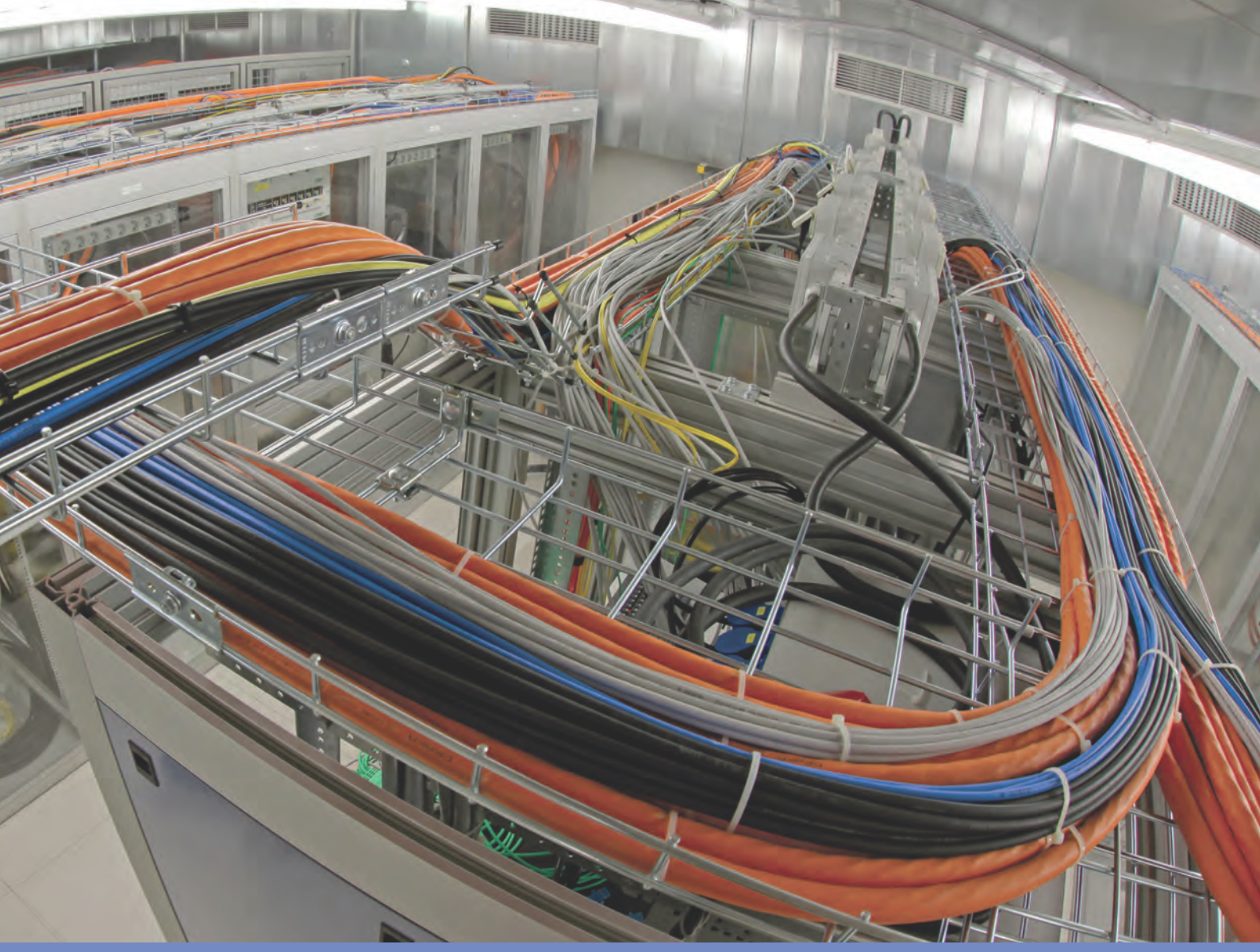


aconet

Austrian Academic Computer Network

2018

JAHRESBERICHT

ACOnet Jahresbericht

2018

www.aco.net | www.vix.at

Inhalt

Vorwort

Liebe Leserin, lieber Leser!

Verglichen mit dem für ACOnet äußerst ereignisreichen Jahr 2017 stand 2018 vor allem im Zeichen diverser Konsolidierungen. Beispielsweise wurden im ACOnet-Backbone mehrere Erweiterungen vorgenommen, um die Vorteile des neuen Trägernetzes auch ausnutzen zu können (siehe Seite 19). Ein zusätzlicher Mehrwert für unsere Teilnehmerorganisationen ergibt sich durch die Umstellung unseres „Class of Service"-Konzepts: Seit November 2018 fällt auch der gesamte VIX-Traffic unter den unlimitierten „akademischen" Datenverkehr (mehr dazu ab Seite 22).

DSGVO & NIS-Richtlinie

Die im Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (DSGVO) hat bekanntlich sehr weitreichende Auswirkungen. Was sich durch die DSGVO im ACOnet-Kontext verändert hat, erfahren Sie ab Seite 28.

Worauf wir schon länger vorbereitet sind und was sich ebenfalls 2018 manifestiert hat: Im Rahmen der nationalen Umsetzung der EU-weiten „Network Information Security"-Richtlinie (NIS-Richtlinie) wird der Vienna Internet eXchange (VIX) als wesentlicher Dienst definiert. Die Universität Wien als „rechtspersönlicher" Betreiber des VIX widmet sich nun intensiv der Dokumentation der gesamten sicherheitsrelevanten Abläufe. Außerdem werden zusätzliche Maßnahmen gesetzt, um bereits bestehende Prozesse zu standardisieren und zu optimieren. Wir orientieren uns bei der Standardisierung unseres Information Security Managements am ISO-27001-Standard, um eine künftige Zertifizierung zu erleichtern. Dies stellt sicher, dass die dabei gewonnenen Erfahrungen in einem zweiten Schritt auch ACOnet zugute kommen werden.

EOSC & PRACE

Besonders hingewiesen sei auf zwei internationale Initiativen, die gänzlich neue Möglichkeiten für die Wissenschafts-Community mit sich bringen: Die European Open Science Cloud (EOSC), die im November 2018 offiziell gestartet wurde, soll künftig dafür sorgen, dass Forschungsdaten aus EU-geförderten Projekten frei nutzbar sind (siehe Seite 31). Das Supercomputing-Netzwerk PRACE vermittelt europäischen WissenschaftlerInnen Zugang zu mehreren Höchstleistungsrechnern für die Durchführung ihrer Forschungen (siehe Seite 34). Beide Services stehen auch für ACOnet-Teilnehmerorganisationen zur Verfügung.

Das Jahr der Jubiläen

2018 waren wieder einige Jahrestage zu feiern: Die drei Jubiläen 30 Jahre Domainendung „.at", 20 Jahre Domain-Registrierungsstelle „nic.at" und Online-Meldestelle „Stopline.at" sowie 10 Jahre „CERT.at" (Computer Emergency Response Team Austria) wurden mit einer gemeinsamen Gala im Marx Palast gewürdigt (siehe Seite 42).

Ebenso beachtlich sind zwei weitere Geburtstage: Das ACOnet-CERT stellt seine Security-Expertise seit mittlerweile 15 Jahren in den Dienst der Community, und das internationale WLAN-Roaming-Service eduroam wurde stolze 10 Jahre alt.

aconet

Austrian Academic Computer Network

Personelles

Auch im vergangenen Jahr waren in unserem Team wieder etliche Veränderungen zu verzeichnen. Abideen Bamgbala hat sich entschieden, sein Dienstverhältnis nicht zu verlängern, sondern ab September 2018 ein Studium im Ausland zu beginnen. Das ACOnet-CERT wiederum hat mit Christoph Campregher seit September 2018 einen äußerst kompetenten neuen Mitarbeiter; dafür hat jedoch Manfred Halper, der ab Dezember 2017 im CERT-Team beschäftigt war, mit Jahresende 2018 in die Privatwirtschaft gewechselt. Wir wünschen unseren beiden scheidenden Kollegen das Beste für ihren weiteren Lebensweg!

Wilfried Wöber erhielt den ersten „Rob Blokzijl Award" der RIPE-Community (© Matthijs Mekking)

Eine sehr seltene – und daher umso erfreulichere – Würdigung soll hier ebenfalls nicht unerwähnt bleiben: Unser Kollege Wilfried Wöber wurde für sein jahrzehntelanges Engagement für die Weiterentwicklung des Internet im Mai 2018 mit dem ersten „Rob Blokzijl Award" der RIPE-Community ausgezeichnet (siehe Foto). Wir gratulieren herzlichst!

Danke

Im vorliegenden Jahresbericht 2018 finden Sie wieder mehrere Beiträge von ACOnet-Teilnehmerorganisationen. Ein großes Dankeschön an alle GastautorInnen!

Wie immer möchte ich mich auch bei meinen MitarbeiterInnen sowie bei der gesamten ACOnet-Community für ihren Einsatz und ihre Kooperationsbereitschaft herzlich bedanken.

Und nun wünsche ich eine interessante Lektüre!

Christian Panigl

Abteilungsleiter ACOnet & VIX

Über ACOnet

Leitbild & Ziele

ACOnet-Leitbild

ACOnet bietet seinen Teilnehmern eine **Kombination aus leistungsfähigem Backbone und zielgruppenorientierten Services**. 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 **nichtkommerzielle, 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, 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 kontinuierlich 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 Teilnehmerorganisationen auch spezifische Anforderungen von **Forschungsprojekten** und Benutzergruppen mit besonders **hohen Qualitätsansprüchen** bedienen zu können.

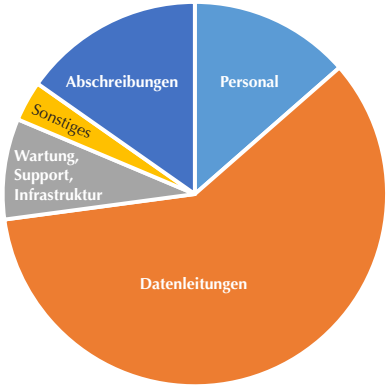
Zahlen, Daten, Fakten

ACOnet-Teilnehmeranschlüsse gesamt (Stand 31. Dezember 2018)	**240**
• Akademische Organisationen (34 Universitäten, 19 Fachhochschulen, 11 sonstige Bildungseinrichtungen)	64
• Studierendenheimträger (mit insgesamt 131 an ACOnet angebundenen Studierendenheimen)	55
• Einrichtungen der öffentlichen Verwaltung	33
• Forschungseinrichtungen	31
• Kulturorganisationen	14
• Regionale EDUnet-Teilnehmer	9
• Gesundheitsinstitutionen	6
• Sonstige	28
davon:	
• **ACONET-Vereinsmitglieder**	**40**
• **GovIX-Teilnehmer**	**32**
Backbone-Standorte	**20**
Glasfaser in km	**3300**

Finanzielle Kennzahlen in Mio. € (Stand 11. März 2019)	**2017**	**2018**
+ Erlöse	**6,0**	**6,2**
– Aufwendungen	**5,8**	**5,9**
• Personal	0,7	0,8
• Datenleitungen	3,4	3,5
• Wartung, Support, Infrastruktur	0,4	0,5
• Sonstiges	0,3	0,2
• Abschreibungen	0,9	0,9
= Ergebnis	**0,2**	**0,3**
• davon Rücklage ACOnet	0,1	0,3
Anlagenanschaffungen	**2,5**	**0,0**

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

Aufwendungen 2018



Unser Team

Das ACOnet-Team ist am Zentralen Informatikdienst der Universität Wien angesiedelt.

Panigl	Christian	Abteilungsleiter

ACOnet & Vienna Internet eXchange (VIX)

Michl	Harald	Teamleiter, Betriebskoordination, Netzwerk-Betrieb
Bamgbala	Abideen	Netzwerk-Betrieb (bis 31. August)
Bauer	Kurt	Identity Federation, Zertifikatsservice, Netzwerk- und Server-Betrieb
Cravos	Romana	Projektmanagement, Eventmanagement (Peering Days)
Genser	Christoph	Webentwicklung, Öffentlichkeitsarbeit

v. l. n. r. : Christian Panigl | Abideen Bamgbala | Peter Schober | Wilfried Wöber | Elisabeth Zoppoth | Kurt Bauer | Monika Schneider

Perzi	Michael	LIR, Teilnehmeradministration, Netzwerk- und Server-Betrieb
Radulescu	Liviu-Radu	Softwareentwicklung
Rennert	Erwin	Netzwerk-Betrieb
Schneider	Monika	Netzwerk-Betrieb
Schober	Peter	Identity Federation, Server-Betrieb
Stadlmann	Tina	Administratives, Veranstaltungen
Wein	Robert	Monitoring, Netzwerk- und Server-Betrieb

Freie Mitarbeiterinnen und Mitarbeiter:

Kreil	Renate	Kunst- und Kulturkommunikation
Wöber	Wilfried	Security, Training, Consulting
Zoppoth	Elisabeth	Webredaktion, Öffentlichkeitsarbeit

Tina Stadlmann | Liviu Radulescu | Erwin Rennert | Romana Cravos | Robert Wein | Harald Michl | Michael Perzi | Christoph Genser

ACOnet-CERT

Alexander Talos-Zens

Christoph Campregher

Manfred Halper

Markus Raditsch

Das Team der Internet Domain Administration
Ansprechpartner für ACOnet-Teilnehmer: Teamleiter Gerhard Winkler (4. von rechts) und Arsen Stasic (3. von rechts)

Computer Emergency Response Team (CERT)

Talos-Zens	Alexander	Teamleiter
Campregher	Christoph	CERT-Betrieb (ab 1. September)
Halper	Manfred	CERT-Betrieb (bis 31. Dezember)
Raditsch	Markus	CERT-Betrieb

Internet Domain Administration

Winkler	Gerhard	Teamleiter
Adam	Achim	Software- und Systementwicklung
Dorner	Clemens	Software-Qualitätssicherung
Englisch	Holger	.ac.at-Domains, Kundensupport
Grünauer	Marcel	Software- und Systementwicklung
Heimhilcher	Markus	DNS-Administration
Hofstetter	Mark	Software- und Systementwicklung
Hörtnagl	Christian	Systemadministration
Papst	Andreas	Projektmanagement
Reicher	Markus	Monitoring und Datenvisualisierung
Reutner-Fischer	Bernhard	Software- und Systementwicklung
Schmidt	David	Software- und Systementwicklung
Stasic	Arsen	ACOnet-Services, GovIX

Netzwerk

ACOnet Standortporträt

Montanuniversität Leoben

Die Montanuniversität Leoben (MUL) ist die kleinste technische Universität Österreichs und genießt aufgrund ihrer einzigartigen Ausrichtung auf Berg- und Hüttenwesen weltweit einen hervorragenden Ruf. Zusammen mit der TU Wien und der TU Graz bildet sie den Verbund der Austrian Universities of Technology (TU Austria). Die MUL ist ACOnet-Teilnehmer der ersten Stunde: Sie ist seit 1990 an ACOnet angebunden.

Seit der Gründung 1840 als „Steiermärkisch-Ständische Montanlehranstalt" durch Erzherzog Johann hat sich das Studien- und Forschungsprofil der Montanuniversität Leoben permanent weiterentwickelt und deckt die gesamte Wertschöpfungskette von der Rohstoffgewinnung bis zur Entsorgung ab. Die „Alma Mater Leobiensis" trägt heute viel zum Erfolg des Wirtschaftsstandortes Steiermark bei.

Derzeit lernen und forschen knapp 4000 Studierende an der Montanuniversität. Der Frauenanteil beträgt 28 %. Viele der angebotenen Studienrichtungen können in dieser Form nur in Leoben belegt werden – mit dem Erfolg, dass die Absolventinnen und Absolventen der MUL zu den begehrtesten Akademikern zählen. Die internationale Bedeutung zeigt der hohe Anteil von 17 % an internationalen Studierenden; diese kommen aus rund 80 verschiedenen Nationen.

Als kleinste technische Universität Österreichs bietet die Montanuniversität ihren Studierenden eine hervorragende Ausstattung und optimale Betreuung durch die Lehrenden. Ihr Vorteil ist die überschaubare Größe: Der intensive Kontakt zwischen Studierenden und Lehrenden ermöglicht es, Herausforderungen im Studienalltag schnell zu lösen. „Massenuniversität" ist in Leoben ein Fremdwort.

Leoben 1 / Leoben 2

Die MUL wurde bereits 1990 an den ersten X.25-Backbone von ACOnet angebunden und betreibt heute zwei ACOnet-Anschlusspunkte (Points

Montanuniversität Leoben
Hörsaalgebäude „Erzherzog-Johann-Trakt"
(© ZID/NOC)

of Presence – PoPs). Der PoP „Leoben1“ befindet sich im zentralen Netzwerk-Verteilerraum des historischen Hauptgebäudes in der Franz-Josef-Straße. Der PoP „Leoben2“ ist im Backup-Serverraum des RWZ (Rohstoff- und Werkstoffzentrum) im Stadtzentrum angesiedelt. Die beiden PoPs sind redundant an die Technische Universität Graz bzw. die Karl-Franzens-Universität Graz angebunden. Die 20 Gebäude des MUL-Campus sind über den zentralen Glasfaser-Backbone mit 10 Gbit/s, wegeredundant und hoch verfügbar, verbunden.

