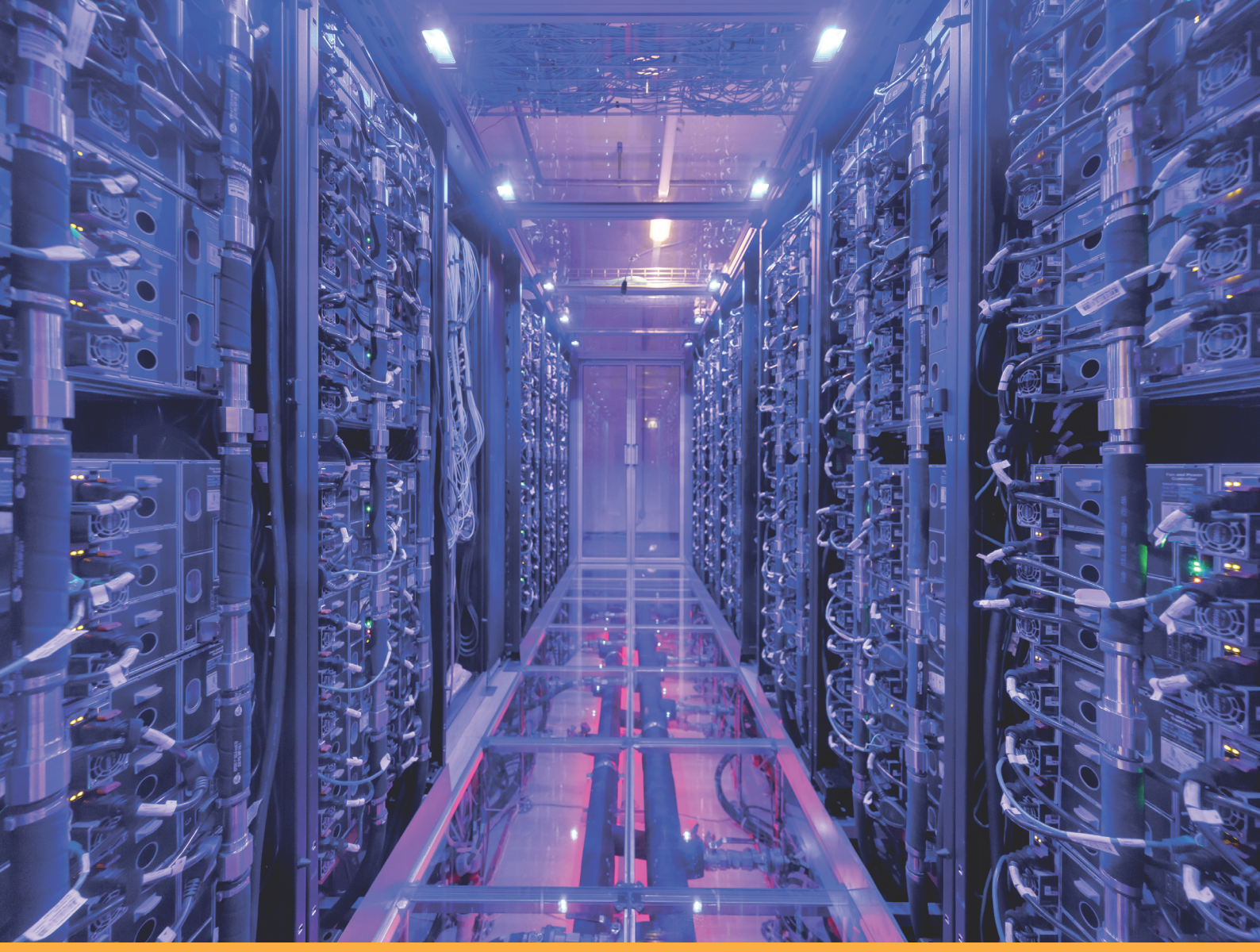


aconet

Austrian Academic Computer Network

2019

JAHRESBERICHT

Cover: Der Supercomputer VSC-4 (© derknopfdruecker.com)

ACOnet Jahresbericht

2019

www.aco.net | www.vix.at

Inhalt

Vorwort

Liebe Leser*innen!

Haben Sie es schon bemerkt? Seit Ende 2019 gilt an der Universität Wien eine neue Leitlinie für den geschlechterinklusiven Sprachgebrauch. Diese Leitlinie empfiehlt die Verwendung des Gendersterns in allen Fällen, wo eine geschlechtsneutrale Formulierung (wie z. B. „Studierende“) nicht möglich ist. Wir schließen uns dieser Regelung unseres Rechtsträgers an, verwenden in diesem Jahresbericht erstmals den Genderstern anstelle des Binnen-I und werden unsere Websites und sonstigen Publikationen sukzessive anpassen. Da unsere Redakteurin das (nicht geregelte) Gendern juristischer Personen entschieden ablehnt, wird es auch künftig keine „ACOnet-Teilnehmer*innen“ geben, „Kursteilnehmer*innen“ hingegen schon.

