aconet
Austrian Academic Computer Network

2014 ACOnet

JAHRESBERICHT

ACOnet Jahresbericht

2014

Inhalt

Vorwort

Christian Panigl
Abteilungsleiter ACOnet & VIX

Das Jahr 2014 war geprägt von vielen Aktivitäten, die zum Teil erst in den kommenden Jahren ihre vollen, positiven Auswirkungen zeigen werden.

Der ACONET Verein hat begonnen, sich konkret mit der Idee einer Cloud- und Service-Broker Organisation zu befassen (siehe Seite 11).

Die europäische Wissenschaftsnetz Community hat eine Restrukturierung ihrer gemeinsamen (Projekt-) Organisation vorgenommen: DANTE Ltd und TERENA wurden in die GÉANT Association unter gemeinsamer Lenkung aller teilnehmenden Wissenschaftsnetze zusammengeführt (siehe Seite 21). Dies ist unter anderem zwecks effizienterer Projekt-Steuerung künftiger GÉANT Projekte im Horizon 2020 Kontext erfolgt.

Wir haben im ACOnet-Team und gemeinsam mit A1 Telekom Austria begonnen, über mögliche Anpassungen der nationalen ACOnet Backbone Struktur basierend auf dem bestehenden Rahmenvertrag zu diskutieren um eine Informationsgrundlage für den ACOnet-Lenkungsausschuss vorzubereiten. Im Jahr 2015 wird hier eine strategische Entscheidung getroffen werden müssen.

Schwerpunkt IKT-Sicherheit

Das Thema IKT-Sicherheit hat 2014 auch bei uns wieder besondere Aufmerksamkeit erfahren (siehe Seiten 25ff): Ganz konkret durch Umsetzung operativer Verbesserungen am ACOnet Backbone und der aktiven Evaluierung neuer Mechanismen zur Absicherung der Routing-Informationen (siehe Seiten 14+15), aber auch durch aktive Mitwirkung beim ISPA „Internet Security Awareness Day“ (siehe Seite 24).

Das Team Internet Domain Administration hat in den Jahren 2013 und 2014 gemeinsam mit dem ACOnet-CERT Team alle Voraussetzungen dafür geschaffen, dass wir als wichtigste Partner und Lieferanten der nic.at GmbH deren ISO 27001 Zertifizierung im Februar 2014 erfolgreich unterstützen konnten. Das in diesem Zusammenhang etablierte gemeinsame ISM-Gremium sorgt nun für die langfristige Sicherung und weitere Verbesserung des Information Security Management Systems (ISMS) für die gemeinsamen Aufgaben (siehe Seite 42).

Schwerpunkt Kunst und Kultur

Unsere Aktivitäten zur Erweiterung des Teilnehmerkreises, insbesondere im Bereich Kunst und Kultur, wurden auch 2014 fortgesetzt und durch mehrere KUKIT-Stammtische unterstützt, erstmals auch in Graz (siehe Seite 31). In Wien konnten die besten Voraussetzungen geschaffen werden, um interessierten Institutionen am Areal des MuseumsQuartier Wien künftig den Anschluss und die Teilnahme an ACOnet zu erleichtern. Eine beispielhafte Kooperation und Synergien mit bestehenden ACOnet Teilnehmerorganisationen hat hier eine effiziente und zukunftsorientierte Lösung ermöglicht (siehe Seite 19).

aconet

Austrian Academic Computer Network

Neue ACOnet Teilnehmer

2014 konnten wir die Salzburg Research Forschungsgesellschaft und die Fachhochschule Campus Wien als neue ACOnet Teilnehmerorganisationen begrüßen (siehe Seiten 44ff).

Workshops und Meetings

Eine Vielzahl an gemeinsamen Meetings, Workshops und die Beteiligung an nationalen und internationalen Arbeitsgruppen und Konferenzen runden das Bild dieses arbeitsreichen und spannenden Jahres ab (siehe Seiten 30ff).

Willkommen im ACOnet Team

Seit März 2014 ist Michael Auß mit Tätigkeitsschwerpunkt interne Softwareentwicklung im ACOnet & VIX Team beschäftigt (in Nachbesetzung der Stelle von Martin Fischer). Mit seiner fundierten Erfahrung unter anderem im Bereich Typo3, Ruby on Rails und OTRS stellt er eine perfekte und lange ersehnte Verstärkung zur Weiterentwicklung interner Tools und Datenbankanwendungen sowie des Web-Portals dar.

Teilnehmerbeitrag Notfallübungen

Auf einen Teilnehmerbeitrag in diesem Jahresbericht möchte ich besonders hinweisen: Die Notfallübungen beim Land Oberösterreich (siehe Seite 51), die äußerst interessante Erkenntnisse auch für andere, insbesondere GovIX-Teilnehmer, geliefert haben. Insgesamt hat sich gezeigt, dass solche, in regelmäßigen Abständen wiederholte, Notfall-Übungen essentiell sind, um die Netzwerk-Betriebssicherheit und Ausfallsicherheitskonzepte auf ihre Ernstfall-Tauglichkeit zu überprüfen.

Aber auch einen herzlichen Dank an alle anderen Gast-Autoren!

Dank ans Team und den anhaltenden „ACOnet Spirit“ der Community

Im Herbst 2014 fand an der TU Wien das 50. Treffen der Technischen Betriebs- und Planungsgruppe von ACOnet statt (siehe Seite 34) und im Jahr 2015 feiern wir 25 Jahre gemeinsame ACOnet Infrastruktur. Es ist eine Freude und Ehre, von Anfang an dabei gewesen zu sein, stets begleitet von hoch motivierten und engagierten Kolleginnen und Kollegen, sowohl im ACOnet Team als auch bei den ACOnet Teilnehmerorganisationen.

Schließen möchte ich also diesmal nicht nur mit einem Dank an mein Team sondern an die gesamte ACOnet Community für den gemeinsamen und anhaltenden „Spirit“, der meiner Meinung nach den größten Wert von ACOnet darstellt!

Ich wünsche eine interessante Lektüre.

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

www.aco.net | www.vix.at


Perrin
IBEROAMERICANO
HISTORIA DEL ARTE

Leitbild & Ziele

ACOnet Leitbild

ACOnet bietet den ACOnet Teilnehmern mit der Kombination aus **leistungsfähigem Backbone und zielgruppenorientierten Services** Anreize und Möglichkeiten zur wissenschaftlichen und innovativen Kommunikation, Kooperation und Weiterentwicklung auf nationaler und internationaler Ebene.

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

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

Strategische Ziele von ACOnet

ACOnet unterstützt vorrangig die teilnehmenden österreichischen Universitäten, 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 ist bemüht, das Kosten-Nutzen-Verhältnis für seine Teilnehmerorganisationen laufend zu verbessern. Die Schwerpunkte liegen hierbei auf Beibehaltung der **Betriebsstabilität** und 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

Kurt Bauer

Romana Cravos

Christine Dworak

Harald Michl

Michael Perzi

Monika Schneider
karenziert

Peter Schober

Tina Stadlmann

Robert Wein

Wilfried Wöber

Team ACOnet & VIX

ACOnet Team

Panigl	Christian	Abteilungsleiter
Auß	Michael	Seit 3. März 2014 im Team, Softwareentwicklung
Bauer	Kurt	Netzwerk & Server Betrieb, Identity Federation, Zertifikatsservice
Cravos	Romana	Projektmanagement, Veranstaltungen, Öffentlichkeitsarbeit
Dworak	Christine	Webentwicklung, Öffentlichkeitsarbeit, Veranstaltungen
Michl	Harald	Netzwerk Betrieb, Betriebskoordination
Perzi	Michael	Netzwerk & Server Betrieb, LIR, Teilnehmeradministration
Schneider	Monika	karenziert seit 3. Mai 2013
Schober	Peter	Server Betrieb, Identity Federation
Stadlmann	Tina	Administratives, Veranstaltungen
Tschikof	Harald	Netzwerk Betrieb, Karenzvertretung von Monika Schneider
Wein	Robert	Netzwerk & Server Betrieb, Monitoring
Wöber	Wilfried	Internationale Kontakte, Security, Consulting

ACOnet Computer Emergency Response Team (ACOnet-CERT)

Talos-Zens	Alexander	Team-Leiter CERT
Kissler	Daniel	CERT Betrieb
Pichler	Patrick	CERT Betrieb

Freie Mitarbeiterin

Kreil	Renate	Kunst- und Kulturkommunikation


MAR
KET

ACONET Verein
ACOmarket Projekt

Das ACOnet Team hat im Februar 2014 die TERENA Arbeitsgruppen „Marketing & Communication“ sowie „Management & Service Portfolios“ (TF-MSP) nach Wien eingeladen (siehe Seite 30). Im Anschluss an das TF-MSP Treffen konnten einige der angereisten Bereichsleiterinnen und Bereichsleitern von vergleichbaren europäischen Wissenschaftsnetzen (NRENs [1]) und vom Dachverband TERENA zu einem halbtägigen Klausur-Workshop mit dem ACONET Vereinsvorstand (= ACOnet Lenkungsausschuss) eingeladen werden. Ziel dieses Workshops war die Vermittlung und Gegenüberstellung von verschiedenen Organisationsformen und Service Portfolios vergleichbarer NRENs.

Besonderes Interesse weckte die Vorstellung der SURFmarket Organisation der holländischen Kollegen als Anregung für eine ähnliche Aktivität in Österreich.

In der Folge und mit Unterstützung der Firma 42virtual wurden vom ACONET Verein mögliche Geschäftsmodelle analysiert und das Business Model eines Cloud Brokers unter dem Titel „ACOmarket“ (mit Referenz SURFmarket) näher untersucht. In einer Reihe von Workshops wurden dabei die Elemente des Geschäftsmodells und deren Dynamik im besonderen Kontext der Universitäten und wissenschaftlichen Einrichtungen betrachtet. Wesentlich für das Geschäftsmodell ist, dass diese Broker-Organisation selbst keine Cloud Produkte erstellt und betreibt, sondern diese primär durch Teilnehmer aus der ACOnet Community bereit gestellt werden sollen, aber bei Bedarf über ACOmarket auch von kommerziellen Service Providern bezogen werden können.

Neben der prinzipiellen Struktur wurden auch Vorschläge zur Priorisierung der Produkte und Dienstleistungen erarbeitet. Auf der Seite der Service Customer haben die rechtlichen Rahmenbedingungen ganz wesentlichen Einfluss darauf, wem die Leistungen des Cloud Service Brokers angeboten werden können. Hier ist die Empfehlung, mit einem definierten Kreis zu starten (Universitäten und ÖAW) und diesen dann sukzessive, gemeinsam mit dem Produktangebot auszubauen.

Es wurden mögliche Organisationsformen evaluiert, woraus sich drei Konstrukte als für weitere Betrachtungen relevant ergeben haben: Verein, Genossenschaft und GmbH. Die rechtlichen, steuerlichen und inhaltlichen Aspekte greifen ineinander und daher wurde vom Vereinsvorstand beschlossen, in einem weiteren Schritt diese drei Varianten unter Beiziehung von externer juristischer und steuerlicher Expertise zu evaluieren. Weiters soll die Ausarbeitung eines Business Case unter Berücksichtigung der Ertrags- und Kostenseite und des passenden Organisationsmodells erfolgen. Diese Ergebnisse sollen im ersten Halbjahr 2015 vorliegen.

[1] Unsere internationalen Gäste beim Klausur-Workshop im Februar:

- CESNET.cz: Jan Gruntorad
- DeIC.dk: Martin Bech
- GARR.it: Claudia Battista
- SURF.nl: Walter van Dijk
- UNINETT.no: Lars Fuglevaag
- TERENA.org: John Dyer

Netzwerk

BCP38
ACOnet implementiert BCP38 Filter

BCP38 – was heißt das? BCP[1] steht für „Best Current Practices“ und beschreibt eine Empfehlung zur bestmöglichen Handhabung eines Themas nach aktuellem Wissensstand.