Flächendeckendes WLAN und „eduroam“ am gesamten Campus sind für eine moderne Universität eine Grundvoraussetzung, wie auch VPN-Zugänge für alle Universitätsangehörigen. Für Gäste und für Wartungszugänge stehen separate Gastticket-Systeme und VPN-Verbindungen zur Verfügung.

Montanuniversität Leoben
– oben: Impulszentrum für Werkstoffe
– unten: Hauptgebäude
(© ZID/NOC)

Network Operations Center (NOC)

Die Aufgabenbereiche des NOC der Montanuniversität Leoben sind vielfältig. Sie umfassen den grundlegenden Aufbau, Betrieb und Wartung der Netzwerk-Infrastruktur, ein zweistufiges Firewallkonzept, Firewalls für Organisationseinheiten, IP- und Video-Telefonie, Collaboration, Monitoring sowie den technischen Betrieb der Info-Screen-Systeme.

Die dafür nötige Server-Infrastruktur (DHCP, DNS, Communication und Collaboration, Monitoring) in Form von physischen und virtuellen Servern wurde durch das NOC selbst aufgebaut. Der Betrieb und die Wartung der Hard- und Software wird ebenfalls vom NOC übernommen.

Das in Zusammenarbeit mit einem Industriepartner vom NOC entwickelte, mandantenfähige Domain- und IP-Adressen-Management „IPAM“ wie auch das Netzwerk-Tool „RIF“ (eine Datenbank-Eigenentwicklung zur Verwaltung von Netzwerkdosen, Räumen, Switches und deren Konfiguration im

Das NOC-Team der Montanuniversität Leoben (© ZID/NOC)

Rahmen des universitären Informations- und Managementsystems „MU-Online“) ermöglichen dem NOC in Zusammenarbeit mit den IT-AdministratorInnen der universitären Organisationseinheiten ein effizientes Management des Netzwerks.

Zum Kundenkreis zählen neben den Organisationseinheiten der MUL (Zentrale Dienste, Institute, Lehrstühle) auch mehrere Studierendenheime und AbsolventInnenvereine, Kompetenzzentren wie das MCL (Materials Center Leoben) und PCCL (Polymer Competence Center Leoben) sowie das LZL (Laserzentrum Leoben) der Joanneum Research.

Die SFG (Steirische Wirtschaftsförderungs GmbH), die ÖAW (Österreichische Akademie der Wissenschaften), das ÖGI (Österreichisches Gießerei-Institut), die TU Austria, mehrere Christian-Doppler-Labore und das ZAT (Zentrum für Angewandte Technologie) sind weitere Kunden, die über Glasfaser am NOC-Backbone angeschlossen sind. Auch die Stadtgemeinde Leoben ist über eine redundante LWL-Anbindung am Standort des PoP „Leoben 2“ mit dem ACOnet verbunden.

Die Außenstelle des Instituts für Geophysik (in Gams bei Frohnleiten) bildet sowohl für Netzwerk als auch Telefonie über einen VPN-Tunnel einen Teil des Netzwerks der MUL.

NOC und ACOnet

Der hochverfügbare und performante ACOnet-Backbone in Verbindung mit einer redundanten Anbindung erlauben es dem NOC, seinen Kunden eine schnelle und sichere Internetanbindung mit höchstem Service-Level zur Verfügung zu stellen.

Während sich von den ACOnet-Services bei den Universitätsangehörigen besonders eduroam großer Beliebtheit erfreut, schätzen die ServeradministratorInnen das Trusted Certificate Service, um schnell und unkompliziert qualitativ hochwertige SSL-Zertifikate zu beziehen. Die aktiven externen Netzwerk-Scans durch das ACOnet-CERT zeigen mögliche Sicherheitslücken in der eigenen IT-Sicherheitsstruktur auf und erlauben es der IT-Security, sowohl auf NOC-Ebene als auch auf Ebene der Organisationseinheiten präventiv Maßnahmen zu ergreifen.

Nicht zuletzt bilden die von ACOnet organisierten Workshops und die ACOnet-Community aufgrund ähnlich gelagerter Problemstellungen bzw. Lösungen einen hochgeschätzten Wissenspool.

Durch den „direkten Draht“ und persönlichen Kontakt zum ACOnet-Team lassen sich Aufgaben, Komplikationen und unmittelbare Bedrohungen schnell und effektiv lösen. Das Wissen des Teams um die besonderen Anforderungen eines Wissenschaftsnetzes sind dabei ein unschätzbarer Vorteil gegenüber jedem anderen Provider.

Josef Zechner

Montanuniversität Leoben
ZID / Netzwerkabteilung (NOC)
zechner@unileoben.ac.at

Neue Wege im ACOnet-Backbone

Im Jahr 2017 lag unser Fokus auf der Erneuerung der Netzwerkkomponenten im ACOnet. Nachdem dies erfolgreich abgeschlossen war, ging es 2018 darum, die Vorteile der neuen Backbone-Topologie auch auszunutzen. Das konnte durch mehrere Direktverbindungen zwischen Standorten und durch die Kapazitätserweiterung einiger Strecken erreicht werden.

ACOnet als Betreiber einer gemeinsamen Netzwerk-Infrastruktur für Wissenschaft, Forschung, Bildung und Kultur will nicht nur bestmögliche Connectivity bereitstellen, sondern auch die Kooperation der Teilnehmer untereinander unterstützen. In den letzten Jahren stiegen sowohl die Datenraten als auch die übertragenen Volumina enorm an. Damit gehen höhere Anforderungen an das darunterliegende Netz einher.

Die Vorgeschichte

Das nationale Backbone-Netzwerk von ACOnet wurde 2007 auf eine von der A1 Telekom Austria AG (A1TA) **eigens errichtete, gemietete Glasfaser-Infrastruktur** umgestellt. Nach einer zehnjährigen Mindestvertragsdauer hatten wir ab 2017 die Möglichkeit, Adaptierungen im Netz vorzunehmen. Die Ziele dabei waren die Vereinheitlichung der eingesetzten Technologien, die Erneuerung des optischen Equipments sowie eine Senkung der monatlichen Betriebskosten.

Erreicht wurde dies durch eine fünfjährige Verlängerung des Vertrags mit der A1TA, verbunden mit einer Topologie-Anpassung und -Erweiterung sowie einem Tausch aller Routerkomponenten. Ersteres führte unter anderem zu **drei neuen Backbone-Standorten** (Bregenz, St. Johann im Pongau und Wiener Neustadt), letzteres zum **Umstieg auf eine neue Gerätegeneration eines neuen Herstellers**. Im Laufe des Jahres 2017 konnte all das erfolgreich umgesetzt werden – im laufenden Betrieb und ohne nennenswerte Ausfälle.

Näheres dazu ist im ACOnet Jahresbericht 2017 ab Seite 16 zu finden (**www.aco.net/jahresberichte**).

Leitmotive

Bei der letzten großen Umstellung im Jahr 2007 lag das Hauptaugenmerk noch auf der Erhöhung der Ausfallsicherheit durch neue Anschlusspunkte – und der damit verbundenen Möglichkeit, dass ACOnet-Teilnehmer auch in den Bundesländern redundante Anschlüsse an die Infrastruktur zu vertretbaren Kosten realisieren können.

Im Jahr 2018 war die Zielsetzung, die Vorteile, die sich aus der neuen physikalischen Infrastruktur ergeben, für die Teilnehmer nutzbar zu machen. Neben der prinzipiellen Verfügbarkeit ist mittlerweile auch die Laufzeit der Datenpakete ein wichtiger Parameter für das Ausspielen der vollen Leistungsfähigkeit vieler Applikationen. So ist oftmals die Übertragungsrate pro Sekunde indirekt proportional zur Laufzeit.

Kurze Verbindungen

Welche Vorteile die neue Topologie in dieser Hinsicht bieten kann, wird an einem Beispiel deutlich: In der alten Topologie wurden alle Datenpakete, die zwischen Innsbruck und Salzburg über-

tragen wurden, in beiden Richtungen über Wien geschickt. Die Laufzeit – dargestellt im sogenannten „Round Trip Delay" – lag in der alten Topologie bei ca. 15 Millisekunden. Durch die neue Direktverbindung zwischen Salzburg und Innsbruck konnte diese Laufzeit auf ca. 3 Millisekunden reduziert werden – also auf ein Fünftel!

Neben der Strecke Innsbruck – Salzburg wurden auch „Abkürzungen" zwischen Innsbruck und Klagenfurt, Klagenfurt und Graz sowie Linz und Salzburg eingerichtet. Sehr schön sieht man die Erweiterung bei einem Vergleich der physikalischen und der logischen Netzwerk-Topologie (siehe Abbildung unten und auf Seite 21 unten).

Kapazitätserweiterungen

Graz und Linz sind neben Wien traditionell die Standorte mit dem höchsten Bandbreitenbedarf. Aus diesem Grund wurden die Strecken der beiden Linzer und Grazer Standorte nach Wien von 10 Gbit/s auf 20 Gbit/s verdoppelt. Durch diese Maßnahme kann eines der Grundprinzipien der Netzwerk-Infrastruktur von ACOnet – nämlich dass bei Ausfall einer Datenleitung kein Engpass in der Übertragung entstehen soll – auch weiterhin gewährleistet werden.

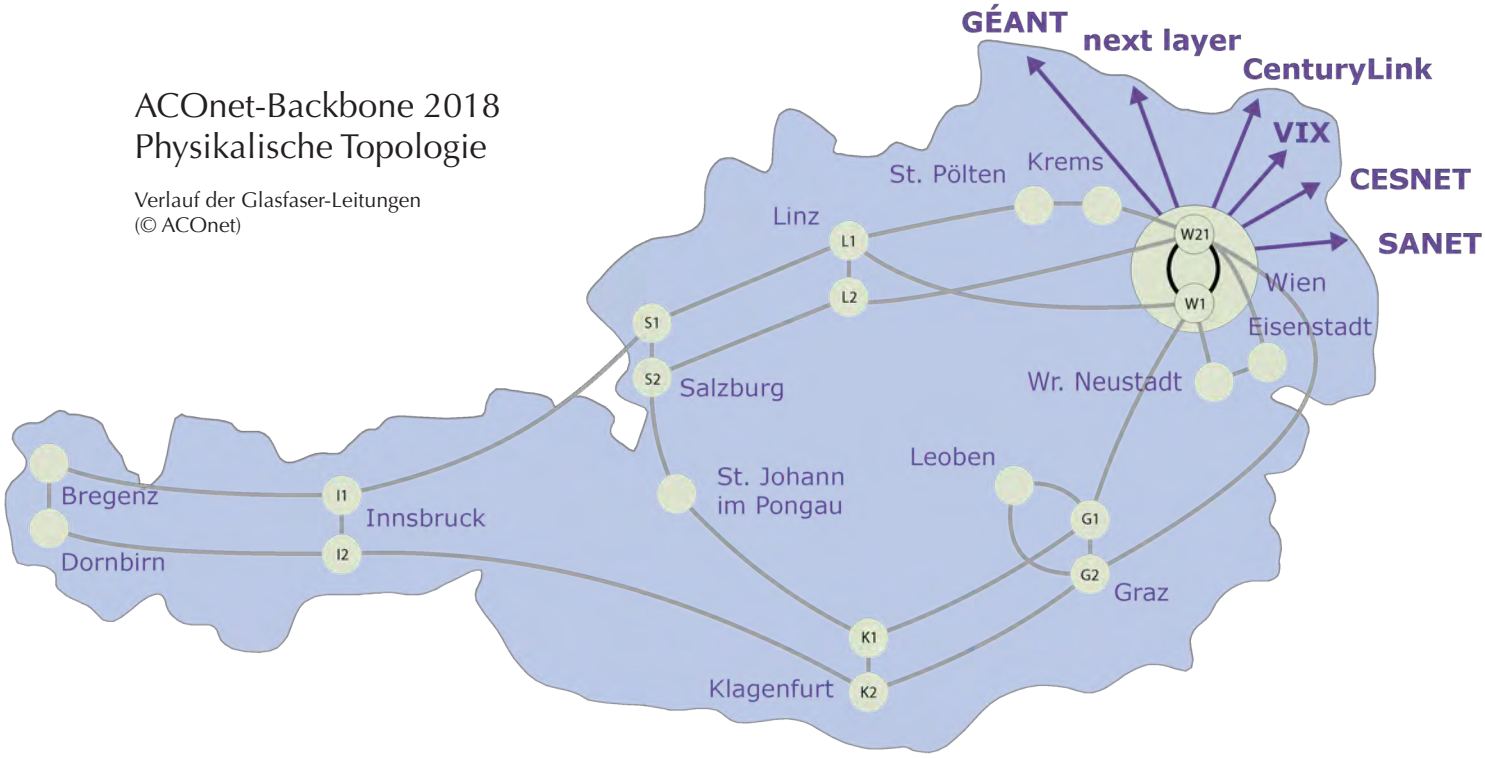
Wir sind überzeugt, mit der aktuellen Topologie und Technologie die besten Voraussetzungen zu haben, um die Anforderungen, die in nächster Zeit auf uns zukommen werden, zu meistern.

Harald Michl

ACOnet
Betriebskoordination

ACOnet-Backbone 2018
Physikalische Topologie

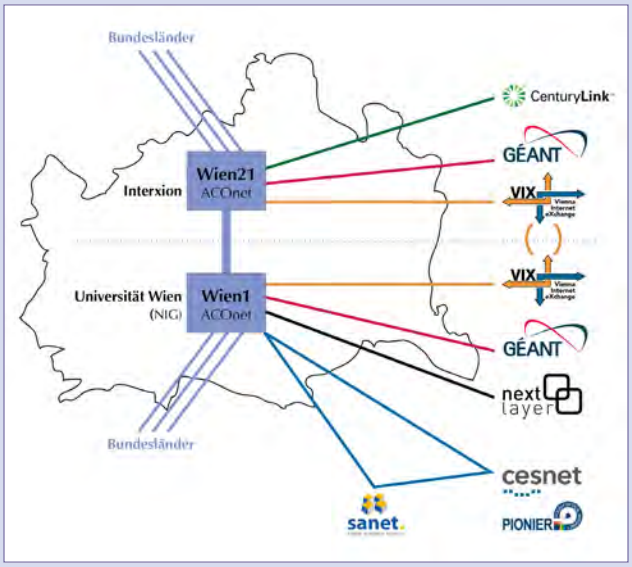
Verlauf der Glasfaser-Leitungen
(© ACOnet)



Uplinks

Bei den internationalen Anbindungen wurde im September ein Upgrade der Anbindung an GÉANT initiiert. Sowohl die Primär- als auch die Backupanbindung sollten hierbei auf 30 Gbit/s ausgebaut werden. Die Erweiterung des Primäranschlusses konnte wie geplant im Oktober 2018 abgeschlossen werden. Für den Upgrade der Backupleitung waren allerdings seitens GÉANT Spezial-Optiken mit weitaus längeren Lieferzeiten notwendig, sodass dieser auf 2019 verschoben werden musste.