Eine weitere Besonderheit des vorliegenden Jahresberichts ist sein spätes Erscheinen: Die wenigen Lücken, die zu Beginn des COVID-19-Lockdowns Mitte März 2020 noch zu füllen waren, blieben in der nachfolgenden Ausnahmesituation noch lange offen. Wir bitten (insbesondere alle Autor*innen, die ihre Beiträge für diesen Jahresbericht bereits vor Monaten geschrieben haben) um Verständnis für diese unerwartete Verzögerung und hoffen, dass Sie uns dennoch gewogen bleiben!

Doch zurück ins Jahr 2019:

Der ACONET-Verein hat im Mai 2019, nach Ablauf der üblichen zweijährigen Funktionsperiode, einen neuen Vereinsvorstand gewählt (mehr dazu auf Seite 9). Angesichts der 2022 bevorstehenden Änderungen im Backbone-Bereich befasst sich dieser Vereinsvorstand in seiner Rolle als ACOnet-Lenkungsausschuss nun intensiv mit strategischen Überlegungen zur künftigen Positionierung und Weiterentwicklung unseres Wissenschaftsnetzes (Näheres siehe Seite 21).

Über unsere Aktivitäten im Jahr 2019 berichten wir in den Rubriken Netzwerk, Services und Community. Besonders hervorheben möchte ich hier den Artikel „Gute Manieren im Netz“ (Seite 22) über eine Initiative zur Vermeidung von Datenmüll im Netzwerk, bei der die Unterstützung unserer Teilnehmerorganisationen sehr willkommen wäre.

Kunst & Kultur im ACOnet

Gute Neuigkeiten gibt es auch im Kulturbereich: Das von ACOnet ins Leben gerufene „net:art coordination center“ hat dank einer finanziellen Unterstützung der Firma Kapsch 2019 eine neue Website erhalten. Unter **www.netart.cc** sind nun die Dokumentationen der bisherigen net:art-Produktionen, Infos zu aktuellen Projekten und vieles andere zum Thema „performing arts over advanced networks“ gesammelt abrufbar (siehe Seite 39).

Die breite Vernetzung, die das net:art coordination center im internationalen Bereich auszeichnet, wird im nationalen Umfeld unter dem Namen KUKIT (Kunst, Kultur & IT) gepflegt. Aus dem regelmäßig veranstalteten „KUKIT-Stammtisch“ ist im Jahr 2019 wieder ein hochinteressantes Projekt entstanden: eine XML-Schnittstelle, die die Abwicklung von Ticketverkäufen zwischen Ticketanbietern (z. B. Museen) und Resellern (z. B. Reisebüros) stark vereinfachen soll – mehr dazu auf Seite 46.

aconet
Austrian Academic Computer Network

Neue Teilnehmer

2019 durften wir fünf neue ACOnet-Teilnehmer, zwei neue GovIX-Teilnehmer und ein neues Mitglied des ACONET-Vereins in unserem Kreis begrüßen. Einer der neuen ACOnet-Teilnehmer – die Silicon Austria Labs GmbH – hat sich dankenswerterweise sogleich bereit erklärt, sein breit gefächertes Forschungsportfolio in unserem Jahresbericht kurz zu präsentieren (siehe Seite 44). Ein großes Danke auch an alle anderen Gastautor*innen!

Über Wolken

Gleich zwei der diesjährigen Gastbeiträge handeln von Clouds: Auf Seite 48 erfahren Sie Näheres über die Cloud-Strategie der Universität Wien. Im Anschluss daran befasst sich der erste englischsprachige Artikel in einem ACOnet Jahresbericht eingehend mit der European Open Science Cloud (EOSC). Die EOSC-Strategie soll dafür sorgen, dass Forschungsdaten aus EU-geförderten Projekten für eine weitere Nutzung verfügbar sind. Dazu sollen europaweit bereits bestehende Infrastrukturen zusammengeführt werden. Der Beitrag „Developing EOSC“ (Seite 50) schildert die Strukturen und den Status dieses komplexen Unterfangens.