Der offizielle Titel von **BCP38[2]** ist „Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing“. Das Ziel der Empfehlungen ist, die Quelladressen der IP-Pakete im Internet zu verifizieren – also zu überprüfen, ob der Absender die richtige Absendeadresse verwendet. **Gefälschte Absendeadressen werden häufig bei „Denial of Service“ Attacken verwendet.** Hier werden Pakete mit dem Attackenziel als Absendeadresse an viele Hosts im Internet versendet, um das eigentliche Ziel mit den Antwortpaketen zu torpedieren. Der attackierte Host sieht nur gültige Quelladressen, nämlich jene von den Antwortgebern. Deswegen ist diesen Attacken nur schwer beizukommen. BCP38 Filter entziehen mit der Quelladressvalidierung diesem Angriffsszenario die Funktionsgrundlage.

Um die Gültigkeit der IP-Quelladressen an den jeweiligen ACOnet Teilnehmeranschlüssen feststellen zu können, war es notwendig, eine automatisierte Filtergenerierung zu schaffen. IP-Adressbereiche können sich verändern und ein falscher Filter würde zum Verwerfen von gültigen IP-Paketen führen – und das wäre die ungünstigste „Verschlimmbesserung“, die eintreten könnte.
Im Mai 2014 wurde die automatische Filterung gemäß BCP38 an allen ACOnet Teilnehmeranschlüssen eingeführt. Die Erkenntnisse dieser Filteraktivierung, wurden bei den ACOnet TBPG Treffen 49 und 50 (siehe Seite 34) präsentiert und lassen sich wie folgt zusammenfassen:

- Fehlkonfiguration von NAT Geräten (privater Adressbereich wird sichtbar)
- Unvollständige Routerkonfiguration (Paketschleifen)
- Tatsächlich falsche Quelladressen

Das Feststellen der einen oder anderen Fehlkonfiguration war ein weiterer Vorteil des Aktivierens der Filter – hier liegt zwar in den meisten Fällen keine Betriebsgefährdung vor, aber es gehört zu den guten Sitten und der Netzhygiene nur valide IP-Pakete „in die weite Welt“ zu versenden.

Alles in Allem ist das ACOnet Team sehr froh, diesen doch gewagten Schritt getan zu haben und damit einen Beitrag zu mehr Betriebssicherheit und besserer Netzhygiene geleistet zu haben.

[1] http://www.rfc-editor.org/categories/rfc-best.html
[2] http://www.bcp38.info/

Harald Michl
ACOnet Betriebskoordination

RPKI
Resource Public Key Infrastructure

Die Forderung nach immer mehr Sicherheit im Internet macht auch vor dem Routing nicht halt. Mit RPKI - also der Resource Certification - gibt es seit einiger Zeit auch in diesem Bereich die Möglichkeit, einen zusätzlichen Sicherheitsgurt einzuziehen. Nachdem diese Technologie jedoch noch in den Kinderschuhen steckt, haben wir RPKI im Sommer 2014 in einem Testbetrieb unter die Lupe genommen.

Ziel von RPKI ist eine Verifizierung der Announcements im BGP (Border Gateway Protocol). Es soll mittels Zertifikaten (sogenannte ROAs[1]) und einem Validierungsmechanismus am Router die Zuordnung aus AS-Nummer und IP-Bereich verifizieren und verhindern, dass falsche Announcements - unabhängig davon, ob bewusst oder auf Grund von Fehlkonfigurationen - in das Routing aufgenommen werden. Quelle für diese ROAs ist die Datenbank des RIPE-NCC, in der bereits sämtliche Daten und Zuordnungen zu dem jeweiligen Teilnehmer eingetragen sind.

Wir haben bei uns im Labor RPKI auf verschiedenen Hardware-Plattformen, die auch im Produktivbetrieb im ACOnet im Einsatz sind, aktiviert und verschiedene Szenarien analysiert. Am Ende sind wir mit einem gemischten Fazit aus diesen Tests gegangen. Es hat sich gezeigt, dass die Idee hinter RPKI sehr gut ist, dass aber noch einiges an Entwicklungsarbeit notwendig ist, um es auch im Produktivbetrieb einsetzen zu können. Zusätzlich zu einigen kleinen Konfigurationshürden werden zum einen noch nicht alle Router Plattformen, die im ACOnet und auch bei unseren Teilnehmern im Einsatz sind, unterstützt. Zum anderen gibt es Limitierungen, die bei Problemen mit dem Validierungssystem zu unerwünschten Effekten im Routing führen können.

Diese Ergebnisse haben dann zu der Entscheidung geführt, RPKI noch nicht in einen Probebetrieb zu übernehmen. Wir werden die weiteren Entwicklungen beobachten und zu gegebenem Zeitpunkt an diese Tests anknüpfen.

An dieser Stelle möchten wir uns noch herzlich bei Abideen Bamgbala und Rene Haas bedanken, die uns als Praktikanten im Sommer 2014 unter anderem bei diesem Projekt erheblich unterstützt haben.

[1] Route Origin Authorisations

Michael Perzi
Ansprechpartner LIR

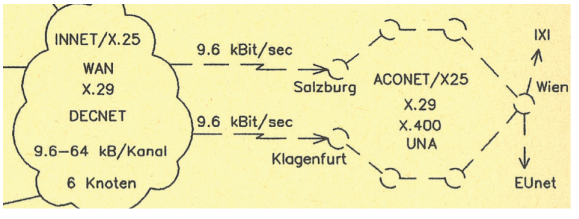
ACOnet Standortportrait

Innsbruck

In den letzten zwei Jahren portraitierten wir die ACOnet PoPs (Points of Presence) in Linz und in Salzburg. 2014 führt uns unsere Serie ins wunderschöne Innsbruck, wo die ACOnet Backbone Router von der Universität Innsbruck und der Medizinischen Universität Innsbruck betreut werden.

Die Universität Innsbruck

ist ACOnet Teilnehmer der ersten Stunde und ging Anfang 1991 mit einer Anschlussbandbreite von 9.6 Kbit/s erstmals über das ACOnet ins globale Internet.



Bereits damals war das Netz redundant ausgelegt, und so führten die Innsbrucker Leitungen nach Salzburg bzw. Klagenfurt, über die dann ringförmig der Netzknoten Wien erreicht wurde.

Was hat sich seither geändert?

Einiges - natürlich haben sich die Anschlussbandbreiten über den Lauf der Zeit vervielfacht, und die heutige Welt ist ohne Internet nicht mehr vorstellbar. Ab 1994 hat die Uni Innsbruck mit dem Internetzugang für alle Universitätsangehörigen (damals über Modem) die Entwicklung des Internet und die Verbreitung hin zu den End- und Privatanwendern in Tirol vorangetrieben.
Mit dem kürzlich erfolgten Umstieg auf eine 10Gb-Anbindung für die Leopold-Franzens-Universität hat sich damit die Bandbreite seit den Anfangstagen um den Faktor eine Million gesteigert.

Im Gegensatz zur TCP/IP-Technologie hat sich an der Universitätsstruktur einiges geändert. Aus der einen, zentral vom Ministerium gesteuerten Universität Innsbruck sind nun mit der Medizinischen Universität, dem Management Center Innsbruck (MCI) und der Leopold-Franzens Universität drei eigenständige akademische Einrichtungen entstanden.

Was ist gleich geblieben?

Walter Müller vom Datennetz- und Betriebs-Team des ZID Universität Innsbruck sagt:

„Wir als Universität haben als ACOnet Teilnehmer über all die Jahre einen äußerst zuverlässigen und kompetenten Partner im Bereich der Netzwerktechnik gehabt. Alle Erweiterungsschritte konnten für uns rechtzeitig und professionell in guter Zusammenarbeit abgewickelt werden.

© MUI/Lackner

So bietet das jetzige 10Gb-Backbone eine gute Basis für die Zusammenarbeit der Universitäten untereinander. Davon profitiert unsere Zusammenarbeit im Bereich High-Performance-Computing ebenso, wie wir in Zukunft bald standortübergreifende Datensicherungskonzepte realisieren wollen."

Worauf sind wir stolz?

Durch laufende Investitionen der Universität in das Datennetz sowie durch die Kompetenz und Einsatzbereitschaft unserer Netz- sowie Betriebsmannschaft konnte die Universität Innsbruck in den letzten fast 25 Jahren in Zusammenarbeit mit dem ACOnet-Team allen angeschlossenen Teilnehmern einen stabilen und reibungslosen Betrieb bieten.

Die Medizinische Universität Innsbruck

ist seit 2006 eigenständiger ACOnet Teilnehmer und wurde mit dem „ACOnet Backbone Neu" Projekt 2007 zum zweiten Innsbrucker PoP.

eduroam ist mit bis zu 1200 gleichzeitigen Benutzerinnen und Benutzern (zu Spitzenzeiten) eines der wertvollsten Services für die Medizinische Universität Innsbruck. 2014 wurde eduroam auch am Campus der Tiroler Landeskrankenanstalten ausgerollt.

Gemeinsam mit der Universität Innsbruck und den Tiroler Landeskrankenanstalten plant die Medizinische Universität Innsbruck eine redundante 10Gb Anbindung an beide PoPs (IBK1 und IBK2). Die Vorarbeiten für dieses Projekt haben bereits 2014 begonnen.
Simon Rumer aus der Abteilung IKT der Medizinischen Universität Innsbruck sagt:

„Das ACOnet bedeutet für uns eine solide Kommunikationsinfrastruktur - eine unkomplizierte und direkte Kommunikation mit dem ACOnet Team, kollegialer Umgang und interessanter Wissens- und Erfahrungsaustausch im Rahmen der regelmäßigen Treffen."

Das ACOnet-Team bedankt sich an dieser Stelle bei Walter und Simon und deren Teams für die jahrelange zuverlässige Partnerschaft und für die Mithilfe zu diesem Artikel und freut sich auf die zukünftigen gemeinsamen Projekte.

© Gian Marco Castelberg

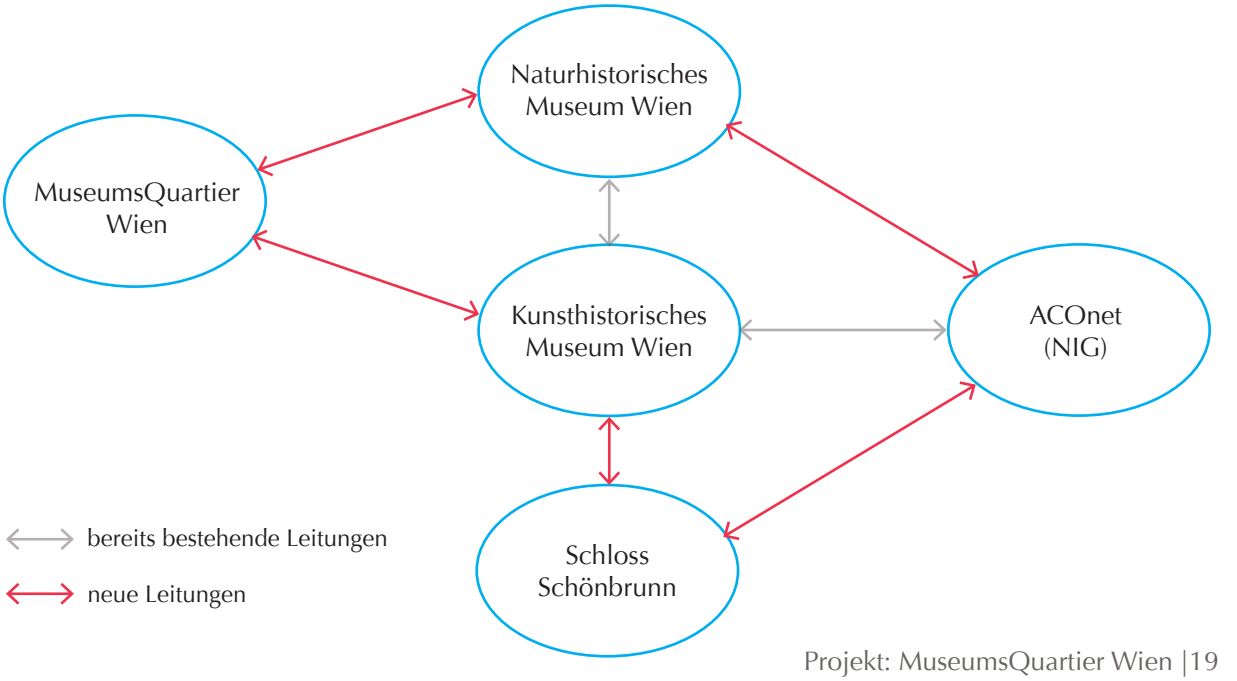
Projekt MuseumsQuartier Wien

Bereits Anfang 2013 gab es eine ACOnet Informationsveranstaltung im MuseumsQuartier Wien und erste Gespräche mit diversen MQ Institutionen sowie der MQ Betreibergesellschaft. In mehreren Phasen entwickelte sich daraus 2014 eine Initiative der MQ Betreibergesellschaft, eine „Open Access" Glasfaser-Infrastruktur am Gelände des MQ den eingemieteten Institutionen einerseits und Service Providern andererseits anzubieten.