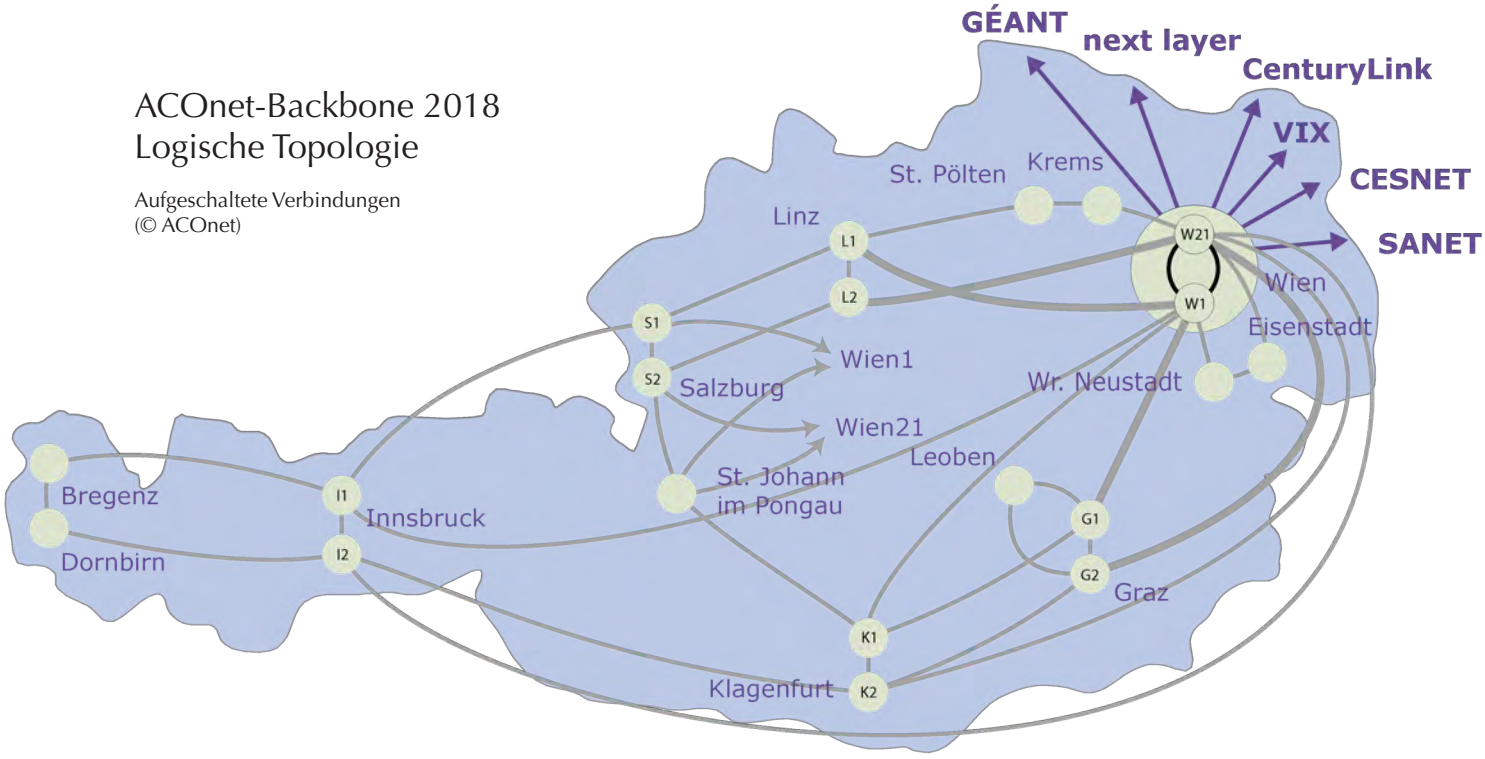
Sobald hier der Upgrade der physischen Bandbreite erfolgt ist, sollen auch die von GÉANT bezogenen Zusatzservices (d. h. das GÉANT Peering Service und die GÉANT Cloud Services), die sich immer größerer Beliebtheit erfreuen, am Backup-Pfad konfiguriert werden.



Internationale Anbindungen von ACOnet in Wien (© ACOnet)

ACOnet-Backbone 2018
Logische Topologie

Aufgeschaltete Verbindungen
(© ACOnet)



ACOnet Class of Service:

VIX-Traffic unlimited

ACOnet nutzt „Class of Service“ (CoS), ein Verfahren zur Markierung von Datenpaketen, um innerhalb seines Backbones den (unlimitierten) akademischen Datenverkehr und den (limitierten) kommerziellen Datenverkehr differenzieren zu können. Seit der Einführung von CoS im ACOnet vor rund 10 Jahren hatte unlimitierter Verkehr innerhalb der Wissenschaft und Forschung stets oberste Priorität. 2018 haben wir unser CoS-Konzept überarbeitet, um der aktuell stark wachsenden Cloud-Nutzung akademischer Institutionen, die zu einem guten Teil über kommerzielle Netze läuft, gerecht zu werden.

CoS im ACOnet, kurz erklärt

Im ACOnet werden zwei Klassen von Datenverkehr unterschieden:

- **Academic** (wissenschaftlicher & lokaler Traffic): Dieser Bereich umfasst im Wesentlichen den Datenaustausch zwischen ACOnet-Teilnehmerorganisationen und mit anderen Wissenschaftsnetzen. Academic Traffic ist – ebenso wie alle Uploads – für ACOnet-Teilnehmer kostenfrei und wird ohne Begrenzung bis zur vollen Kapazität der jeweiligen Zubringerleitung zugestellt, unabhängig von der subskribierten Anschaltbandbreite des Teilnehmers.

- **Commodity**: Als Commodity Traffic wird jener Datenverkehrs-Anteil bezeichnet, der über kommerzielle Upstream Provider ins ACOnet gelangt. Die Zustellung von Commodity Traffic ist limitiert auf die vertraglich subskribierte Bandbreite eines Teilnehmers (die allerdings nach dem Fair-Use-Prinzip temporär um bis zu 1600 % überzogen werden kann).

Um diese beiden Klassen voneinander abgrenzen zu können, werden alle hereinkommenden Datenpakete an den ACOnet-Außengrenzen abhängig vom „Datenlieferanten“ automatisch markiert. Das geschieht mit Hilfe des DSCP-Feldes im IP-Header (DSCP = Differentiated Services Codepoint). An der Schnittstelle zu den Teilnehmern können die Datenpakete dann anhand ihres DSCP-Wertes je nach Herkunft unterschiedlich behandelt werden.

Neue Anforderungen

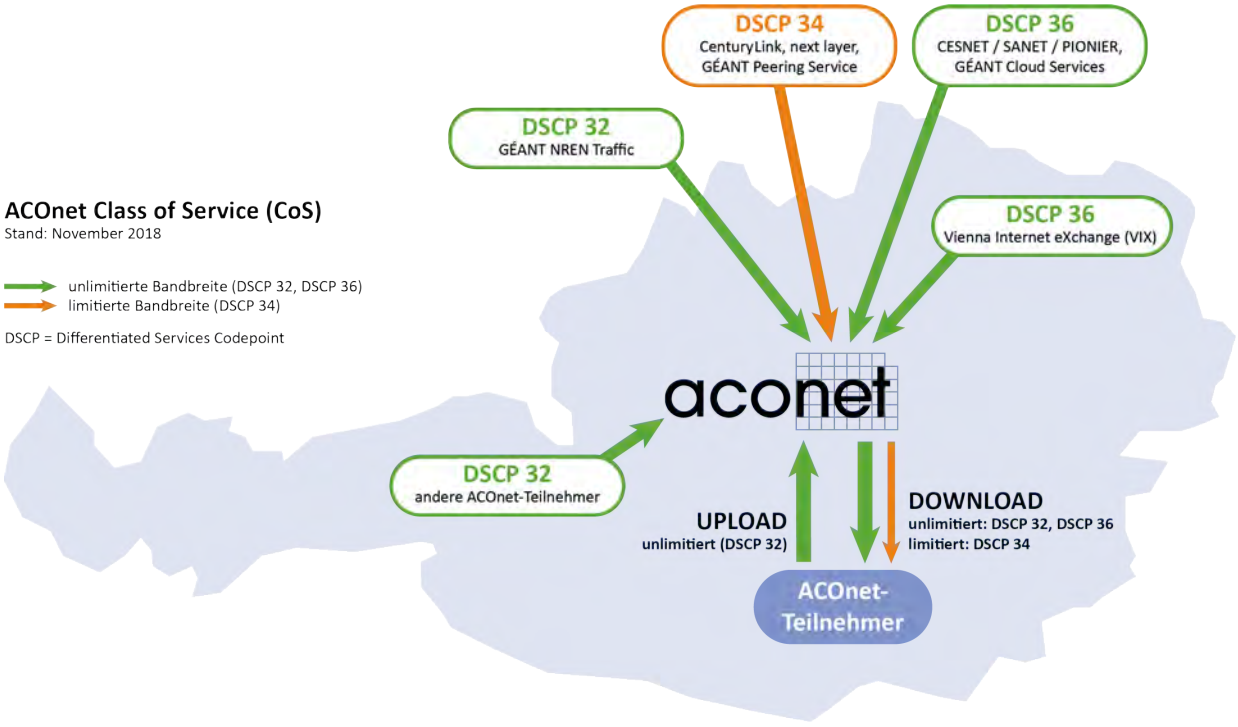
Bisher fielen folgende Datenlieferanten in den Commodity-Bereich:

- CenturyLink
- next layer
- GÉANT Peering Service
- Vienna Internet eXchange (VIX)

Im Laufe des Jahres 2018 wuchs der über den VIX laufende Commodity-Anteil beständig an. Die Ursache: Immer mehr ACOnet-Teilnehmerorganisationen nutzen diverse Cloud-Services, deren Anbieter großteils auch am VIX vertreten sind. Der Verkehrsweg über den VIX ist aufgrund direkter Peerings meist der kürzeste und somit der bevorzugte. Das betrifft auch Cloud-Anbieter aus dem Rahmenvertrag der GÉANT Cloud Services (mehr dazu auf Seite 33). Vor diesem Hintergrund hat der ACOnet-Lenkungsausschuss unserem Vorschlag zugestimmt, auch VIX-Traffic unlimitiert an die Teilnehmer zuzustellen.

Neue Herausforderungen

Die Umsetzung bedurfte allerdings einer grundsätzlichen Änderung des bisherigen CoS-Konzepts. Einer der Hauptgründe dafür liegt in der Gefahr von „Denial of Service“-Attacken (DoS). Ein nicht



unerheblicher Teil des von potenziellen DoS-Attacken verursachten Datenverkehrs würde voraussichtlich über den VIX transportiert werden; daher wäre eine Saturierung der Teilnehmer-Anbindungen möglich, wenn der VIX-Traffic mit demselben DSCP-Wert markiert wäre wie der akademische Datenverkehr.

Neue Lösungen

Aus diesem Grund wurde für Academic Traffic ein zweiter DSCP-Wert implementiert. Diese Markierung wird für alle Datenpakete verwendet, die vom VIX, von den GÉANT Cloud Services oder von unseren bilateralen NREN-Peering-Partnern (CESNET, SANET und PIONIER) einlangen. Die Markierung für den wissenschaftlichen (GÉANT NRENs) und lokalen (ACOnet-Teilnehmer) Datenverkehr blieb unberührt.

Zum Einsatz kommen nun folgende Markierungen mittels DSCP-Werten:

Akademischer/lokaler Verkehr (unlimitiert):

DSCP 32 (binär 100000):
- ACOnet-Teilnehmer
- GÉANT NREN Traffic

DSCP 36 (binär 100100):
- Vienna Internet eXchange (VIX)
- bilaterale NREN-Peerings
- GÉANT Cloud Services

Kommerzieller Verkehr (limitiert):

DSCP 34 (binär 100010):
- CenturyLink
- next layer
- GÉANT Peering Service

Für die mit DSCP 36 markierten Datenpakete wurde ein „Sicherheitsgurt" implementiert, der bewirkt, dass mit solchen Paketen maximal 80 % eines Teilnehmeranschlusses ausgelastet werden können. Dadurch ist es für ACOnet-Teilnehmer auch während einer DoS-Attacke noch möglich, Datenpakete mit anderen Teilnehmern auszutauschen.

Die Implementierung im ACOnet-Backbone wurde Ende Oktober 2018 umgesetzt. Bereits nach kurzer Zeit war bei den Teilnehmern eine Reduzierung des Commodity-Anteils am Datenverkehr feststellbar, die in der Regel zwischen 20 und 40 % lag. Das Ziel, allen ACOnet-Teilnehmern einen Mehrwert zu verschaffen, konnte somit erreicht werden.

Michael Perzi

ACOnet

Services

ACOnet-CERT 2018: Meltdown, Spectre, OpenVAS

Durch die IT-Security-Brille betrachtet, war 2018 ein sehr interessantes Jahr. Abgesehen vom Inkrafttreten der EU-Datenschutz-Grundverordnung (die zwar in den Security-Bereich hineinspielt, in diesem Rückblick aber außer Acht gelassen wird), waren es vor allem zwei außergewöhnliche neue Sicherheitslücken, die die Computer Emergency Response Teams (CERTs) weltweit beschäftigten: Meltdown und Spectre. Das ACOnet-CERT hat darüber hinaus mit OpenVAS ein neues Service in Betrieb genommen und etliche Altlasten bereinigt.

Jahresauftakt mit Aufregung: Meltdown und Spectre

Das Knallen der Sektkorken war noch kaum verhallt, als Meltdown und Spectre durch die Medien geisterten. Business as usual? Irgendjemand entdeckt irgendeine Sicherheitslücke, dekoriert sie mit Name, Logo und Webseite und verbreitet damit Angst und Schrecken? Bald sind Angriffsvektor und betroffene Software bekannt, ein Upgrade oder Bugfix behebt das Problem und alles ist paletti?

Diesmal nicht. Diesmal war Hardware im Fokus, und das warf ungewohnte Fragen auf:

- Können wir dieses Problem überhaupt nachvollziehen?
- Ist es in der Praxis relevant?
- Wie könnte man Hardware „bugfixen“?
- Wie können die Sicherheitslücken ausgenutzt werden?
- Betreffen sie alle Anwendungen, nur bestimmte Systeme, oder stehen wir kurz vor dem digitalen Weltuntergang?

Meltdown und Spectre zeigten vor, was man bis dahin nicht als realistisches Szenario in Betracht gezogen hatte: aus dem Timingverhalten des Prozessors nicht preisgegebene Informationen abzuleiten. Die Zugriffskontrollen im Prozessor funktionierten spezifikationsgemäß, nur eben in datenabhängiger Zeit – ist das überhaupt ein Fehler? Falls ja, wer ist schuld?

Das ist sensationell, weil grundlegende Designprinzipien aktueller Prozessorarchitekturen neu überdacht werden müssen. Inwieweit aktuelle Systeme wenigstens notdürftig mit Microcode-Updates im Prozessor und mit Softwaretricks gegen diese Angriffe resistent gemacht werden können, muss sich erst herausstellen. Auch für potenzielle Angriffsszenarien wurde ein eigenes Forschungsfeld eröffnet.

Als eines der ersten Computer Emergency Response Teams weltweit hat das ACOnet-CERT der Community eine Einschätzung der Lage zur Verfügung gestellt. Die gute Nachricht: Reale Angriffe im Netz sind eher aufwendig und bis dato nicht bekannt geworden. Die schlechte: Grundsätzliche Lö-

sung gibt es mittelfristig keine, und es ist mit weiteren Entdeckungen zu rechnen. Um die Angriffsfläche möglichst gering zu halten, ist neben den selbstverständlichen Betriebssystem-Updates auch auf die Aktualisierung des Prozessor-Microcodes zu achten – sei es via BIOS des Mainboards oder beim Booten des Betriebssystems.

OpenVAS – was?

Kaum jemand wird bestreiten, dass Server sicher konzipiert, sicher konfiguriert und regelmäßig gewartet werden sollen. Ebenso allgemein bekannt ist, dass es trotz aller Sorgfalt gelegentlich zu Sicherheitslücken kommen kann. Ein Security-Scan kann helfen, hier sozusagen als zweites Augenpaar über eine Installation „drüberzuschauen".

Besonders aussagekräftig ist es, wenn ein solcher Scan von außerhalb des eigenen Netzes geschieht, da so die exponierten Services aufgezeigt werden. Zu diesem Zweck wurde für ACOnet-Teilnehmerorganisationen das Service „Vulnerability Assessment Scan" eingerichtet.

Der Scan erfolgt mit Hilfe des Open-Source-Tools OpenVAS, ist auf maximal 256 IP-Adressen beschränkt und kann von zwei Adressen aus erfolgen, um dem Assessment z. B. unterschiedlich durchlässige Firewallkonfigurationen zugrunde zu legen. Einige Beispiele für Schwachstellen, die ein solcher Scan aufdecken kann:

- Konfigurationsschwächen bei Übertragungsprotokollen,
- veraltete Protokoll- oder Cipher-Versionen,
- offene Betriebssystem- bzw. Software-Lücken,
- Schwachstellen in CMS- oder Wiki-Systemen,
- OpenSSL Vulnerabilities,
- versehentlich laufende Telnet-Server,
- prinzipiell erreichbare Samba-Shares,
- offene Mailrelays
- und vieles andere.

Alle Einzelheiten dazu sind im ACOnet-Webportal unter dem Punkt „Netzwerk / CERT Online" zu finden (**https://www.aco.net/webportal** – Login nur für berechtigte IT-MitarbeiterInnen von ACOnet-Teilnehmerorganisationen möglich).

Kehraus im ACOnet

Damit das ACOnet seinen guten Ruf – und damit auch seine gute Vernetzung – behält, kümmert sich das ACOnet-CERT routinemäßig um all die sicherheitsrelevanten Fälle, die auch ohne genauen Scan ins Blickfeld rücken.

In der Hauptsache betrifft das Systeme, die an „Denial of Service"-Angriffen (DoS-Angriffen) teilnehmen, Spammail versenden oder bei Sensoren für Bot-Netze auffallen. Eher selten passiert es, dass regelrechte Beschwerden bei ACOnet eintreffen. Nach ausgewählten Schwachstellen sucht das ACOnet-CERT selbst: Das sind vor allem Server, die als UDP-basierte Reflektoren für DoS-Angriffe dienen können.