Über ein drittes Thema aus dem Cloud-Bereich wird erst im Jahresbericht 2020 gebührend berichtet werden: Das OCRE-Projekt (Open Clouds for Research Environments, **https://ocre-project.eu**) kann als Nachfolger der „IaaS Cloud Services Framework“-Ausschreibung von GÉANT betrachtet werden, deren Rahmenverträge Ende 2020 auslaufen. Die OCRE-Rahmenverträge werden nicht nur Angebote zu Infrastructure as a Service (IaaS) umfassen, sondern auch Angebote zu Platform as a Service (PaaS) und Software as a Service (SaaS), in weiterer Folge auch spezielle Angebote von und für „Earth Observation Services“. Die intensiven Vorarbeiten im Rahmen des OCRE-Projekts mündeten in einer ersten Ausschreibungsveröffentlichung im April 2020. Die ersten OCRE-Rahmenverträge sollen ab Anfang 2021 verfügbar sein.

Personelles

Marcel Grünauer hat sich nach vielen Jahren im Team der Internet Domain Administration entschlossen, ab Mai 2019 neue Wege zu gehen, und Badran Farwati hat von September 2019 bis Februar 2020 das ACOnet-CERT-Team unterstützt. Wir bedanken uns für die gute Zusammenarbeit und wünschen beiden Kollegen alles Gute!

Wie immer möchte ich mich an dieser Stelle bei meinen Mitarbeiter*innen sowie bei der gesamten ACOnet-Community für ihren Einsatz und ihre Kooperationsbereitschaft herzlich bedanken.

Und nun wünsche ich Ihnen eine interessante Lektüre. Bleiben Sie gesund!

Christian Panigl

Abteilungsleiter ACOnet & VIX

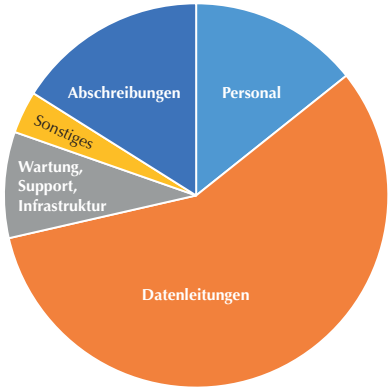
Über ACOnet

Zahlen, Daten, Fakten

ACOnet-Teilnehmeranschlüsse gesamt (Stand 31. Dezember 2019)	**245**
• Akademische Organisationen (35 Universitäten, 19 Fachhochschulen, 11 sonstige Bildungseinrichtungen)	65
• Studierendenheimträger (mit insgesamt 131 an ACOnet angebundenen Studierendenheimen)	55
• Einrichtungen der öffentlichen Verwaltung	34
• Forschungseinrichtungen	33
• Kulturorganisationen	15
• Regionale EDUnet-Teilnehmer	9
• Gesundheitsinstitutionen	6
• Sonstige	28
davon:	
• **ACONET-Vereinsmitglieder**	**41**
• **GovIX-Teilnehmer**	**34**
Backbone-Standorte	**20**
Glasfaser in km	**3300**

Finanzielle Kennzahlen in Mio. € (Stand 26. März 2020)	**2018**	**2019**
+ Erlöse	**6,2**	**6,4**
– Aufwendungen	**5,9**	**5,6**
• Personal	0,8	0,8
• Datenleitungen	3,5	3,2
• Wartung, Support, Infrastruktur	0,5	0,5
• Sonstiges	0,2	0,2
• Abschreibungen	0,9	0,9
= Ergebnis	**0,3**	**0,8**
Anlagenanschaffungen	**0,0**	**0,3**

Aufwendungen 2019



Das ACOnet-Budget ergibt sich aus den Erlösen aus Nutzungsvereinbarungen mit den ACOnet-Teilnehmerorganisationen. Das Ergebnis wird einer Rücklage zugebucht, die zweckgebunden für ACOnet verwendet wird.

ACONET-Verein:

Neuer Vereinsvorstand

Für die Funktionsperiode 2019–2021 wurde im vergangenen Mai ein neuer ACONET-Vereinsvorstand gewählt. Die bisherige Vorstandsvorsitzende Brigitte Haidl und ihr Stellvertreter Florin Guma wurden von Bernd Logar (TU Wien) und Andreas Schildberger (Universität für Bodenkultur Wien) abgelöst.

Am 28. Mai 2019 wurde die 17. Mitgliederversammlung des ACONET-Vereins mit Vorstandswahlen abgehalten. Der ACONET-Vereinsvorstand wird jeweils für eine Funktionsperiode von zwei Jahren gewählt und fungiert auch als Lenkungsausschuss für den ACOnet-Betrieb.

Brigitte Haidl (Medizinische Universität Wien), Vorstandsvorsitzende seit 2013, stand ebenso wie ihr Stellvertreter Florin Guma (Universität Salzburg) für eine Wiederwahl nicht mehr zur Verfügung. Der ACONET-Verein dankt beiden für ihr Engagement und ihre wertvolle Mitarbeit im Lenkungsausschuss und wünscht ihnen das Beste für ihre Zukunft!

