit überschaubarem Aufwand entsprochen werden kann und die zusätzlichen Standorte relativ leicht realisierbar sind. Auch auf kaufmännischer Ebene kam im Laufe des Jahres 2016 in mehreren Iterationen (und nach jeweiliger Rückabstimmung mit ACOnet-Lenkungsausschuss und Rektorat) ein gutes Ergebnis zustande: Trotz Redundanzverbesserungen und zusätzlicher Standorte konnte eine Senkung der operativen Kosten für die weiteren fünf Jahre erreicht werden.

Die Verlängerung des Rahmenvertrags mit A1TA bis Mitte 2022 und die Beauftragung der Topologie-Anpassung wurden vom Rektorat der Universität Wien im November 2016 unterzeichnet.

Die Neuerungen im Backbone

Die bisher in einer Gigabit-Variante angebundenen und durch die NÖ Forschungs- und Bildungsges.m.b.H. (NFB) finanzierten Standorte Krems (Donau-Universität) und St. Pölten (NÖ Landesregierung, Ausweichrechenzentrum) werden ab etwa Mitte 2017 vollfunktional in den DWDM-Backbone von ACOnet integriert (Dense Wavelength Division Multiplexing).

Ein zusätzlicher ACOnet-Point of Presence (PoP) an der FH Wiener Neustadt konnte bereits im Herbst 2016 realisiert werden. Zwei weitere neue ACOnet-Anschlusspunkte, einer in Bregenz (VTG, Land Vorarlberg) und einer in St. Johann/Pongau (Zentrales Ausweichsystem des Bundes – ZAS), werden etwa Mitte 2017 in Betrieb genommen.



Die bisherige ACOnet-Topologie wird in der ersten Ausbaustufe über die bestehenden Router und die neue physische DWDM-Topologie weiterhin virtuell abgebildet. Zusätzliche direkte Verbindungen zwischen benachbarten Bundesländern können bei Bedarf und vorhandener Finanzierung kurzfristig ergänzt werden. Um diese flexiblen Auf- und Durchschaltungen zu ermöglichen, werden alle wesentlichen Backbone-Knoten mit OADM-Funktionalität (Optical Add-Drop Multiplexer) ausgestattet

Die gesamte Topologie-Anpassung und die Aufrüstung der DWDM-Knoten soll bis Herbst 2017 abgeschlossen sein.

Neue Backbone-Router

Die bisher im ACOnet-Backbone verwendeten Switches und Router nähern sich nach rund zehnjährigem Einsatz ihrem Lebensende. Sie können nun nicht mehr durch geringfügige Upgrades auf aktuellen Stand gebracht werden. Nachdem daher ein Tausch praktisch aller Komponenten an allen Standorten bevorsteht, beschränkte sich die Betrachtung möglicher Nachfolgelösungen nicht auf den bisherigen Hersteller Cisco.

Nach eingehenden Recherchen und Einholung von Vergleichsangeboten von verschiedenen Herstellern und Lieferanten zeichnete sich relativ bald ab, dass der verfügbare Budgetrahmen durchaus eine Herausforderung darstellt. Glücklicherweise hat offenbar jener Hersteller, der im Zuge der technischen Verifikationen durch das ACOnet-Team die meisten Pluspunkte sammeln konnte, auch großes Interesse, im universitären und Wissenschaftsnetz-Umfeld eine Referenzinstallation zu platzieren. Daher fiel der Trade-In-Rabatt hier von Anfang an besonders großzügig aus.

The winner is: Nokia mit der aus der Fusion mit Alcatel-Lucent stammenden 7750-Service-Router-Plattform. Die rechtskonforme Beschaffung wird über die Bundesbeschaffung GmbH (BBG) durchgeführt. Lieferant und Umsetzungspartner ist die A1 Telekom Austria AG, die auch im eigenen Netzwerkbetrieb mit diesen Produkten sehr gute Erfahrungen gemacht hat. Die Umsetzung erfolgt voraussichtlich im Frühjahr und Sommer 2017 nach entsprechender Detailplanung und Abstimmung mit allen Standorten.

Dem ACOnet-Team und allen Kolleginnen und Kollegen, die unsere Standorte in den Bundesländern betreuen, steht also für 2017 ein besonders spannendes Jahr bevor. Die Zusammenarbeit mit der A1 Telekom Austria AG und den Expertinnen und Experten von Nokia Österreich erwies sich erfreulicherweise bereits im Jahr 2016 als überaus konstruktiv und effizient, sodass wir mit großer Zuversicht an diese Aufgabe herangehen.

Christian Panigl

Abteilungsleiter ACOnet & VIX

ACOnet Standortportrait

Technische Universität Graz & Karl-Franzens-Universität

In Graz gibt es zwei ACOnet-Anschlusspunkte: einen an der Technischen Universität Graz und einen an der Karl-Franzens-Universität Graz. Einer der größten ACOnet Teilnehmer an diesem Punkt ist der Virtuelle Campus Graz (VCGraz), der für über 5.300 Studierende in den angeschlossenen Studierendenheimen den Internetzugang bereitstellt.

Beide Universitäten haben ihre Standorte im Grazer Osten, nahe dem Stadtzentrum. Die beiden ACOnet-Anschlusspunkte (Points of Presence – PoPs) sind etwa 1,5 km Luftlinie voneinander entfernt. Sie sind über ihre jeweiligen Backbone- Sekundärstandorte jeweils an den zweiten, nichtlokalen PoP angeschlossen. Die interuniversitäre Verbindung erfolgt über eine Glasfaser-Infrastruktur, die bereits Anfang der 90er-Jahre im Auftrag der Grazer Universitäten errichtet wurde.

Graz 1

Der ACOnet-Anschlusspunkt Graz 1 befindet sich an der Technischen Universität Graz, die 1811 von Erzherzog Johann gegründet wurde und an der heute über 13.000 Studierende und 3.200 Bedienstete arbeiten, studieren und forschen.

Der ACOnet-PoP ist in einem der Rechnerräume des Zentralen Informatikdienstes am Campus Neue Technik untergebracht. Hier erfolgt seit drei Jahren eine kontinuierliche und grundlegende Sanierung sowie eine Neugestaltung des Netzwerks hin zu einem Next Generation Network. Im Zuge dessen konnte im Jahr 2016 die ACOnet-Anbindung der TU Graz auch innerhalb des TU-Netzes mit 10Gbit/s ausgeführt werden. Zudem erfolgte in diesem Rahmen die Verlegung des Backup-Routers in einen neu errichteten Serverraum für Hochleistungsrechnen am Campus Inffeld.

Ein großer Grazer ACOnet-Teilnehmer ist der Virtuelle Campus Graz (VCGraz), der für mehr als 30 Studierendenheime mit über 5.300 Bewohnerinnen und Bewohnern den ACOnet- bzw. Internetzugang bereitstellt. Die dafür notwendige lokale Routing-Infrastruktur wird ebenfalls von der TU Graz gehostet und betreut.

Graz 2

Der ACOnet-Anschlusspunkt Graz 2 hat seine Heimat im Jahr 2009 an der Karl-Franzens-Universität Graz gefunden. Sie wurde bereits 1585 gegründet und ist mit über 32.000 Studierenden sowie 4.200 Mitarbeiterinnen und Mitarbeitern die größte Forschungs- und Bildungseinrichtung der Steiermark.

Die Räumlichkeiten der Karl-Franzens-Universität Graz, in denen sich der ACOnet-PoP befindet, sind schon etwas in die Jahre gekommen. Daher werden sie derzeit modernisiert und energietechnisch im Sinne

Produktionstechnikzentrum 2, Campus Inffeld © TU Graz

Karl-Franzens-Universität, Hauptgebäude © Uni Graz

eines „Nachhaltigen Campus“ optimiert. Die Infrastruktur wird beinahe komplett erneuert: angefangen von der Stromversorgung mit neuen Gebäudetransformatoren (Ende 2016) bis hin zur Wärmerückgewinnung. Im Zuge des Umbaus der Universitätsbibliothek soll dieser Umbau innerhalb der nächsten drei Jahre realisiert werden.

Flexibilität und Sicherheit

ACOnet ist der optimale Partner für die Grazer Universitäten, weil die angebotenen Services weit über die eines Providers hinausgehen. Ein schneller, zuverlässiger und redundant aufgebauter Backbone bildet die Grundlage für viele weitere Dienste, aber auch für die Anbindung von Außenstellen.

Besonders populär ist der international verfügbare WLAN-Zugang über eduroam.„Open your laptop and be online“ – dieser Slogan wird in der Praxis auch wirklich so wahrgenommen: Immer wieder berichten uns begeisterte Universitätsangehörige, wo sie sich überall erfolgreich mit eduroam verbinden und WLAN kostenlos nutzen konnten. Sowohl an der TU Graz als auch an der Universität Graz wurden in den letzten Jahren die universitätseigenen WLAN-SSIDs durch eduroam ersetzt.

Wichtig ist für uns auch die enge Zusammenarbeit in Security-Fragen. Insbesondere die proaktiven Benachrichtungen des ACOnet-CERT-Teams bei Sicherheitsproblemen und die professionelle Unterstützung bei DDoS-Attacken haben uns in der Vergangenheit immer wieder sehr geholfen.

Philipp Rammer

TU Graz
IT-Basisinfrastruktur

Georg Binder

Universität Graz
Netzwerk und Infrastruktur

40 Jahre Netz-werken im Rückspiegel

Ein Rückblick von Wilfried Wöber

Meine Pensionierung mit Ende Juni 2016 ist wohl ein passender Anlass, um nach 42 Arbeitsjahren „im Netz“ Rückschau zu halten. Die erste Hälfte dieser Zeit (ich war damals an der Technischen Universität Wien beschäftigt) fiel noch in die Steinzeit der Datenkommunikation. Die zweite Hälfte, an der Universität Wien, war vor allem vom Siegeszug des Internet geprägt.

Im Nachhinein betrachtet ist es erstaunlich, welche interessanten technischen Entwicklungen und Ereignisse ich miterleben und zum Teil auch mitgestalten durfte. Daher möchte ich im Folgenden einige – natürlich subjektiv ausgewählte – Stationen auf meinem Weg durch das Netzwerk beleuchten und die Entstehung jener Technologien nachzeichnen, auf die wir uns heute als „das Internet“ ganz selbstverständlich verlassen.

1974: Lötkolben und Telefondrähte

Rund 15 Jahre vor der Erfindung des WorldWideWeb hatte eine Abteilung des EDV-Zentrums der TU Wien ein aus heutiger Sicht triviales Problem: Zur Datenerfassung bei Experimenten der Physik-Institute wurde ein Minicomputer ausgeschrieben und beschafft. Die Wahl fiel auf ein PDP-11-System von DEC (Digital Equipment Corporation), das im Bereich des TU-Hauptgebäudes in der Paniglgasse aufgebaut wurde. Ein anderer Minicomputer, eine IBM 1800, war bereits im Gebäudekomplex Gußhausstraße für Experimente und Messungen aus dem Bereich der Elektrotechnik im Einsatz. Naheliegenderweise wurde daher in der Ausschreibung auch eine Online-Verbindung zwischen diesen beiden Systemen bzw. Standorten gefordert.

Im Zuge der Installation und Abnahme der PDP-11 stellte sich dann allerdings heraus, dass der Lieferant nicht in der Lage war, eine Verbindung zwischen den beiden verschiedenen Rechnern zu realisieren. Damals entwickelte nämlich jeder Computerhersteller seine eigene Systemarchitektur, die zwar innerhalb der eigenen Produktlinien eine gewisse Kompatibilität sicherstellte, aber mit Geräten anderer Hersteller nicht zusammenarbeitete. Die Unterschiede lagen dabei nicht nur in den Schnittstellen für die Peripheriegeräte, sondern auch in den Datenformaten im Hauptspeicher, den komplett unterschiedlichen Filesystemen und den verschiedenen elektrischen Ausführungen der Schnittstellen für die Rechner-zu-Rechner-Kommunikation.

Genau damit waren wir in diesem Fall konfrontiert: Das IBM-System und das DEC-System verwendeten an den seriellen Schnittstellen unterschiedliche elektrische Standards. Ethernet und Wireless LAN lagen noch in ferner Zukunft; die einzige uns zugängliche Übertragungstechnologie waren die paarweise verdrillten Kupferleitungen der Telefonie zwischen den TU-Gebäuden. Ein direktes Verbinden der Schnittstellen über die Drähte der Telefonanlage war aber aufgrund ihrer Inkompatibilität unmöglich – ähnlich wie es nicht ratsam wäre, einen für 110V Gleichstrom gebauten Haartrockner an eine Steckdose mit 230V Wechselstrom anzuschließen.

Erste Erfolge

Die Lösung des Problems lag im Design und Eigenbau von Umsetzern, die die elektrischen

Digital PDP-11 Minicomputer

Signale an die jeweils geforderten Parameter an den Schnittstellen der beiden Systeme anpassten. Damit konnte dann ein Drahtpaar aus den Anschlüssen für die Telefone angeschaltet und Daten seriell in eine Richtung zwischen den Rechnern gesendet werden. Für die Gegenrichtung, also um Daten zu empfangen, waren ein zweiter Signalumsetzer und ein zweites Drahtpaar notwendig. Dass auch noch ein selbstgebasteltes kleines Programm auf beiden Rechnern laufen musste, war nur eine unwesentliche Nebenfront. Immerhin konnten wir nun Daten online austauschen!

Im Rausch der Geschwindigkeit

Nach mehreren Verbesserungen auf allen Ebenen waren wir schließlich in der Lage, Informationen mit einer Geschwindigkeit von ein paar hundert Bauds (1 Baud = 1 Nutz-Bit pro Sekunde) bis zu wenigen tausend Bits pro Sekunde zu übertragen, bevor uns das Telefonsystem technische Grenzen setzte.

Die Kombination aus Telefondrähten, Signalumsetzern und weiterentwickelten eigenen Programmen ermöglichte mittelfristig die Übertragung von Programmen, Programmteilen und Messdaten zwischen den dedizierten Mikrocomputern, die nach und nach direkt bei den Experimenten zur Steuerung eingesetzt wurden, und dem zentralen System.

Das alles erforderte aufgrund der beschränkten Bandbreiten recht viel Zeit, war aber doch eine wesentliche Verbesserung im Vergleich zum damaligen Stand der Technik – nämlich die Programme für die Micro-PDP-Systeme am zentralen System zu entwickeln, zusammenzubauen und in Erasable Programmable Read-Only Memories (EPROMs) zu „brennen“.