In all diesen Fällen wird der Security-Kontakt des jeweiligen ACOnet-Teilnehmers per E-Mail verständigt. Zumeist ist das Problem in kürzester Zeit gelöst. Die Ausnahme bestätigt aber die Regel, und so hatten sich über 200 offene Vorfälle angesammelt; die meisten davon waren schon länger offen.

Dies nahm das CERT zum Anlass, die Karteileichen in unzähligen Mails, Telefonaten und Nachforschungsaktionen zu bearbeiten. Nur in ganz wenigen Ausnahmefällen war es erforderlich, als Notmaßnahme zur Sperre einer IP-Adresse zu greifen.

Der Erfolg kann sich sehen lassen: Die offenen Fälle sind auf ein Zehntel gesunken und die DoS-Angriffe selten geworden.

Alexander Talos-Zens

Teamleiter ACOnet-CERT

DSGVO: Auswirkungen auf Registries und ACOnet

Die Datenschutz-Grundverordnung (DSGVO) regelt und vereinheitlicht die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Einrichtungen in Österreich. Sie ist die Umsetzung einer Direktive der Europäischen Union (General Data Protection Regulation, GDPR) in nationales Recht. Im Folgenden wird beschrieben, welche Konsequenzen die DSGVO für Name Registries, IP Number Registries und für den Betrieb von ACOnet hat.

Richtlinien

Die DSGVO ist seit Mai 2018 anzuwenden und regelt, einfach gesprochen, den Umgang mit Daten von „natürlichen Personen" auf der Basis einiger Grundsätze, die allerdings auch schon im bisher gültigen Datenschutzgesetz adressiert wurden. Die wichtigsten dieser Prinzipien sind:

Die Verarbeitung personenbezogener Daten ist nur unter bestimmten Voraussetzungen zulässig – im Wesentlichen dann, wenn dafür eine Einwilligung gegeben wurde, wenn die Daten zur Erfüllung eines Vertrages bzw. einer rechtlichen Verpflichtung notwendig sind oder wenn spezielle Interessen (z. B. öffentliches Interesse, lebenswichtiges Interesse) gewahrt werden müssen.

Sind diese Voraussetzungen gegeben, müssen bei der Datenverarbeitung bestimmte Regeln nachweislich eingehalten werden, andernfalls kann die Nichteinhaltung geahndet werden. Diese Regeln spezifizieren, dass mit den verwendeten Daten „pfleglich", also verantwortungsvoll, umgegangen werden muss. So dürfen die Daten nur für einen festgelegten Zweck verarbeitet werden, nur die dafür unbedingt notwendigen Daten dürfen erfasst werden und diese nur so lang wie nötig verwendet und gespeichert werden. Insbesondere ist auf Vertraulichkeit zu achten. Die gespeicherten Daten sind auf Anfrage zu beauskunften, zu aktualisieren, zu korrigieren oder gegebenenfalls zu löschen.

Diese Vorgaben bilden nun einen modernen rechtlichen Rahmen, in dem Daten zu betrachten sind. In unserem Fall betrifft das jene Daten, die für die Registrierung von Domains und IP-Netzen notwendig sind, konkret die Namen und Kontaktinformationen der jeweiligen Inhaber und Ansprechpersonen. Diese Daten sind über eine spezielle Schnittstelle – das „whois"-Service der .at-Domainverwaltung – öffentlich einsehbar. Auf diesem Weg waren bisher Inhaber und Kontaktinformationen von Domains jederzeit abfragbar, und zwar unabhängig davon, ob der Inhaber eine Privatperson, eine Firma oder eine Behörde ist.

Seit dem Inkrafttreten der DSGVO ist es nicht mehr möglich, diese Daten undifferenziert der Öffentlichkeit anzuzeigen. Wie eingangs dargestellt, geht es bei der DSGVO explizit um personenbezogene Daten (also die Daten von natürlichen Personen), nicht aber um Daten einer Firma. Daher ist nun prinzipiell zwischen diesen Kategorien zu unterscheiden und darauf zu achten, dass die Daten von Privatpersonen gesondert behandelt werden.

Domains

Die folgenden Beispiele illustrieren zwei unterschiedliche Szenarien aus dem Bereich der Domainvergabe: einerseits die von einer natürlichen Person unter .at registrierte Domain, andererseits die von einer juristischen Person unter .ac.at registrierte Domain.

```
domain:          papst.at
registrar:
registrant:      <data not disclosed>
tech-c:          <data not disclosed>

[ – technische Details gelöscht – ]

changed:         20071218 15:33:22
source:          AT-DOM
```

Abb. 1 (oben): whois-Output – Domain einer natürlichen Person unter .at

Abb. 2 (rechts): whois-Output – Domain einer juristischen Person unter .ac.at

.at

Da es sich in diesem Szenario um die Domain einer natürlichen Person handelt und diese Person nicht explizit eine Offenlegung der Daten beantragt hat, werden alle personenbezogenen Daten ausgeblendet – sowohl die des Domaininhabers als auch die der weiteren Kontakte. Abbildung 1 zeigt den (gekürzten) whois-Output für dieses Beispiel.

.ac.at

Domains unter .ac.at werden ausschließlich an Organisationen, also juristische Personen, vergeben. In diesem Szenario können die Daten also vollständig dargestellt werden. Interessant an diesem Beispiel ist, dass der administrative Kontakt (admin-c) eine natürliche Person ist und deshalb ausgeblendet wird. Hingegen sind die technischen Kontakte (tech-c) sogenannte „Rollen". Diese Daten sind keiner natürlichen Person zugeordnet und werden daher vollständig angezeigt (siehe Abbildung 2).

IP-Adressen & AS-Nummern

Ein weiterer Bereich, in dem ACOnet Daten erfasst, speichert und weiterleitet, ist unsere Local Internet Registry (LIR) zur Vergabe von global eindeutigen IP-Adressen und Autonomous System (AS) Numbers. Dieses Service für ACOnet-Teilnehmerorganisationen wird im Rahmen eines Vertragsverhältnisses mit dem RIPE NCC in

```
domain:          univie.ac.at
registrar:
registrant:      UWZI7674410-NICAT
admin-c:         <data not disclosed>
tech-c:          UH1428893-NICAT
tech-c:          UN566897-NICAT

[ – technische Details gelöscht – ]

changed:         20190109 10:47:49
source:          AT-DOM

personname:
organization:    Universitaet Wien
                 (Zentraler Informatikdienst)
street address:  Universitaetsstrasse 7
postal code:     1010
city:            Vienna
country:         Austria
phone:           +431427714277
fax-no:          +431427714279
e-mail:          domain-admin@univie.ac.at
nic-hdl:         UWZI7674410-NICAT
changed:         20101202 21:00:00
source:          AT-DOM

personname:      UNIVIE Hostmaster
organization:
street address:  Universitaetsstrasse 7
postal code:     1010
city:            Vienna
country:         Austria
phone:           +431427714277
fax-no:          +431427714279
e-mail:          domain-admin@univie.ac.at
nic-hdl:         UH1428893-NICAT
changed:         20180201 16:15:02
source:          AT-DOM

personname:      UNIVIE Netadmin
organization:
street address:  Universitaetsstrasse 7
postal code:     A-1010
city:            Vienna
country:         Austria
phone:           +431427714030
fax-no:          +43142779140
e-mail:          net-admin@univie.ac.at
nic-hdl:         UN566897-NICAT
changed:         20050909 09:23:41
source:          AT-DOM
```

Amsterdam erbracht. Das RIPE NCC als (übergeordnete) Regional Internet Registry führt das Verzeichnis der vergebenen, global eindeutigen „Internet Number Resources“ und macht diese Informationen ebenfalls über ein whois-Service – ähnlich wie in der Welt der Domains – zugänglich.

Die ACOnet-LIR erfasst nur jene Daten (und leitet sie nach Amsterdam weiter), die im Rahmen des „RIPE NCC Standard Service Agreement“ und der RIPE Policies vereinbart sind. Im Rahmen dieses Vertragsverhältnisses hat die ACOnet-LIR die Verpflichtung, die Daten für die Registry aktuell und richtig zu halten und gegebenenfalls zu entfernen.

Der Betrieb der Regional Internet Registry in den Niederlanden unterliegt selbstverständlich ebenfalls den Vorgaben der Datenschutzgrundverordnung und den nationalen Gesetzen. Eine Sammlung von Artikeln zum Umgang des RIPE NCC mit diesen Vorgaben ist unter **https://labs.ripe.net/Members/Athina** zu finden.

ACOnet-Betrieb & spezifische Services

Last but not least sind für den geordneten Betrieb von ACOnet auch technische und administrative Informationen über die teilnehmenden Organisationen und die jeweiligen Kontaktpersonen, sowie Daten im Rahmen der Vertragsverhältnisse für einzelne Services notwendig. Wie auch schon vor dem Inkrafttreten der DSGVO gilt das Prinzip, dass nur jene Daten erfasst und gespeichert werden, die für den Betrieb des Netzverbundes, für einzelne spezifische Services und zur Kontaktaufnahme bei Betriebsstörungen oder sicherheitsrelevanten Vorfällen notwendig sind. Diese Daten werden laufend überprüft und aktualisiert und nach einem geordneten Ende der Teilnahme an ACOnet entfernt.

Im Gegensatz zu den whois-Services der Domain und Number Registries werden diese Daten – besonders jene, die der DSGVO unterliegen – nicht öffentlich zugänglich gemacht und grundsätzlich nicht weitergegeben, außer die Weitergabe ist im Rahmen eines Vertragsverhältnisses oder einer Vereinbarung für ein spezifisches Service notwendig.

Gerhard Winkler

Teamleiter
Internet Domain Administration

Wilfried Wöber

ACOnet
Security, Training, Consulting

European Open Science Cloud: Startschuss in Wien

Am 23. November 2018 fand im Rahmen der österreichischen EU-Ratspräsidentschaft im Großen Lesesaal der Universität Wien der „Launch Event" der European Open Science Cloud (EOSC) statt. Die EOSC soll zukünftig dafür sorgen, dass Forschungsergebnisse aus EU-geförderten Projekten für eine weitere Nutzung verfügbar sind.

2015 begannen die Vorarbeiten zur European Open Science Cloud (EOSC)[1], mit der ein digitaler Binnenmarkt für Forschungsdaten entsteht. Die Europäische Union hat in den letzten 10 Jahren mit mehr als 120 Milliarden Euro verschiedenste Forschungsprojekte gefördert, in denen Daten produziert wurden. Diese sollen künftig über die EOSC für Folgeprojekte aus Forschung und Wirtschaft zur Nachnutzung bereitgestellt werden.

Dazu bedarf es nicht nur einer entsprechenden Infrastruktur, sondern auch genauer Spielregeln, die definieren, wie die unterschiedlichen Stakeholder zusammenarbeiten können. Daher ist die EOSC keine Cloud im herkömmlichen Sinne, sondern vielmehr ein Prozess, der darauf abzielt, den Übergang zu einem offenen und innovativen digitalen Binnenmarkt zu schaffen, in dem Forschung unterstützt wird und Kooperationen mit der Wirtschaft möglich sind. Mit der EOSC werden vertrauenswürdige Dienste, Systeme und Archive für Daten etabliert, die über Forschungsdisziplinen und geografische Grenzen hinweg genutzt werden können. Dabei sollen keine neuen Infrastrukturen geschaffen, sondern bereits existierende zusammengeführt werden.

„Science should have no borders"

Die EOSC wurde am 23. November 2018 mit einem feierlichen Launch Event im Großen Lesesaal der Universitätsbibliothek Wien offiziell gestartet. Carlos Moedas, EU Commissioner for Research, Science and Innovation, sagte in der Videobotschaft, die er zum Launch Event nach Wien sendete: „Science should have no borders."[2] Moedas stellte eine Verbindung zu Kaffeehäusern des 16. Jahrhunderts her, in denen sich Personen unterschiedlichster Herkunft trafen und Ideen austauschten. Die EOSC ist ein Ort, an dem man Daten von öffentlich geförderten Forschungsprojekten finden kann – und jeder darf diese nutzen.[3]

Über das EOSC-Portal, das (inklusive Anwendungen) ebenfalls am Launch Event in Wien vorgestellt wurde, können bereits Daten abgerufen werden.

Daten stehen im Zentrum

Die EOSC vereinigt Dienste und Archive für Forschungsdaten, damit diese effektiv aufbereitet und geteilt werden können. Sie kann über drei Kernelemente begriffen werden: Dateninfrastruktur zum Speichern und Verwalten von Daten, Netzwerkinfrastruktur mit hoher Bandbreite sowie leistungsfähige Computersysteme, um die Daten zu verar-

Foto: Der EOSC Launch Event an der Universität Wien
(© Joseph Krpelan)

Prominente Gäste beim EOSC Launch Event:
Vizerektorin Regina Hitzenberger (Universität Wien), Bundesminister Heinz Faßmann (BMBWF), Generaldirektor Jean-Eric Paquet (GD für Forschung und Innovation der EU-Kommission), Sektionschefin Barbara Weitgruber (BMBWF)
(© Joseph Krpelan)

beiten. Zusätzlich spielen auch die FAIR-Prinzipien für Daten eine wesentliche Rolle: Im Kontext nachhaltigen Datenmanagements sind diese Prinzipien ein Leitmotiv und für die EOSC von hoher Bedeutung. FAIR steht für „Findable, Accessible, Interoperable, Reuseable" und zielt damit unter anderem auch auf einen maschinellen Zugang zu den Daten ab. Mit zunehmender Automatisierung wird es immer wichtiger, dass nicht nur Menschen auf Inhalte zugreifen können, sondern auch Applikationen einen guten Zugang erhalten. Das FAIR-Prinzip für Daten wurde von Beginn an als Grundlage der EOSC gesehen: „The EOSC is indeed European, but it should also be interoperable with the Internet of FAIR data and services and be an accessible infrastructure for modern research and innovation." 1/Seite 8)

Austria takes initiative

Am 30. Oktober 2018 gab es in Wien bereits eine Vorgängerveranstaltung zum Launch Event. Diese fand ebenfalls an der Universität Wien statt, stand unter dem Motto „Austria takes initiative" und ganz im Zeichen österreichischer Infrastrukturen und Services, die im Sinne der EOSC Forscherinnen und Forscher unterstützen. Bei dieser Veranstaltung wurden Projekte vorgestellt, die alle bereits im Sinne der EOSC agieren: Hochschulraum-Strukturmittel-Projekte wie z. B. e-Infrastructures Austria[4)] und kooperative Infrastrukturen wie der Vienna Scientific Cluster[5)], aber auch Infrastrukturen, die direkt mit der EOSC zusammenhängen – z. B. AUSSDA[6)], das Austrian Social Science Data Archive. AUSSDA ist ein Teil von CESSDA (Consortium of European Social Science Data Archives), jener Organisation, die den Bereich der Sozialwissenschaften in der EOSC vertritt. Alle Vorträge der Veranstaltung können über die Homepage des Events abgerufen werden.[7)]

Vienna Declaration

Am Launch Event der EOSC in Wien wurde die große Vision von mehreren Seiten präsentiert. Die ersten Ergebnisse zeigen, wie das EOSC-Portal den

1) European Commission: Realising the European Open Science Cloud. First report and recommendations of the Commission High Level Expert Group on the European Open Science Cloud. Luxembourg: Publications Office of the European Union, 2016. **https://ec.europa.eu/research/openscience/pdf/realising_the_european_open_science_cloud_2016.pdf**

2) Videomessage von Carlos Moeda im Video „Introduction and Welcome: EOSC Launch Event" (Start bei 00:16:07): **https://phaidra.univie.ac.at/o:918356**

3) Digital „coffeehouse" to spark new scientific ideas now ready for use; Horizon – The EU Research & Innovation Magazin: **https://horizon-magazine.eu/article/digital-coffeehouse-spark-new-scientific-ideas-now-ready-use.html**

4) Webauftritt des Projekts e-Infrastructures Austria: **https://www.e-infrastructures.at/**

5) Webauftritt des Vienna Scientific Cluster: **https://vsc.ac.at/**

6) Webauftritt des Austrian Social Science Data Archive: **https://aussda.at/**

7) Videos der Veranstaltung „The European Open Science Cloud: Austria takes initiative": **https://eosc18-ati.univie.ac.at/programme/**

8) The Vienna Declaration on the European Open Science Cloud. Vienna, 23. 11. 2018. **https://phaidra.univie.ac.at/view/o:918643**

9) Webauftritt des EOSC Launch Events: **https://eosc-launch.eu/**

Weg für die Zukunft vorbereitet. Es wurden sowohl die Governance-Struktur als auch die nächsten Schritte vorgestellt, die die EOSC zu einem erfolgreichen „Digital Marketplace“ für ForscherInnen aus Europa und darüber hinaus machen sollen.