Der neue Vereinsvorstand setzt sich nun wie folgt zusammen:

Vorstandsvorsitzender:	**Bernd Logar**
Vorstandsvorsitzender-Stv.:	**Andreas Schildberger**
Kassier:	**Maximilian Sbardellati**
Kassier-Stv.:	**Petra Karlhuber**
Schriftführer:	**Michael Redinger**
Schriftführer-Stv.:	**Christoph Wild**

Andreas Schildberger muss hier wohl nicht näher vorgestellt werden: Er ist seit 1993 an der Universität für Bodenkultur Wien beschäftigt und leitet die BOKU-IT seit 2007, ist im ACOnet-Umfeld also bestens bekannt.

Anders verhält es sich beim neuen Vorstandsvorsitzenden: Bernd Logar ist seit April 2017 CIO der TU Wien und begleitet seit April 2019 als Leiter des .digital office die digitale Transformation der TU Wien. Davor war er rund 20 Jahre lang bei global agierenden IT-Dienstleistern in verschiedenen Rollen tätig – zuletzt bei NTT DATA. Bernd Logar sieht seinen persönlichen Schwerpunkt im Verein darin, die rasch voranschreitende Digitalisierung in Forschung und Lehre an den teilnehmenden österreichischen Forschungs- und Bildungseinrichtungen durch innovative und integrative ACOnet-Projekte prägend zu unterstützen.

Die Schwerpunkte des neuen Vereinsvorstands liegen unverändert in der strategischen Ausrichtung von ACOnet und der Vorbereitung der Backbone-Erneuerung im Jahr 2022 (mehr dazu auf Seite 21).


Bernd Logar


A. Schildberger


M. Sbardellati


Petra Karlhuber


Michael Redinger


Christoph Wild

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
Bauer Kurt	Identity Federation, Zertifikatsservice, Netzwerk- und Server-Betrieb
Cravos Romana	Projektmanagement, Eventmanagement (Peering Days)
Genser Christoph	Webentwicklung, Öffentlichkeitsarbeit
Perzi Michael	LIR, Teilnehmeradministration, Netzwerk- und Server-Betrieb

v. l. n. r.: Christian Panigl | Kurt Bauer | Erwin Rennert | Michael Perzi | Romana Cravos | Christoph Genser |

Radulescu Liviu-Radu	Softwareentwicklung
Rennert Erwin	Netzwerk-Betrieb
Schneider Monika	Netzwerk-Betrieb
Schober Peter	Identity Federation, Server-Betrieb
Stadlmann Tina	Assistenz
Wein Robert	Monitoring, Netzwerk- und Server-Betrieb

Freie Mitarbeiter*innen:

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

| Robert Wein | Peter Schober | Tina Stadlmann | Monika Schneider | Elisabeth Zoppoth | Harald Michl

ACOnet-CERT

Alexander
Talos-Zens

Christoph
Campregher

Badran Bacha
Farwati

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
Farwati Badran Bacha	CERT-Betrieb (ab 2. September 2019)
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
Ferra-Reicher Markus	Monitoring und Datenvisualisierung
Grünauer Marcel	Software- und Systementwicklung (bis 30. April 2019)
Heimhilcher Markus	DNS-Administration
Hofstetter Mark	Software- und Systementwicklung
Hörtnagl Christian	Systemadministration
Papst Andreas	Projektmanagement
Reutner-Fischer Bernhard	Software- und Systementwicklung
Schmidt David	Software- und Systementwicklung
Stasic Arsen	ACOnet-Services, GovIX

Netzwerk

ACOnet Standortporträt:

FH Vorarlberg

Die Fachhochschule Vorarlberg wurde vor 25 Jahren in Dornbirn gegründet. Ihre Entwicklung war überaus erfolgreich: Aus den anfänglich rund 50 Studierenden sind mittlerweile fast 1400 geworden. Zudem haben sich sechs Forschungszentren etabliert. In den nächsten Jahren soll weiter ausgebaut werden.

Campusgebäude in der Hochschulstraße (© FH Vorarlberg)

Prozessanpassung für die PVD-Beschichtung im Mikrotechnik-Reinraumlabor der FHV (© FH Vorarlberg)

Die Fachhochschule Vorarlberg ist seit 1993 – damals noch unter dem Namen „Technikum Vorarlberg" – Teilnehmer am österreichischen Wissenschaftsnetz ACOnet. Durch die von Beginn an hohe Qualität der Anbindung und die gute Vernetzung mit anderen Hochschulen konnte die FH Vorarlberg bereits im Jahr 1998 ein Fernstudium über Telepresence mit der Universität Linz anbieten.