Diese Entscheidung kam den Überlegungen des ACOnet Betreibers entgegen, einen Anschlusspunkt am Gelände des MQ zu errichten, um den MQ Institutionen die ACOnet-Teilnahme zu erleichtern. Der konkrete Bedarf des Naturhistorischen Museums, dessen beide Außenstellen im MQ mit dem Haupthaus zu verbinden, sowie das konkrete Interesse des MUMOK an einer ACOnet-Teilnahme stellte den „Business Case" dar um dieses Vorhaben in Angriff zu nehmen. Gerade noch rechtzeitig konnte im Rahmen eines KUKIT-Stammtisches (siehe Seite 31) eine Synergie mit einem weiteren Glasfaser-Vernetzungsprojekt der ACOnet-Teilnehmer Kunsthistorisches Museum, Schloß Schönbrunn und mdw - Universität für Musik und darstellende Kunst Wien gefunden werden.

Daraus resultierte die Herstellung eines Glasfaserringes, der alle beteiligten Standorte ausfallsicher und wege-redundant untereinander sowie mit dem ACOnet Core-Standort Wien1 an der Universität Wien (NIG) verbindet. Die ersten Strecken konnten noch im Dezember 2014 übergeben werden. Die Fertigstellung dieses Ringes wird für April 2015 erwartet.

Christian Panigl
Abteilungsleiter ACOnet & VIX



CASE STUDY

Òpera Oberta and research and education networks bring opera to students across the world

High capacity networks work together to broadcast performances to universities around the globe

Allowing students interested in the arts to experience cultural performances is central to sharing knowledge and helping them learn. However the scale and size of many productions, such as operas, mean that they cannot be staged locally due to a lack of resources and budget.

To bridge this gap and help make opera better known to students all around the world, the Gran Teatre del Liceu in Barcelona has created the Òpera Oberta programme. This produces and broadcasts high quality operatic performances to students in over 40 universities around the world. Since its foundation in 2001, Òpera Oberta has grown rapidly, and now has an average of 1,300 students from universities in Europe and Latin America watching every broadcast. Each performance is supported by a full package of learning materials, including a lecture before each opera outlining the plot and background, images and archived documentation. Students receive course credits for their virtual attendance, with every performance streamed simultaneously to all participating institutions.

As the operas are recorded using the most advanced broadcast video and sound technologies, sharing the files requires reliable, high capacity, cost-effective network links. Consequently Òpera Oberta relies on the speed and power of research and education networks, which deliver the guaranteed performance to ensure that every student receives a high quality experience.

The number of universities involved and their locations across the globe make simultaneous transmission a technical challenge. This is solved through a collaboration between a growing number of National Research and Education Networks (NRENs) and their international counterparts.

Broadcast files are first sent using multicast IP from the Liceu to the Catalan Research and Education Network, managed by CSUC, which is connected to the Spanish RedIRIS network. The high speed pan-European GÉANT network then transmits the performances across the continent to NRENs in individual countries, such as GRNET in Greece, and, worldwide through its global links to networks in other regions. For example, in Latin America the RedCLARA network then distributes the broadcast to the NRENs of Columbia (RENATA), Mexico (CUDI) and Ecuador (CEDIA). The NRENs then transmit the opera to individual universities in each country. The advanced multicast IP technology used makes it possible to send the same stream simultaneously to all participating institutions, wherever they are located, reducing complexity and minimising delays.

L'incoronazione di Poppea, © Rubén Ferrer Cherta

The Challenge

To introduce students to opera by combining world class performances with the latest broadcasting technologies.

The Solution

Performances are broadcast simultaneously using multicast technology across national and international research and education networks, such as GÉANT and RedIRIS, providing a compelling experience for students around the world.

Key Benefits

Wherever they are students can learn about and experience the beauty of opera through high quality broadcasts, thanks to the collaboration between Òpera Oberta and research and education networks.

CSUC Consorci de Serveis Universitaris de Catalunya

Gran Teatre del Liceu

Red IRIS

GÉANT Association

Am 7. Oktober 2014 haben sich TERENA[1] und DANTE[2] zusammengeschlossen und unter dem Namen GÉANT Association neu organisiert.

Diese Restrukturierung, auf Wunsch der NREN[3] Community, kennzeichnet nach fast 30 Jahren eine neue Phase der Zusammenarbeit für Forschungs- und Bildungnetze in Europa.

Bob Day, Executive Director of JANET, dem britischen NREN, wurde der neue interimistische CEO der GÉANT Association. Er ist der Meinung, dass die Restrukturierung ein Mittel schafft um die Vorgehensweise der Community bzgl. des Horizon2020 Programms der Europäischen Kommission besser zu koordinieren.

Für die NREN Community bedeutet der Zusammenschluss eine gebündelte Kommunikation im Europäischen Wissenschaftskontext, eine vereinfachte Verwaltung und ein effizienteres Management.

Erhalten bleiben natürlich die Services, wie die jährliche Networking Conference (TNC), das bekannte und gern genutzte Zertifikatsservice TCS, die Task-Forces und vieles mehr. Alles unter dem gemeinsamen Namen der GÉANT Association.

www.geant.org

Trusted Certificate Service TCS

Das unter dem Namen „TERENA Certificate Service" bekannte Zertifikatsservice bekam durch die Restrukturierung in die GÉANT Association den neuen Namen „Trusted Certificate Service".

Da im Juli 2015 der Vertrag mit Comodo als „Certificate Authority" auslaufen wird, erfolgte im Jahr 2014 eine neue Ausschreibung.
Die GÉANT Association entschied sich im Dezember 2014 für DigiCert als neue „Certificate Authority" für die nächsten zwei Jahre.

DigiCert bietet neben einer breiten Palette an Zertifikatstypen auch ein Zertifikats-Portal und verspricht außerdem eine bessere, einfachere und schnellere Verifikation.

[1] TERENA	Trans-European Research and Education Networking Association
[2] DANTE	Delivery of Advanced Network Technology to Europe - Betreiber des Pan-europäischen Wissenschafts- und Forschungsnetzverbundes GÉANT
[3] NREN	National Research and Education Network - z.B. ACOnet

Services

ISPA Internet Security Awareness Day

Da im Rahmen der ersten Arbeitsgruppensitzung der AG Security bereits zahlreiche interessante Themenfelder lokalisiert werden konnten, organisierte die AG Security am 18. September 2014 den ganztägigen ISPA Internet Security Awareness Day.

Die Veranstaltung wurde in zwei Panels gegliedert und konnte dabei die zahlreichen technikaffinen Vertreterinnen und Vertreter von Industrie und Wissenschaft zu spannenden Diskussionen über Cyber-Security anregen. Am Vormittag setzten sich die Teilnehmerinnen und Teilnehmer mit Themen aus den Bereichen der E-Mail Transport Security und Anti-Spam auseinander. Im Nachmittagspanel wurden beispielsweise die Probleme bei DDoS Bekämpfung oder Anti Spoofing erörtert. Die Vortragenden waren Otmar Lendl (CERT.at), Harald Michl (ACOnet), Christoph Loibl (next layer) und Wolfgang Breyha (Universität Wien).

www.ispa.at

Quelle: ISPA

IKT Sicherheit

Ein österreichisches Langzeitprojekt in Public-Private-Partnership

Nach den grundlegenden Aktivitäten der letzten Jahre zur schrittweisen Verbesserung der IKT Sicherheit in Österreich (z.B. Beschluss der nationalen IKT-Sicherheits Strategie 2012, Österreichische Strategie für Cybersicherheit 2013) stand das **Jahr 2014 eher im Zeichen der Umsetzung in die Realität**. Wie schon in den Jahren davor war ich für das Sicherheits-Team des ZID der Universität Wien und ACOnet eingeladen, an folgenden Projekten mitzuarbeiten:

- Erstellung des Vorschlages für die Geschäftsordnung der **Cyber Security Plattform CSP** (unter der Federführung von Bundeskanzleramt und BMI), wo ich die Erfahrungen mit bereits länger existierenden Gruppen aus dem nationalen und internationalen Bereich einbringen konnte. Die Beratungen und Abstimmungen mit den anderen Aktivitäten (wie der österreichische CERT Verbund[1] und die „Austrian Trust Circles"[2]) zu diesem Thema waren sehr interessant und aufschlussreich. Besonders aus dem Gesichtspunkt des Aufbaus und der Intensivierung von Kontakten zu den „Stake-Holdern" in der Sicherheitslandschaft hat sich der Aufwand wohl gelohnt.
Die Errichtung der CSP war ursprünglich bereits für Herbst 2014 geplant, wurde dann aber aus logistischen Gründen in das Jahr 2015 verschoben.

- Mitarbeit in der „Experts-Group" zur Vorbereitung der **Sicherheits-Übung „CE.AT"** im Oktober 2014. Die Abkürzung „CE" steht für „Cyber Europe", eine bereits mehrmals abgewickelte Sicherheits-Übung, die gleichzeitig in mehreren Ländern der EU stattfindet. CE.AT, der für Österreich relevante Teil, konzentrierte sich diesmal auf Unternehmen aus dem Bereich der Energieversorgung, auf ISPs als Plattform für Kommunikation und die öffentliche Verwaltung (Regulator, Ministerien, GovCERT). Der Schwerpunkt lag eher auf Kommunikation und Eskalation als auf technischen Details. Durch die direkte Teilnahme an den Absprachen zu dem Übungsdrehbuch war es möglich, technische Fehlannahmen zu korrigieren und falsche Erwartungen zurecht zu rücken.

Sicherheit im GÉANT Netzwerk-Verbund

Neben den regelmäßigen Überprüfungen der Betriebssicherheit in GÉANT wird von DANTE (später GÉANT Association, siehe Seite 21) auch regelmäßig eine „Security Working Group" eingeladen mit dem Ziel, eher strategische Themen zur Sicherheit des Netzwerkes zu diskutieren und gegebenenfalls entstehende Betriebsblindheit frühzeitig zu identifizieren.

Nach dem Ausscheiden, bedingt durch Job-Wechsel, eines Mitglieds dieser internationalen Arbeitsgruppe wurde ich eingeladen, den Kollegen zu ersetzen. Die zwei in Cambridge verbrachten Tage waren sehr interessant, besonders weil einige der diskutierten Themen auch für das ACOnet Betriebsumfeld relevant sind.

Wilfried Wöber
Ansprechpartner Security & Internationale Koordination

ACOnet-CERT

Computer Emergency Response Team

Das Jahr 2014 hatte aus CERT-Sicht einen eindeutigen Themenschwerpunkt: Sicherheitslücken.