Zum Abschluss der Veranstaltung präsentierten Bundesminister Heinz Faßmann, Karina Angelieva (stellvertretende Ministerin für Bildung und Forschung in Bulgarien) sowie Ciprian Preda (Staatssekretär für Forschung und Innovation in Rumänien) „The Vienna Declaration on the European Open Science Cloud“.[8] Der gesamte Event wurde aufgezeichnet und kann über die Website abgerufen werden.[9]

Raman Ganguly

Universität Wien / ZID
Leiter der Stabsstelle „Software Design & Development“

IaaS Cloud Services 2018

Das GÉANT „IaaS Cloud Services“ Framework (siehe Jahresbericht 2017 ab Seite 30) wurde laut Rückmeldung der Anbieter im Jahr 2018 von sechs ACOnet-Teilnehmerorganisationen in einem Gesamtumfang von rund 111.000 Euro in Anspruch genommen – offenbar vorwiegend zum Testen und Erfahrungen sammeln.

ACOnet-seitig haben wir 2018 an der Verbesserung unserer IaaS-Dokumentation gearbeitet (siehe **https://www.aco.net/geant-iaas.html**) sowie als Pilot-Teilnehmer an der Vereinfachung des Zugriffs auf die – mittlerweile DSGVO-kompatiblen – Vertragsdokumente des GÉANT „IaaS Cloud Services“ Framework per halbautomatisiertem Formular mitgearbeitet. Unser Ferialpraktikant Fabian Jusufi hat zusätzlich eine Wiki-Dokumentation zum Thema „IaaS Cloud Services“ aus Sicht der Universität Wien erstellt (**https://wiki.univie.ac.at/display/iaas**).

Der ZID der Universität Wien hat Mitte 2018 ein Projekt gestartet, das eine Empfehlung für eine „Cloud-Strategie“ für das Rektorat der Universität Wien erarbeiten soll. Im Zuge dieses Projekts wird auch eine Abstimmung und Zusammenarbeit mit anderen Universitäten angestrebt. Ein erster Informationsaustausch dazu hat am 27. 11. 2018 an der Universität Wien stattgefunden; VertreterInnen von zwölf österreichischen Universitäten haben daran teilgenommen.

Im Rahmen der Aktivitäten zur „European Open Science Cloud“ soll unter dem 2018 initiierten OCRE-Projekt (Open Clouds for Research Environments, **https://www.ocre-project.eu/**) im Laufe des Jahres 2019 eine weitere Rahmenvertrags-Ausschreibung für Cloud-Ressourcen stattfinden – diesmal in einer Kooperation von GÉANT, CERN und weiteren Projektpartnern. ACOnet wird sicherstellen, dass alle Teilnehmerorganisationen wieder Zugriff auf die Ergebnisse haben.

Rückfragen zu unseren Cloud-Aktivitäten richten Sie bitte an die Mailadresse **cloud@aco.net**.

Christian Panigl

Abteilungsleiter ACOnet & VIX

Partnership for Advanced Computing in Europe

Österreich ist seit Juli 2018 Mitglied von PRACE, dem Partnership for Advanced Computing in Europe, wodurch Forschende Zugang zu europäischen Höchstleistungsrechnern bekommen. Der ACONET-Verein als Vertreter eines Konsortiums österreichischer Universitäten ist der institutionelle österreichische Repräsentant im PRACE-Rat.

Seit 11. Juli 2018 ist Österreich – vertreten durch den ACONET-Verein – Mitglied des europäischen Supercomputing-Netzwerks PRACE (Partnership for Advanced Computing in Europe, **www.prace-ri.eu**). Dadurch eröffnen sich neue Möglichkeiten im Bereich „High Performance Computing" (HPC) für Forschende und Studierende in Österreich.

Spitzenforschung mit Supercomputern

Ohne Höchstleistungsrechner ist Spitzenforschung kaum mehr möglich. Höchstleistungsrechner, auch Supercomputer genannt, werden verwendet, um hochkomplexe und datenintensive Fragen aus Grundlagenforschung und Technik sowie zu gesellschaftsrelevanten Themen zu beantworten. Sie werden für Simulationen eingesetzt (z. B. wenn reale Experimente zu lange dauern würden, zu gefährlich oder zu teuer wären oder aus anderen Gründen nicht durchführbar sind), aber auch als Ergänzung zu tatsächlich durchgeführten Experimenten. Wettervorhersagen und Klimaforschung, Astrophysik, Strömungsmechanik, Materialwissenschaften, Medizin und Pharmazie sind nur einige der Gebiete, für die der Zugang zu Supercomputern extrem wichtig ist.

Internationale Zusammenarbeit

Derzeit gibt es hierzulande zwei Hochleistungsrechner, die jeweils von einem Konsortium österreichischer Universitäten betrieben werden: den Vienna Scientific Cluster (VSC, **vsc.ac.at**) in Wien und MACH-2, ein Shared-Memory-System in Linz (siehe Seite 53).

Durch den PRACE-Beitritt stehen Forschenden nun noch schnellere und leistungsstärkere Maschinen zur Verfügung, um noch komplexere wissenschaftliche Fragestellungen beantworten zu können. Wie das Bundesministerium für Bildung, Wissenschaft und Forschung betont, ist dies ein „Zwischenschritt", bis Ende 2020 die ersten Systeme im Rahmen von EuroHPC bereitstehen werden. Das Ziel von EuroHPC ist die Stärkung europäischer IT- und HPC-Aktivitäten, um im wissenschaftlichen Wettbewerb mit den USA und Asien im Spitzenfeld bestehen zu können.

Austria joined PRACE

„The PRACE Council is very pleased to welcome Austria as a member of PRACE and is looking forward to a fruitful collaboration. By joining PRACE, Austria sends a strong signal that it supports the scientific and industrial application of HPC at the highest level. The Austrian research community will benefit in many ways from having access to the tip of the European HPC ecosystem."

Prof. Dr. Dr. Thomas Lippert,
Chair of the PRACE Council

Fotos:
Österreichs Vertreter im PRACE Council:
links Delegate Christoph Dellago
(© Universität Wien / Barbara Mair),
rechts Advisor Alexander Ostermann
(© Universität Innsbruck)

Grafik: PRACE Fact Sheet (© PRACE)

PRACE-Forschungsinfrastruktur

Das Ziel von PRACE ist es, grundlegende wissenschaftliche Erkenntnisse und die Entwicklung der Ingenieurwissenschaften durch Höchstleistungsrechner-Ressourcen zu unterstützen. Die europaweit nutzbare Forschungsinfrastruktur von PRACE besteht derzeit aus sieben Supercomputern, die von fünf Ländern (Deutschland, Frankreich, Italien, Schweiz und Spanien) zur Verfügung gestellt werden. Der Zugang zu diesen Supercomputern ist durch ein internationales Peer-Review-Verfahren möglich, wofür zweimal jährlich (im Frühling und im Herbst) ein Einreichungsfenster für Projektanträge bekannt gegeben wird.

Wissenschaft und Industrie

Die PRACE-Forschungsinfrastruktur und alle Services können sowohl von Forschenden aus dem akademischen Umfeld als auch von Teilnehmern aus der Industrie gleichermaßen verwendet werden. Für industrielle NutzerInnen gibt es zusätzlich die spezielle Förderschiene SHAPE, die sich vor allem an kleine und mittelständische Unternehmen richtet, sowie ab Frühjahr 2019 einen sogenannten „Improved Industry Access Track“ für Projektanträge.

PRACE-Services

Zur effizienten Nutzung der Supercomputer bietet PRACE auch weitere Services an. Besonders erwähnt werden soll hier der sogenannte „Preparatory Access“, der die Optimierung und Skalierungstests der eigenen Applikationen (mit oder ohne ExpertInnen-Unterstützung) ermöglicht.

PRACE entfaltet zudem eine Reihe von thematisch verwandten Aktivitäten wie ein europaweites Kursprogramm durch zehn „PRACE Training Centers“, Sommerschulen, Arbeitsgruppen und Kooperationen zu Themen wie Beschaffung von Rechnersystemen, neue Technologien und Energieeffizienz.

ACONET-Verein vertritt Österreich

Formal ist Österreich durch den ACONET-Verein in PRACE vertreten. Das ist besonders zu begrüßen, weil praktisch alle österreichischen Forschungseinrichtungen sowie zahlreiche andere Organisationen zu den ACOnet-Teilnehmern zählen.

- PRACE in Österreich: **www.aco.net/prace**
- PRACE Österreich Mailingliste: **noc.aco.net/mailman/listinfo/prace**
- PRACE Webseite: **www.prace-ri.eu**

Claudia Blaas-Schenner
TU Wien / VSC Research Center
claudia.blaas-schenner@tuwien.ac.at

DNSSEC für .ac.at

Das Domain Name System, kurz DNS, regelt die Zuordnung von Domainnamen (z. B. www.aco.net) zu IP-Adressen (z. B. 193.170.140.135) und bildet somit die Voraussetzung dafür, dass zur Identifizierung von Rechnern im Internet auch Domainnamen verwendet werden können. Das DNS ist ein Basis-Service des Internet. Sicherheitsaspekte wurden aber erst nachträglich – mit den DNS Security Extensions (DNSSEC) – implementiert.

Das ursprüngliche Design des DNS hatte mögliche Probleme in Zusammenhang mit Sicherheit nicht oder nur marginal im Fokus. Zum Zeitpunkt der Entwicklung des Dienstes standen Funktionalität und Performance im Vordergrund. Aspekte wie die ungewollte Offenlegung von Daten, Attacken oder Kompromittierung von Services stellten sich damals nicht in der heutigen Form. Im Laufe der Zeit gewannen diese Fragen aber zunehmend an Bedeutung, und sie werden weiterhin immer wichtiger. Es musste daher zusätzliche Funktionalität in das DNS gebracht werden – primär mit dem Ziel, die Sicherheit zu erhöhen. Nach einer langen Entwicklungszeit von etwa 10 Jahren wurden die RFCs („Requests for Comments", die De-facto-Standards im Internet) zu DNSSEC (DNS Security Extensions) schließlich 2005 verabschiedet.

DNSSEC löst einige Probleme im Zusammenhang mit Sicherheit, wie Authentizität (= Echtheit) und Integrität (= Vollständigkeit) von Daten. Andere Themen wie Vertraulichkeit werden allerdings nicht behandelt. Das bedeutet, dass DNSSEC zwar punktuell die Sicherheit des DNS verbessert, aber nicht die Lösung für alle Probleme darstellt. Dazu kommt, dass DNSSEC mit kryptografischen Methoden arbeitet, was einerseits einen zusätzlichen administrativen Aufwand (Key Management) und andererseits ein gewisses Risiko im operativen Bereich mit sich bringt, da die Komplexität steigt.

Die Einführung von DNSSEC war und ist daher ein lang andauernder Prozess; ein flächendeckender Einsatz ist bis heute nicht gegeben. Für bestimmte Anwendungen und neuere Funktionen ist die DNSSEC-Infrastruktur allerdings eine Voraussetzung, sodass der Aufbau dieser Infrastruktur sukzessive und gezielt vorangetrieben wurde.

Was bisher geschah

Ein Grundprinzip von DNSSEC ist, dass von der Wurzel des DNS-Namensbaumes (Root) über die Top-Level-Domains bis hin zu den Teilnehmer-Domains eine „Chain of Trust" gebildet wird, also eine Vertrauenskette, wo stets die übergeordnete Zone für die nächste delegierte („niedrigere") Zone bürgt. Dies wird durch kryptografische Methoden mittels wohlbekannter asymmetrischer Verfahren (Private Key / Public Key) sichergestellt.

Deshalb war es notwendig, mit der Signierung der Wurzel – also mit der Root-Zone – zu beginnen, was 2010 erfolgte. Der nächste Schritt war die Signierung der Top-Level-Domain .at, die im Jahr 2012 durchgeführt wurde. Damit war die Infrastruktur geschaffen, um bei Bedarf auch darunterliegende Zonen signieren zu können.

Allerdings war der Bedarf bzw. das Interesse für Domains in der Zone .ac.at zu diesem Zeitpunkt noch nicht nennenswert gegeben. Daher wurde auf eine sofortige Signierung dieser Zone verzichtet; dies bot zusätzlich die Möglichkeit, aus den Erfahrungen im Betrieb von .at zu lernen. Im Laufe der letzten Jahre wurden jedoch neue Anwendungen entwickelt (bzw. fanden größere Verbreitung), die DNSSEC benötigen. Eine Signierung von .ac.at war nun unumgänglich, um allen BesitzerInnen von .ac.at-Domains die Möglichkeit zu geben, diese zu signieren und in die „Chain of Trust" einzuhängen.

Daher wurde Anfang 2018 die nötige Infrastruktur zur Signierung von .ac.at aufgebaut und getestet. Im Herbst 2018 wurde die signierte .ac.at-Zone schließlich in .at eingehängt. Seither können die ACOnet-Teilnehmerorganisationen bei Bedarf ihre .ac.at-Domains signieren und DNSSEC nutzen (siehe Kasten rechts).

Stolpersteine ...

Abgesehen vom zusätzlichen operativen Aufwand liegt eine große Hürde bei DNSSEC darin, dass ein unmittelbarer Sicherheitsgewinn gerade für die EndanwenderInnen schwer darstellbar ist.

Einerseits fehlt es an flächendeckender Infrastruktur zur Validierung der DNSSEC-signierten Domains, speziell in den Anwendungen und den Endgeräten. Selbst wenn dort eine solche Prüfung erfolgt, ist die „technisch richtige" Konsequenz einer ungültigen Signatur (beispielsweise dass eine Webseite nicht angezeigt wird) für die betroffenen BenutzerInnen häufig nicht hilfreich oder nicht erwünscht.

Andererseits gibt es – insbesondere im Bereich des „Surfens" durch Webseiten – bereits mehrere alternative Methoden, wie etwa Zertifikate, welche die Sicherheit für die EndanwenderInnen erhöhen sollen. Damit konkurrieren dann aber verschiedene Ansätze um die Aufmerksamkeit der BenutzerInnen und produzieren Unsicherheiten im Hinblick darauf, welches Verfahren nun Sicherheit signalisiert oder welchem Verfahren wann zu trauen ist – obwohl doch eine einfache, eindeutige Information oder Reaktion erwartet wird.

... und neue Perspektiven

Auf anderer Ebene allerdings wurden etliche Verfahren entwickelt, genormt und eingeführt, die auf der DNSSEC-Infrastruktur aufsetzen und in unterschiedlichen Bereichen zur Sicherheit beitragen. Hier ist explizit DANE („DNS-based Authentication of Named Entities") hervorzuheben. DANE bietet die Möglichkeit, Zertifikate mittels DNSSEC-gesicherter DNS-Einträge in der Zone abzulegen. Diese können dann verwendet werden, um eine gesicherte Kommunikation zwischen Mailservern aufzubauen – in der Form, dass TLS („Transport Layer Security") verwendet werden muss, also eine Kommunikation nur dann stattfindet, wenn gültige, validierende Zertifikate existieren.

Auch wenn die Verbreitung solcher weiterführenden Verfahren nur langsam zunimmt: DNSSEC bietet den nötigen Grundstock, um die Sicherheit im Internet durch neu entwickelte Methoden sukzessive zu erhöhen.

Voraussetzungen

Damit DNSSEC für eine .ac.at-Domain aktiviert werden kann, müssen folgende Vorbedingungen erfüllt sein:

- Die betroffene .ac.at-Domain muss delegiert und aktiv sein.
- Sie muss darüber hinaus bereits mit DNSSEC signiert sein.
- Für die Übermittlung des DS-Records setzen Sie sich bitte mit dem Team „Internet Domain Administration" in Verbindung (siehe unten).

Kontakt

Bei Fragen dazu, oder auch generell zu DNSSEC, wenden Sie sich bitte an:

domain-admin@univie.ac.at

Gerhard Winkler

Teamleiter
Internet Domain Administration

Community

Meetings & Workshops

6. – 7. März
CEE Peering Days 2018

13. März
16. KUKIT-Stammtisch

12. – 13. April
10. ArgeStorage-Meeting

20. April
DNSSEC-Workshop

CEE Peering Days 2018

6. – 7. März 2018
Berlin / Deutschland

Die „Central and Eastern European Peering Days" wurden 2018 im aufregenden Berlin abgehalten und boten – wie immer – anregende Vorträge und Diskussionen sowie ausreichend Zeit für Networking und bilaterale Meetings. Auch im vergangenen Jahr nahmen wieder mehr als 200 internationale Gäste an der zweitägigen Konferenz teil. Der Schwerpunkt des Programms lag aus gegebenem Anlass auf diversen Aspekten der EU-Datenschutz-Grundverordnung (DSGVO) sowie der EU-Richtlinie zur Netz- und Informationssicherheit (NIS).

CEE Peering Days

Die **Fachtagung** wird seit 2013 einmal jährlich veranstaltet und richtet sich primär an Internet Service Provider aus Österreich, Ungarn, der Tschechischen Republik sowie aus dem zentral- und osteuropäischen Raum.