Der Campus

2005 wurde in der Hochschulstraße in Dornbirn ein modernes Hochschulgebäude für die FH errichtet. Im Verbund mit dem Gebäude Achstraße ist eine zentral gelegene Campus-Hochschule entstanden, die ihren Studierenden alles bietet, was sie brauchen: Bestens ausgestattete Laborräume für Techniker*innen, moderne Ateliers für Gestalter*innen, Arbeitsräume für Teams – alles ist 24 Stunden am Tag, 7 Tage die Woche für die Studierenden zugänglich.

Information Services

Sämtliche IT-Dienstleistungen der Fachhochschule Vorarlberg werden von der Abteilung Information Services angeboten. Die insgesamt 18 Mitarbeiter*innen dieser Abteilung kümmern sich unter anderem um das Netzwerk, um die Server-Infrastruktur, um Software-Entwicklung sowie um AV- und IT-Support. Zusätzlich wird auch das Tochterunternehmen Schloss Hofen in der Außenstelle in Lochau von der Abteilung Information Services betreut.

ACOnet-Anschlusspunkt Dornbirn

Der ACOnet-PoP (Point of Presence) in Dornbirn versorgt nicht nur die FH Vorarlberg mit einer Anbindung an den ACOnet-Backbone, sondern auch das EDUnet – d. h. die öffentlichen Schulen des Bundeslandes – und eine Außenstelle der Universität Innsbruck. Der ACOnet-PoP befindet sich am Standort Hochschulstraße. Er ist redundant an die Universität Innsbruck und an die Medizinische Universität Innsbruck angebunden, wobei eine der beiden Leitungen nach Innsbruck seit dem Jahr 2017 (als ein weiterer ACOnet-Anschlusspunkt bei der VTG in Bregenz errichtet wurde) über Bregenz geführt wird. Im Zuge dieser Umstellung wurde auch die Bandbreite der Anbindung auf 10 Gbit/s erhöht.

In den nächsten Jahren werden vom Land Vorarlberg 50 Mio. Euro in Neu- und Erweiterungsbauten der Hochschule investiert. Unter anderem wird

auch ein neues Datacenter am Standort Achstraße entstehen. Zur Zeit terminieren beide ACOnet-Leitungen am Standort Hochschulstraße; nach der Fertigstellung des neuen Datacenters soll jedoch eine Leitung an den Standort Achstraße übersiedelt werden, um die Redundanz weiter zu verbessern.

Warum ACOnet?

Das ACOnet-Beitragsmodell sieht vor, dass akademischer Datenverkehr, Traffic vom Vienna Internet eXchange und alle Uploads kostenlos sind; für die verrechnete Bandbreite aus kommerziellen Netzwerken gibt es einen großzügigen Überziehungsrahmen. Die Kosten für die ACOnet-Teilnahme bleiben dadurch trotz steigender Bandbreitenanforderungen im finanzierbaren Rahmen.

FH Vorarlberg

www.fhv.at | info@fhv.at

- **15 Studiengänge** in den Bereichen
  - Wirtschaft
  - Technik
  - Gestaltung
  - Soziales und Gesundheit
- **6 Forschungszentren**:
  - Digital Factory Vorarlberg
  - Energie
  - Mikrotechnik
  - Nutzerzentrierte Technologien
  - Prozess- und Produkt-Engineering
  - Sozial- und Wirtschaftswissenschaften
- **1378 Studierende**, davon 47 % berufsbegleitend
- **300 Mitarbeiter*innen**
- **119 weltweite Kooperationen** mit Partnerhochschulen

Ein unbezahlbarer Benefit sind jedoch die inkludierten Services. Die FH Vorarlberg profitiert insbesondere von folgenden ACOnet-Angeboten:

- **Kostenlose SSL-Zertifikate**: Durch das Inkrafttreten der DSGVO und die damit eingeführte Datenklassifizierung werden zusätzlich zu den gewohnten Server-Zertifikaten auch vermehrt Client-Zertifikate zur E-Mail-Verschlüsselung ausgestellt.
- **eduroam**: Im mobilen akademischen Umfeld ist es unerlässlich, einen stets funktionierenden WLAN-Zugang ohne vorherige bürokratische Hürden gewährleisten zu können – sei es für Erasmus-Studierende, für Gastlektor*innen oder für Forschungspartner*innen.
- **eduID.at**: Über die ACOnet Identity Federation sind immer mehr Services mit den gewohnten Login-Daten bequem nutzbar. Dadurch entfällt z. B. der zusätzliche VPN-Zugang für Online-Recherchen in Bibliotheken.
- Ein weiterer Bonus ist die große **Community**: Da viele Bildungseinrichtungen mit ähnlichen Fragestellungen konfrontiert sind, ist der Austausch untereinander immer wieder nützlich. Zudem veranstaltet das ACOnet-Team laufend spannende technische Workshops.
- Mit den wachsenden Bedrohungen wie DDoS-Attacken etc. sind vor allem kleine Institutionen personell überfordert. Das **CERT-Team** von ACOnet warnt proaktiv bei Sicherheitslücken, und es wird die Möglichkeit der Mitigierung von DDoS-Attacken geboten.