Dafür waren spezielle Geräte notwendig, der Ladevorgang nahm erhebliche Zeit in Anspruch, und die Speicherchips mussten sequenziell nacheinander programmiert werden. Wenn der Inhalt der Speichermodule geändert werden sollte (z. B. um einen Fehler im Programm zu beheben), wurden die EPROMs unter einer starken UV-Lampe eine Weile „gegrillt“ und dadurch gelöscht; danach konnten sie wieder neu programmiert werden.

Auch wenn die Umsetzung heute archaisch anmutet: Die Online-Verbindung der Microcomputer und das Online-Laden von Programmen boten damals neue Möglichkeiten für die Wissenschaft, um Experimente zu steuern bzw. um Daten in Echtzeit zu erfassen und später weiterzuverarbeiten. Wir waren aber selbstverständlich nicht die einzige Gruppe, die mit solchen oder anderen Ansätzen Pionierarbeit leistete. Unsere klobigen Werkzeuge wurden daher nach und nach von universeller einsetzbaren Programmen wie z. B. Kermit abgelöst.

Jeder kocht sein eigenes Süppchen

In unserer Abteilung „Prozessrechenanlage“ des EDV-Zentrums der TU Wien lag der Schwerpunkt anfangs auf der Unterstützung der Institute bei der Kontrolle von Experimenten, der Erfassung von Messdaten und der Auswertung von Ergebnissen. Dabei kamen primär Rechner von IBM und DEC zum Einsatz. Mit der Zeit drängten in der noch jungen IT-Welt aber auch neue Anwendungen und Anbieter auf den Markt. An der TU Wien gingen damals z. B. Systeme für CAD (Computer Aided Design) zur Entwicklung von Leiterplatten in Betrieb.

Mit der Zahl der Bewohner des „Technologie-Zoos“ wuchs auch die Notwendigkeit, digitale Informationen online auszutauschen – zuerst innerhalb einer Systemarchitektur oder Anwendung, später auch zwischen unterschiedlichen Rechnern. Das entpuppte sich als große Herausforderung, denn wie bereits erwähnt verfolgte praktisch jeder Hersteller einen eigenen Ansatz bezüglich der Protokolle und Lösungen für „sein“ Netzwerk: IBM entwickelte die Token-Ring-Technik und SNA (Systems Network Architecture), DEC setzte auf eine Reihe von Verbindungstechniken und DECnet als gemeinsame Softwarelösung, Apollo pflegte den Apollo-Ring. Den Weitverkehr dominierten die Telekom-Anbieter von Synchron-Schnittstellen (für Standleitungen) und X.25 (für dynamisch aufgebaute Verbindungen).

1980: Ethernet wird geboren, aber ...

Ein ganz wesentlicher Meilenstein in dieser Zeit war die Spezifikation von Ethernet, die 1980 durch ein Konsortium aus Xerox, Intel und DEC als Standard für eine herstellerunabhängige Local Area Network-Technologie veröffentlicht wurde. Die Eckpunkte dieser Spezifikation waren: Vergabe einer global eindeutigen Seriennummer („MAC-Adresse“) für jedes Interface, Absicherung der Datenübertragung durch eine Prüfsumme und Standardisierung eines Coax-Kabels als „shared medium“ für die Signalübertragung. Kurze Zeit später erschien die nachgebesserte Ethernet-Version II, die ursprünglich für 10 Mbit/s und eine maximale Paketgröße von 1500 Byte ausgelegt war.

Die meisten Firmen stellten relativ rasch Ethernet-Schnittstellen für ihre Geräte zur Verfügung, sodass sich diese Technik bald allgemein durchsetzte. Die anfänglichen Einschränkungen (teure Coax-Kabel, aufwendige Anschlussprozedur, geringe Maximalentfernung) wurden durch die Weiterentwicklung der relevanten IEEE 802-Standards überwunden, die billigere Leitungen, höhere Geschwindigkeiten, Full-Duplex-Betrieb und später auch die Funktechnik spezifizierten.

Während Ethernet auf der Netzwerkebene hinsichtlich Kompatibilität und Bandbreite einen Quantensprung darstellte, blieben die übergeordneten Software-Architekturen der Hersteller weiterhin unterschiedlich. Das führte dazu, dass in der Regel mehrere Protokolle nebeneinander über dasselbe Kabelsystem betrieben werden mussten. Der Datenaustausch zwischen diesen Parallelwelten erfolgte über sogenannte Gateways (meist kostenpflichtige Software oder spe-

zielle Vorschaltrechner) bzw. im Extremfall über externe Datenträger wie z. B. Magnetbänder.

Dessen ungeachtet ebnete das weit verbreitete, erschwingliche und später auch sehr schnelle Ethernet den Weg für Workstation-Cluster, redundante Rechenzentren und zentralisierte Massenspeicher. Auch die TU Wien setzte – wie viele andere Universitäten und Forschungszentren – sehr früh auf Ethernet als LAN-Technologie. Die Datenübertragung mittels Telefondrähten oder fix geschalteten Punkt-zu-Punkt-Verbindungen zwischen Gebäuden wurde damit zu einem Stück Geschichte, dem niemand wirklich nachweinte.

Internationale Verbindungsaufnahme

In den 1980er Jahren existierten und entstanden rund um uns verschiedenste Netzwerke und Projekte, die die Zusammenarbeit diverser Forschungsgemeinschaften vereinfachen sollten. Gekennzeichnet waren diese Aktivitäten dadurch, dass sie meist eine bestimmte Netzwerkarchitektur voraussetzten und/oder von namhaften Herstellern unterstützt wurden. Nachfolgend werden (ohne Berücksichtigung der zeitlichen Abfolge) jene Netze kurz vorgestellt, die den größten Einfluss auf die Entwicklung unseres nationalen Netzwerkumfelds hatten.

BITNET, EARN, EASINET (IBM)

An vielen Universitäten und Forschungseinrichtungen wurden damals IBM-Großrechner als zentrale Systeme („Hosts“) betrieben. Die Rechenaufgaben („Jobs“) der Benutzerinnen und Benutzer wurden in den Host eingespielt und dann im Stapelbetrieb nacheinander abgearbeitet. Wollte man – z. B. im Rahmen einer größeren Forschungskooperation – einen Job an einem „fremden“ Standort abarbeiten lassen, musste man die Programme bzw. Daten zunächst auf Lochkarten oder Magnetbändern dorthin transportieren. Der Ruf nach Netzwerkverbindungen zwischen den Hosts wurde folglich immer lauter.

Mit Unterstützung von IBM begannen daher die Bildungs- und Forschungsorganisationen, ihre IBM-Hosts durch Standleitungen zu verbinden – meist über das Telefonsystem mit 9,6 kbit/sec, später auch schneller. Als Kernkomponenten dienten die IBM-Netzwerkarchitektur und das Modell des Network Job Entry (Rechenaufgaben wurden aus der Ferne übermittelt und in die Warteschlange zur Abarbeitung eingereiht). Darauf aufbauend konnten elektronische Post und die Übertragung von Datenbeständen als Services genutzt werden.

In Nordamerika entstand auf diese Weise BITNET und in Europa EARN (European Academic Research Network). EARN war insbesondere für jene Universitäten wichtig, die einen Zentralrechner von IBM verwendeten; die erforderlichen Protokolle zur Teilnahme an diesem Netzwerk waren aber auch für andere Rechner und Betriebssysteme verfügbar. Der „nationale EARN-Knoten“ für Österreich befand sich an der Johannes Kepler Universität Linz und war mittels einer 64 kbit/s-Standleitung mit dem CERN in Genf (und von dort aus mit dem BITNET) verbunden. Über viele Jahre hinweg wurden anschließend

auch Universitäten in Osteuropa mit „donated equipment“ versorgt und an Netzwerkknoten in Zentral- und Mitteleuropa angeschlossen – wenn möglich über Standleitungen, sonst über Satellitenlinks.

Eine Weiterentwicklung dieser Aktivitäten war EASINET (European Academic Supercomputer Initiative, ebenfalls von IBM unterstützt). Im Rahmen dieses Projekts realisierte die Universität Wien 1990 eine 64 kbit/s-Standleitung zum CERN in Genf. Von dort konnte die transatlantische Verbindung zum NSFnet in den USA mitbenutzt werden. Für relativ lange Zeit war dies eine der beiden 64 kbit/s-Standleitungen über die Landesgrenzen hinaus; die zweite versorgte den EARN-Knoten in Linz.

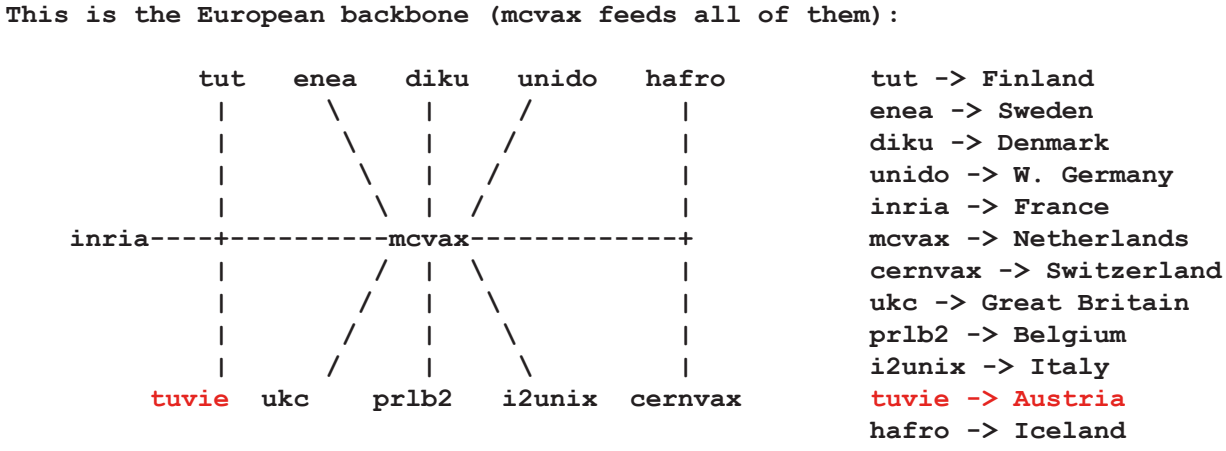
HEPnet/SPAN (DEC)

Ein anderer wichtiger Netzverbund wurde als „High Energy Physics Network“ und „Space Physics Analysis Network“ aufgebaut: HEPnet/SPAN basierte auf der DECnet-Architektur, die auf allen Systemen der Digital Equipment Corporation (DEC) als Standard implementiert war. Deshalb war dieses Netzwerk nicht nur für PhysikerInnen relevant, sondern für alle Forschungsorganisationen mit DEC-Rechnern. Insbesondere in den technischen Wissenschaften setzte man viele Jahre lang auf DEC – im Bereich der Datenerfassung und Prozesssteuerung kamen hauptsächlich PDP-11-Systeme unter dem Betriebssystem RSX, später VAX/VMS-Systeme und Workstation-Cluster zum Einsatz. Der große Vorteil der DECnet-Architektur war die vollständige Integration der Netzwerkfunktionen in die Betriebssysteme und in die Filesysteme. In diesem homogenen Umfeld war es einfach, Daten auf anderen Knoten im Netz zu speichern oder über das Netz mit lokalen Programmen Daten auszuwerten, die auf anderen Knoten verfügbar waren.

Allerdings bekam DECnet im Laufe der Zeit gravierende Probleme mit der Skalierbarkeit. Zum einen befanden sich alle Netzknoten in einem unstrukturierten Namensraum, ebenso wie das damals auch im EARN/BITNET und im noch jungen Internet der Fall war. Man musste sich daher auf Konventionen für die Namensvergabe einigen – z. B. begann der Knotenname aller DECnet-Knoten der TU Wien mit dem Buchstaben E. Zum anderen war der numerische Adressraum nur 16 Bits „breit“, also theoretisch für die Unterscheidung von maximal 64K (= 216 = 65536) Knoten ausgelegt. In der Praxis waren aber deutlich weniger Rechner im Netzverbund konfigurierbar, weil einige Bits für die Unterscheidung von 63 „areas“ mit jeweils maximal 1023 Knoten reserviert waren. Ähnlich wie später im Internet (Stichworte: RFC 1918, Private Addresses) wurden daher oft „hidden areas“ konfiguriert, aus denen dann über dedizierte Knoten Verbindungen mit eindeutigen Adressen zum Core Network aufgebaut werden konnten.

Usenet (Unix)

Parallel zu diesen Netzen, die von den jeweiligen Herstellern stark beeinflusst und teilweise auch finanziell unterstützt wurden, entwickelte sich ab 1979/80 ein von proprietären Systemen unabhängiges „poor man‘s network“: Usenet,



European Usenet Backbone, Stand: Dezember 1987

das Unix User Network. Die Kernkomponente dieses Verbundes war uucp (unix to unix copy), seine wichtigsten Services waren elektronische Post und Newsgroups.

Im Sommer 1985 nahm die TU Wien (unterstützt durch ein Forschungsprojekt des Bundesministeriums für Wissenschaft und Forschung) einen Usenet-Backbone-Knoten für Österreich in Betrieb. Es handelte sich dabei um eine PDP-11 mit Ultrix, der DEC-Version von Unix, die den Namen „tuvie“ erhielt. Die Verbindungen zu den anderen Usenet-Knoten wurden über Telefonleitungen, über den DATEX-P-Dienst der Post und Telekom Austria (PTA) sowie über eine Verbindung zum Vermittlungssystem des damaligen Interfakultären EDV-Zentrums in Wien abgewickelt.