Die **Tagungsgäste** setzen sich großteils aus PeeringKoordinatorInnen, Cloud-AdministratorInnen sowie Netzwerk- und Datacenter-BetreiberInnen zusammen.

Das **Programm** ist eine Kombination aus technischen Workshops, professionellen Präsentationen und Networking.

Alle Infos: **www.peeringdays.eu**

KUKIT – Kunst, Kultur & IT

16. KUKIT-Stammtisch

13. März 2018
Anton Bruckner Privatuniversität, Linz

17. KUKIT-Stammtisch

23. Oktober 2018
Albertina, Wien

Das Thema des 16. KUKIT-Stammtisches in Linz wurde von Raman Ganguly, Leiter der Stabsstelle „Software Design & Development" am ZID der Universität Wien, vorgetragen: Datenmanagement und Langzeitarchivierung am Beispiel des Archivsystems Phaidra. Die TeilnehmerInnen wurden von Rektorin Ursula Brandstätter begrüßt. Dem Vortrag ging eine Führung durch das Haus voraus. Besonders beeindruckend war der Computermusik-Konzertsaal „Sonic Lab", der uns von Andreas Weixler und Se-Lien Chuang präsentiert wurde.

Im Oktober 2018 waren wir zum zweiten Mal in der Albertina zu Gast. Einer Führung durch die aktuelle Ausstellung „Monet" folgte eine moderierte Diskussion über Online-Plattformen für Kunst- und Kulturinstitutionen: Wo stehen wir? Was ist inhaltlich gewünscht und sowohl technisch als auch budgetär umsetzbar? Welche Erfahrungswerte helfen uns, neue Herausforderungen zu bewältigen, und wie können wir diese gemeinsam realisieren?

Der KUKIT-Stammtisch wird über eine Mailingliste organisiert. Um sich für diese anzumelden, senden Sie einfach eine E-Mail mit dem Betreff „subscribe" an die Adresse **kukit-subscribe@lists.aco.net**.

ArgeStorage

10. ArgeStorage-Meeting

12. – 13. April 2018
Universität Innsbruck

11. ArgeStorage-Meeting

19. – 20. November 2018
Johannes Kepler Universität Linz

Das Frühjahrsmeeting 2018 der ArgeStorage führte uns in den Westen Österreichs an die Universität Innsbruck. 25 Personen nahmen teil und kamen in den Genuss von acht Vorträgen. Neben den üblichen Themen (Ceph, OpenStack mit Ansible, Proxmox, FreeNAS, Seafile etc.) wurde auch über Storage-Ausschreibungen und Parallele Filesysteme diskutiert. NetApp hielt einen Gastvortrag über StorageGRID Webscale. Darüber hinaus gab es auch ausreichend Zeit für Diskussionen. Wie bereits bei den vorangegangenen Meetings absehbar wurde, erweitert sich der Themenkreis zusehends in Richtung Virtualisierungs- und Containertechnologien.

Das Herbstmeeting fand an der Johannes Kepler Universität Linz statt. 29 TeilnehmerInnen lauschten acht Vorträgen. Die Präsentationen umfassten wieder Themen aus dem Storage-Bereich wie iSCSI, Pure Storage, WAN Storage-Replizierung, Tape Libraries und Object Storage bis hin zu CI/CD-Pipelines mit Ansible und GitLab und Monitoring von Storage-Infrastruktur. Diesmal gab es keinen Gastvortrag. Langeweile kam dennoch nicht auf, da die TeilnehmerInnen zahlreiche Themen einbrachten. Die Vortragenden erhielten auch einiges an Rückmeldungen aus dem Publikum.

DNSSEC-Workshops

20. April 2018 & 25. Mai 2018
Universität Wien

6. Juni 2018
FH Vorarlberg, Dornbirn

19. Juni 2018
Land Oberösterreich, Linz

DNS-Workshop

18. Juni 2018
Land Oberösterreich, Linz

Die Workshops zu DNSSEC bzw. DNS wurden gemeinsam mit Norbert Stubenvoll vom Magistrat Wien und Wolfgang Breyha von der Universität Wien abgehalten – herzlichen Dank an beide! Norbert widmete sich hauptsächlich dem Thema Monitoring von DNSSEC und Wolfgang beleuchtete die Bereiche DANE und Mailing. Bei den fünf Ganztags-Terminen wurden insgesamt 111 TeilnehmerInnen mit den Grundlagen von DNSSEC bzw. DNS vertraut gemacht.

Neben theoretischem Wissen wurde viel Wert auf die Praxis und den täglichen Betrieb gelegt. Alle TeilnehmerInnen haben selbständig einen BIND-Nameserver konfiguriert und eine Schulungsdomain erfolgreich mit DNSSEC signiert. Es wurden auch hilfreiche Tipps bezüglich Monitoring und Überwachung gegeben sowie auf mögliche Risiken und Probleme von DNSSEC hingewiesen.

Technische Betriebs- und Planungsgruppe

57. TBPG-Sitzung

7. Juni 2018
FH Vorarlberg, Dornbirn

58. TBPG-Sitzung

7. – 8. November 2018
Wirtschaftsuniversität Wien

In der Frühjahrssitzung der TBPG konnte über den erfolgreichen Abschluss der Backbone-Umstellung im Jahr 2017 berichtet werden. Jedoch: Nach der Migration ist vor der Migration – dementsprechend wurden zugleich auch schon die Pläne für die Inbetriebnahme „kurzer Verbindungen" zwischen einzelnen Standorten vorgestellt (siehe Seite 19). Bei der Herbstsitzung konnte hierzu dann ebenfalls eine Erfolgsmeldung präsentiert werden.

Ergänzt wurden die TBPG-Sitzungen durch Teilnehmerbeiträge (z. B. „Internetrouter selbst gebaut aus Serverhardware" oder Berichte seitens des Kunsthistorischen Museums Wien und des Landes Tirol über Netzwerksetups von eher unbekannten Herstellern) mit anschließenden Diskussionen in der Arbeitsgruppe.

Die Herbstsitzung wurde – wie im Zweijahresrhythmus üblich – gemeinsam mit der ArgeSecur durchgeführt. Die TeilnehmerInnen der beiden Arbeitsgruppen für sich überschneidende Themen an einen Tisch zu bringen hat sich bewährt und soll daher beibehalten werden.

Internet-Jubiläumsgala

26. September 2018
Marx Palast, Wien

Im Jahr 2018 wurde nicht nur „100 Jahre Republik Österreich" gefeiert, auch in Bezug auf das Internet waren mehrere Jubiläen fällig:

- 30 Jahre Domainendung „.at"
- 20 Jahre Domain-Registrierungsstelle „nic.at" und Online-Meldestelle „Stopline.at"
- 10 Jahre „CERT.at" (Computer Emergency Response Team Austria)

Die nic.at GmbH nahm dieses geballte Auftreten von Jahrestagen zum Anlass, für ihre Mitarbeiter, Freunde und Partner eine festliche Jubiläumsgala im Wiener „Marx Palast" zu veranstalten. ACOnet und der Vienna Internet eXchange waren als Mitveranstalter bzw. Sponsoren beteiligt.

Stermann & Grissemann führten im Rahmen einer Sonderausgabe von „Willkommen Österreich" mit Showgästen aus der vergangenen und aktuellen Internetgeschichte durch den Abend. Dabei entlockten sie ihren Gästen interessante Details: So verriet etwa Peter Rastl, ehemaliger ZID-Leiter der Universität Wien und oft als „Vater des Internets in Österreich" bezeichnet, dass er ursprünglich nicht an den Siegeszug des Internets geglaubt hatte.

Unter den Gratulanten waren auch die deutsche und die Schweizer Domain-Registrierungsstellen DENIC und SWITCH, mit denen nic.at eine enge Zusammenarbeit pflegt.


© Gerard Spee

Kunst & Kultur im Kontext eines NREN

Der von ACOnet und dem KHM-Museumsverband initiierte KUKIT-Stammtisch verfolgt das Ziel, die digitalen Herausforderungen von Kunst- und Kulturinstitutionen in Österreich gemeinsam zu meistern. Das ebenfalls von ACOnet ins Leben gerufene net:art coordination center hingegen agiert international, in Zusammenarbeit mit zahlreichen National Research and Education Networks (NRENs).

KUKIT extended

Im Juni 2018 diente die Reise zum TBPG-Treffen in Dornbirn als Anlass für zwei Zwischenstopps in Salzburg und Bregenz. Hintergrund dafür war der Wunsch, in Zukunft auch jene Kunst- und Kulturinstitutionen zu erreichen, die indirekt (d. h. über Landes- und Stadtregierungen) an ACOnet angebunden sind, um sie über die verschiedenen Kooperationsmöglichkeiten zu informieren. Nach den ersten Meetings im Mozarteum Salzburg und bei der Vorarlberger Energienetze GmbH sollen diese Treffen im Herbst 2019 fortgesetzt werden.

net:art coordination center

Bereits zum zweiten Mal folgten wir 2018 einer Einladung der New World Symphony nach Miami. Thema unseres Vortrags in der größten Orchesterakademie der USA war nicht nur unsere Produktion „net:art | near in the distance 3“, sondern auch unser Plan, das net:art coordination center aufzubauen. Inzwischen ist beides unter **https://www.netart.cc/** umfassend dokumentiert.

Seit 2013 beschäftigt sich ACOnet mit „performing arts over advanced networks“ (kurz net:art) – dem Traum, dass KünstlerInnen, die an verschiedenen Orten der Welt performen, in Echtzeit interagieren können. Die Hochleistungsdatennetze, die dafür notwendig sind, werden von NRENs betrieben. Die Softwarelösungen, die dafür notwendig sind (z. B. LOLA und UltraGrid), wurden von den KollegInnen von GARR und CESNET entwickelt. Der Beitrag, den ACOnet für diese faszinierende Entwicklung leistet, schöpft aus den Ressourcen eines international vielbeachteten Kulturlandes – mit all seinen hervorragenden Kunst- und Kulturinstitutionen, Hochschulen und KünstlerInnen der performativen und bildenden Kunst, die sich den Herausforderungen einer digitalen Welt stellen.

Internationale Kooperationen

Der Vortrag in Miami führte zu mehreren Projekten mit Anilla Cultural, Cultural Ring Latin America–Europe in Urugay: Am 4° Congreso Internacional Online de Educación y Nuevos Medios (Mai 2018) konnten wir „net:art | near in the distance 3“ gleich zweimal vorstellen. Im September 2018 unterstützten wir die Kooperation von Anilla Cultural mit dem Ars Electronica Festival, die mit Live-Einstiegen und Interviews das Festival der lateinamerikanischen Community präsentierte, und durften im KHM Wien die Konferenz „MuRe – Museography Network. Results 2017“ bei exzellenter Anbindung international übertragen.

Renate Kreil

ACOnet
Kunst- und Kulturkommunikation

Neue ACOnet-Teilnehmer 2018

Pädagogische Hochschule Oberösterreich

Beiträge von ACOnet-Teilnehmern

Telepresence @ Austrian Universities

Die Medizinische Universität Innsbruck war Ende 2015 damit konfrontiert, in kurzer Zeit eine leistungsfähige Infrastruktur für Videokonferenzen aufbauen zu müssen. Aus dieser Anforderung entwickelte sich die Idee, im Rahmen eines HRSM (Hochschulraum-Strukturmittel)-Projekts auf Basis der ACOnet-Infrastruktur ein österreichisches Service nach dem Vorbild der Videoconferencing-Plattform des DFN aufzubauen.

Die österreichischen Universitäten sind traditionell gut vernetzt. Neben der Universitätenkonferenz und ihren verschiedenen Unterausschüssen (z. B. Forum Budget, Forum Lehre) gibt es für nahezu alle Fachbereiche der universitären Administration Arbeitsgruppen, die dem Erfahrungsaustausch sowie der gemeinsamen Innovation dienen.

Meist finden hierzu 1–2 Mal pro Jahr Tagungen der jeweiligen Gruppen statt, bei denen alle TeilnehmerInnen an einem Ort sein müssen. Kurzfristig anberaumte und themenspezifische Treffen sind (außerhalb des Ballungsraums Wien) schon alleine aufgrund der Anzahl der TeilnehmerInnen und der notwendigen Anreise schwierig zu koordinieren.

E-Mail und Telefon

Als Kommunikationsmittel werden vorwiegend E-Mail oder Telefon verwendet, wobei der Diskurs in einer größeren Gruppe meist asynchron und mit Hilfe von Mailinglisten erfolgt. Selbst Telefonkonferenzen mit mehr als drei TeilnehmerInnen kommen vergleichsweise selten vor.

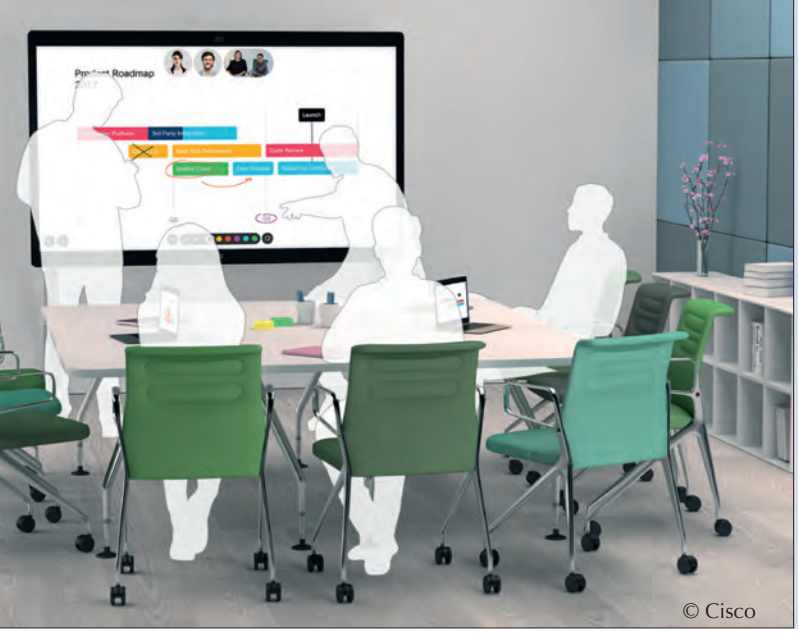
Videokonferenzen werden nur gelegentlich für die universitätsübergreifende Zusammenarbeit genutzt. Einerseits, weil die vorhandene Infrastruktur sehr inhomogen ist und mit unterschiedlichen technischen Standards (u. a. H.323, SIP) arbeitet. Andererseits wird für Konferenz-Anrufe mit mehr als drei teilnehmenden Endpunkten eine zentrale Multipoint Control Unit (MCU) mit ausreichender Kapazität benötigt, um die Datenströme zu verarbeiten und an alle TeilnehmerInnen zu verteilen.

Eine zentrale Plattform

Ziel des HRSM-Projekts „Telepresence @ Austrian Universities“ ist es, für Österreich eine zentrale Basisinfrastruktur zur verstärkten Nutzung von Videokonferenzen zu schaffen. Die Funktionsweise und die Implementierung des Dienstes orientieren sich dabei an erfolgreichen Beispielen aus dem Bereich der nationalen Forschungsnetzwerke, wie dem Service DFNconf des deutschen Forschungsnetzwerks.

Durch die Verfügbarkeit einer niederschwelligen Möglichkeit zur Nutzung von Telepresence-Technologien soll der Austausch zwischen den Universitäten über formelle Treffen hinaus gefördert werden. Auch weitere Partner der Universitäten wie die Ministerien, das Bundesrechenzentrum oder die BBG sollen motiviert werden, auf Telepresence zurückzugreifen und Abstimmungs- oder Briefing-Veranstaltungen vermehrt auch ohne die Notwendigkeit einer Anreise nach Wien abzuhalten.

Die Nutzung der ACOnet-Infrastruktur, über die alle Universitäten und auch viele der Partner bereits direkt miteinander verbunden sind, ermöglicht hierbei nicht nur eine hohe Qualität der Übertragung von Ton und Bild, sondern – durch den Aufbau als privates Netzwerk – auch einen hohen Grad an Sicherheit.


© Cisco

Partner des HRSM-Projekts „Telepresence @ Austrian Universities“

- ACOnet
- Medizinische Universität Graz
- Medizinische Universität Innsbruck
- Medizinische Universität Wien
- Technische Universität Graz
- Universität für Bodenkultur
- Universität für Musik und darstellende Kunst Wien
- Universität Mozarteum
- Veterinärmedizinische Universität Wien

Umsetzung und Nutzung

Anfang 2017 wurde nach Vorliegen der Finanzierungszusage durch das BMBWF mit dem Aufbau der zentralen Plattform und der Integration der Endpunkte bei den Projektpartnern begonnen. Zum Einsatz kamen hierfür Komponenten aus dem Telepresence-Portfolio der Firma Cisco, da diese im Rahmen von Tests, die von der Medizinischen Universität Innsbruck bereits 2015/16 durchgeführt worden waren, bei der Integration von SIP- und H.323-Endpunkten diverser Hersteller am besten abgeschnitten hatten.