Christian Bösch

FH Vorarlberg | Information Services
Ansprechpartner ACOnet
christian.boesch@fhv.at

ACOnet-Backbone 2019:

Standort-Übersiedelung in Innsbruck

2019 wurde ein wichtiges Projekt im ACOnet-Backbone realisiert: die Übersiedelung unseres Anschlusspunktes (Point of Presence, kurz PoP) an der Medizinischen Universität Innsbruck. Die MedUni Innsbruck bezog ein neues Gebäude, das ACOnet-Equipment musste mitwandern.

Die MedUni Innsbruck beherbergt von Beginn an einen der beiden ACOnet-PoPs in Innsbruck. Bisher befand sich dieser PoP in einem Gebäude in der Schöpfstraße, das von der MedUni Innsbruck jedoch zugunsten eines neu adaptierten Standorts in der Fritz-Pregl-Straße aufgegeben wurde. Dabei wurden auch die Serverräume aufgelassen, und das gesamte Equipment musste übersiedelt werden.

Bereits im Frühjahr wurden die ersten Gespräche mit allen Beteiligten geführt, um die notwendigen Arbeiten zu identifizieren und zu koordinieren. Die Kernpunkte hierbei waren die Übersiedelung der Backbone-Glasfaserstrecken und der Leitungsendpunkte der Teilnehmer-Anbindungen.

Gemeinsam wurde der 19. November 2019 als Übersiedlungstag gewählt. Durch Ausnutzung der vorhandenen Redundanzen konnten einige notwendige Arbeiten schon tagsüber erfolgen – z. B. Spleißarbeiten zur Umlegung einer der Backbone-Strecken innerhalb Innsbrucks. Durch Redundanzkonzepte konnten auch Teilnehmeranschlüsse in Absprache bereits vorab außer Betrieb genommen und entsprechend vorbereitet werden.

Die eigentliche Abschaltung und Übersiedelung unseres Equipments wurde dann um 17:00 Uhr gestartet. Durch die umfassenden Vorbereitungen konnten die Arbeiten in weniger als zwei Stunden abgeschlossen werden. Die eingeplante Zeitreserve am Folgetag war nicht notwendig, alle Services waren bereits am Abend wieder in Betrieb.

Ein großer Dank geht an die Kolleg*innen in Innsbruck, die an der Planung, Koordination und Vorbereitung maßgeblich beteiligt waren!

... und Nokia-Updates

Zwei weitere Erneuerungen im ACOnet-Backbone waren 2019 ebenfalls notwendig: Die Backbone-Router liefen bislang mit jener Software-Version, die bei ihrer Installation im Jahr 2017 aktuell war. Aufgrund zusätzlicher Features – und natürlich Bugfixes – haben wir uns entschlossen, 2019 das erste großflächige Software-Upgrade seit der Inbetriebnahme der Plattform durchzuführen. Die Updates wurden in mehreren Wartungsfenstern erfolgreich und ohne Komplikationen eingespielt.

Aufgrund von Bauteilproblemen mussten zudem die ACOnet-Komponenten an allen Access-Standorten präventiv getauscht werden. Dank unserer Standortbetreuer*innen und der Unterstützung von Nokia konnte auch das erfolgreich realisiert werden.

Michael Perzi

ACOnet

eduroam in the city: Klagenfurt

eduroam steht für „education roaming“. Das Service entstand aus einem Projekt von GÉANT, dem paneuropäischen Datennetzverbund für Forschung und Bildung. Dank eduroam können die Studierenden und Mitarbeiter*innen jeder teilnehmenden Bildungseinrichtung kostenlos und unkompliziert einen gesicherten WLAN-Zugang verwenden. Der Clou: Das funktioniert nicht nur am heimatlichen Campus, sondern auch bei allen anderen eduroam-Teilnehmern – weltweit.

eduroam ist mittlerweile an tausenden Institutionen und öffentlichen Orten in über 100 Ländern verfügbar. In Österreich wird es derzeit von mehr als 50 ACOnet-Teilnehmerorganisationen angeboten. Abgesehen davon verbreitet sich eduroam zunehmend auch im öffentlichen Raum: In den Jahren 2015–2017 wurden große Teile der öffentlichen WLAN-Infrastruktur in Wien, Graz und Innsbruck für eduroam-Benutzer*innen zugänglich gemacht. Mit der „Eroberung“ Klagenfurts folgte 2019 der nächste Schritt.