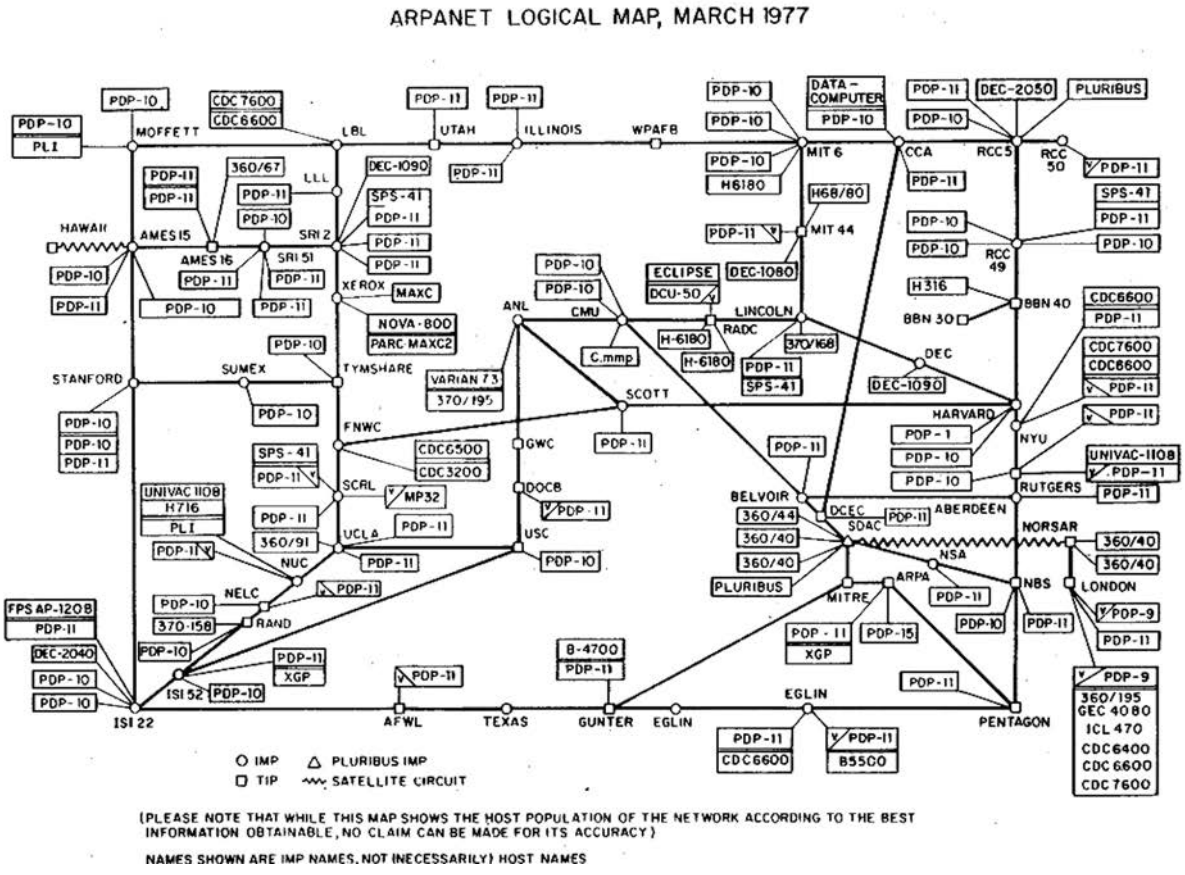
Babylonischen Protokollverwirrung

Inmitten all dieser interessanten Entwicklungen im Bereich der Übertragungstechnik suchte man verständlicherweise intensiv nach Möglichkeiten, die Systeme verschiedener Hersteller zu einer für alle Benutzerinnen und Benutzer homogen verwendbaren Umgebung zu verbinden.

ISO/OSI

In Europa wurde dafür das Modell der Open Systems Interconnection (OSI) favorisiert. Dieses basierte auf einem Satz mächtiger Standards, die von der ISO (International Organization for Standardization) und der ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) gemeinsam entwickelt wurden. Das OSI-Modell war und ist aus theoretischer Sicht faszinierend, insbesondere durch seine klare, umfassende Definition von Abstraktionen und durch die Aufteilung der Netzwerkfunktionen auf sieben übereinander gestapelte Schichten („ISO/OSI-7-Schichtenmodell“).

Damals galt OSI zudem als politisch korrekt, weil es im Gegensatz zum nachfolgend beschriebenen ARPANET nicht dem Dunstkreis des amerikanischen Militärs entstammte. Beim Versuch der Umsetzung unter dem Namen EuropaNET entpuppte es sich aber leider als sehr komplex und aufwendig in der Implementierung – zahl-



reiche unvorhergesehene Probleme und Verzögerungen waren die Folge.

ARPANET

Das amerikanische Pendant wurde parallel dazu im Auftrag einer Abteilung des US-Verteidigungsministeriums (konkret der Defense Advanced Research Projects Agency, kurz DARPA) entwickelt. Es setzte wie OSI auf Paketvermittlung, jedoch auf ein einfacheres Datenübertragungsmodell, die „TCP/IP Protocol Suite“ (Transmission Control Protocol / Internet Protocol). Das reale Ergebnis dieses Projekts hieß zunächst DARPANET, später ARPANET, noch später NSFnet. Es wurde kontinuierlich weiterentwickelt und für Teilnehmer aus Wissenschaft und Forschung – auch außerhalb der USA – zugänglich gemacht. Herzstück dieses Netzwerks waren anfänglich die sogenannten IMPs (Interface Message Processors), eine Art „Vorrechner“, an die die Backbone-Leitungen angeschaltet wurden. Die IMPs stellten die notwendigen Anpassungen und Umsetzungen für jene Systeme bereit, die TCP/IP nicht selbst implementiert hatten, und kümmerten sich um die Wegesuche und entsprechende Weiterleitung der Datenpakete. Sie waren somit auch die ersten Router.

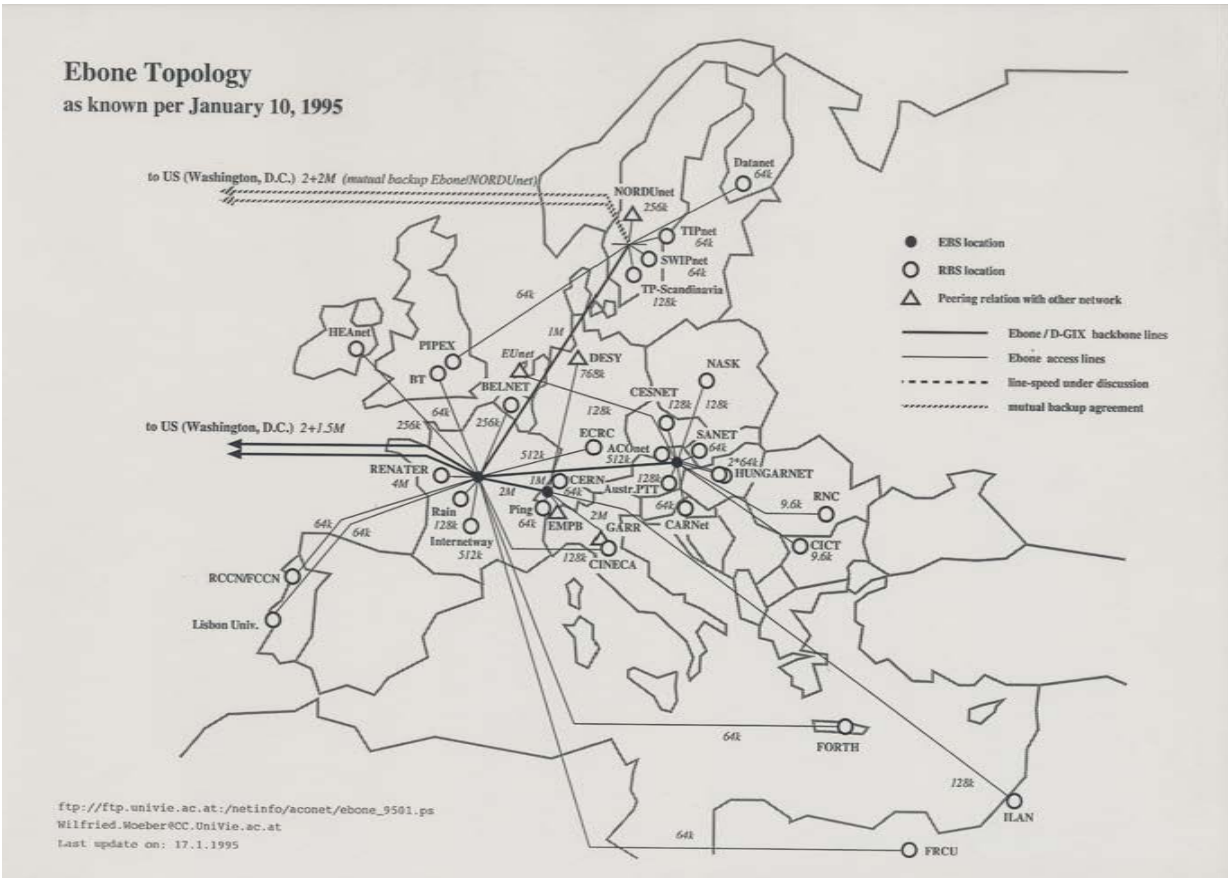
Ebone

Während man in Nordamerika mit TCP/IP rasche Fortschritte machte, wuchs in der europäischen Forschungsgemeinde der Frust: Für gemeinsame Projekte mit Partnerorganisationen aus den USA benötigte man Netzwerkdienste; der Aufbau von

EuropaNET kam aber nicht so recht vom Fleck, und es mangelte zudem an ISO/OSI-kompatibler Netzwerksoftware auf den Endsystemen.

Vor diesem Hintergrund formierte sich 1991 ein Konsortium aus europäischen Universitäten, Forschungszentren, nationalen Wissenschaftsnetzen und anderen interessierten Organisationen mit dem Ziel, ein voll funktionsfähiges, leistungsfähiges Netzwerk auf TCP/IP-Basis aufzubauen. Schon rund ein Jahr später wurde dieses Netz unter dem Namen Ebone erfolgreich in Betrieb genommen. Auch ACOnet und die Universität Wien waren daran beteiligt – und ich durfte als Koordinator des Ebone Operations Teams unendlich viel über Netzwerkerei, Gruppendynamik und auch Netzpolitik lernen. Besonders interessant an Ebone war, dass es ohne finanzielle Unterstützung realisiert wurde und daher keine spezielle Acceptable Use Policy oder differenzierte Preisgestaltung durchsetzen musste. Das machte Ebone auch außerhalb des Wissenschaftsbereichs attraktiv und erfolgreich: „In year 2000 Ebone provided international transit for around 100 Internet Service Providers based in most of the European countries." (Quelle: https://en.wikipedia.org/wiki/EBONE)

Ebone wurde 2001 von KPNQwest gekauft und am 2. Juli 2002, nach der Insolvenz von KPNQwest, abgeschaltet. Für die Academic Community war das zu diesem Zeitpunkt allerdings kein



fundamentales Problem mehr, weil sich TCP/IP mittlerweile allgemein durchgesetzt hatte und bereits TEN34 als europaweiter IP-basierter Backbone für die nationalen Wissenschaftsnetze zur Verfügung stand. TEN34 und später TEN155 wurden im Rahmen des Programms „Trans European Networks“ von der EU gefördert.

Goldene Zeiten

Aus meiner (natürlich subjektiven) Sicht waren die 15 Jahre zwischen 1992 und 2007 eine Art „goldenes Zeitalter“ für die Netzwerkerei – wohl auch weil ich an einigen hochinteressanten Projekten mitarbeiten und sie aktiv mitgestalten durfte. In diese Periode fallen Planung, Aufbau und Weiterentwicklung von Ebone, aber auch das von der EU-Kommission geförderte Projekt 6net mit seinem formalen Beginn (nach längerer Vorbereitung) im Jahr 2001.

Ziel von 6net war der Aufbau eines europaweiten Netzwerks auf Basis der „neuen“ Protokoll-Familie IPv6. Die im Rahmen der umfangreichen Tests gewonnenen Erkenntnisse waren sowohl für die Weiterentwicklung der Funktionen und Konfiguration von IPv6 (Adressierung, Routing, DNS) als auch für den Aufbau des IPv6-Pilotbetriebs im ACOnet enorm wichtig.

Neben dem Siegeszug von Ethernet und von TCP/IP als universellen Übertragungsprotokoll für fast alle Anwendungen fand in diesem Zeitraum auch die Verbreitung von Lichtleitertechnik im Weitverkehrsbereich statt. Der diesbezüglich wichtigste Meilenstein im ACOnet-Umfeld war die Unterzeichnung des Rahmenvertrags zwischen der Universität Wien und der Telekom Austria AG im Juli 2007, mit dem der Ausbau des Wissenschaftsnetzes auf Basis von Glasfaserstrecken durch ganz Österreich in die Wege geleitet wurde.

Entstehung: RIPE NCC und CERT

Auch im Bereich der Infrastruktur konnten wesentliche Aktivitäten geplant und umgesetzt werden, ohne die ein Netzwerkbetrieb heute nicht mehr vorstellbar wäre:

Für die Vergabe und Registrierung von IP-Adressen und Autonomous System Numbers wurde als (weltweit erste) Regional Internet Registry das RIPE NCC in Amsterdam als eigenständige Organisation etabliert. Damit konnten Vergabe und Administration eindeutiger Adressen von Europa aus in einem geordneten, hierarchischen System angeboten werden. Die nationale Local Internet Registry „at.aconet“ wurde 1993 in Kooperation mit dem RIPE NCC eingerichtet und versorgt seither die ACOnet-Teilnehmerorganisationen mit eindeutigen Kennungen.

Eine andere wichtige „Baustelle“ lag im Bereich der Netzwerksicherheit: Im Laufe der Zeit entstanden immer mehr Computer Emergency Response Teams (CERTs). Solche CERTs können bei sicherheitsrelevanten Vorfällen im Internet geordnet und vor allem rasch reagieren, Gegenmaßnahmen ergreifen und diese – auch über die Grenzen von einzelnen Netzwerken hinaus – koordinieren.

Als Kommunikationsplattform, primär für CERTs

aus dem akademischen Bereich, wurde bereits 1999 die TF-CSIRT (Task Force Computer Security Incident Response Teams) unter der Schirmherrschaft von TERENA gegründet. Diese Gruppe ist immer noch sehr aktiv. Obwohl sie relativ bald eigene Statuten, ein Steering Committee und eine (fast) unbegrenzte Lebenszeit zugestanden bekam, ist der Begriff „Task Force" im Namen erhalten geblieben. Das ACOnet-CERT war hier von Beginn an involviert, und ich wurde für mehrere Amtsperioden in das Steering Committee gewählt.

Im Kontext der TF-CSIRT wurde auch ein Trainingsprogramm namens TRANSITS entwickelt, das den Aufbau von neuen CERTs oder die Schulung von neuen Mitarbeiterinnen und Mitarbeitern in solchen Teams durch Kursunterlagen und Trainingsmodule unterstützt. Aufgrund meiner Aktivitäten als TRANSITS-Trainer, die mich einmal sogar zu einem Kurs für Banken nach Südafrika führten, gelang es mir auch einige Male, solche Schulungen nach Wien zu bringen.