Den Anfang machte gleich eine ganze Klasse von Schwachstellen, die seit vielen Jahren völlig unbemerkt schlummerten: Dienste, die sich für sogenannte **UDP reflection amplificaiton DOS attacks** missbrauchen lassen.

Das Szenario: Mit nur ganz wenig Bandbreite kann ein Angreifer verwundbare Server dazu veranlassen, ein Ziel mit ganz viel Daten zu bombardieren. Hat der Angreifer viel Bandbreite oder gar ein Botnet zur Verfügung, dann verschwindet auch schon mal eine größere Einrichtung von der Internet-Bildfläche.

Bemerkenswert ist dabei, dass weder ein Programmierfehler noch eine schwere Fehlkonfiguration schuld sind. Wenn ein Service unfreiwillig an einer DOS-Attacke teilnimmt, sind drei Faktoren aus völlig verschiedenen Verantwortungsbereichen beteiligt:

- Access Provider lassen zu, dass IP-Pakete mit gefälschter Quell-Adresse ihr Netz verlassen
- das Protokolldesign des missbrauchten Dienstes macht es möglich, dass Anfragen von ungeprüften Absendern mit großen Datenmengen beantwortet werden
- der Dienst wird weltweit ohne rate-limit zur Verfügung gestellt.

Erschreckend ist die Vielfalt an solchen Services, die zum Teil selbstverständlich weltweit offen zugänglich sind: DNS- und Time-Server, aber auch unnötigerweise snmp-agents in Switches, Druckern, Servern, embedded devices, etc.

Die Gegenmaßnahmen gehen in zwei Richtungen:

- das Fälschen von IP-Adressen unterbinden. ACOnet hat dazu BCP38 (siehe Seite 14) implementiert
- Services abschotten oder so umkonfigurieren, dass sie nicht mehr für Angriffe missbraucht werden können.

CERT scannt

Das ACOnet-CERT hat diese Situation zum Anlass genommen, selbst nach Schwachstellen zu suchen. Mit einer generischen Scan-Engine können nun verschiedenste Tests durchgeführt werden; die Ergebnisse werden automatisch ausgewertet und die Betreiber von entdeckten Problem-Diensten benachrichtigt. Dabei war es ein zentrales Anliegen, nicht einfach die Scans zu duplizieren, die von anderen CERTs und Institutionen bereits „im gesamten Internet“ durchgeführt werden.

Weniger ist manchmal viel mehr: Es werden nicht alle IP-Adressen gescannt, sondern nur jene, die in den Netzwerkstatistiken als aktiv erscheinen. Das ist insofern viel mehr, als auf diese Weise auch IPv6-Adressen erfasst werden, was wegen ihrer großen Zahl anders nicht möglich wäre.

Schicksalstag 8. April 2014

Am 8. April wurde die IT-Welt erschüttert: Microsoft hat den Support für Windows XP samt Internet Explorer 6 eingestellt, Schwachstellen werden nicht mehr behoben. Verschiedenen Schätzungen zufolge lief damals noch etwa jeder vierte PC weltweit auf dieser Antiquität aus dem Jahr 2001. Von Sonderfällen wie dem ohne Netzwerkanschluss betriebenen Elektronenmikroskop abgesehen ist das eigentlich fahrlässig.

Doch aller Aufmerksamkeit war bereits auf den kryptographischen Supergau des Jahrzehnts gerichtet: auf **Heartbleed**.

Die Sicherheitslücke Heartbleed

wurde mannigfach beschrieben, dennoch ist sie auch im Rückblick bemerkenswert. Zum einen gab es schon lange, vielleicht seit SQL Slammer im Jahr 2003, kein vergleichbares Ereignis, bei dem „das gesamte Internet" schnell auf eine Bedrohung reagieren musste. Das hat recht gut funktioniert, echte Schadensfälle sind kaum bekannt. Die eben erst eingerichtete Scan-Engine kam natürlich auch sofort zum Einsatz.

Im Zuge von Heartbleed, später sekundiert von „Beast", „Poodle" und „Freak", wurde immer wieder das Ende von Verschlüsselung mit TLS (ehemals SSL) ausgerufen. Es gibt Meinungen, das Protokoll sei von der NSA kompromittiert, die Certification Authorities undemokratisch und korrupt u.v.m. Tatsächlich ist Skepsis angebracht: Was heute mit einem aktuellen Verfahren verschlüsselt wird, kann in 15 Jahren vielleicht schon geknackt werden. Welche Möglichkeiten Geheimdienste haben, weiß man sowieso nicht so sicher. Doch fehlt auch den größten Kritikern die bessere Alternative, und bei der Absicherung unserer alltäglichen Geschäfte hat sich das Verfahren auch im Lichte der bekanntgewordenen Schwächen hervorragend bewährt.

A propos Verunsicherung in Sachen Kryptographie: Die Entwicklung der Verschlüsselungssoftware TrueCrypt wurde im Mai 2014 unerwartet mit dem Hinweis auf angebliche Sicherheitsprobleme eingestellt. Worin diese bestehen sollen, konnt allerdings bislang nicht nachvollzogen werden.

Shellshock: Patch Management am Prüfstand

Im Herbst folgte mit Shellshock eine weitere Herausforderung der besonderen Art:

Von der Lücke wurde etwas zu aufgeregt in zahreichen Medien berichtet, denn es war kaum klar, wie sie denn ausgenützt werden könnte. Im Gegensatz zu Heartbleed war es keineswegs leicht zu entscheiden, ob bzw. wann kritische Produktionssysteme zwecks Wartung heruntergefahren werden sollen oder ob die Medizin mehr Schaden als Nutzen stiftet. Noch eine Frage tauchte auf: Wer entscheidet auf welcher Grundlage? Tatsächlich haben viele Organisationen ihre Shellshock-Updates in ein passendes Wartungsfenster gelegt - offenbar zu Recht.

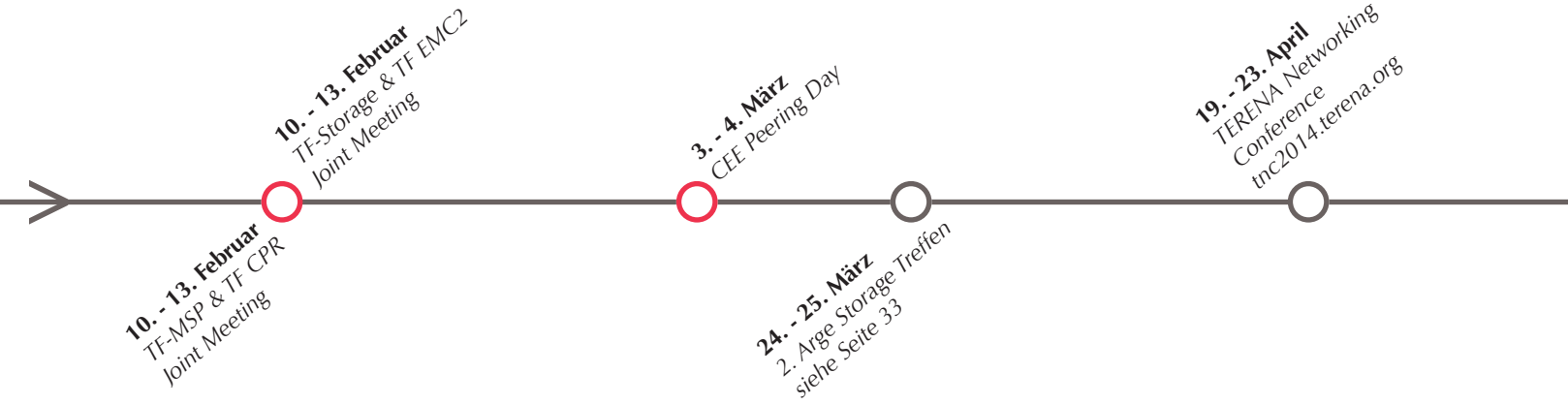
Nicht jede Organisation hat eine definierten Prozess zum Patch Management. Das fängt damit an, reproduzierbar über Sicherheitslücken informiert zu werden - nicht alles ist mit Auto-Updates und der Gratiszeitung in den Öffis abgedeckt. Dann müssen die Anwendbarkeit, Dringlichkeit und die möglichen Auswirkungen analysiert werden und Gegenmaßnahmen gefunden bzw. bewertet werden. Wer befindet letztliche über die weitere Vorgangsweise? Bei Heartbleed haben viele Admins völlig autonom sofort gehandelt und das war wohl gut so, aber im Sinne der reinen Lehre ist das nicht. Es ist für alle Beteiligten hilfreich, wenn Informationsquellen, Entscheidungsprozesse und -kompetenzen vorab geregelt sind.

Fazit

Schwachstellen in IT-Systemen sind nichts Neues. Im Gegensatz zu allgegenwärtigen, hier nicht namentlich genannten, Dauerdesastern haben diese eine hohe mediale Aufmerksamkeit erlangt und wurden in der Regel rasch behoben. Was bleibt, ist die Herausforderung, auch in Zukunft Sicherheitslücken zeitgerecht zu erkennen, mit kühlem Kopf zu bewerten und professionell zu beheben.

Alexander Talos-Zens
ACOnet-CERT
http://cert.aco.net

Workshops & Meetings



TERENA Task Forces

TF-CPR & TF-MSP

Task Force on Communications and Public Relations
Task Force on Management and Service Portfolios

Diese TERENA Task Forces (nun GÉANT Association siehe Seite 21) unterstützen die Zusammenarbeit der Verantwortlichen aus den Bereichen "Marketing & Kommunikation" sowie "Management" der verschiedenen Wissenschaftsnetze in Europa. Sie treffen sich zumindest zweimal jährlich und auch ACOnet ist dort regelmäßig vertreten.

Von 10. bis 13. Februar 2014 fand das TF-CPR Meeting in Kombination mit dem Meeting der TF-MSP in Wien statt und wurde von ACOnet gehostet.

Die Themen der TF-CPR reichten von **PeaR dem Community Newsletter**[1], über **Social Media Strategien** bis hin zur **FileSender Promotion**.

Die TF-MSP konzentrierte sich auf „Joint Procurement and Service Delivery", „NREN Compendium and Service Maps", „Green ICT for NRENS & GÉANT".

[1] https://www.terena.org/news/community/

CEE Peering Day

Am 3. und 4. März 2014 fand der **Central and Eastern European Peering Day 2014** in Wien statt.

Diese **Fachtagung der Internetwirtschaft** richtete sich primär an Internet Service Provider aus Österreich und der Tschechischen Republik sowie aus dem zentral- und osteuropäischen Raum und wurde bereits zum zweiten Mal vom **„Vienna Internet eXchange" VIX** gemeinsam mit dem „**Neutral Internet eXchange" NIX.CZ** aus Prag organisiert.

Die Konferenz war mit knapp 150 Tagungsgästen gut besucht und verfolgte das Ziel, den Wert von Internet Exchange Points zu vermitteln, die Kommunikation untereinander zu fördern und neue Kontakte herzustellen.