Die Plattform stellt derzeit fünf virtuelle Räume für die Abhaltung von Videokonferenzen mit insgesamt maximal 25 TeilnehmerInnen bereit. Die Einwahl in Konferenzen ist mittels SIP und H.323 von professionellen Telepresence-Endpunkten verschiedener Hersteller aus möglich. Darüber hinaus kann mittels WebRTC von jedem modernen Browser aus sowie über Telefon teilgenommen werden. Die lokalen Systeme wurden vor allem nach dem Gesichtspunkt einer möglichst einfachen Bedienung durch die EndanwenderInnen ausgewählt und konfiguriert.

Über eine Buchungsplattform, die derzeit an der Technischen Universität Graz entsteht, wird es allen universitären NutzerInnen möglich sein, einen von fünf weiteren Konferenzräumen auf der Anlage zu reservieren und für Videokonferenzen zu nutzen. Die Anmeldung am System wird dabei über die ACOnet Identity Federation erfolgen.

Aktuell wird das Telepresence-Service bereits von verschiedensten Projekten und Gruppen genutzt, wobei vorwiegend einzelne Abstimmungstreffen abgehalten werden. Darüber hinaus gibt es auch einige regelmäßige NutzerInnen, die Sitzungen oder Lab-Meetings über die Infrastruktur des Projekts abwickeln. So finden z. B. die Sitzungen des ACOnet-Lenkungsausschusses seit Ende 2017 einmal pro Monat und zum Großteil über Videokonferenz statt.

Ausblick

Derzeit entsteht eine zentrale Dokumentation für das Projekt, die, abgesehen von Informationen über das System und diversen Anleitungen, vor allem die Kompatibilität mit Endpunkten diverser Hersteller widerspiegeln soll. Mit Verfügbarkeit der Buchungsplattform ist zudem geplant, an den beteiligten Universitäten die MitarbeiterInnen über das Service breiter zu informieren.

Parallel dazu wird im Augenblick eine Integration des Systems mit der „Webex Teams“-Plattform sowie die Nutzung der dazugehörigen Endpunkte getestet. Ein solcher Zusammenschluss hätte nicht nur den Vorteil einer stärkeren Personalisierung des Service, sondern eröffnet auch neue Anwendungsgebiete wie beispielsweise die Abhaltung von Lehrveranstaltungen und Trainings.

Christoph Wild

Medizinische Universität Innsbruck
Leiter Informationstechnologie
christoph.wild@i-med.ac.at

Statistik Austria:

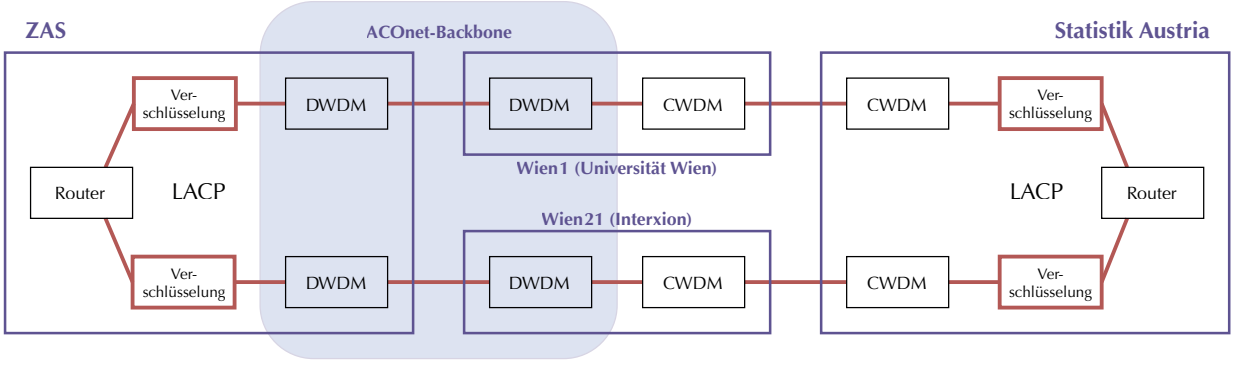
Katastrophenvorsorge via ACOnet-Backbone

Statistik Austria nutzt das Zentrale Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau seit Ende der 1970er Jahre für die Auslagerung der Datensicherung. Seit 2018 erfolgt die Datenauslagerung über eine redundante, breitbandige ACOnet-Anbindung, was den Nutzen dieser Infrastruktur drastisch erhöht.

Statistik Austria ist in Österreich für die Erstellung der amtlichen Statistik zuständig. Das bedeutet, objektive, nach wissenschaftlichen Methoden gewonnene statistische Informationen für Politik, Verwaltung, Wirtschaft, Medien und für alle BürgerInnen bereitzustellen. In dieser Rolle hat die Einhaltung der Informationssicherheit für Statistik Austria einen sehr hohen Stellenwert.

Um das Schutzziel der Verfügbarkeit gegenüber Risiken (wie beispielsweise dem Datenverlust durch Brand) abzudecken, werden seit Ende der 1970er Jahre Datenauslagerungen in das Zentrale Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau vorgenommen. Diese Datenauslagerungen erfolgten lange Zeit mittels Sicherungen auf Magnetbändern, die physisch an den Katastrophenvorsorgestandort ZAS transportiert und eingelagert wurden (dieses Verfahren ist auch unter dem Namen PTAM oder „Pickup Truck Access Method“ bekannt).

Damit im Katastrophenfall auf die Daten zugegriffen und der Betrieb kritischer Systeme gewährleistet werden kann, wurde von Statistik Austria – wie auch von anderen Institutionen der öffentlichen Verwaltung – ein gemeinsam genutztes „Cold Standby“-Mainframe-System (d. h. ein bei Bedarf manuell in Betrieb gesetzter Großrechner am ZAS) verwendet.



Akronyme: CWDM = Coarse Wavelength Division Multiplexing | DWDM = Dense Wavelength Division Multiplexing | LACP = Link Aggregation Control Protocol | ZAS = Zentrales Ausweichsystem des Bundes

Netzwerkverbindung zwischen Statistik Austria und ZAS über den ACOnet-Backbone (© Statistik Austria)

Datenauslagerung via Netzwerk

Erst als Mitte der 2000er Jahre die Bandbreite für Anbindungen via WAN („Wide Area Network“) erschwinglich wurde, konnte die Auslagerung der Datensicherung auf netzwerkbasierte Methoden umgestellt werden. Die höhere Frequenz der Datenauslagerungen und der Wegfall des physischen Transports reduzierten sowohl das RPO („Recovery Point Objective“ – der Zeitraum zwischen der letzten Datensicherung und dem Fehlerereignis) als auch den Aufwand, zumal die Manipulation und Verwaltung der Datenträger entfiel.

Aus Kostengründen war jedoch die Bandbreite begrenzt und somit ein limitierender Faktor für die Durchlaufzeit und das Volumen der Datensicherung. Auch die fehlende Redundanz hatte bei der Wartung der Netzwerkverbindung einen direkten Einfluss auf die Durchführung der Datenauslagerung und daher auch auf das RPO.

Aktuelle Anbindung

Mit dem Ausbau des ACOnet-Backbones im Jahr 2017 boten sich neue Möglichkeiten, das Rechenzentrum von Statistik Austria und den Katastrophenvorsorgestandort netzwerkmäßig zu verbinden: ACOnet-Teilnehmer haben die Möglichkeit, zwischen zwei Backbone-Standorten eine dedizierte (private) Punkt-zu-Punkt-Verbindung über DWDM („Dense Wavelength Division Multiplexing“) mit einer Bandbreite von 10 Gbit/s oder 100 Gbit/s zu nutzen – und das ZAS war nun ein vollwertiger ACOnet-Standort.

Um das aktuelle Datenaufkommen, das geplante Wachstum und eine Erhöhung der Verfügbarkeit abzudecken, wurden für Statistik Austria zwischen Wien und St. Johann im Pongau zwei wegeredundante Punkt-zu-Punkt-Verbindungen mit jeweils 10 Gbit/s Bandbreite realisiert (siehe Grafik auf Seite 48). Die Anbindung des Rechenzentrums von Statistik Austria an die beiden ACOnet-Standorte Wien1 (Universität Wien) und Wien21 (Interxion) erfolgt mittels CWDM („Coarse Wavelength Division Multiplexing“). Diese CWDM-Verbindungen übertragen neben der 10 Gbit/s-Datenverbindung für den Standort ZAS auch den Internet-Uplink von ACOnet sowie andere Services.

Netzwerkverschlüsselung

Die Datenverbindung zum ZAS läuft sowohl über den ACOnet-Backbone als auch über gemietete WAN-Leitungen. Daher ist auch hier das Informationssicherheitsschutzziel der Vertraulichkeit zu gewährleisten. Um ein Abhören des Datenverkehrs zu verhindern, wurde die etablierte Netzwerk-Verschlüsselungsinfrastruktur auf die beiden redundanten 10 Gbit/s-Verbindungen erweitert. Die zwei verschlüsselten Verbindungen sind mittels LACP („Link Aggregation Control Protocol“) zu einem Port Channel zusammengefasst und bilden eine sichere und hochverfügbare Netzwerkverbindung zwischen den Standorten in Wien und dem ZAS. Die Umsetzung dieser redundanten Netzwerkverbindungen erfolgte im zweiten Halbjahr 2018.

Fazit

Die Nutzung der neuen Backbone-Infrastruktur von ACOnet brachte für Statistik Austria eine Erhöhung der Bandbreite sowie eine höhere Ausfallsicherheit der Verbindungen aufgrund der wegeredundanten Streckenführung – ohne Einbußen im Bereich der Vertraulichkeit. Durch die Steigerung der Redundanz können die am Standort ZAS für die Katastrophenvorsorge verfügbaren Infrastruktur-Komponenten nun besser genutzt werden. Auch finanziell ist diese Lösung sehr attraktiv: Trotz einer Steigerung der Bandbreite um den Faktor 10 liegt die Amortisationszeit unter einem Jahr.

Richard Plasun

Statistik Austria / IT-Abteilung
Stellvertretender IT-Leiter
richard.plasun@statistik.gv.at

Missbräuchliche Nutzung des Tor-Netzwerks

Das Institut für Netzwerke und Sicherheit (INS) betreibt an der Johannes Kepler Universität in Linz einen Tor Exit-Knoten und untersucht, wie dieser genutzt wird. Im letzten Jahr wurde spezifisch der DNS-Traffic analysiert und nach verschiedenen Aspekten ausgewertet – z. B. dahingehend, ob es nationale Unterschiede gibt (ja, gibt es) und wie es mit missbräuchlicher Nutzung aussieht. Dieser Beitrag berichtet über den zweiten Punkt: Malware bzw. Angriffe über (aber nicht auf) Tor Exit-Knoten.

Das INS untersuchte 2018 an seinem Tor Exit-Knoten insbesondere die Nutzung von DNS. Hintergrund ist, dass DNS-Abfragen („Welche IP-Adresse gehört zu welchem Domainnamen?“) in jedem Fall unverschlüsselt erfolgen und genauer sind als eine bloße Untersuchung der Ziel-IP-Adressen. Die Daten wurden über einen separaten DNS-Server aufgezeichnet, um das Caching beeinflussen zu können und um die DNS-Anfragen vom Eingangs- bzw. Ausgangs-Datenverkehr strikt zu trennen.

Untersuchungen & Ergebnisse

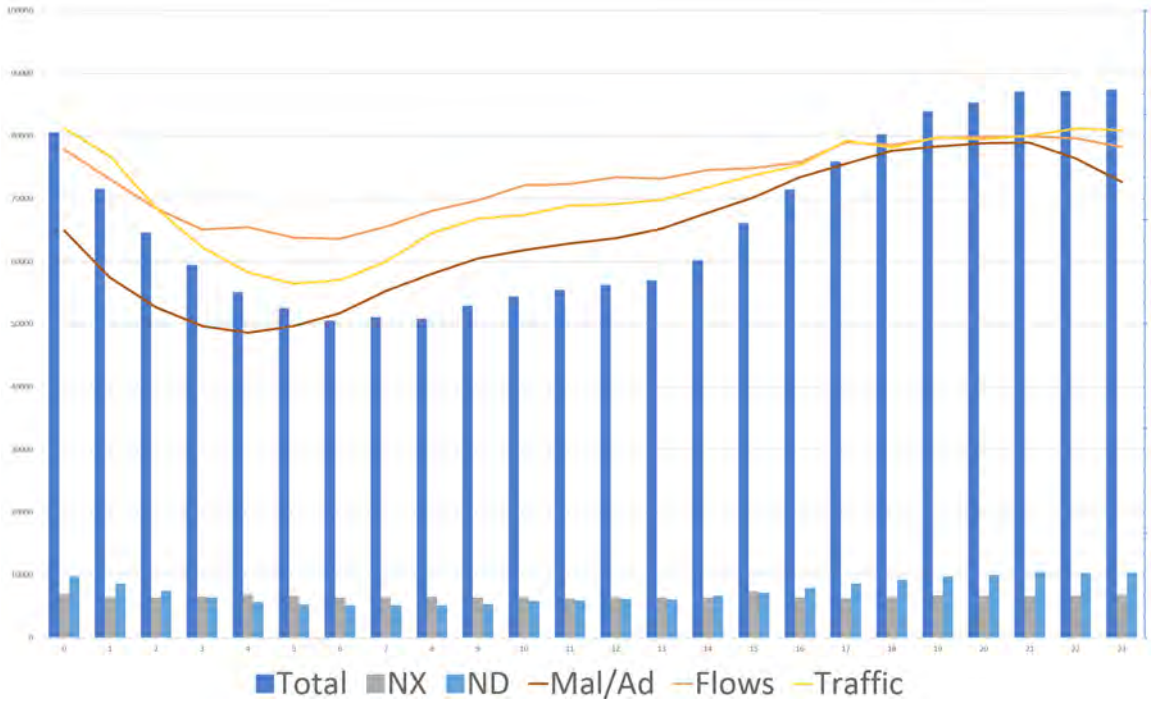
Festgestellt wurde z. B. **Reverse DNS Scanning**, also die systematische Abfrage, ob zu ganzen Subnetzen Domainnamen existieren. Konkret betraf dies drei spanische Universitäten sowie die spanische Post. Hierbei handelte es sich jeweils um /16-Subnetze, die binnen kürzester Zeit (fast) vollständig abgefragt wurden. Dass es sich tatsächlich um einen Scan handelte, war daraus abzulesen, dass sich die Datenmenge und die Anzahl der Verbindungen nicht von anderen Tagen unterschied. Für einen Angreifer bringt die Nutzung von Tor hier den üblichen Vorteil, dass seine IP-Adresse geheim bleibt (nachdem diese Institutionen ihre DNS-Server selbst betreiben, fällt ein derartiger Scan vermutlich auf und könnte somit zu Gegenmaßnahmen führen).

Ebenso konnten **direkte DNS-Scans** nachgewiesen werden, wobei hier anscheinend automatisiert und nach Wortlisten vorgegangen wird. Da sich trotz einer sehr großen beobachteten Zahl kein allgemeines Muster ergibt, kann vermutet werden, dass solche Scans (im Gegensatz zu den Reverse-Scans) über mehrere Exit-Knoten hinweg erfolgen. Neben den Scans werden auch sehr viele Fehler offenbar, wie Domainnamen, die nicht mehr existieren („geo.mozilla.org“) oder einfach fehlerhaft

Das Tor-Projekt der JKU

Tor ist ein Anonymisierungsnetzwerk, das es erlaubt, die eigene IP-Adresse beim Websurfen oder anderen Tätigkeiten im Internet zu verschleiern, indem jede Verbindung über drei (häufig wechselnde und idealerweise in verschiedenen Ländern befindliche) Server geleitet wird. Zudem werden alle Inhalte innerhalb des Tor-Netzwerks verschlüsselt übertragen.

Seit 2015 betreibt das INS an der Johannes Kepler Universität (JKU) in Linz einen Tor Exit-Knoten zu Forschungszwecken, der bereits im ACOnet Jahresbericht 2017 näher vorgestellt wurde. ACOnet unterstützt das Projekt, indem es die benötigte Bandbreite kostenlos zur Verfügung stellt. Das Forschungsprojekt wurde kürzlich bis Ende 2019 verlängert. Mehr Informationen dazu finden Sie unter: **https://ins.jku.at/infrastructure/tor-exit-node**



Tageszeitliche Verteilung des Datenverkehrs am Tor Exit-Knoten der JKU Linz (© JKU / INS)
NX = nicht existierend | ND = No-Data | Die Linien sind individuell skaliert und entsprechen daher nicht der linken Skala.

sind (z. B. „index.php“ oder „web.archive.orghttp“). Teilweise handelt es sich auch um normale Vorgänge, etwa wenn aussschließlich IPv4-DNS-Einträge verfügbar sind, aber nach IPv6 gefragt wird (was nebenbei auch die Verwendung von IPv6 nachweist). Beispielsweise wird durchschnittlich 7400-mal pro Tag nach der IPv6-Adresse von „e13829.x.akamaiedge.net“ gefragt – für diesen Rechner existieren jedoch nur IPv4-Einträge, was „No-Data“-Antworten erzeugt.