Eine wesentliche Unterstützung für diese Veranstaltungen kam vom mittlerweile gegründeten nationalen Team CERT.at, das als Informationsdrehscheibe für andere österreichische Teams fungiert, aber z. B. auch gemeinsam mit dem Bundeskanzleramt das Service GovCERT ins Leben gerufen hat.

In der Rückschau ist es faszinierend, wie viele dieser Services heute als essenziell empfunden und regelmäßig genutzt werden, obwohl sie vor geraumer Zeit in ganz kleinem Rahmen gestartet wurden!

Und ACOnet?

Wie bereits beschrieben, waren in den Anfangszeiten der Netzwerkerei viele Dienste nur innerhalb einer Systemarchitektur bequem zu nutzen. Für besonders beliebte Services (z. B. E-Mail) gab es meist Gateways; für manche andere Funktionen existierten Client-Softwarepakete für verschiedene Plattformen, die aber oft eher mühsam zu bedienen waren.

Abgesehen davon betrieben viele Universitätsstandorte Rechner von verschiedenen Herstellern – ihre Mitarbeiterinnen und Mitarbeiter benötigten daher Zugang zu mehreren Netzen. Auch in Österreich wurde deshalb schon früh darüber nachgedacht, wie die Unterschiede in den Systemarchitekturen in den Griff zu bekommen wären und wie die nationalen Wissenschafts- und Forschungsinstitutionen mit einer gemeinsamen Infrastruktur versorgt werden könnten.

Das Ergebnis dieser Überlegungen war die Gründung des ACONET-Vereins (1986) und der Aufbau von ACOnet (1990). Die erste Variante einer landesweiten Infrastruktur bestand aus einem privaten Netz mit Übergängen in den DATEX-P-Dienst der Post und Telekom Austria (PTA).

Als Topologie wurde ein einfacher Ring aus fixen Verbindungen durch Österreich gewählt, als Zugangsprotokoll X.25, und die verfügbaren Bandbreiten betrugen anfangs 9,6 kbit/s, später 64 kbit/s. Im Rahmen eines internationalen Projekts entstand dann IXI (International X.25 Interconnect), das eine einheitliche Adress-Struktur

für öffentliche und private X.25-Netze einführte. Über diesen Weg war z. B. auch das Palo Alto Research Center (PARC) von uns aus erreichbar.

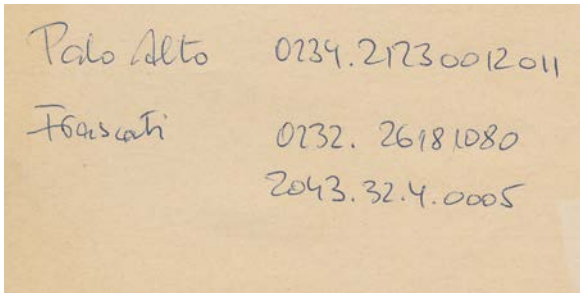
SMDS - ISDN - ATM - WDM

Einer der kapitalen Stolpersteine war die Tatsache, dass das X.25-Protokoll und seine technischen Umsetzungen nicht in der Lage waren, den rasant steigenden Bedarf an Bandbreite zu unterstützen. Deshalb wurden die Standleitungen und X.25 im Jahr 1994 durch das SMDS (Switched Multi-Megabit Data Service) der PTA abgelöst, das eine Bandbreite von 2 Mbit/s bot.

Schon damals war es wichtig, im Netzwerk eine gewisse Redundanz zu haben oder zumindest einen Notbetrieb aufrechterhalten zu können. Bei Ausfall einer SMDS-Verbindung wurden daher Backup-Wege über ISDN dynamisch aufgebaut.

Auch SMDS/ISDN konnte den Hunger nach Bandbreite nicht lange befriedigen. Daher wurde in den Jahren 1996 und 1997 ATM (Asynchronous Transfer Mode) als Transportprotokoll im ACOnet eingeführt – zum Teil schon über Fiber-optik-Wege.

ATM war eine Weiterentwicklung des Konzepts von fix oder dynamisch geschalteten Verbindungen zwischen Endpunkten. Um die verschiedenen Prioritäten unterschiedlicher Dienste zu unterstützen, wurden alle Pakete – egal ob Sprache, Massendaten oder Multimedia – zu gleich großen (bzw. kleinen) Datenkonfetti geschreddert, sodass man z. B. Sprachschnipsel zwischen die Klötzchen eines Filetransfers mischen konnte.



X.25 Adressen Forschungszentren in Palo Alto und Frascati.

Grundlage dafür war ein Format von jeweils 53 Bytes großen Paketen, die jeweils 48 Bytes Nutzdaten aufnehmen konnten; die restlichen 7 Bytes wurden für Ziel- und Steuerinformationen verwendet. Im Endeffekt entpuppten sich allerdings auch bei ATM die architektonisch vorgegebenen Beschränkungen, der Betriebsaufwand und der Overhead als unüberwindbare Hürden – die Komplexität dieser Technologie war rückblickend ein Geburtsfehler.

Ab 2001 wurde daher gezielt auf den Einsatz von Lichtleitern und Gigabit-Ethernet übergegangen. Auch im Weitverkehrsbereich und bei Unterseekabeln verdrängten die Fiberoptik-Kabel die Kupferwege. Im Moment sieht es so aus, als wäre damit für eine Weile ein Wachstumspfad verfügbar: 10 Gbit/s ist mittlerweile etablierter Standard, 100 Gbit/s ist bereits verfügbar, an noch höheren Geschwindigkeiten wird geforscht und getestet. Zudem können mittlerweile auch

bereits bestehende Wege durch Wavelength Division Multiplexing (WDM, die gleichzeitige Übertragung von Datenströmen auf verschiedenen Frequenzbändern oder „Farben“) in der Kapazität aufgerüstet werden.

Persönliche Worte

Erst mit etwas zeitlichem Abstand wird erkennbar, wie wichtig ein stabiles Umfeld für den Erfolg solcher Projekte und Entwicklungen ist. Das umfasst nicht nur Geld, Zeit und Equipment, sondern auch immaterielle Dinge wie Motivation, geringe personelle Fluktuation in den Projektteams und inhaltliche Unterstützung für die Projektziele durch das jeweilige Management bzw. die übergeordneten Organisationen.

Vor dem Aufkommen von „ordentlichem“ Projektmanagement, kleinteiligen Strukturen von Arbeitspaketen sowie regelmäßigen Reports und Reviews war diese Kontinuität ein entscheidender Faktor für das Gelingen von Projekten über die Grenzen von Institutionen, Ländern und Zeitzonen hinweg.

Im Bereich der IT-Security waren und sind darüber hinaus der persönliche Kontakt zwischen den involvierten Menschen, Handschlagqualität und gegenseitiges Vertrauen unverzichtbar, im Extremfall kann es sogar lebenswichtig sein.

Ich bin unendlich dankbar, dass ich dieses gegenseitige Vertrauen und die uneingeschränkte Bereitschaft zur Zusammenarbeit über all die Jahre hinweg im ACOnet-Umfeld erleben durfte. Genauso faszinierend und interessant waren (und sind) die Kontakte zu Kolleginnen und Kollegen aus zahlreichen Ländern von allen Kontinenten, mit denen ich immer wieder für eine gewisse Zeit am gleichen Strang ziehen durfte und von denen viele zu Freundinnen und Freunden geworden sind.

Es war eine spannende Zeit, es hat fast immer sehr viel Spaß gemacht, und wir haben gemeinsam einige Projekte verwirklicht, die die heutige IT-Welt maßgeblich beeinflusst haben.

Mein Dank gilt ganz besonders auch den Kolleginnen und Kollegen im ACOnet-Team, denen ich weiterhin viel Erfolg bei allen zukünftigen Aktivitäten wünsche!

Wilfried Wöber
Ansprechpartner
Security, Training & Consulting

Services

Nameserver

In Jahr 2016 wurden die Synergieeffekte der beiden Nameserver-Anycast-Netzwerke ns10 und ns11 endlich genutzt.

ns10 und ns11 sind zwei Domain Name Services, die von ACOnet für zwei unterschiedliche Teilnehmerkreise angeboten werden. Während das Nameserver-Anycast-Netzwerk ns10 allen ACOnet Teilnehmern zur Verfügung steht, richtet sich ns11 ausschließlich an Teilnehmer des Government Internet eXchange (GovIX).

Beide Netzwerke hatten getrennte Instanzen an unterschiedlichen Lokationen, wie etwa Wien, Frankfurt, London und Stockholm. Da es aber ähnliche Services mit gleichen Funktionen sind, wurde beschlossen, die betrieblichen und strukturellen Synergien besser zu nutzen.

Dies wurde folgendermaßen umgesetzt:

- An jedem Standort läuft sowohl eine ns10- als auch eine ns11-Instanz
- An jedem Standort befindet sich das gleiche Setup, bestehend aus einem Server mit virtuellen Maschinen
- Netzwerktechnische Besonderheiten wurden harmonisiert (die IP-Adressen befinden sich im selben Netz, gleiches Routing)

Dadurch stehen beiden Nameserver-Anycast-Netzwerken insgesamt mehr Nodes zur Verfügung, was die Ausfallsicherheit beider Services verbessert.

Als Nebeneffekt wurde damit auch erreicht, dass alle jene Domains, die in der ns10-Wolke gehostet werden nun auch direkt im GovIX verfügbar sind.

Kurzdomains

In der .at-Zone wurden 2016 ein- und zweistellige Subdomains eingeführt. Dadurch ergaben sich knapp 5.000 neue mögliche Domains.

Die Domainvergabe-Richtlinien für die .at-Zone sahen bisher vor, dass keine ein- und zweistelligen Domains vergeben werden dürfen (mit Ausnahme offizieller Subdomains wie beispielsweise .ac.at oder .gv.at). Diese Einschränkung hatte historische Gründe, die im Laufe der Zeit obsolet wurden, weshalb viele andere Länder-Registries diese Restriktion aufhoben.

Daher war die Zeit gekommen, auch die .at-Zone für Kurzdomains zu öffnen. Es wurde entschieden, dass der Öffnungsprozess in mehreren Phasen ablaufen sollte:

1. Vergabe einer Domain an denjenigen, der ein Markenrecht daran vorweisen kann
2. Vergabe im Rahmen einer Auktion
3. Landrush: Vergabe nach dem First-Come-First-Served-Prinzip ab einem bestimmten Stichzeitpunkt

Diese Schritte wurden in der zweiten Jahreshälfte 2016 durchgeführt, die Öffnung für den Landrush erfolgte am 6. Dezember 2016 exakt um 12:00 Uhr Mitteleuropäische Zeit (MEZ). Von den knapp 5.000 möglichen Domains (inklusive Umlaute und Sonderzeichen) wurden im Rahmen dieses Verfahrens etwa 1.500 Domains delegiert. Die verbliebenen Domains stehen weiterhin zur Vergabe zur Verfügung.

Gerhard Winkler

Teamleiter
Internet Domain Administration

Update der Website

Seit dem Frühjahr 2016 kommt auf dem ACOnet-Webserver eine neue TYPO3-Version zum Einsatz. Bei dieser Gelegenheit wurde ein neues, responsives Webdesign eingeführt und die Möglichkeit geschaffen, die Webportal-Anmeldung über die ACOnet Identity Federation abzuwickeln.

Der nach zehn Jahren auslaufende Support des von uns eingesetzten Content Management Systems TYPO3 V4 hat im März 2016 ein Update des ACOnet-Webservers (https://www.aco.net) notwendig gemacht. Neben der Beibehaltung der bisherigen Funktionalität waren ein neues Design und die Umstellung der Webportal-Anmeldung Hauptziele des 18 Monate dauernden Projekts. Insgesamt mussten dafür 16 eigenentwickelte TYPO3-Erweiterungen (rund 23.000 Zeilen Code) überarbeitet und zum Teil komplett neu geschrieben werden.

Responsive Design

Durch die rasche Verbreitung von Smartphones, Tablets und hochauflösenden Monitoren seit dem letzten Redesign der Website im Jahr 2006 war es notwendig, das bisherige, für die „Nullerjahre“ typische tabellenartige Webdesign über den Haufen zu werfen. Stattdessen kommt nun ein moderneres, minimalistisches Design zum Einsatz, das eine Anpassung des Layouts an das jeweils benutzte Endgerät erlaubt.

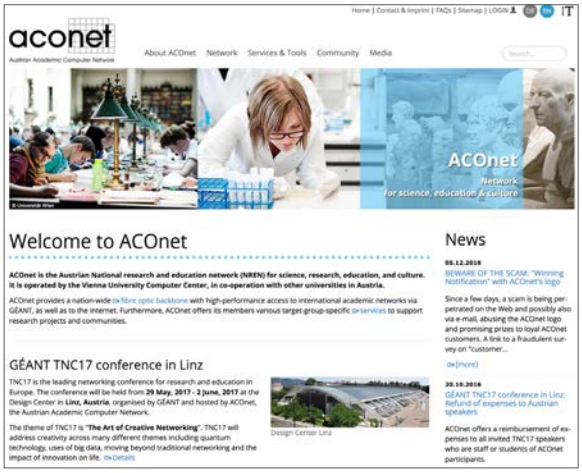
Webportal-Anmeldung

Da zum Zeitpunkt der Einführung des Webportals für ACOnet-Teilnehmerorganisationen (im Juli 2007) die ACOnet Identity Federation noch nicht existierte, wurde zur Benutzerauthentifizierung auf Infrastruktur der Universität Wien zurückgegriffen. Das notwendige Update im März 2016 bot jedoch die ideale Gelegenheit, auf das ACOnet-eigene Service umzusteigen.

Seither haben ACOnet-Teilnehmerorganisationen, die einen Identity Provider (IdP) in der Federation betreiben, die Möglichkeit, ihre Benutzerinnen und Benutzer über diesen Weg zu authentifizieren. Organisationen ohne eigenen IdP können alternativ dazu weiterhin lokale Accounts verwenden.

Nach dem Update ist vor dem Update

Nachdem der 10-jährige Supportzeitraum von TYPO3 V4 nur eine einmalige Ausnahme war (üblich sind 3 Jahre), sind wir bereits mit den Vorbereitungsarbeiten für das nächste Update beschäftigt. Die gesamte Website wird darüber hinaus seit Herbst 2016 auch inhaltlich überarbeitet und ergänzt und soll noch im Laufe des Jahres 2017 in neuem Glanz erstrahlen.