Eine Fortsetzung des CEE Peering Days ist 2015 in Bratislava geplant.

www.peeringday.eu

www.vix.at

VIX Vienna Internet eXchange

© Naturhistorisches Museum Wien - Foto: Peter Wienerroither

29. April
6. KUKIT Stammtisch

8. - 9. Mai
29. Arge Secur Treffen
Bozen

27. Mai
7. KUKIT Stammtisch

12. - 13. Juni
49. TBPC Treffen
siehe Seite 35

KUKIT

Renate Kreil
Kommunikation Kunst & Kultur

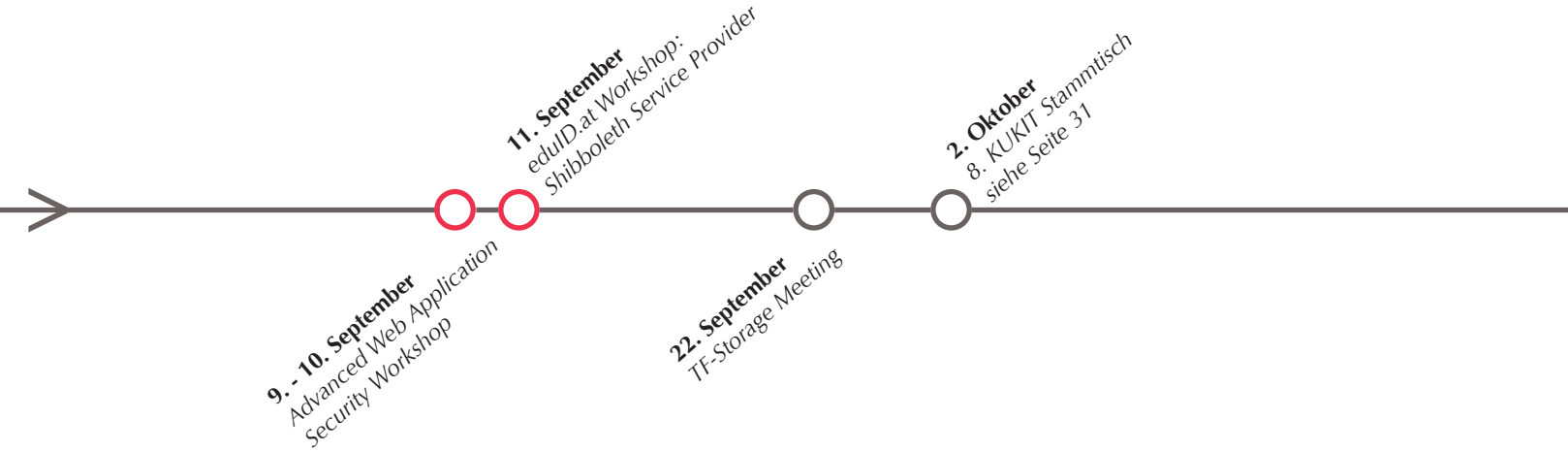
2014 war ein starkes Jahr für den sogenannten KUKIT-Stammtisch, eine Initiative des Kunsthistorischen Museum Wien und ACOnet.

Vor zwei Jahren entwickelte sich die Idee zwischen mehreren IT-Leitern von Kunst- und Kulturinstitutionen ein Forum zu etablieren, das wichtige IKT-Themen der Gegenwart und Zukunft zur Diskussion stellt. Dabei sollte auch das Know-how eines international agierenden Wissenschaftsnetzes nicht fehlen. Aus diesem Grund sollte eine Gemeinschaft gebildet werden, die gemeinsam Vorträge und Workshops organisiert, allgemeine Anforderungen formuliert und Erfahrungen austauscht, die sich unter anderem in einem positiven Zeit- und Finanzmanagement manifestieren sollten.

Gastgeberhäuser 2014 waren die Albertina, das Österreichische Museum für angewandte Kunst / Gegenwartskunst, das Naturhistorisches Museum und zum ersten Mal wurde ein KUKIT-Stammtisch in ein anderes Bundesland eingeladen - in das Universalmuseum Joanneum/Kunsthaus Graz.

Die Themen reichten im Jahr 2014 von „Wissenschaftsnetze, eine Chance für Kunst- und Kultur“ über „Langzeitarchivierung/Digitalisierung von Kulturgut/phaidra.lab“ bis hin zu „Digital Signage und der Tiefenspeicher der Albertina“.

Eine Vorschau für 2015 sei erlaubt, da dieses Infrastrukturprojekt mit Signalwirkung aus den letzten 9 KUKIT-Stammtischen hervorgegangen ist. 2015 soll Wien einen neuen Ring bekommen. Der LWL-WienMitte/Wien West ein redundanten Glasfaserring, wird führende Kunst- und Kulturinstitutionen direkt miteinander verbinden und geht voraussichtlich Anfang April in Betrieb.



Advanced Web Application Security Workshop

Aufgrund zahlreicher Interessentinnen und Interessenten aus dem ACOnet Teilnehmerkreis buchte ACOnet letztes Jahr den Kurs "Advanced Web Application Security" bei HM Training Solutions.

Der Workshop wurde vom 9. bis 10. September von Michael Thumann und seinem Kollegen abgehalten. Als eine für ACOnet Teilnehmer auf zwei Tage komprimierte Spezialausgabe, konzentrierte sich der Workshop auf technische Themen und die Zielgruppe Webentwickler.

Gezeigt und erklärt wurden unter anderem Bedrohungen durch SQL Injections, Cross Site Scripting, Session Management aufgelockert mit vielen praktischen Übungen.

Am Folgetag, dem 11. September, wurde zusätzlich ein kostenloser **ACOnet / eduid.at Workshop zum Thema "Shibboleth Service Provider"** von Peter Schober angeboten bei dem die Integration eigener Web-basierter Resourcen in ein SAML-basiertes WebSSO System behandelt wurde.

Handysignatur Workshop

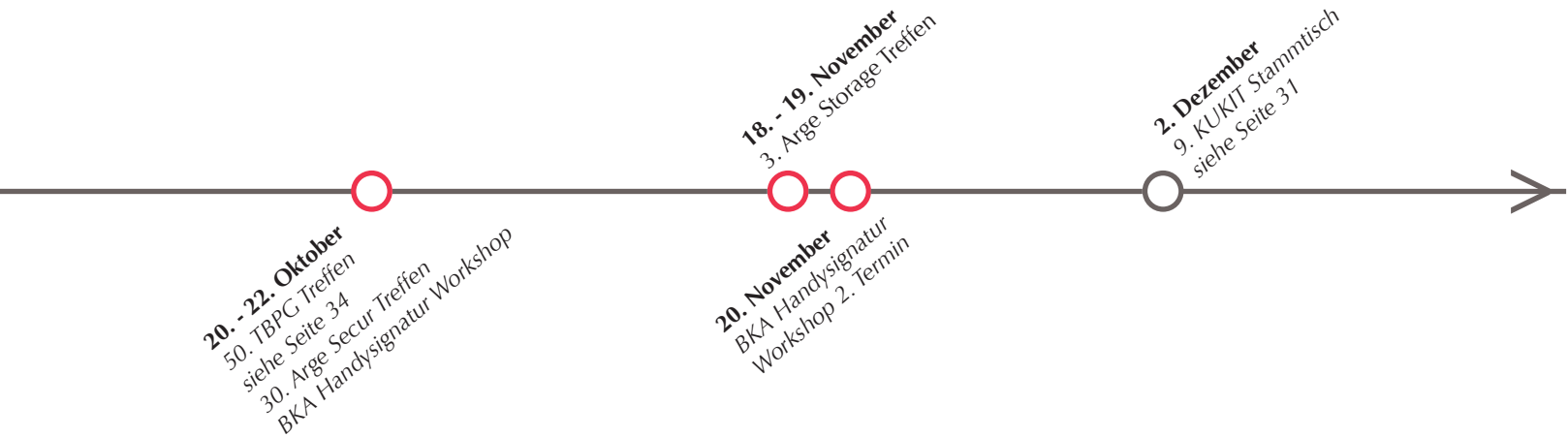
Zum 50. TBPG Treffen (siehe Seite 34) wurde vom Bundeskanzleramt ein Handysignatur Workshop organisiert, wo die Teilnehmerinnen und Teilnehmer zum **Registration Officer und Trainer** ausgebildet wurden.

Handysignaturen werden immer häufiger in offiziellen Abläufen verwendet. Mit der Ausbilung zum Handysignatur Officer können die Teilnehmerinnen und Teilnehmer in ihrer Institution ebenfalls Handysignaturen ausstellen und als Trainer andere Officer in ihrer Institution ausbilden.

Da sich diese Schulung großer Nachfrage im ACOnet Teilnehmerkreis erfreute, wurde Ende November noch ein zweiter Termin an der Universität Wien organisiert.

DIGITALES ÖSTERREICH

BUNDESKANZLERAMT ÖSTERREICH



ArgeStorage

Die 2013 gestartete Arbeitsgemeinschaft Storage (ArgeStorage) konnte 2014 weitergeführt und hinsichtlich Teilnehmerzahl auch noch deutlich ausgebaut werden.

Das 2. ArgeStorage Meeting, welches im Frühjahr am Management Center Innsbruck (MCI) stattfand, war mit 41 TeilnehmerInnen erfreulicherweise schon recht gut besucht und wurde vom 3. ArgeStorage Meeting im Herbst an der Wirtschaftsuniversität Wien mit 55 Teilnehmenden noch übertroffen.

Es wurden die Themenbereiche Storage Virtuallisierung, Backup, Langzeitarchivierung, Cloud Storage, Collaboration Services, ownCloud uvm. behandelt. Bei beiden Meetings konnten internationale Experten als Vortragende gewonnen werden.

Die ArgeStorage bietet den ACOnet-Teilnehmern ein Forum rund um das große Themengebiet „Storage und Collaboration“. Die Anforderungen an Storage-Systeme und Collaboration-Software sind bei vielen Institutionen recht ähnlich, doch die Lösungen können durchaus sehr unterschiedlich ausfallen. Die ArgeStorage soll einen Rahmen bieten, in dem Experten Erfahrungen, Probleme und dessen Lösungen miteinander austauschen können.

Arsen Stasic
Ansprechpartner
GovDNS & ACOmaster
ArgeStorage

TBPG Treffen

Technische Betriebs- und Planungsgruppe

Die „ACOnet technische Betriebs- und Planungsgruppe“ hat die Funktion eines technischen Benutzerbeirates und tagt zweimal im Jahr. Alle ACOnet Teilnehmerorganisationen sind eingeladen ihre technischen Experten zu entsenden, um betriebliche und technische Erfahrungen auszutauschen.

Das ACOnet Team nutzt diese Treffen um die Teilnehmerinnen und Teilnehmer über neue Services zu informieren, auf sicherheitsrelevante Probleme hinzuweisen und betriebliche Neuerungen zu präsentieren.

Das erste „**ACOnet Systemmanagertreffen**“, wie es damals genannt wurde, fand am 28. März 1990 an der Technischen Universität Wien statt.
Anlass dazu war das Ergebnis der Ausschreibung des Bundesministeriums für Wissenschaft und Forschung vom 2. Februar 1990 über „ACONET-Stufe 1“, **der Verwirklichung eines österreichischen Wissenschaftsnetzes**.
27 Teilnehmerinnen und Teilnehmer zählte dieses erste Treffen. Viele davon haben das ACOnet jahrelang begleitet und einige sind heute noch regelmäßig an den Treffen der technischen Betriebs- und Planungsgruppe beteiligt.

2014 konnten wir ein Jubiläum feiern: das **50. TBPG Treffen** führte uns zurück an die TU Wien, wo auch das ACOnet selbst seine Wurzeln hat.

Von 20. bis 22. Oktober 2014 kamen insgesamt 126 Teilnehmerinnen und Teilnehmer in den prunkvollen Kuppelsaal zu diesem Jubiläumstreffen, das in Kombination mit dem **30. ArgeSecur Meeting** und einem Handysignaturworkshop des Bundeskanzleramtes (siehe Seite 32) organisiert wurde.

Neben den IT-Security Themen wie beispielsweise die SHA-1 Deprecation[1], BCP38 (siehe Seite 14) oder die „E-Mail Transport Security“ wurde der Fokus auf die Netztopologieänderungen einiger Universitäten gerichtet.
Universität Wien, TU Graz, Universität Innsbruck und Universität Salzburg präsentierten ihre neuen Campus Architekturen, die Hürden, die sie bewältigen mussten und teilten ihre positiven sowie negativen Erfahrungen. (u:core Projekt der Universität Wien: siehe Seite 52)

Die zahlreich erschienenen Ehrengäste machten dieses Treffen zu einem würdigen Jubiläum, da sie seit den ersten Stunden ACOnet begleitet und gefördert haben.