Anfang April 2019 wurde das „CityWLAN Klagenfurt“ eröffnet, ein glasfaserbasiertes öffentliches WLAN-Netzwerk, das mit einer Bandbreite von 100 Mbit/s zu den schnellsten in Österreich zählt. Insgesamt 25 Access Points sorgen dafür, dass man an vielen Plätzen in der Klagenfurter Innenstadt, aber auch im Strandbad und im Hallenbad kostenlos „surfen“ kann. Künftig sollen zudem auch die rund 70 Stadtbusse der Klagenfurt Mobil GmbH an das CityWLAN angeschlossen werden.

Durch eine Kooperation der Universität Klagenfurt mit den Stadtwerken Klagenfurt, die das CityWLAN betreiben, wird auf allen öffentlichen Hotspots auch ein gesicherter eduroam-Zugang angeboten. Auf neu installierten Access Points wird eduroam ebenfalls automatisch ausgestrahlt werden. Im Gegensatz zum „normalen“ CityWLAN gibt es für den eduroam-Zugang in Klagenfurt keine Bandbreitenlimitierung. Ein weiterer Vorteil ist die gewohnt unkomplizierte Handhabung: Einmal auf einem mobilen Gerät eingerichtet, verbindet sich eduroam automatisch, sobald ein eduroam-Zugang in Funkreichweite ist.

Eine Liste aller eduroam-Teilnehmer in Österreich und weitere Informationen zum Service finden Sie unter **www.eduroam.at**.

Der via eduroam anfallende Datenverkehr wird von den Stadtwerken direkt zur Universität Klagenfurt geleitet. Alle weiteren technischen Notwendigkeiten (Radius-Authentifizierung, DHCP, IP-Adressbereich etc.) werden von ACOnet abgewickelt. Sowohl für die Universität Klagenfurt als auch für die Stadtwerke Klagenfurt sind der technische und administrative Aufwand daher minimal. Für die Studierenden, Mitarbeiter*innen und Gäste der Universität Klagenfurt bedeutet das Service jedoch ein großes Plus an „Arbeitsfläche“ – und entsprechend populär ist es auch.

Peter Gruber

Universität Klagenfurt
Zentraler Informatikdienst
peter.gruber@aau.at

ACOnet, quo vadis?

Gemeinsam mit dem ACOnet-Lenkungsausschuss (siehe Seite 9) wurde im Jahr 2019 der Rahmen für eine „ACOnet-Strategie 2020–2025“ erarbeitet und abgestimmt, mit Fokus auf der Backbone-Erneuerung 2022.

Folgende Grundprinzipien für den gemeinnützigen Betrieb und für die Weiterentwicklung von ACOnet wurden bestätigt:

- Die **ACOnet-Community** (das ACOnet-Kernteam gemeinsam mit den Teilnehmerorganisationen) ist ein wichtiger **Know-how-Träger**. Sie baut Wissen innerhalb der Community auf und sorgt für dessen Vermittlung.

- Die Kernkompetenz des ACOnet-Teams ist der Betrieb des gemeinsamen **Datennetzes** (in Kooperation mit den Standortbetreuer*innen) und der zugehörigen Middleware-**Services**.

- **Nachhaltigkeit, Qualität und Flexibilität** sind bei der Erneuerung von Infrastruktur und Services von höchster Priorität.

Ein Ziel der nächsten Jahre ist auch die nachhaltige **Sicherung der Governance-Struktur** von ACOnet. Konkret sollen die kooperative strategische Planung und die Abstimmung zum Finanzmanagement zwischen dem ACOnet-Lenkungsausschuss und dem ACOnet-Betreiber (ZID der Universität Wien) intensiviert werden. Im Zuge dessen ist auch eine Schärfung des Memorandum of Understanding zwischen dem ACONET-Verein und der Universität Wien geplant.

Erneuerung des Backbone-Vertrags

Da die Verträge für unsere Netzwerk-Infrastruktur mit der A1 Telekom Austria AG im Jahr 2022 auslaufen, ist der ACOnet-Backbone neu zu planen.