Christoph Genser

Webmaster

Notfallwebseite

Seit 2016 ist für ACOnet-Teilnehmer das Service „Notfallwebseite“ auch über Hypertext Transfer Protocol Secure (HTTPS) verfügbar. Mit einer Notfallwebseite kann im Krisenfall die Kommunikation nach außen aufrechterhalten werden. Diese Funktionalität wird auch im bevorstehenden österreichischen Cybersicherheitsgesetz eine Rolle spielen.

Das Service „Notfallwebseite“ bietet ACOnet-Teilnehmerorganisationen die Möglichkeit, statische HTML-Seiten auf einem von ACOnet betriebenen Webserver bereitzustellen. Tritt ein Strom- oder Netzwerkausfall ein, kann der eigene Webauftritt mit einem einzigen DNS-Eintrag auf die Notfallwebseite umgeleitet werden. Somit ist sichergestellt, dass wichtige Informationen auch während netzwerktechnischer Krisen nach außen weitergegeben werden können.

Verschlüsselte Kommunikation

Dieses Service wurde nun um das wichtige Feature SSL/TLS erweitert, das es ermöglicht, die Kommunikation zwischen der Notfallwebseite und den nutzenden Personen kryptografisch gesichert abzuwickeln (siehe Infobox). Mittlerweile ist es State of the Art, Webseiten durch das verschlüsselte Hypertext Transfer Protocol Secure (HTTPS) abzusichern.

Die Notfallwebseite war ursprünglich nur über das unverschlüsselte HTTP erreichbar. Wurde ein umgeleiteter Webauftritt über Bookmarks (Lesezeichen) aufgerufen, die als HTTPS-Links gespeichert waren, so erhielt man anstelle der Notfallwebseite eine Fehlermeldung. Dieses Manko wurde nun durch die Implementierung von SSL/TLS beseitigt: Die betroffenen Benutzerinnen und Benutzer werden ohne Fehlermeldung verschlüsselt auf die Notfallwebseite weitergeleitet, der Informationsfluss bleibt somit weiterhin gewährleistet.

Die Kommunikationsmöglichkeit im Krisenfall wird auch in der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie), die am

SSL/TLS

Secure Socket Layer (SSL) bzw. die daraus weiterentwickelte Transport Layer Security (TLS) ist eine Technologie zur Verschlüsselung der Kommunikation zwischen Browser und Webserver. SSL/TLS bildet die Basis für HTTPS und gewährleistet, dass die übertragenen Inhalte nicht abgehört oder während der Übertragung modifiziert werden können. Besonders wichtig ist dieses Absichern der Kommunikation, wenn Daten auf einer Webseite eingetragen werden sollen. Die Browser zeigen eine erfolgreiche Verschlüsselung durch ein Vorhängeschloss-Symbol in der Adresszeile an. ACOnet-Teilnehmerorganisationen haben die Möglichkeit, ihre Server über das kostenlose TCS-Zertifikatsservice (siehe https://www.aco.net/tcs.html) entsprechend abzusichern.

8. August 2016 in Kraft getreten ist, sowie im darauf aufbauenden österreichischen Cybersicherheitsgesetz thematisiert. Ziel des Cybersicherheitsgesetzes ist es, die IT-Infrastruktur EU-weit besser gegen technische Störungen und Angriffe von außen abzusichern. Solche sicherheitsrelevanten Vorfälle treten immer häufiger auf und sind immer schwerer in den Griff zu bekommen.

Das Cybersicherheitsgesetz wird aller Voraussicht nach vor allem kritische Infrastrukturen fokussieren – etwa im Bereich Energie, Verkehr und Banken oder bei der Gesundheits- und Trinkwasserversorgung. Bundeskanzleramt und Verteidigungsministerium bereiten den Gesetzesentwurf für die erste Jahreshälfte 2017 vor; der Entwurf soll in der zweiten Jahreshälfte begutachtet werden und schließlich fristgerecht bis Mai 2018 in Kraft treten.

ACOmaster

ACOnet-Teilnehmerorganisationen können mit dem Service „Notfallwebseite“ schon jetzt dafür sorgen, dass ihr Informationsfluss nach außen auch im Krisenfall funktioniert. Wir empfehlen, als Ergänzung unbedingt auch das Nameservice-Angebot „ACOmaster“ als Notfall-Master einzusetzen: Damit bleibt die eigene Domain selbst bei einem Ausfall der eigenen IT-Infrastruktur editierbar, was eine Grundvoraussetzung für die sinnvolle Nutzung der Notfallwebseite ist.

Bei Fragen zu diesen Services wenden Sie sich bitte an die Mailadresse domain-admin@univie.ac.at.

Arsen Stasic

Ansprechpartner
Notfallwebseite

Anti-DDOS-Maßnahmen

Mittlerweile sind die früher eher seltenen „Distributed Denial of Service (DDoS) Attacks“ in der Mitte der Gesellschaft angekommen. ACOnet versucht, anhand von Verkehrsanomalien solche Attacken möglichst schnell zu erkennen und Gegenmaßnahmen zu entwickeln. In Zeiten des „Internet of Things“ (IoT) ist das oftmals kein leichtes Unterfangen.

Der Begriff „DDoS“ (siehe Box) hat im Jahr 2016 die allgemeine Öffentlichkeit erreicht. Waren früher oft nur einzelne Services betroffen, so kann heutzutage jede Person ins Visier geraten – und dabei leider auch aktiver Teil solcher Attacken werden, in den meisten Fällen ohne es selbst zu wissen.

In den letzten Jahren haben sich sowohl Attacken als auch Ziele verändert. Dazu kommt, dass es immer leichter wird, DDoS-Angriffe auszuführen. Heute gibt es schon Anbieter, bei denen derartige Attacken einfach gekauft werden können – was unter dem Stichwort „DDoS as a Service“ läuft. Je nach Dauer und Intensität der Attacke ergibt sich dann der Preis.

Auch die Anzahl der Geräte, die potentiell missbraucht werden können, nimmt ständig zu. Vor allem bei Geräten, deren Hersteller im Normalfall keine Kernkompetenzen im Bereich IT-Security haben (Internet of Things), ist die Gefahr groß: Es kommt hier leider immer wieder vor, dass Sicherheitsmechanismen sehr simpel ausgehebelt werden können oder sogar gänzlich fehlen. Solche Geräte können daher leicht für Angriffszwecke missbräuchlich verwendet werden. Ein gutes Beispiel dafür ist das Mirai-Botnet, das in der zweiten Jahreshälfte 2016 die bis dahin größten DDoS-Attacken durchgeführt und dazu vor allem IoT-Geräte mit nicht geändertem Default-Password verwendet hat.

DDoS-Attacke

Unter einer „Distributed Denial of Service“ (DDoS)-Attacke versteht man die Überlastung eines Systems durch eine immense Anzahl an gleichzeitigen Anfragen, mit denen entweder ein Internet-Anschluss, ein Server oder auch nur gewisse Dienste so überlastet werden, dass normale Anfragen nicht mehr bewältigbar sind. Dabei kommen die Anfragen nicht nur von einem Quellsystem, sondern werden von mehreren (oft gekaperten) Systemen oder von Botnetzen verschickt. Das Zielsystem muss meistens wegen Überlastung seinen Dienst einstellen oder funktioniert nur mehr sehr langsam. Ziel solcher Attacken ist in den meisten Fällen, dem Ansehen des attackierten Unternehmens zu schaden oder das Unternehmen zu erpressen.

Was tun gegen DDoS?

Wichtige Faktoren bei der DDoS-Bekämpfung sind das rechtzeitige Erkennen von Verkehrsanomalien im weitesten Sinn (bis hin zu Attacken) und die Wahl der geeigneten Gegenmaßnahmen. Präventiv kann auch die Angriffsfläche verkleinert werden, indem mehrere idente Server im Internet verteilt betrieben werden.

Auf der Seite der Gegenmaßnahmen stehen uns als Netzbetreiber verschiedene Möglichkeiten zur Verfügung. Wir können zum Beispiel unsere Upstream-Lieferanten automatisiert dazu brin-

gen, Datenverkehr zu Attackenzielen schon auf ihrer Seite wegzuwerfen. Diese Maßnahme zielt vor allem darauf ab, Kollateralschäden zu minimieren. Denn: Wird ein Ziel innerhalb des ACOnet mit Internetverkehr „beschossen“, so kann dies dazu führen, dass unsere gesamte externe Anbindungskapazität ausgelastet ist und somit auch alle anderen ACOnet-Teilnehmer von den Auswirkungen des Angriffs betroffen sind.

Dieses Wegwerfen des Verkehrs sorgt dafür, dass die Anbindungsleitungen vom Attackenverkehr befreit werden. Allerdings spielt man dem Angreifer damit in die Hände: Da alle Datenpakete zum Attackenziel verworfen werden, werden auch legitime Anfragen oder Antworten aus dem Internet nicht zugestellt – somit war die Attacke erfolgreich.

Solange jedoch die ACOnet-Infrastruktur in der Lage ist den Verkehr zu transportieren, können andere Gegenmaßnahmen ergriffen werden. Beispielsweise können einzelne Verkehrsströme umgeleitet und „reingewaschen“ werden: Der als „gut“ klassifizierte Verkehr wird zugestellt, „schlechter“ Verkehr verworfen.

Grundlegendes Ziel dieser Internetverkehr-Waschstraße ist es nicht, jeglichen schlechten Verkehr wegzufiltern, sondern die Erreichbarkeit des Service zu gewährleisten. Im Zweifelsfall wird daher eher schlechter Verkehr weitergeschickt als legitimer Verkehr verworfen.

Das ACOnet-Betriebsteam beschäftigt sich seit langem mit dem Thema DDoS und möglichen Gegenmaßnahmen. Die ersten Erfahrungen konnten bereits in den frühen 2000er-Jahren gemacht werden. Damals waren die häufigsten DDoS-Opfer im ACOnet-Umfeld sogenannte Internet Relay Chat (IRC)-Server. Diese Server stellen kein kritisches Service dar; daher gab es anfänglich Überlegungen, einfach den Betrieb einzustellen oder die Sichtbarkeit im Internet einzuschränken, um die Angriffsfläche zu verringern. Als Backbone-Betreiber entschieden wir uns aber dafür, die Herausforderung anzunehmen. Dabei bot sich die ideale Möglichkeit, den Umgang mit derartigen Problemen zu lernen – und zwar bevor wirklich brisante Ziele attackiert werden.

Generell verfolgt ACOnet bei der Lösung der DDoS-Problematik einen kollaborativen Ansatz. Die Entwicklung von Gegenstrategien erfolgt immer im Konsens, und das Wissen um diese Strategien wird unter den ACOnet-Teilnehmern weitergegeben. Das ist einer der Gründe, warum DDoS-Attacken im ACOnet bis jetzt immer relativ unbeschadet überstanden werden konnten.

Harald Michl

Betriebskoordination

Meetings & Workshops

performing arts over advanced networks 2016

net:art

Zugegeben, die Definition „performing arts over advanced networks“ ist etwas sperrig. Doch sie drückt genau das aus, worum es geht: eine großartige Präsentationsform für darstellende Kunst über das Medium Internet bzw. über Hochleistungsdatennetze, die sich zusehends als eigenständige Kunstform etabliert.

Die heutigen technischen Möglichkeiten, Künstlerinnen und Künstler weltweit in Echtzeit zu einer gemeinsamen Performance (oder mehreren) zu vernetzen, sind eine Errungenschaft der Forschungslabors der internationalen Wissenschaftsnetze.

Durch die schnelleren und zuverlässigeren Netzwerkinfrastrukturen und die entsprechenden Übertragungstechnologien wie LOLA und UltraGrid haben sich beispielsweise die Transportverzögerungen (Latenzen) und Transportschwankungen (Jitter) signifikant verringert. Dies ermöglicht heute die Übertragung von Bild- und Tondaten über digitale Netze in einer Qualität, die eine künstlerische Interaktion in Echtzeit auch über große Distanzen zulässt.

The art of connecting people

Wie alle Community-Services von ACOnet werden auch die Aktivitäten im Bereich Kunst und Kultur durch kollektives Handeln bestimmt. Unter dem Überbegriff **net:art** sind nun alle Aktivitäten im Bereich performing arts over advanced networks auf der ACOnet-Website publiziert (siehe https://www.aco.net/netart.html) – unter anderem auch die jährlichen Treffen von Spezialistinnen und Spezialisten, die sich mit dieser Thematik beschäftigen.