Das 50. TBPG Treffen, 24 Jahre nach der Geburtsstunde des ACOnets, war bereits ein Vorbote auf das kommende Jahr und deutet schon darauf hin, dass wir 2015 dann 25 Jahre ACOnet und gleichzeitig 25 Jahre Internet in Österreich feiern dürfen.

1 SHA-1 Deprecation: „Signature Hash Algorithm" der heute meist verwendete Algorithmus um Zertifikate zu signieren. Gilt seit 2005 als (theoretisch) verwundbar. 2011 gab es die erste mathematisch bewiesene Attacke. Darauf basierende mathematische Modelle berechnen, dass spätestens im Jahr 2018 aktuelle Standard Hardware diese Attacke in sinnvoller Zeit durchführen kann. Jedes SHA-1 signierte Zertifikat gilt demnach ab 01.01.2017 als ungültig und wird dementsprechend markiert. Die Lösung bietet SHA-2.

49. TBPG Treffen

von 12. bis 13. Juni 2014
an der Alpen Adria Universität Klagenfurt

Der Austragungsort des Sommermeetings 2014 war direkt am Wörthersee an der Universität Klagenfurt.

Peter Gruber und Harald Michl wurden als neue Arbeitsgruppen-Leitung angenommen.

Die Themen reichten von RIPE Atlas, über die ACOnet Identity Federation bis zu Heartbleed (siehe Seite 27)

Im Rahmen der Veranstaltung wurde, um die Security-Awareness zu erhöhen, eine PGP Key Signing Party organisiert.

Internet Domain Administration

Team Internet Domain Administration

Internet Domain Administration und Schwerpunkte

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

Das Referat „Internet Domain Administration“ ist seit 2011 Teil der Abteilung „ACOnet & Vienna Internet eXchange“ am Zentralen Informatikdienst der Universität Wien.

Die Internet Domain Administration erbringt unter anderem Domain Name Services sowie System- & Netzwerk-Monitoring Services für den ACOnet Bereich.

Neue Top Level Domains

Die letzten Jahre waren weitgehend von Tätigkeiten geprägt ein Umfeld für den Betrieb der neuen Top Level Domains (TLDs) zu schaffen. Das waren sowohl Arbeiten zur detaillierten Spezifikation der Funktionsweise, als auch dann die konkreten Implementierungen der Software (siehe auch ACOnet Jahresberichte der vergangen Jahre).

Im Laufe der Jahres 2014 wurden die Implementierungen finalisiert, wobei durch sehr spät publizierte, oder im letzten Moment geänderte Anforderungen seitens ICANN immer wieder einige Hürden genommen werden mussten. Trotzdem konnten alle Arbeiten zeitgerecht abgeschlossen werden, sodass den einzelnen Inbetriebnahmen nichts mehr im Wege stand. Diese folgten dann auch wirklich Schlag auf Schlag das ganze Jahr begleitend:

Februar	.wien
	.berlin
April	.voting
Juli	.reise
	.hamburg
August	.versicherung
September	.brussels
	.vlaanderen
November	.tirol

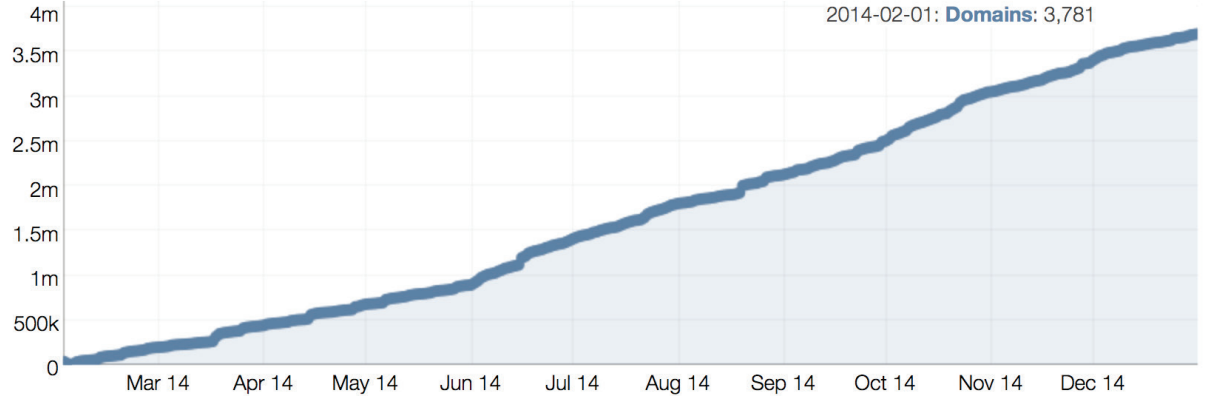
In diesem Zusammenhang sei hier auch kurz erwähnt, dass eine Inbetriebnahme nicht einfach ein Einschalten bedeutet, wo danach schnell Domains registriert werden können. Vielmehr ist ein komplexer Prozess der aus unterschiedlichen Phasen, wie „sunrise“, „landrush“, „general availability“, besteht einzuhalten.

Dieses aufwendige Verfahren resultiert aus der Notwendigkeit Marken (trademarks) gesondert behandeln zu müssen. Dafür steht ein eigener, von den Registries unabhängiger Apparat, das sogenannte Trademark Clearinghouse (TMCH), zur Verfügung. Daran müssen sich alle Registries orientieren und die einzelnen Phasen der Domain Vergabe abstimmen.

Weitgehend alle diese Phasen wurden im Rahmen der Inbetriebnahmen der oben erwähnten Top Level Domains im Laufe des Jahres erfolgreich abgewickelt, einige davon laufen noch bis in das Jahr 2015.

Die Entwicklung der Domain Registrierungen ist erfreulich, der Betrieb stabil und die entwickelte Software läuft zufriedenstellend und fehlerfrei. Diese Umstände haben bewiesen, dass auch ein im Vergleich kleiner Betrieb und eine engagierte Mannschaft gegenüber wirklichen Größen der internationalen Branchen ihren Platz finden kann.

Gerhard Winkler
Teamleiter
Internet Domain Administration



Quelle: https://ntldstats.com

Begleitend zur Softwareentwicklung mussten auch andere Bereiche forciert behandelt werden, nämlich der Bereich des Release Management und der Bereich des Testens, respektive des automatisierten Testens. Der Einsatz derselben Software auf unterschiedlich konfigurierten Systemen (verschiedene features der einzelnen TLDs) mit unterschiedlichen Registrierungsphasen erfordert einerseits ein parametrisierbares System und andererseits die Möglichkeit features, bugs und bestimmte Softwarestände zuordnen, verwalten und ausliefern zu können. Weiters ist eine eigene Infrastruktur notwendig, die es ermöglicht einen bestimmten Softwarestand für alle unterstützten TLDs gegen Anforderungen oder gegen versehentliche Funktionsänderungen testen und prüfen zu können. Diese Mechanismen müssen schon aus dem Grund der Skalierbarkeit automatisch ablaufen können. Allein für diese Fragestellungen und Anforderungen wurde eine eigene Testsoftware entwickelt und Personalkapazität dediziert zur Qualitätssicherung zur Verfügung gestellt.

Mit den Tätigkeiten des Jahres 2014 konnte eine solide Basis eingerichtet werden, die es ermöglicht auf kommende feature Wünsche, neue Anforderungen seitens ICANN reagieren und natürlich den Tagesbetrieb bewältigen zu können.

ISO 27001 Zertifizierung
der nic.at GmbH

Die internationale Norm ISO 27001 definiert Anforderungen an ein Information Security Management System (ISMS). Das Kernthema dabei ist das „Managen" von IS-Risiken, wobei hier nicht nur direkt auf IT-Systeme eingegangen wird, sondern auch auf die damit verbundenen Prozesse und personelle Ressourcen, also generell auf Risiken hinsichtlich der Sicherheit von Information und Informationsverarbeitung.

Die Etablierung eines definierten und funktionierenden Risikomanagements ist in diesem Sinne essentiell. Dabei fordert dieses Modell einen evolutionären Prozess, also ein System, das zyklisch die einzelnen Status „Planen", „Durchführen", Überprüfen" und „Verbessern" durchläuft. Damit einher geht natürlich auch ein Prozess, die eigene Organisation für dieses ISMS zu adaptieren, entsprechende Richtlinien zu formulieren und ISM Prozesse einzurichten. Alle diese Komponenten bedeuten sowohl bei der Einführung, als auch dann im laufenden Betrieb des Informationsicherheit Management Systems einen bewussten Umgang mit, sowie das Erkennen und Einschätzen, von Risiken.

Im Jahr 2012 begann die nic.at GmbH mit den Vorbereitungen für eine ISO27001-Zertifizierung. Im Februar 2014 wurde nic.at erfolgreich zertifiziert.

Doch was bedeutete das eigentlich für die Gruppe Internet Domain Administration?
Durch die Kooperation und Leistungsvereinbarung mit nic.at, also etwa die Entwicklung von Software oder den Betrieb von IT-Systemen, ist die Internet Domain Administration „Lieferant" (vgl. Control A.15 supplier relationship) im Sinne der ISO Norm. Eine zertifizierte Organisation muss ihre Lieferanten (supplier) im Sinne von „ensure protection of the organization's assets that is accessible by suppliers" und „maintain an agreed level of information security and service delivery in line with supplier agreements" unter „Kontrolle" haben.

Durch diese Anforderungen ist die Internet Domain Administration „gezwungen", die geforderten Qualitätskriterien zu erfüllen oder einzelnen Mindestanforderungen zu genügen. Viele dieser Anforderungen wurden bereits im täglichen Betrieb erfüllt, da sie eine Notwendigkeit in der

Patrick Pichler
ACOnet-CERT

Gerhard Winkler
Teamleiter
Internet Domain Administration

gelebten Praxis eines sorgfältigen und pflichtbewussten Betreibers darstellen. Trotzdem ist die Erfüllung der ISO Kriterien eine neue Herausforderung, da sie eine viel bessere Strukturierung des Arbeitsumfeldes und daher ein Mehr an Ressourcen, vor allem in personeller Hinsicht, bedeutet. Herausfordernd dabei ist auch die Gratwanderung zwischen den Sicherheitsanforderungen des Kunden einerseits und der Flexibilität und Innovationskraft, die im akademischen Umfeld nötig ist, andererseits.

Der Zentrale Informatikdienst und insbesondere die Internet Domain Administration unterstützen nic.at bei der Erfüllung der ISO 27001 Auflagen. Die Unterstützung mündet vor allem darin, der nic.at ein verlässlicher und „sicherer", in ISO-Terminologie, „supplier" zu sein.

Wiederum in ISO-Terminologie werden Kriterien wie „Addressing security within supplier agreements", „Reporting information security events" oder allgemeiner „Information security policy for supplier relationships" formuliert.

Zur Umsetzung dieser Erfordernisse wurde ein Apparat implementiert, der genau diese Kriterien adressiert, wie etwa ein Code of Conduct zur Regelung eines gemeinsamen Verständnisses der Zusammenarbeit (hinsichtlich ISM), oder die Einrichtung eines gemeinsamen Gremiums zur regelmäßigen Abstimmung der konkreten (Security- oder ISM-) Themen. Das bildet die Basis und die Rahmenbedingungen für ein gemeinsames Risikoverständnis und Bewusstsein über die Machbarkeit allfälliger Umsetzungsanforderungen. Hiermit haben nic.at und das Team der Internet Domain Administration die Möglichkeit, abgestimmte Maßnahmen zur Erhöhung der Sicherheit zu treffen, damit die Risiken zu minimieren und zuletzt jenen Beitrag zu leisten, der zur Umsetzung der Anforderungen hinsichtlich eines zertifizierten ISMS der nic.at notwendig ist.