Über eine **Untersuchung des zeitlichen Ablaufs** konnte festgestellt werden, dass die fehlerhafte Benutzung (No-Data: ND) „normal“ zu sein scheint in dem Sinne, dass sie zur normalen Nutzung synchron läuft (viel Datenverkehr → viele Fehler, siehe Abbildung oben). Demgegenüber sind die Scans (nicht existierend: NX) von der Tageszeit unabhängig. Die Besuche von Ad-/Malware-Sites entsprechen wiederum ungefähr der tageszeitlichen Verteilung.

Eine weitere Untersuchung erfolgte auf Basis einer populären **Blacklist für Ad-/Malware**. Obwohl diese Liste (https://github.com/StevenBlack/hosts) „nur“ ca. 60.000 Einträge besitzt, sind 5,1 % aller DNS-Anfragen darauf zu finden. Dies kann unter Umständen damit erklärt werden, dass hauptsächlich ansonsten gesperrte Websites über Tor besucht werden bzw. dass diese Liste auch Werbetracker umfasst, welche sehr oft Einsatz finden.

Wie schon in früheren Untersuchungen festgestellt, fand auch eine Vielzahl von **Whois-Abfragen** statt (ca. 4400 Anfragen pro Tag nach „whois.*“). Der Grund hierfür ist immer noch unklar und könnte wahrscheinlich nur über die Untersuchung des Inhalts der Verbindungen („Nach welchen Domainnamen wird gefragt?“) eruiert werden. Dies ist aber rechtlich jedenfalls verboten. Unter Umständen wird die Zahl derartige Anfragen in Zukunft sinken, da aufgrund der Datenschutz-Grundverordnung (DSGVO) bei vielen Providern die öf-

fentlich ohne individuelle Begründung abrufbaren Angaben im Whois enorm reduziert wurden.

Über eine Offline-Klassifikation mittels Shalla's Blacklists (Online-Klassifikationsdienste kamen aus Datenschutzgründen nicht in Frage) wurde auch versucht, sich der **Legalität der Tor-Nutzung** anzunähern. Hierbei konnten wir feststellen, dass ein sehr großer Anteil höchstwahrscheinlich legale Nutzung darstellt (siehe Tabelle unten) – allerdings konnten nur ca. 10 % der DNS-Anfragen auch entsprechend klassifiziert werden.

DNS-Anfragen nach Kategorien

Kategorie	Anzahl	Anteil
Porn	3.400.700	14,30 %
Socialnet	3.001.751	12,60 %
Shopping	2.765.896	11,60 %
Adv	2.074.556	8,71 %
News	2.063.338	8,55 %
Forums	1.504.763	6,32 %
Movies	1.385.006	5,82 %
Tracker	1.339.224	5,62 %
Searchengine	1.264.996	5,31 %
Imagehosting	797.450	3,35 %
Downloads	637.854	2,68 %
ISP	520.920	2,19 %
Chat	355.395	1,49 %
Government	352.259	1,48 %
Webmail	239.451	1,01 %
Rest		8,87 %

Eindeutig „problematische" Domains kommen in dieser Liste erst sehr weit unten vor:

- Downloads ..... 2,68 %
  (vieles davon könnte urheberrechtswidrig sein)
- Spyware ..... 0,82 %
- Warez ..... 0,81 %
- Gamble ..... 0,49 %
- Hacking ..... 0,08 %
- Drugs ..... 0,07 %

Der letzte Punkt „Drogen" umfasst in Summe 15.924 (von insgesamt rund 238 Millionen) DNS-Anfragen in einem Zeitraum von 5 Monaten – wovon nicht alle, aber wohl zumindest der Großteil illegale Inhalte oder Geschäfte betreffen dürfte.

Zusammenfassung

Wie den Ergebnissen zu entnehmen ist, kommt Missbrauch im Tor-Netzwerk vor. Dies war jedoch zu erwarten.

Demgegenüber konnte ebenso festgestellt werden, dass ein sehr großer Teil höchstwahrscheinlich legale Inhalte betrifft. Hier ist insbesondere hervorzuheben, dass der Ausspruch „The Internet is for Porn" zwar noch stimmt, da dies die häufigste Kategorie ist – aber nur sehr knapp: Soziale Netzwerke und Shopping folgen unmittelbar danach.

Dies konnte auch mit (hier nicht dargestellten) Auswertungen mit Fokus auf einzelne Ziel-Länder validiert werden: In manchen Ländern scheinen Soziale Netzwerke sowie Kommunikationsdienste eine besonders große Rolle zu spielen. Anonymität ist somit auch bei „normaler" Betätigung für viele Personen sehr wichtig.

Michael Sonntag

Johannes Kepler Universität Linz
Institute of Networks and Security
michael.sonntag@ins.jku.at

Das Kooperationsprojekt „Supercomputer MACH-2“

MACH-2 ist ein Hochleistungsrechner, der von der Johannes Kepler Universität (JKU) Linz betrieben wird. Ein Konsortium österreichischer Universitäten und Forschungseinrichtungen greift auf diese Maschine im Rahmen eines Kooperationsprojekts über das ACOnet zu. MACH-2 wurde 2018 in Betrieb genommen und stellt einen der weltweit größten Rechner mit gemeinsamem Speicher dar.

MACH-2 ist der Nachfolger des (nach dem österreichischen Physiker und Philosophen Ernst Mach benannten) Supercomputers MACH, der von der JKU Linz und der Universität Innsbruck von 2011 bis 2017 gemeinsam finanziert und betrieben wurde. Für die Nachbeschaffung der in die Jahre gekommenen Maschine und den zukünftigen Betrieb wurde der Benutzerkreis im Jahr 2016 auf ein österreichweites Konsortium erweitert.

Das Projekt

Das Konsortium „Supercomputer MACH-2“ umfasst die JKU Linz, die Universität Innsbruck, die Paris Lodron Universität Salzburg, die Technische Universität Wien und das Johann Radon Institute for Computational and Applied Mathematics (RICAM) der Österreichischen Akademie der Wissenschaften (ÖAW). Die Anschaffung wurde durch das Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) im Rahmen eines von 2017 bis 2021 laufenden HRSM-Projekts finanziert (HRSM = Hochschulraum-Strukturmittel). Die Kosten für den laufenden Betrieb werden durch die teilnehmenden Partner selbst getragen.

Die Maschine wird vom Team für Wissenschaftliches Rechnen am JKU Informationsmanagement (= Zentraler Informatikdienst der JKU) betrieben. Sie wurde im Herbst 2017 installiert und ging mit Anfang 2018 offiziell in Betrieb. Der Zugriff auf MACH-2 erfolgt via ACOnet; die Nutzung durch die Projektpartner erfolgt nach dem „Fair Use“-Prinzip entsprechend der Beteiligung an den Betriebskosten. Im Rahmen von Kooperationen mit den Konsortialpartnern können auch andere akademische Einrichtungen diese Maschine nutzen. Insbesondere ist dies durch einen Kooperationsvertrag zwischen der JKU Linz und der TU Wien auch den Mitgliedern des Vienna Scientific Cluster (VSC) möglich.

Systemarchitektur

Die meisten Hochleistungsrechner sind Cluster von über ein Netzwerk lose verbundenen Knoten, bei denen jedes parallele Programm so auf Prozesse aufgeteilt werden muss, dass jeder Prozess nur auf den Speicher seines Knotens zugreift und damit auskommt. Die Kommunikation zwischen auf verschiedenen Knoten laufenden Prozessen erfolgt über den – vergleichsweise langsamen – Versand von Nachrichten (Prinzip des „Distributed Memory“, des verteilten Speichers). Für die Verwendung von Cluster-Architekturen müssen daher mittels spezieller Programmiermodelle (z. B. dem „Message Passing Interface“ MPI) entsprechende Programme entwickelt werden.

Im Gegensatz dazu ist MACH-2 eine Maschine vom Typ „Non-Uniform Memory Access“ (NUMA), bei der eine Kombination von Hardware und Software-Mechanismen einen über alle „Blades“ (siehe Kasten auf Seite 54) verteilten Adressraum realisiert – also einen einzigen großen virtuellen Speicher, auf den alle Prozesse gemeinsam Zugriff

JOHANNES KEPLER UNIVERSITÄT LINZ

TECHNISCHE UNIVERSITÄT WIEN

universität innsbruck

RICAM
JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS

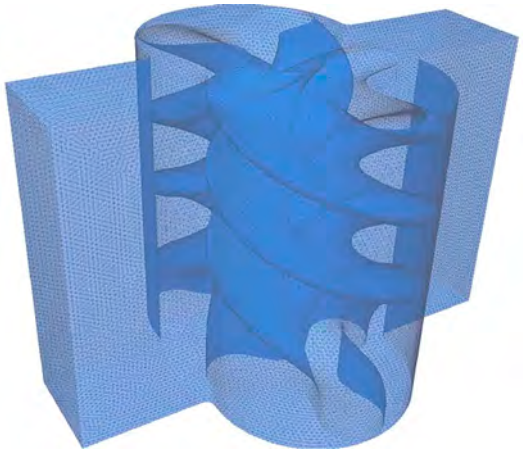
UNIVERSITÄT SALZBURG

Bundesministerium
Bildung, Wissenschaft
und Forschung

MACH-2

- Der Supercomputer MACH-2 ist eine Maschine vom Typ „**SGI UV 3000**“ des früheren Herstellers Silicon Graphics International (SGI), jetzt Hewlett Packard Enterprise (HPE).
- Es handelt sich um ein Bladesystem, bestehend aus 3 Schränken („Racks“ – siehe Foto) mit insgesamt **72 Einschubplatinen („Blades“)**.
- Jede Blade umfasst 2 Prozessoren vom Typ **Intel Xeon E5-4650V3** mit jeweils 12 Rechenkernen („Cores“).
- 64 Blades sind mit **je 256 GB** Speicher, 8 weitere Blades mit **je 512 GB** Speicher ausgerüstet.
- Insgesamt umfasst der Supercomputer damit **1728 Rechenkerne und 20 Terabyte Speicher**.
- In Bezug auf Rechenkerne und Speichergröße ist MACH-2 **eine der weltweit größten Installationen** dieser Architekturklasse.
- Die Maschine erreicht eine maximale Leistung („Peak Performance“) von **77,4 TeraFLOPS**.
- Sie ist mit **verschiedenen Datenspeicherlösungen und Netzwerkanbindungen** ausgestattet.

Foto: Der Hochleistungsrechner MACH-2
(© JKU / Johann Messner)



Grafik: Berechnung von Raum-Zeit-Finite-Elemente-Methoden auf MACH-2
Details siehe https://www3.risc.jku.at/projects/mach2/use/langer/

(© JKU / Ulrich Langer)

haben (Prinzip des „Shared Memory“, des gemeinsamen Speichers). Während auch hier der Zugriff auf den Speicher anderer Blades notwendigerweise etwas langsamer erfolgt als der auf den lokalen Speicher (die Zugriffszeiten sind also „non-uniform“), sind mit der bei MACH-2 verwendeten proprietären Verbindungstechnologie NUMALINK „enger gekoppelte“ Programme möglich als mit den vergleichsweise „lose gekoppelten“ Cluster-Architekturen. Insbesondere ist auch die effektive Nutzung von Programmierparadigmen möglich, die auf der Kommunikation über gemeinsamem Speicher beruhen (automatische Parallelisierung in Fortran und C, OpenMP, Multithreading in C, C++, Java, Python etc.).

Verwendung

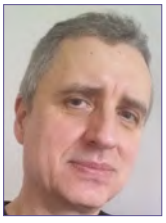
Aus Sicht der AnwenderInnen stellt sich der Supercomputer im Wesentlichen wie ein herkömmlicher (unter dem Betriebssystem Linux) laufender Rechner dar: Auf MACH-2 stehen alle bekannten Linux-Anwendungen zur Verfügung. Insbesondere ist auch die einfache Nutzung weitverbreiteter mathematischer, technischer und naturwissenschaftlicher Softwarepakete (MATLAB, Mathematica, Maple, SageMath, ...) möglich. Diese können somit von einer großen Anzahl von Rechenkernen und einem großen Speicher profitieren, ohne speziell adaptiert werden zu müssen. Die Zuteilung der Maschinen-Kapazität erfolgt durch das Lastverteilungssystem PBSPro, mit dem sich die NutzerInnen für die Ausführung einer interaktiven Sitzung oder eines nicht-interaktiven Rechenjobs einen Teil der Maschine reservieren können. Nach Voranmeldung sind auch Berechnungen möglich, die die Ressourcen der gesamten Maschine nutzen.

Die NUMA-Architektur von MACH-2 zielt auf das „Capability Computing“ ab (die möglichst schnelle Lösung eher schwer zu verteilender Probleme). Sie stellt damit eine komplementäre Ergänzung der Cluster-Architekturen dar, die mehr auf „Capacity Computing“ ausgerichtet sind (die möglichst kosteneffektive Lösung vergleichsweise leicht zu verteilender Probleme). So bietet zwar das aktuelle VSC-3-System des Vienna Scientific Cluster um eine Größenordnung mehr Rechenkerne (32320) als MACH-2 (1728); MACH-2 kann aber einem Prozess um zwei Größenordnungen mehr Speicher (20480 GB globaler Speicher) zur Verfügung stellen als VSC-3 (64 GB lokaler Speicher pro Knoten). Dies macht die Verwendung von MACH-2 auch für nicht-parallele, aber speicherintensive Anwendungen interessant.

MACH-2 unterstützt eine Vielzahl von Programmiermodellen und Softwarepaketen und wird von den Projektpartnern für zahlreiche Anwendungen aus den verschiedensten Wissenschaftsbereichen verwendet. Neben den vorrangig die Maschine nutzenden naturwissenschaftlichen, technischen und mathematischen Feldern (Physik, Chemie, Biologie, Neurowissenschaften, Numerische und Symbolische Mathematik, Statistik, Künstliche Intelligenz, …) finden sich, begünstigt durch die vergleichsweise einfache Nutzung von MACH-2, auch Anwendungen aus anderen Disziplinen (Ökonometrie, Produktionsmanagement, Logistik, …).

Details

Weitere Informationen finden Sie auf der Webseite **https://www3.risc.jku.at/projects/mach2/**, die insbesondere auch den Prozess der Beantragung von Nutzerkennungen erklärt, den Zugriff auf die Maschine beschreibt sowie deren aktuelle Auslastung anzeigt.



Wolfgang Schreiner

JKU Linz / Research Institute for Symbolic Computation (RISC)
Projektkoordinator „MACH-2“
wolfgang.schreiner@risc.jku.at

Impressum

Universität Wien
Zentraler Informatikdienst
Abteilung ACOnet & VIX
Universitätsstraße 7
1010 Wien, Österreich

www.aco.net
admin@aco.net
+43-1-4277-14030

ISSN: 2616-7972

Redaktion & Gestaltung: Elisabeth Zoppoth
Druck: Onlineprinters GmbH

GastautorInnen

Wir danken den folgenden Personen für ihre Beiträge zu diesem Jahresbericht:

- Josef Zechner, Montanuniversität Leoben
- Raman Ganguly, Universität Wien
- Claudia Blaas-Schenner, VSC Research Center
- Christoph Wild, Medizinische Universität Innsbruck
- Richard Plasun, Statistik Austria
- Michael Sonntag, Johannes Kepler Universität Linz
- Wolfgang Schreiner, Johannes Kepler Universität Linz

Fotocredits

Cover: © Peter Wienerroither | Seite 5: © Matthijs Mekking | Seite 8: © ACOnet | Seite 10/11: © Michael Perzi | Seite 12 (unten): © Michael Perzi | Seite 16–18: © ZID/NOC der Montanuniversität Leoben | Seite 20–23: © ACOnet | Seite 26: © Natascha Eibl | Seite 30: © Stockwerk-Fotodesign – Fotolia | Seite 31–32: © Joseph Krpelan | Seite 33 (Grafik): © atabik1 – Fotolia | Seite 35 (Foto Dellago): © Universität Wien / Barbara Mair | Seite 35 (Foto Ostermann): © Universität Innsbruck | Seite 35 (Grafik): © PRACE | Seite 43: © Gerard Spee | Seite 47: © Cisco | Seite 48: © Statistik Austria | Seite 51: © JKU / INS | Seite 54: © JKU / Johann Messner | Seite 55 (Grafik): © JKU / Ulrich Langer

Kontakt:

Universität Wien
Zentraler Informatikdienst
Abteilung ACOnet & VIX
Universitätsstraße 7
1010 Wien, Österreich

www.aco.net
admin@aco.net
+43-1-4277-14030

ISSN: **2616-7972**

universität wien