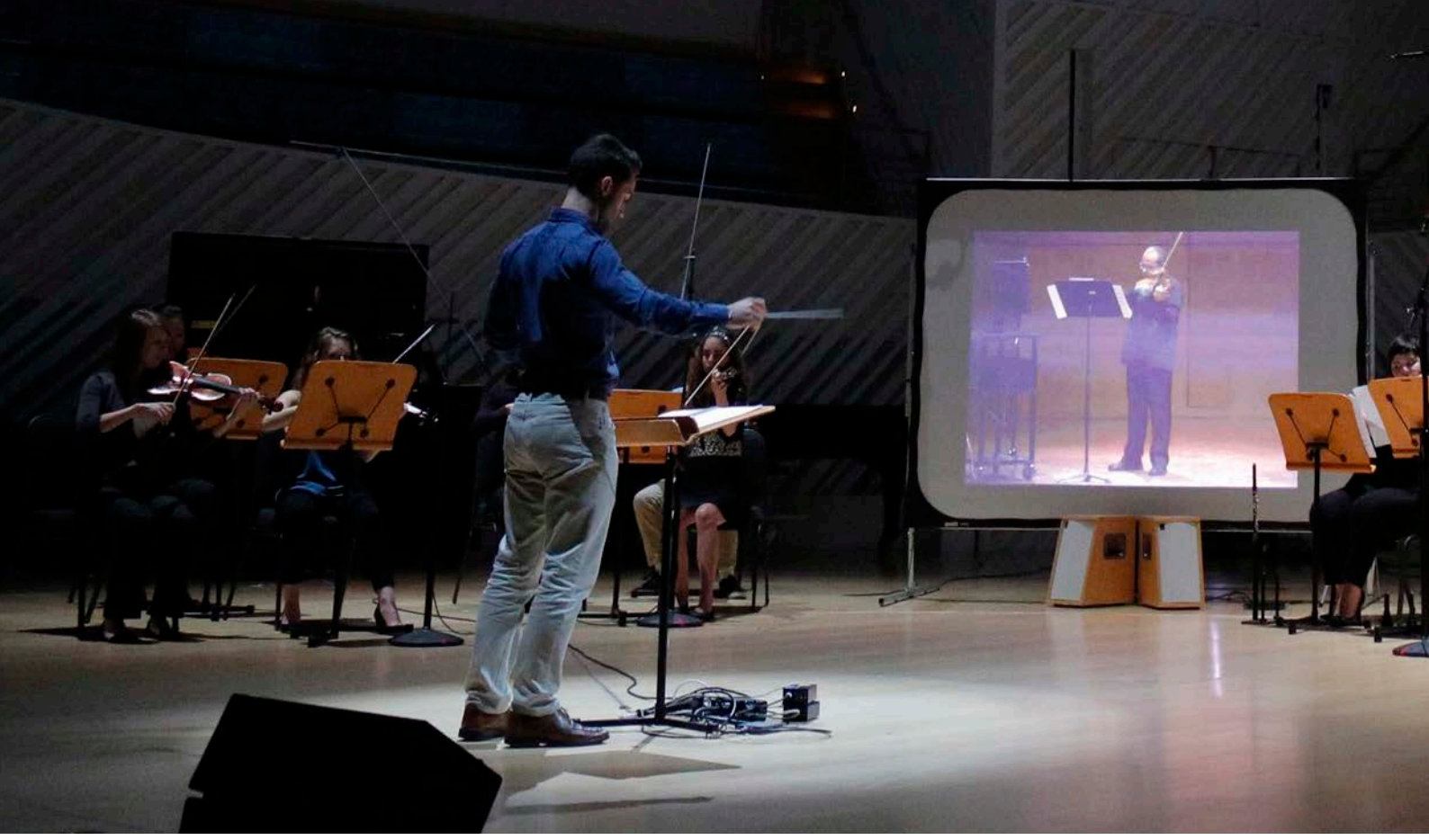
Workshop in Miami

Im März 2016 kamen NetzwerkerInnen, KomponistInnen, ProduzentInnen, EntwicklerInnen, MusikerInnen u.v.m. an der New World Symphony in Miami zusammen, um neue Wege für die Implementierung und Verwendung von Spitzentechnologie für Produktionen der darstellenden Kunst zu erforschen und zu diskutieren. Neben Vortragenden wie Chris Chafe, dem Leiter des Stanford Center for Computer Research in Music and Acoustics (CCRMA), war auch ACOnet mit einem einstündigen Vortrag vertreten.

2015 near in the distance 2

Thema des Vortrags: die Produktion net:art | near in the distance 2, eine Multi-Site-Performance, die 2015 im MuseumsQuartier Wien realisiert wurde.

Diese Produktion wurde im Rahmen der Jubiläumsveranstaltungen von „20 Jahre Internet in Österreich“ und „650 Jahre Universität Wien“ präsentiert. Erstmals konnten sechs internatio-



© Justin Trieger

nale Veranstaltungsorte mit über 40 KünstlerInnen in Echtzeit vernetzt werden – net:art | near in the distance 2 war somit nicht nur eine Uraufführung, sondern in technischer Hinsicht eine Weltpremiere. Der herausragende Livestream unseres Kooperationspartners mdw – Universität für Musik und darstellende Kunst Wien ermöglichte eine internationale Ausstrahlung, die letztlich für die Einladung an die New World Symponi ausschlaggebend war.

Gemeinsam mit Maria Isabel Gandía Carriedo (Communication Manager von CSUC, dem katalanischen Wissenschaftsnetz) wurden im ACOnet-Vortrag die Produktionsabläufe dieser Sound/Dance-Performance, an der mehr als 120 Mitwirkende beteiligt waren, fokussiert.

Miloš Liška, Mitarbeiter des tschechischen Wissenschaftsnetzes CESNET und des Entwicklerteams der Übertragungstechnologie UltraGrid, erläuterte in einem eigenen Vortrag die technischen Details. Er bezeichnete net:art | near in the distance 2 dabei als „the most crazy production".

Performance Miami – Detroit

Alle Produktionen, die bei dem Workshop in Miami präsentiert wurden, waren aufsehenerregend und haben auf verschiedenste Art und Weise gezeigt, wie individuell darstellende Kunst über Hochleistungsdatennetze interpretiert werden kann und welch grenzenloser Spielraum an Kreativität dabei möglich ist.

Besonders beeindruckend war eine Performance zwischen Miami und Detroit: Zwei Gruppen von Streetdancern lieferten sich, unter Anleitung von zwei ChoreografInnen in Miami und einem Choreografen in Detroit, ein „Battle" – in Begleitung eines Bläserensembles und eines DJs.

Ganz abgesehen davon, dass das gesamte Ensemble aus hervorragenden TänzerInnen und MusikerInnen bestand, drückte gerade diese Performance aus, dass in nächster Zukunft derartige Produktionen auch kompatibel für „Tourneen" sein könnten.

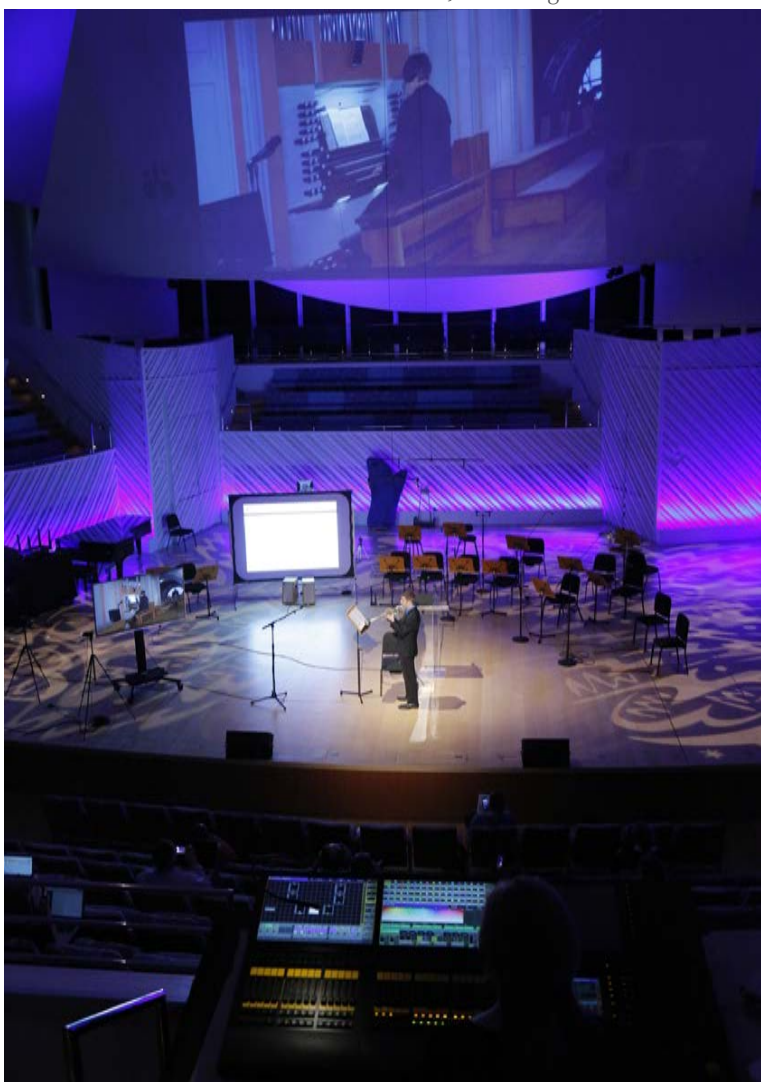
net:art Coordination Center

Diese und andere Herausforderungen sollen auch im net:art Coordination Center thematisiert werden, das 2016 gegründet wurde. Der Wissensaustausch auf nationaler und internationaler Ebene beschäftigt sich damit, in welcher Form die Implementierung von Hochtechnologie die Produktionsprozesse und Präsentationsmöglichkeiten verändern wird. Dazu gehören auch Überlegungen, was machbar und sinnvoll ist. Technologie und Kunst sind dabei aufeinander angewiesen. Es gilt Wege zu finden, Multisite-Performances oder partielle Anwendungen von „performing arts over advanced networks“ in den alltäglichen Kunstbetrieb zu integrieren.

Renate Kreil

Kommunikation Kunst & Kultur

© Justin Trieger



30. – 31. März
CEE Peering Days 2016

11. – 12. April
6. ArgeStorage

13. – 15. April
IPv6-Workshop, Salzburg

2. – 4. Mai
IPv6-Workshop, Wien

ArgeStorage

6. ArgeStorage-Meeting

11. – 12. April 2016
Universität Mozarteum Salzburg

Das 6. ArgeStorage-Meeting war geprägt von Teilnehmerbeiträgen und behandelte Themen wie OpenStack, Ceph, ownCloud, Docker und DRBD. Die meisten dieser Technologien sind sehr schnelllebig – neue Softwareversionen werden im Halbjahrestakt (oder in kürzeren Abständen) produziert. Das gesamte Auditorium profitierte von den Informationen zu Problemlösungsstrategien, die einige ACOnet-Teilnehmer umsetzen mussten, um Komplikationen beim Upgrade zu begegnen. In einem Gastvortrag wurde das Distributed Filesystem RozoFS vorgestellt.

7. ArgeStorage-Meeting

24. – 25. November 2016
APA IT, Wien

Die Vortragsthemen beim 7. ArgeStorage-Meeting waren OpenStack, Ceph, ownCloud, DRBD und Seafile. Obwohl einige dieser Themen bereits zum wiederholten Male besprochen wurden, traten neue Aspekte in den Vordergrund und führten zu wichtigen Diskussionen. Das Umweltbundesamt, das zum ersten Mal bei der ArgeStorage vertreten war, stellte das interessante EU-Projekt EUDAT vor. Der Gastvortrag beschäftigte sich mit ScaleIO und Neutrino.

Über ArgeStorage

Die ArgeStorage hat sich mittlerweile als Fixpunkt unter den ACOnet-Arbeitsgruppen etabliert. Die Meetings werden im Schnitt von 30 bis 40 Personen besucht und finden im Halbjahresrhythmus statt.

Zusätzlich zu den Meetings dient eine Mailingliste dem Erfahrungsaustausch (siehe https://noc.aco.net/mailman/listinfo/argestorage).

1. – 2. Juni
Routing-Workshop

2. – 3. Juni
53. TBPG

7. Juni
12. KUKIT-Stammtisch

IPv6-Workshop

13. – 15. April 2016
Universität Mozarteum, Salzburg

02. – 04. Mai 2016
Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW), Wien

Langsam, aber kontinuierlich wird die „neue" IP-Protokollfamilie IPv6 für die ACOnet-Community zu einem aktuellen Thema. Ob jetzt IPv6 bei einigen bereits im Testbetrieb läuft und nur einen kleinen Schubs braucht, um in den Pilotbetrieb zu gehen, oder ob ein erster Einstieg in die Thematik gesucht wurde, in beiden Fällen bot sich der Workshop als ideale Starthilfe an. Die erste Veranstaltung in Salzburg war mit 23 Teilnehmern von 13 verschiedenen Organisation gut besucht und verlief in einer sehr angenehmen Atmosphäre.

Beim zweiten Termin in Wien war der Andrang noch größer, und nach Rücksprache mit dem „Localhost" konnten letztendlich deutlich mehr Teilnehmer als ursprünglich geplant aufgenommen werden.

Die beiden Veranstaltungen waren von breitgefächerten Präsentationen und lebendigen Diskussionen geprägt. Besonderer Dank geht an die Kollegen der FH Oberösterreich, der Johannes Kepler Universität Linz und des BMWFW für die interessanten Beiträge zu ihren lokalen Konfigurationen und Erfahrungen, sowie am die beiden „Localhosts" Universität Mozarteum in Salzburg und BMWFW in Wien.

Routing-Workshop

01. – 02. Juni 2016 (2 Halbtage)
Montanuniversität Leoben

Als Reaktion auf Anfragen aus der Community entwickelte das ACOnet-Team im Frühjahr 2016 einen Workshop zum Thema „Routing im Internet". Bei der Planung der Inhalte wurden auch grundlegende Informationen zu Konzepten und Funktionen der verschiedenen Routing-Protokolle eingebunden, der Schwerpunkt wurde aber bewusst auf das Protokoll BGP4+ gelegt. Die vorbereiteten Konfigurations-Beispiele wurden ganz auf das Umfeld und die Funktionalitäten von ACOnet abgestimmt.

Als Rahmen für die erstmalige Durchführung dieses Workshops bot sich die 53. ACOnet-TBPG-Sitzung in Leoben an. 31 Teilnehmerinnen und Teilnehmer aus 20 verschiedenen Organisationen nutzten die Gelegenheit, sowohl den Routing-Workshop als auch das TBPG-Meeting als Paket zu buchen. Unser besonderer Dank gilt dabei der Montanuniversität Leoben, die an beiden Halbtagen die Räume für den Workshop zur Verfügung stellte.

Aufgrund der großen Nachfrage wurde noch 2016 mit den Planungen für eine Neuauflage des Workshops im ersten Quartal 2017 im Raum Wien begonnen.

4. Oktober
13. KUKIT-Stammtisch

16. November
Mini-Workshop E-Mail-Verschlüsselung und -Signatur

16. – 17. November
54. TBPG

E-Mail-Verschlüsselung und -Signatur Workshop

16. November 2016
Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW), Wien

Im Rahmen des 54. TBPG-Meetings fand ein Workshop zum Thema E-Mail-Verschlüsselung und -Signatur statt. Fokus des Workshops war, Basiswissen zu diesem Thema zu vermitteln und Einstiegshürden zu vermindern.

Konkrete Implementierungen auf Endgeräten aber auch die Theorie dahinter, wurden skizziert. Dabei wurde Interessierten ein leicht verständlicher Einblick in heute gängige Methoden gegeben und gezeigt, wie eine praktische Handhabung möglich ist.

Der Workshop legte unter anderem großen Wert auf die Vermittlung der Tatsache, dass das grundsätzliche Verständnis der Theorie, das Beherrschen der Software und die Schlüsselverwaltung zusammenspielen. Die Verschlüsselung und Signatur von E-Mails und Dokumenten sorgt dafür, dass vertrauliche Informationen auch vertraulich bleiben können. Durch die Signatur wird außerdem sichergestellt, dass der Inhalt der Nachricht am Weg nicht verändert wurde und auch wirklich von dem angegebenen Absender stammt. Fazit des Workshops war, dass alle Beteiligten gut geschult in diesen Prozess einsteigen sollten, um das Ziel einer sicheren Kommunikation untereinander zu erreichen.