Diese ersten großen organisatorischen aber auch technischen Schritte konnten erfolgreich bewältigt werden, weitere sind aber im Sinne des kontinuierlichen Verbesserungsprozesses auch zukünftig nötig. Daher wird uns dieses Thema auch weiterhin begleiten.

Neue ACOnet Teilnehmer 2014

Salzburg Research Forschungsgesellschaft m.b.H.

FH Campus Wien

Beiträge von ACOnet Teilnehmern

Salzburg Research

Ein Jahr ACOnet, der Rückblick

Der Wunsch des Beitritts der Salzburg Research zum österreichischen Wissenschaftsnetz, dem ACOnet, ist schon etwas älter. Bereits im Jahr 2007 wurde erstmalig über eine Anbindung an das ACOnet diskutiert. Auch in den folgenden Jahren war es immer wieder Thema, doch erst mit Anfang 2013 kam Bewegung in die Sache, als wir uns zu ersten konkreten Gesprächen mit dem ACOnet und der Universität Salzburg trafen.

Nachdem beide Seiten ihre Kooperation und Unterstützung zusicherten, kam es in der Folge zu intensiven Gesprächen mit dem Ziel, die Salzburg Research über den Standort der Computerwissenschaften der Universität Salzburg an das ACOnet anzubinden. Schließlich konnten wir im April 2014 nach intensiver planerischer sowie technischer Vorbereitung die Leitung unseres kommerziellen Internetproviders durch die Anbindung an das ACOnet ersetzen.

Wir profitieren seitdem von der großen Bandbreite der Leitung, der hohen Verfügbarkeit des Backbones und der direkten Anbindung an die europäischen Forschungsnetze. Mit der Universität Salzburg haben wir im technischen Fehlerfalle immer kompetente Ansprechpartner vor Ort, mit denen wir vertrauensvoll und eng zusammenarbeiten können.

Unsere Mitarbeiterinnen und Mitarbeiter profitieren vor allem von folgenden Vorteilen:

- Die Ausstellung kostenloser SSL Server-Zertifikate gewährleistet die Vertraulichkeit (durch Verschlüsselung), Datenintegrität und Authentizität unserer Datenverbindungen und Server-Dienste.
- Der Zugang zum Wireless LAN über das eduroam an jeder teilnehmenden Institution war einer der größten Wünsche unserer international forschenden Mitarbeiterinnen und Mitarbeiter.
- Die Teilnahme an der ACOnet Identity Federation ermöglicht uns die Ausstellung von persönlichen SSL-Zertifikaten zum Signieren und Verschlüsseln von Nachrichten und Dokumenten. Im Hinblick auf die immer wichtiger werdende Vertraulichkeit der Daten im Internet wird dieser Dienst von unseren Mitarbeiterinnen und Mitarbeitern gut angenommen und intensiv genutzt.

Nicht zuletzt darf sich die Salzburg Research Forschungsgesellschaft durch den ACOnet Teilnehmerstatus und den Besitz der ac.at Domäne über eine erhöhte Reputation und Sichtbarkeit in der internationalen Forschung freuen.

Ausblick

ACOnet bietet auch für die Zukunft noch genug spannende Themen. So steht beispielsweise die Einführung von nativem IPv6 bei Salzburg Research vor der Türe und auch die Identity Services sollen für intern genutzte Ressourcen um Single-Sign-On (SSO) erweitert werden.

Peter Allgeyer
Salzburg Research Forschungsgesellschaft m.b.H.
IT-Security und Systemintegration
peter.allgeyer@salzburgresearch.at

salzburgresearch

Die Salzburg Research Forschungsgesellschaft

Salzburg Research ist ein unabhängiges Forschungsinstitut mit dem Schwerpunkt Informationstechnologien (IT). Die Forschungsgesellschaft versteht sich als visionärer Ideengeber, verbindender Netzwerker und professioneller Forschungspartner. Die Forschungslinien beraten in technischen IT-und Innovationsthemen und gestalten in nationalen und internationalen Forschungsprogrammen sowie im Auftrag der Industrie.

FH CAMPUS WIEN

UNIVERSITY OF APPLIED SCIENCES

© APA-Fotoservice/Schedl

FH Campus Wien

Neuer ACOnet Teilnehmer

Ein Jahr dabei

Die IT-Services der FH Campus Wien sind für die Bereitstellung qualitativ hochwertiger Ressourcen unter Berücksichtigung von Datenschutz und Datensicherheit verantwortlich. Dem System- und Netzwerkmanagement kommt hier eine besondere Bedeutung zu. Vor einem Jahr haben wir uns aufgrund der positiven Referenzen von Partnerhochschulen dazu entschlossen, uns am Österreichischen Wissenschaftsnetz ACOnet zu beteiligen. Das bringt sowohl für MitarbeiterInnen als auch für Studierende unserer Fachhochschule Vorteile.

Vielfältige Möglichkeiten

Die Teilnahme an ACOnet erlaubt es, sowohl an der FH Campus Wien als auch bei anderen teilnehmenden Organisationen Internet komplikationslos via W-LAN (**eduroam**) nutzen zu können. Auch der Bestellvorgang für **u:books**, also Notebooks, die zu speziellen Konditionen für Studierende, MitarbeiterInnen und Organisationseinheiten von österreichischen Universitäten und Fachhochschulen angeboten werden, vereinfacht sich durch ACOnet. Weiters stehen der FH Campus Wien durch die Mitgliedschaft kostenfreie SSL-Zertifikate in jeder gewünschten Menge zur Verfügung. Das reduziert unseren Verwaltungsaufwand deutlich und trägt zu einer Kostenersparnis bei.

FH Campus Wien

Die FH Campus Wien ist mit ihren vier Standorten Wien-Favoriten, Campus Vienna Biocenter, Muthgasse – BOKU, Schloss Laudon – Oktogon und den drei Kooperationsstandorten der Vinzenz-Gruppe Wien, Linz und Ried eine der größten Fachhochschulen Österreichs. Ab Herbst 2015 gibt es in Kooperation mit dem Wiener Krankenanstaltenverbund (KAV) zwei weitere FH-Studienstandorte am SMZ Süd und SMZ Ost. Im laufenden Studienjahr 2014/15 bildet die FH Campus Wien rund 5.000 Studierende in über 50 Bachelor- und Masterstudiengängen sowie Lehrgängen in den Departments Applied Life Sciences, Bauen und Gestalten, Gesundheit, Public Sector, Soziales und Technik aus. Sie kooperiert mit den österreichischen Universitäten Uni Wien, MedUni Wien, BOKU, VetMed, TU Wien, MU Leoben, Uni Innsbruck und zahlreichen internationalen Hochschulen. Die FH Campus Wien ist mit Unternehmen, Verbänden, Schulen und öffentlichen Einrichtungen vernetzt. Darüber hinaus unterhält die Hochschule eigene Forschungsgesellschaften, über die zahlreiche F&E-Projekte der Studiengänge und externe Auftragsforschung abgewickelt werden.

Horst Schönkirsch
FH Campus Wien
Leiter IT-Services
horst.schoenkirsch@fh-campuswien.ac.at

Notfallübungen beim Land Oberösterreich

Die Abteilung IT beim Amt der OÖ Landesregierung ist der IT-Dienstleister für sämtliche Dienststellen des Landes und betreibt dafür eine umfassende Infrastruktur an Hard- und Softwarekomponenten. Die Server sind zentral in Linz in einem Rechenzentrum mit mehreren Systemräumen situiert, als Backup steht ein weiterer gemieteter Systemraum in einem Fremdrechenzentrum zur Verfügung. **Alle wichtigen Dienste sind redundant mit gegenseitigem Abgleich auf die beiden Standorte verteilt und netzwerkseitig ausfallsicher angebunden**, sie werden im Fehlerfall beinahe ausnahmslos automatisch auf den verfügbaren Standort umgeschaltet.

Um die Brauchbarkeit und Funktionalität der Konzepte zur Betriebssicherheit bzw. für einen etwaigen Katastrophenfall zu überprüfen, führt die Abteilung IT seit 2009 jährlich einen Notfalltest durch. Die angenommenen Szenarien reichen von einem Stromausfall in einem Rechenzentrum über einen lokalen Brand bis zu einer notwendigen Evakuierung wegen eines Bombenalarms. Bei diesen Übungen werden organisatorische und technische Abläufe in einer realen Situation (z.B. nur mit eingeschränkter IT-Mannschaft) auf Tauglichkeit überprüft.

Die Ergebnisse der Notfallübungen aus den letzten Jahren haben eindeutig gezeigt, dass Papierkonzepte für einen sicheren Betrieb nicht ausreichend sind. In der Praxis treten meist Probleme auf, mit denen nicht gerechnet wurde (Murphys Gesetz) oder die außerhalb des Einflussbereichs der IT liegen, oftmals sind sie nicht technischer sondern organisatorischer Art. Diese Probleme treten nur bei einem „echten" Ausfalltest auf, wo sie erkannt und anschließend beseitigt werden können.

Die **Notfallübung 2014 fand am Samstag, 14. Juni statt** und hatte zwei verschiedene Übungsannahmen bzw. –ziele. Der Hauptteil der Übung umfasste den angenommenen Ausfall des Hauptrechenzentrums, der durch eine komplette Stromabschaltung des Gebäudes simuliert wurde. Das Ziel war die Überprüfung der installierten Redundanzkonzepte, das heißt die (automatische) Übernahme aller IT-Dienstleistungen durch das Ausfallrechenzentrum.

Der andere Teil der Übung (der vorher durchgeführt wurde) ging vom Szenario eines Ausfalls des öffentlichen Internet aus (z.B. absichtliche Abschaltung wegen einer DoS-Attacke). Da das Land Oberösterreich von Beginn an Teilnehmer des GovIX (Government Internet Exchange) ist, der eine komplementäre und vom Internet (weitestgehend) unabhängige Netzwerkinfrastruktur für die öffentliche Verwaltung in Österreich darstellen soll, war es Ziel des Tests, dieses Konzept in der Praxis zu prüfen.

Die Vorbereitung der Übung umfasste die Erstel-

lung eines detaillierten Testplans, die Vorinformation der betroffenen ISPs und die Ankündigung der Abschaltung auf der Homepage des Landes und in den Medien. Der schwierigste Teil war die Erhebung der zu testenden Applikationen und Funktionen. Vereinzelt sind externe Anwendungen unserer User der IT nicht bekannt bzw. viele Applikationen konnten bezüglich ihrer Relevanz für den Betrieb durch die IT nur schwer eingeschätzt werden. Schließlich wurden die auszuführenden Tests Personen zugewiesen, die die Ergebnisse protokollieren mussten.

Der eigentliche Test wurde nach einer kurzen Anfangsbesprechung um 7:05 Uhr gestartet. Der gesamte Testplan (Applikationen und Funktionen) wurde mit aktiviertem Internet durchgeführt, um den aktuellen „Normalbetrieb" festzuhalten. Anschließend wurden alle Zugänge zum öffentlichen Internet (je 2 ISPs an jedem Standort) deaktiviert, sämtliche DNS Server und Portale neu gestartet sowie alle Proxy-Caches gelöscht. Ab diesem Zeitpunkt war nur mehr Kommunikation über GovIX möglich und es standen die darüber erreichbaren Services (z.B. DNS) zur Verfügung.

Der Testplan wurde erneut durchgeführt und die auftretenden Mängel wurden protokolliert. Nach der Reaktivierung der Internet-Zugänge erfolgte die Sammlung und Auswertung der Ergebnisse. Es zeigte sich – wie erwartet – dass DNS die Basis aller Dienste ist und sich Probleme mit DNS gravierend auf die Funktionalität und Performance auswirken. Lokale Redundanzkonzepte wie z.B. mehrere konfigurierte DNS Resolver auf den Clients erweisen sich in der Praxis als nicht brauchbar, weil Timeouts bei DNS Abfragen (durch nicht erreichbare Server) zu einer unbefriedigenden Erfahrung beim User führen. Als Verbesserung wurde mittlerweile beim Land Oberösterreich ein DNS Anycast Service installiert.