Technische Betriebs- und Planungsgruppe

53. TBPG

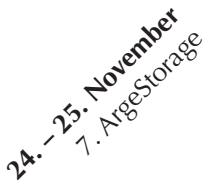
02. – 03. Juni 2016
Montanuniversität Leoben

Die 53. Sitzung der Technischen Betriebs- und Planungsgruppe fand bei einem langjährigen ACOnet-Teilnehmer, der Montanuniversität Leoben, statt. Auf der Agenda standen u.a. eine Vorstellung der geplanten ACOnet-Topologieänderungen, Erfahrungsberichte zu Netzwerkumstellungen bei Teilnehmerorganisationen, Neuigkeiten und Projekte aus dem Kunst- und Kulturbereich sowie aktuelle Security-Themen.

54. TBPG

16. – 17. November 2016
Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW), Wien

Die zweite Sitzung der ACOnet-TBPG im Jahr 2016 wurde gemeinsam mit der ArgeSecur am BMWFW in Wien abgehalten. Neben den üblichen ACOnet-Updates und aktuellen Berichten von ACOnet-Teilnehmerorganisationen stand diese Sitzung ganz im Zeichen der Security. Der Fokus lag dabei auf dem Bereich DDoS (Distributed Denial of Service) und umfasste Informationen über aktuelle Bedrohungsszenarien, Fallbeispiele und entsprechende Gegenmaßnahmen. Ein Fachvortrag zur neuen Datenschutzgrundverordnung rundete das Schwerpunktthema ab.



KUKIT – Kunst, Kultur und IT

12. KUKIT-Stammtisch

07. Juni 2016
Museum moderner Kunst Stiftung Ludwig Wien

Nach einer Führung durch die beeindruckende Ausstellung „Painting 2.0 – Malerei im Informationszeitalter" wurde das brandaktuelle Thema „Die neue Datenschutz-Grundverordnung, die Veränderungen und deren Bedeutung für das Verhältnis zu GeschäftspartnerInnen, KundInnen (BesucherInnen) und MitarbeiterInnen" im Interesse aller aufgegriffen. Wir danken Herrn Mag. Andreas Krisch für den interessanten Vortrag und die umfassende Einführung in die komplexe Thematik.

13. KUKIT-Stammtisch

04. Oktober 2016
WUK, Wien

Der 13. KUKIT-Stammtisch fand am 4. Oktober im WUK statt und widmete sich inhaltlich dem Wissensaustausch zum Update auf Windows 10 (Image-Erstellung, GPO-Einstellungen, Windows 10 in virtuellen Umgebungen, Profileigenheiten etc.). Als Moderator fungierte dankenswerterweise Peter Gregorc vom KHM-Museumsverband.

CEE Peering Days 2016

30. – 31. März 2016
Hilton Budapest City

Die Central and Eastern European Peering Days 2016 fanden im wunderschönen Budapest statt und boten wieder ein abwechslungsreiches Programm mit viel Zeit für Networking und bilaterale Meetings.

Spannende Vorträge wie der zur Software Freerouter (die auch als „Schweizer Messer für Netzwerke" bezeichnet wird) konnten das Fachpublikum vor Ort begeistern. Weitere Schwerpunkte waren die Analyse eines Vergleiches von Routing Datenbanken, ebenso wurden Themen wie DDoS und Flowspec ausführlich behandelt. Abgerundet wurde das Programm von einem RIPE-Workshop zu den Themen BGP und BCP38 und einem Social Event in der pulsierenden Budapester Innenstadt.

Die Peering Days als Fachtagung richten sich primär an Internet Service Provider aus Österreich, Ungarn, der Tschechischen Republik sowie generell aus dem zentral- und osteuropäischen Raum. Auch heuer waren wieder mehr als 200 Tagungsgäste die sich aus Peering Koordinatoren, Cloud Administratoren sowie Netzwerk- und Datacenter-Betreibern zusammen setzten. Das Programm ist eine Kombination aus technischen Workshops, professionellen Präsentationen und Networking.

Neue ACOnet-Teilnehmer 2016

Wirtschaftskammer Steiermark
Bundesministerium für Europa, Integration und Äußeres
Complexity Science Hub Vienna
MODUL University Vienna GmbH
Parlamentsdirektion
UMIT - Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik GmbH
Bundestheater-Holding
Private Pädagogische Hochschule Wien/Krems
FHW Fachhochschul-Studiengänge Betriebs- und Forschungseinrichtungen der Wiener Wirtschaft GmbH
Bundesministerium für Wirtschaft
Fachhochschule Kufstein Tirol Bildungs GmbH
Land Burgenland

Beiträge von ACOnet-Teilnehmern

Netzwerkvirtualisierung beim Land Oberösterreich

Netzwerkvirtualisierung ist ein Konzept aus dem Umfeld von Dienstleistern in der Telekommunikation. Sie ermöglicht es, eine physische Netzwerkinfrastruktur mandantenfähig zu machen, das heißt, jedem Kunden sein eigenes privates Netzwerk zur Verfügung zu stellen. Beim Land Oberösterreich wird diese Funktionalität für unterschiedlichste Anwendungsfälle genutzt.

Virtualisierung ist eines der Schlagwörter unserer Zeit. Im Netzwerkbereich gibt es bereits seit Jahren das Konzept des virtuellen Local Area Network (VLAN), das den Betrieb voneinander getrennter lokaler Netzwerke auf einem gemeinsamen physischen LAN erlaubt. Netzwerkvirtualisierung ist die Generalisierung dieses Konzepts auf alle Komponenten einer physischen Netzwerkinfrastruktur, vom Anschlussport über die Netzwerkpfade bis zum Server im Data Center. Somit erscheint jedes virtualisierte Netzwerk als komplette Instanz seiner physischen Basis, vollständig getrennt von jedem anderen virtuellen Netzwerk und mit einem eigenständigen Adressraum (IPv4 bzw. IPv6).

Analog zum Beispiel der VLANs, die durch eine aktive Netzwerkkomponente miteinander verbunden werden können, kann man auch separierte virtuelle Netzwerke wieder zusammenschalten; dies erfolgt typischerweise durch Firewalls.

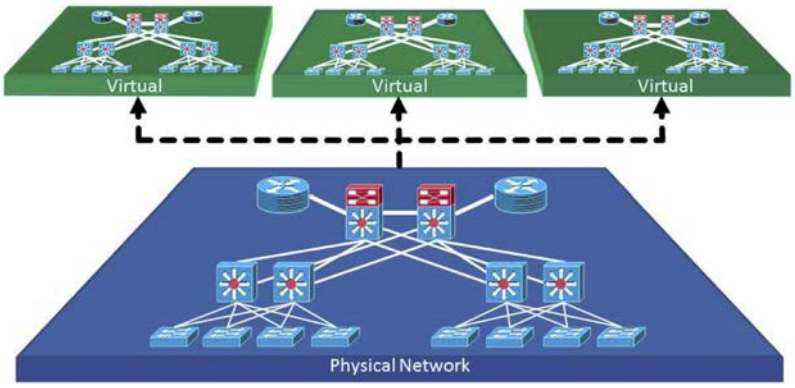
Vorteil

Der Vorteil der Netzwerkvirtualisierung liegt auf der Hand: auf einer physischen Infrastruktur lassen sich beliebig viele voneinander getrennte logische Netzwerke in einer Organisation betreiben. Mögliche Anwendungsfälle sind eigenständige Netzwerke für IP-Telefonie, Haustechnik oder Internet für Gäste. Auch Netzwerkbereiche, die aus Sicherheitsgründen voneinander getrennt sein sollen, lassen sich mit Netzwerkvirtualisierung elegant implementieren.

Voraussetzung

Technische Voraussetzung für die Umsetzung ist die vollständige Isolation des Kommunikationspfades vom Anschlussport bis zum Server. Es gibt verschiedene Ansätze zur Lösung dieses Problems. Die weitaus mächtigste und skalierbarste Technologie dafür ist MPLS-VPN (Multiprotocol Label Switching – Virtual Private Network), standardisiert im RFC 4364. Die Separation der virtuellen Netzwerke erfolgt dabei durch ein (zusätzliches) MPLS-Label. Als Kontrollprotokoll für die einzelnen VPNs wird das Multiprotocol Border Gateway Protocol (MBGP) eingesetzt.

Die Anbindung der virtuellen Netzwerke (VPNs) an den Backbone erfolgt über Provider Edge (PE) Router, optional kann zusätzlich ein Customer Edge (CE) Router eingesetzt werden. Im Backbone werden Provider (P) Router verwendet. Die PE-Router kommunizieren untereinander mit Internal BGP, daher ist aufgrund der erforderlichen Vollvermaschung ab einer gewissen Netzwerkgröße der Einsatz von BGP Route Reflectors ratsam.



© Amt der ÖO Landesregierung

Umsetzung

Beim Land Oberösterreich ist seit 2011 eine Netzwerkvirtualisierung mittels MPLS-VPN implementiert. Derzeit sind damit 13 virtuelle Netzwerke realisiert, die unterschiedliche Anwendungen abdecken. Die Basisinfrastruktur wird von 230 MPLS- bzw. BGP-fähigen Cisco-Routern (PE-Router) gebildet, aus Skalierungsgründen werden 3 BGP Route Reflectors eingesetzt. Als Routingprotokoll für MPLS wird IS-IS verwendet.

Seit 2016 sind aus Sicherheitsgründen sämtliche Netzwerkteilnehmer einem der 13 VPNs zugewiesen, sodass die globale Routing Table in den Routern nur mehr die IP-Adressen der Infrastruktur umfasst. Zur Verbesserung der Konvergenzzeiten bei Ausfall einer Netzwerkkomponente oder einer Datenleitung wird BFD (Bidirectional Forwarding Detection) eingesetzt.

Günther Schmittner

Amt der OÖ Landesregierung
Abteilung IT

Requests for Comments (RFC) – eine Sammlung von Dokumenten, die Protokolle und Methoden beschreiben, die für die Zusammenarbeit unterschiedlicher Systeme im Internet notwendig sind.

Multiprotocol Label Switching (MPLS) – Übertragung von Datenpaketen entlang eines zuvor aufgebauten Pfades.

Border Gateway Protocol (BGP) – ein Routingprotokoll, das verschiedene autonome Systeme miteinander verbindet. Routing-Entscheidungen werden bei diesem Protokoll sowohl strategisch als auch technisch-metrisch getroffen.

Route Reflector – sammelt die verschiedenen Routen von autonomen Systemen und verteilt sie an die anderen Systeme. Dadurch fallen weniger Verbindungen an, und ein komplexes Netzwerk kann so vollständig vermascht werden.

Virtual Private Network (VPN) – ein in sich geschlossenes Kommunikationsnetz, das ein bestehendes Kommunikationsnetz (z. B. das Internet) als Transportmedium verwendet.

Bidirectional Forwarding Detection (BFD) – ein Netzwerkprotokoll, das zur Fehlerermittlung bei bidirektionalen Übertragungen eingesetzt wird (definiert im RFC 5880).

Die neue EU-Daten-schutz-Grundverordnung

In rund einem Jahr muss die europaweite Neuregelung zum Umgang mit personenbezogenen Daten umgesetzt sein. Unternehmen, Behörden und andere Institutionen haben neue rechtliche, technische und organisatorische Anforderungen zu erfüllen, die teilweise mit aufwendigen Vorbereitungs- und Anpassungsarbeiten verbunden sind.

Nach langjährigen Diskussionen zur Modernisierung des europäischen Datenschutzrechts ist im Mai 2016 die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Sie ist ab 25. Mai 2018 anzuwenden. Als EU-Verordnung gilt sie unmittelbar in jedem Mitgliedsstaat; rund 50 Öffnungsklauseln ermöglichen es dem nationalen Gesetzgeber darüber hinaus, bestimmte Details national zu regeln.

Die DSGVO bringt zahlreiche Neuerungen zum Umgang mit personenbezogenen Daten. Besonders wichtig ist in diesem Zusammenhang die erhöhte Selbstverantwortung der betroffenen Institutionen. Es gibt weniger Meldepflichten, Vorabkontrollen und Genehmigungen – im Gegenzug dazu aber wesentlich stärkere Dokumentations-, Nachweis- und Informationspflichten. Die DSGVO bringt zudem eine Ausweitung der Rechte der Betroffenen und der Pflichten des Verantwortlichen sowie eine massive Verschärfung der Sanktionen mit sich. Alle Institutionen sind daher gut beraten, sich bereits jetzt intensiv mit der DSGVO und den notwendigen Schritten zu ihrer Umsetzung auseinanderzusetzen.

Neben den rechtlichen Anforderungen kommen mit der DSGVO auch eine ganze Reihe neuer technischer und organisatorischer Anforderungen auf Unternehmen, Behörden und andere Institutionen zu. Einige zentrale Aspekte dazu sollen im Folgenden näher beleuchtet werden.

Sicherheit der Verarbeitung

Ähnlich wie §14 DSG 2000 fordert auch die DSGVO risikogerechte, dem Stand der Technik und dem Umfang und Zweck der Verarbeitung angemessene technische und organisatorische Sicherheitsmaßnahmen (Artikel 32). Neben der Forderung nach Vertraulichkeit, Integrität und Verfügbarkeit wird auch die Belastbarkeit der Systeme und Dienste thematisiert. Die DSGVO zählt eine Reihe möglicher Sicherheitsmaßnahmen auf (etwa Verschlüsselung und Pseudonymisierung), aber auch Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Sie schreibt jedoch – wie auch die bisherige Gesetzgebung – keine Details oder verbindlichen Maßnahmen vor. Wichtig ist auch hier die Selbstverantwortung der Organisationen, die aus einer Risikoanalyse und -bewertung geeignete Maßnahmen abzuleiten haben.

Neu ist die Möglichkeit, die Erfüllung der Sicherheitsanforderungen mittels Zertifizierungen nachzuweisen (Artikel 42 und 43). Welche Zertifizierungen und Gütesiegel hier konkret zum Einsatz kommen können, ist in der DSGVO nicht

festgelegt und derzeit Gegenstand lebhafter Diskussionen in Fachkreisen. Zertifizierungen müssen jedenfalls immer freiwillig und transparent sein und entheben den Verantwortlichen oder den Auftragsverarbeiter nicht seiner Verantwortung.

Datenschutz-Folgenabschätzung

Für Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Betroffenen darstellen, ist vorab vom Verantwortlichen eine Datenschutz-Folgenabschätzung durchzuführen. Unter Umständen muss vor der Aufnahme der Verarbeitung die Aufsichtsbehörde konsultiert werden.

Zu beachten ist, dass Datenanwendungen, die bereits jetzt im Datenverarbeitungsregister (DVR) eingetragen sind, nicht automatisch den Anforderungen der DSGVO entsprechen. Daher muss auch für solche Verarbeitungen geprüft werden, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

Data Protection by Design, Data Protection by Default

„Datenschutz durch Technikgestaltung“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (so die Begriffe im Deutschen) stellen zwei neue Grundsätze im Datenschutzrecht dar. Data Protection by Design bedeutet, ein System so zu gestalten, dass es von vornherein möglichst wenig in das Recht auf Privatsphäre eingreift. Dazu bedient man sich u.a. spezieller technischer Verfahren (Privacy Enhancing Techniques, PETs) – etwa Verschlüsselung, Anonymisierung, Pseudonymisierung, Onion Routing (Tor) und Steganographie.

Data Protection by Default bedeutet, Voreinstellungen so zu treffen, dass personenbezogene Daten nur im tatsächlich erforderlichen Ausmaß verarbeitet werden. Unter Umständen sind Änderungen in Anwendungen notwendig, um entsprechende Einstellungsmöglichkeiten zu schaffen.

Verzeichnis von Verarbeitungstätigkeiten

Mit dem Inkrafttreten der neuen DSGVO sind sowohl Verantwortliche als auch Auftragsverarbeiter verpflichtet, ein schriftliches Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses Verzeichnis hat alle Verarbeitungen zu umfassen; der erforderliche Inhalt ist in Artikel 30 der DSGVO beschrieben.

Die lückenlose Erfassung der Verarbeitungen, die Angabe der erforderlichen Informationen und die laufende Pflege sollten hinsichtlich Aufwand keineswegs unterschätzt werden, und die Herangehensweise zur Erstellung sollte je nach Organisation gut überlegt sein. Daher gilt die dringende Empfehlung, sich möglichst bald mit der Einführung des Verzeichnisses auseinanderzusetzen. Das Verzeichnis muss nicht veröffentlicht werden, ist aber der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Ausnahmeregelungen zum Führen des Verzeichnisses lassen wenig Spielraum, sodass diese vermutlich nur in seltenen Fällen greifen werden.

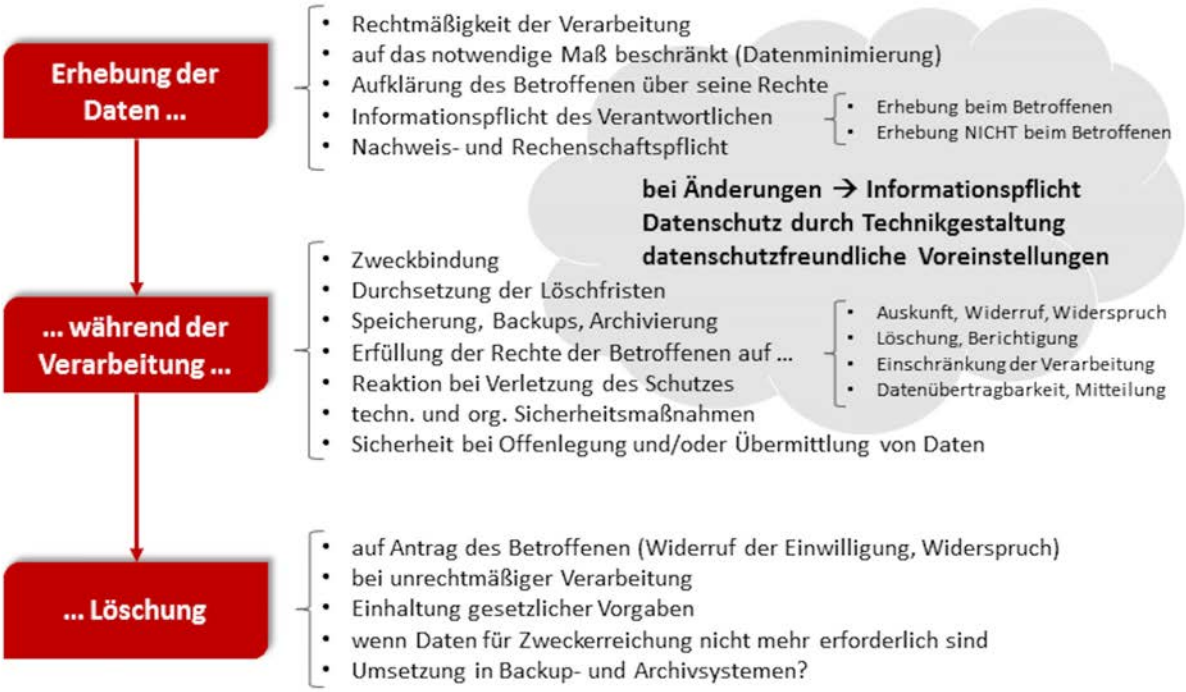
Prozesse in der Organisation

Im Allgemeinen gilt es die Prozesse innerhalb der Organisation an die Anforderungen anzupassen oder gegebenenfalls neu zu etablieren. Insbesondere zu beachten sind die Vorgaben zur Informationspflicht des Verantwortlichen (Artikel 13 und 14), zum Auskunftsrecht des Betroffenen (Artikel 15) sowie zu Meldepflichten bei der Verletzung des Schutzes von personenbezogenen Daten (Artikel 33 und 34). Personen sind ausführlich über sie betreffende Verarbeitungen zu informieren – z.B. Zweck der Verarbeitung, Empfänger und Übermittlung von Daten, Speicherfristen oder das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling. Je nachdem, wo die personenbezogenen Daten erhoben werden, gibt es unterschiedliche Fristen zur Informationspflicht.

Neben dem Auskunftsrecht über verarbeitete Daten werden den Betroffenen noch weitere Rechte eingeräumt – z.B. Recht auf Datenlöschung, Datenberichtigung oder Einschränkung der Verarbeitung (Artikel 16 bis 22). Wird der

Handlungsbedarf

- Benennung eines Datenschutzbeauftragten, wenn erforderlich
- Identifikation aller Verarbeitungstätigkeiten
- Überprüfung der Verarbeitungen, ob diese nachweislich den Grundsätzen der DSGVO entsprechen (Rechtmäßigkeit, Minimalprinzip, …) -> Rechenschaftspflicht!
- Design und Erstellung des Verzeichnisses von Verarbeitungstätigkeiten:
  - Festlegung der Verantwortlichkeiten und Zugriffsberechtigungen
  - Unterstützt das Verzeichnis bei der Erfüllung der Pflichten? (Data Breach Notification, Informations- und Auskunftspflicht, ...)
  - Sicherstellung der Aktualität
- Überprüfung und ggf. Aktualisierung des Sicherheitskonzeptes
- Prüfung, für welche Verarbeitungen eine Datenschutz-Folgenabschätzung (DPIA) durchzuführen ist? Wie wird eine DPIA durchgeführt?
- Umsetzung der Nachweispflicht für die Einwilligung eines Betroffenen (Adaptierung Datenbanken, Anpassung von (Web-)Formularen, …)
- Entwicklung und Einführung von Prozessen für:
  - Informationspflicht des Verantwortlichen
  - Auskunftsrecht der Betroffenen:
    Wer darf beauskunften und unter welchen Umständen (z.B. 4-Augen-Prinzip, Identitätsprüfung der Person)?
  - Umsetzung weiterer Rechte der Betroffenen (z. B. Löschung, Berichtigung, Einschränkung, …)
  - Data Breach Notification und Communication



Schutz von personenbezogenen Daten verletzt, so ist dies unverzüglich der Aufsichtsbehörde zu melden (Data Breach Notification). Bei einem hohen Risiko für die betroffene Person ist auch diese zu benachrichtigen (Data Breach Communication).

Datenschutzbeauftragter

Die DSGVO fordert für Behörden und öffentliche Stellen sowie in bestimmten anderen Fällen die Benennung eines Datenschutzbeauftragten (Artikel 37). Abhängig von den internen Kompetenzen bzw. Ressourcen und der Organisationsgröße kann es auch für nicht dazu verpflichtete Unternehmen hilfreich sein, einen Datenschutzbeauftragten zu bestellen oder sich fachlichen Rat von einem externen Dienstleister (z.B. Rechtsberatung) zu holen.

Ingrid Schaumüller-Bichl

FH Oberösterreich
Information Security Compliance Center (ISCC)
Kontakt: iscc@fh-ooe.at

Andrea Kolberger

FH Oberösterreich
Information Security Compliance Center (ISCC)
Kontakt: iscc@fh-ooe.at

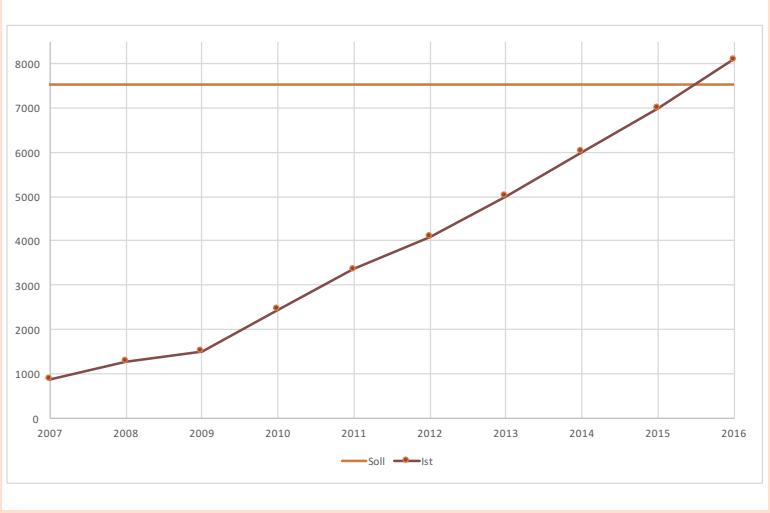
Anhang

Zahlen, Daten & Fakten

ACOnet-Teilnehmer gesamt		**229**
• Akademische Organisationen		59
• Universitäten	33	
• Fachhochschulen	17	
• Sonstige Bildungseinrichtungen	9	
• Forschungseinrichtungen		30
• Kulturorganisationen		14
• Gesundheitsinstitutionen		5
• Einrichtungen der öffentlichen Verwaltung		31
• Regionale EDUnet-Teilnehmer		9
• Studierendenheimträger		53
• Studierendenheime	130	
• Sonstige		28
davon		
• ACONET-Vereinsmitglieder		39
• GovIX-Teilnehmer		30

Backbone-Standorte	20
Glasfaser in km	4.500

Abb: Investition 2007 und jährliche Investitionsrücklagen



Das ACOnet-Budget ergibt sich aus den Erlösen aus Leistungsvereinbarungen mit den Teilnehmerorganisationen.

Jahresbudget (in tausend Euro)	**2015**	**2016**
	Summe	Summe
Erlöse aus Leistungsvereinbarungen	5.696 k€	5.786 k€
Ausgaben (in tausend Euro)	4.732 k€	4.682 k€
Personalkosten	696 k€	751 k€
Sachkosten	3.802 k€	3.805 k€
• Backbone & Transit	3.376 k€	3.420 k€
• HW&SW Wartung & Support	180 k€	168 k€
• Datacenter Miete	68 k€	78 k€
• Mitgliedsbeiträge	56 k€	61 k€
• Reisekosten	16 k€	25 k€
• Fortbildung	4 k€	5 k€
• Öffentlichkeitsarbeit	95 k€	45 k€
• Sonstige Kosten	7 k€	3 k€
Anlageinvestitionen	155 k€	48 k€
Innerbetriebliche Leistungsverrechnung	79 k€	78 k€
Ergebnis (in tausend Euro)	**964 k€**	**1.104 k€**

Das Jahresergebnis wird jeweils zum Wiederaufbau der Investitionsrücklage in Höhe der 2007er Investition verwendet:

Investition ACOnet Backbone 2007	**Soll-Wert**	**- 7.525 k€**
Investitionsrücklage 2007	684 k€	884 k€
Investitionsrücklage 2008	664 k€	396 k€
Investitionsrücklage 2009	694 k€	233 k€
Investitionsrücklage 2010	752 k€	946 k€
Investitionsrücklage 2011	724 k€	898 k€
Investitionsrücklage 2012	695 k€	730 k€
Investitionsrücklage 2013	688 k€	929 k€
Investitionsrücklage 2014	627 k€	1.003 k€
Investitionsrücklage 2015	502 k€	964 k€
Investitionsrücklage 2016	542 k€	1.104 k€
Differenz zum Zielwert bis Ende 2017		**+ 562 k€**

Impressum

Universität Wien
Zentraler Informatikdienst
ACOnet
Universitätsstraße 7
1010 Wien
Österreich
admin@aco.net
+43 1 4277 140 30

Wir danken den folgenden Personen für ihre Beiträge zu diesem Jahresbericht:
- Philipp Rammer, Technische Universität Graz
- Georg Binder, Karl-Franzens-Universität Graz
- Ingrid Schaumüller-Bichl und Andrea Kolberger, FH Oberösterreich
- Günther Schmittner, Amt der OÖ Landesregierung / Abteilung IT

Fotos:
Cover: © Universität Wien / Barbara Mair
Seite 6: © Denis Ismagilov, Fotolia
Seite 17: Produktionstechnikzentrum 2, Campus Inffeld © Philipp Rammer, TU Graz
Seite 17: Karl-Franzens-Universität, Hauptgebäude © Uni Graz
Seite 19: Digital PDP-11 © Florian Schäffer (Creative Commons BY-SA 4.0)
Seite 23: ARPANET © Defense Advanced Research Projects Agency
Seite 25: EBone © Wilfried Wöber
Seite 35: © akf, Fotolia
Seite 37: © sdecoret, Fotolia
Seite 40-43: © Justin Trieger
Seite 51: © Amt der OÖ Landesregierung Abteilung IT
Seite 53: © Trueffelpix, Fotolia
Seite 55: © FH Oberösterreich

Redaktion & Gestaltung: Romana Cravos, Christoph Genser, Elisabeth Zoppoth
Druck: Onlineprinters GmbH

Kontakt:

ACOnet
Zentraler Informatikdienst der Universität Wien
Universitätsstraße 7
1010 Wien
www.aco.net
admin@aco.net
T +43-1-4277-14030

universität
wien