Bei einigen über GovIX erreichbaren Kommunikationspartnern haben sich ebenfalls verschiedene DNS-Probleme ergeben. In Applikationen und Funktionen werden Domains verwendet, die nicht über GovIX erreichbar sind bzw. deren DNS Server sich im Internet befinden. Es gibt sogar GovIX-Teilnehmer, deren DNS Server nicht über GovIX erreichbar sind. Ein weiteres jedoch bereits vorher bekanntes Problem sind jene Betreiber oder auch Benutzer von kritischen Applikationen und Funktionen, die nicht GovIX-Teilnehmer sind. Diese Situation kann nur durch deren Teilnahme an der GovIX-Infrastruktur bereinigt werden.

Günther Schmittner
Amt der OÖ Landesregierung
Abteilung IT

Projekt u:core

Das neue Core-Netzwerk der Universität Wien

Der Backbone des Datennetzwerks der Universität Wien ist durch laufendes Wachstum und neue Anforderungen in den letzten Jahren an seine Grenzen gestoßen. Das bestehende Netzwerk wurde als flache Layer 2 STP[1] Infrastruktur mit ca. 800 beteiligten Geräten betrieben und konnte nicht mehr die benötigte Stabilität und Skalierbarkeit bereitstellen.

Daher wurde **Ende 2013** das **Projekt u:core** gestartet. Projektziele waren unter Anderem eine Modernisierung der Core-Router auf aktuelle Technologien und die Einführung von 40Gbit Verbindungen sowie eine Vereinfachung des SPT-Aufbaus.

Im Zuge der Konzeptions- und Testphasen ist die Entscheidung für eine klare Trennung des Access-Bereiches von der Routing-Infrastruktur gefallen.
Im Bereich der lokalen Verteiler wurden keine Änderungen geplant - die Router sollten auf MPLS[2] umgestellt werden. Als Transportprotokoll für die Layer 2 Netzwerke über den Backbone wurde VPLS[3] mit BGP[4] Autodiscovery gewählt.
Durch diese Kombination wird die **Netzwerkprovisionierung im Backbone weitgehend automatisiert.**

Dieses Konzept wurde im April 2014 im CPOC[5] Labor London mit Unterstützung der Partner Kapsch BusinessCom und Cisco Systems auf der geplanten Hardware Cisco Catalyst 6500 und Cisco ASR 9006 einer einwöchigen Testserie unterzogen.

Die Ergebnisse haben das grundsätzliche Konzept bestätigt und viele Erkenntnisse für die Detailplanung geliefert.
Bei Leistung und Skalierbarkeit der VPLS Verbindungen für ca. 600 VLANs[6] und voller Verkehrslast konnte insbesondere die ASR Plattform mit **hoher Stabilität und sehr schnellen Redundanz-Umschaltzeiten** überzeugen.

Im August 2014 wurde ein Parallelaufbau der beiden zentralen ASR 9006 durchgeführt, die ersten beiden 40Gbit Verbindungen in Betrieb genommen und mit dem bestehenden Produktiv-Netzwerk verschalten. Als temporäre Verbindungstechnologie dafür wurde ICCP-SM[7] gewählt.
Vor dem Beginn des Wintersemesters 2014 wurden die Internet Uplinks zum **ACOnet** umgestellt und zwei große Rechenzentren in die neue Infrastruktur migriert. Einige Software Fehler und ein daraus resultierender Ausfall wurden durch das hervorragende Projektteam mit Unterstützung von KBC rasch behoben.

Im Laufe des Wintersemesters wurde der Rollout an allen großen Standorten der Universität Wien durchgeführt und die lokalen Catalyst 6500 und 6800 auf VPLS PE Router umgestellt.

Das Projekt u:core wurde im Zeitplan mit **Ende 2014 erfolgreich abgeschlossen**. Es wurde damit die Grundlage für die langfristige Funktionsfähigkeit des Datennetzwerks der Universität Wien und zukünftige Erweiterungen geschaffen.

Auch für die Services von **ACOnet** und **nic.at**, die in den Rechenzentren der Universität Wien angesiedelt sind, bedeutet die neue Infrastruktur **höhere Stabilität und Ausfallssicherheit**.

universität wien

zentraler informatik dienst

[1] Spanning Tree Protocol
[2] Multi Protocol Label Switching
[3] Virtual Private LAN Service
[4] Border Gateway Protocol
[5] Cisco Customer Proof of Concept
[6] Virtual Local Area Network
[7] Interchassis Communication Protocol - Service Multihoming

Daniel Schirmer
Teamleiter Network Services
Zentraler Informatikdienst der Universität Wien

u:cloud

Cloudspeicher für Angestellte der Universität Wien

Kommerzielle Cloudanbieter werden an der Universität Wien sehr häufig verwendet, weil sie eine einfache Möglichkeit bieten Daten abzuspeichern und von überall abzurufen. Diese haben jedoch den großen Nachteil, dass die Benutzerin oder der Benutzer nicht weiß, wo ihre/seine Daten physisch abgelegt wurden. Deswegen war das Ziel eine cloudbasierte Speicherlösung, die den Anforderungen der Universität Wien in Bezug auf Usability und Sicherheit der Daten gerecht werden, anzubieten.

Nach eingehenden Tests fiel die Entscheidung auf die an Popularität stetig wachsende Open-Source-Software **„ownCloud“**, welche bereits von zahlreichen Wissenschaftsnetzen (z.B. das niederländische SURFnet, schweizer SWITCH) und Universitäten in Europa (z.B. TU Berlin, ETH Zürich) erfolgreich eingesetzt wird. Der große Vorteil dieser Software ist die Speicherung der persönlichen Daten auf geschützten Servern der Universität Wien. Ein weiterer Grund war die Möglichkeit, ownCloud in der Enterprise-Variante im Corporate Design der Universität Wien zu gestalten. Hierbei konnte über ACOnet ein besonders günstiges Lizenz-Angebot von ownCloud an die Wissenschaftsnetz-Community genutzt werden (ownCloud/TERENA Rahmenvereinbarung).

Die Möglichkeiten in die u:cloud zu gelangen sind breit angelegt. Man kann sich mit Hilfe von Programmen am PC und auf mobilen Endgeräten verbinden. Daten können über die Weboberfläche mit anderen Personen geteilt werden.
Die Testphase der u:cloud an der Universität Wien erstreckte sich über 9 Monate. Forschungsgruppen aus den verschiedensten Bereichen, wie etwa Physik, Astronomie oder Mathematik, waren mit eingebunden. Eines der langfristigen Ziele war es, Forscherinnen und Forscher das kollaborative Arbeiten zu ermöglichen.

Zur Bewusstseinsbildung der u:cloud-Anwenderinnen und Anwender wird die Thematik „Datenschutz in der Cloud“ zusätzlich in die Schulungen der IT-Security mitaufgenommen.

Christian Kracher
Projectmanagement
ZID Universität Wien

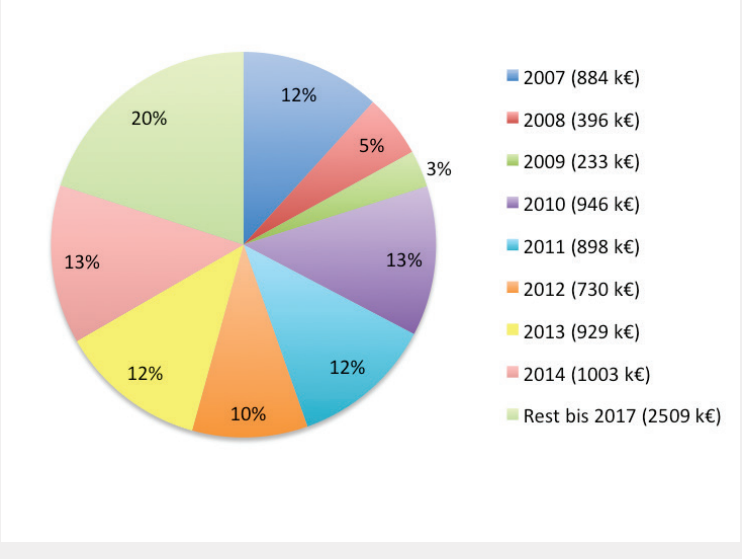
Anhang

Zahlen, Daten & Fakten

ACOnet Teilnehmer gesamt		**204**
• Akademische Organisationen		49
• Universitäten	30	
• Fachhochschulen	12	
• Sonstige Bildungseinrichtungen	7	
• Forschungseinrichtungen		28
• Kulturorganisationen		12
• Gesundheitsinstitutionen		5
• Einrichtungen der öffentlichen Verwaltung		23
• Regionale EDUnet Teilnehmer		9
• Studierendenheimträger		53
• Studierendenheime	131	
• Sonstige		25
davon		
• ACONET Vereinsmitglieder		35
• GovIX Teilnehmer		19

Backbone-Standorte	20
Glasfaser in km	4500

Abb: Investition 2007 und jährliche Investitionsrücklagen



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

Jahresbudget (in tausend Euro)	**2013**		**2014**	
		Summe		Summe
Erlöse aus Leistungsvereinbarungen		5.571 k€		5.619 k€
Ausgaben (in tausend Euro)		4.642 k€		4.616 k€
Personalkosten		661 k€		692 k€
Sachkosten		3.820 k€		3.831 k€
• Backbone & Transit	3.437 k€		3.439 k€	
• HW&SW Wartung & Support	158 k€		188 k€	
• Datacenter Miete	80 k€		79 k€	
• Mitgliedsbeiträge	53 k€		59 k€	
• Reisekosten	31 k€		28 k€	
• Fortbildung	3 k€		2 k€	
• Öffentlichkeitsarbeit	40 k€		26 k€	
• Sonstige Kosten	18 k€		10 k€	
Anlageinvestitionen		82 k€		14 k€
Innerbetriebliche Leistungsverrechnung		79 k€		79 k€
Ergebnis (in tausend Euro)		**929 k€**		**1.003 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€
Differenz zum Zielwert bis Ende 2017	502 k € / Jahr	**- 1.506 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:

- Peter Allgeyer und Günther Sauermoser, Salzburg Research Forschungsgesellschaft m.b.H.
- Christian Kracher, Zentraler Informatikdienst der Universität Wien
- Walter Müller, Leopold-Franzens-Universität Innsbruck & Team
- Simon Rumer, Medizinische Universität Innsbruck & Team
- Daniel Schirmer, Zentraler Informatikdienst der Universität Wien
- Günther Schmittner, Amt der Oberösterreichischen Landesregierung
- Horst Schönkirsch, FH Campus Wien

Fotos:
Universität Wien, VSC3, Leopold-Franzens-Universität Innsbruck, Medizinische Universität Innsbruck, Naturhistorisches Museum Wien, Universalmuseum Joanneum, MAK, Albertina, Amt der oberösterreichischen Landesregierung, MUMOK

Fotoquellen:
Universität Wien, Zentraler Infomatikdienst, Peter Wienerroither, mdw - Universität für Musik und darstellende Kunst Wien mdw/molllom, Leopold-Franzens-Universität Innsbruck, Medizinische Universität Innsbruck, Universalmuseum Joanneum - Foto: Eduardo Martinez, MAK, Ansicht Stubenring - Foto: Gerald Zugmann/MAK, Albertina, Wien - Foto: Harald Eisenberger, Salzburg Research, FH Campus Wien: APA-Fotoservice/Schedl, freeimages.com/DaVinciS, freeimages.com/svilen001, MuseumsQuartier Wien: Gian Marco Castelberg

Gestaltung: Christine Dworak
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
F +43-1-4277-14338

universität wien