Die 2020/21 notwendigen Ausschreibungen bzw. Beschaffungsmaßnahmen werden auf folgenden Grundsätzen beruhen:

- langfristige Sicherung der für den Betrieb eines Wissenschaftsnetzwerks notwendigen Flexibilität (Betriebskonzept),

- Beibehaltung der bisherigen hochverfügbaren Netzwerk-Infrastruktur und Topologie,

- Prüfung von Maßnahmen zur Erhöhung des Wettbewerbs.

Als vorbereitende technische Weiterbildung haben wir 2019 am „10th Customer Empowered Fibre Networks Workshop“ in Prag teilgenommen (siehe **www.cesnet.cz/events/cef2019**). Zudem befassen wir uns intensiv mit der OTE-Rahmenvertragsausschreibung von GÉANT (OTE = Optical Transmission Equipment) und führen zahlreiche Gespräche mit Herstellern, anderen Wissenschaftsnetzen und künftigen Bedarfsträgern. Letzteres betrifft vor allem

- quantenoptische Projekte wie OpenQKD und QUAPITAL, die von der Österreichischen Akademie der Wissenschaften und dem Austrian Institute of Technology betrieben werden, und

- messtechnische Experimente im Rahmen des European Metrology Programme for Innovation and Research (EMPIR), an denen das Bundesamt für Eich- und Vermessungswesen sowie das Atominstitut der TU Wien beteiligt sind.

Christian Panigl

Abteilungsleiter ACOnet & VIX

Gute Manieren im Netz

Je weniger Müll produziert wird, desto weniger Aufwand verursacht seine Entsorgung. Diese Binsenweisheit lässt sich auch auf das Internet übertragen: Wenn fehlerhafte oder gefälschte Datenpakete möglichst früh ausgefiltert werden, ist das Gesamtsystem gesünder. Die Initiative MANRS (Mutually Agreed Norms for Routing Security, „manners" gesprochen) hat ein Bündel einheitlicher Maßnahmen zusammengestellt, mit denen Netzbetreiber*innen gemeinsam mehr Sicherheit und Stabilität im Internet erreichen können.

Wir alle werden in Beruf und Alltag immer abhängiger von Internet-Services. Je essentieller bzw. populärer ein Service ist, desto unangenehmer ist es, wenn es ausfällt – sei es durch technische Gebrechen, Fehlkonfigurationen oder böswillige Angriffe auf seine Verfügbarkeit. Letzteres wird immer wichtiger: Waren die ersten Attacken im Internet noch eher „sportlich" motiviert, so ist heute daraus ein Geschäftsmodell krimineller Kräfte geworden.

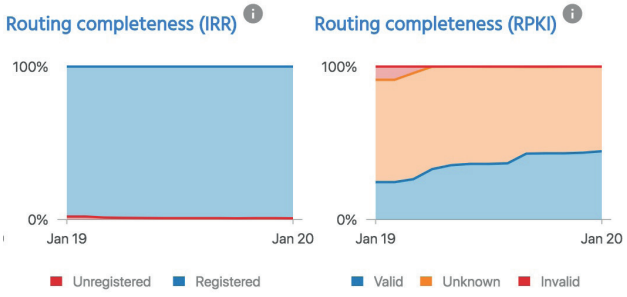
Attacken auf die Verfügbarkeit eines Service basieren oft darauf, zunächst möglichst viele unzureichend abgesicherte Geräte im Internet ausfindig zu machen und sie (von ihren Besitzer*innen unbemerkt) zu kapern. In Folge werden Tausende dieser ferngesteuerten Geräte benutzt, um gemeinsam konkrete Ziele im Netz anzugreifen. Eine Methode dafür sind „Reflection Attacks". Dabei werden an ein geeignetes Service unzählige kleine Anfragen geschickt, die große Antworten generieren. Fälscht man die Absendeadresse der Anfragen, so erhält die angebliche Quelladresse unzählige große Antworten – mit dem Ergebnis, dass ihr Internetzugang blockiert ist, was durchaus wirtschaftlichen Schaden verursachen kann.

Das Übel an der Wurzel packen

Ein Grundproblem liegt darin, dass Pakete mit falschen Quelladressen im Internet überhaupt transportiert und zugestellt werden. Dieser Umstand erklärt sich allerdings aus der Funktionsweise von Routern: Genau wie die traditionelle Post achten sie normalerweise nämlich nur auf die Zieladresse und versuchen, dieses Ziel auf möglichst kurzem Weg zu erreichen.

Auch bei einem Datenpaket wird es mit zunehmender Entfernung vom Ursprungsrechner immer aufwendiger festzustellen, ob die Absendeadresse korrekt ist – denn es gibt meist zahlreiche legitime Wege, über die ein Datenpaket bei einem Router im Netz einlangen kann. Sitzt man hingegen nahe an der Quelle, können falsche Absendeadressen viel eher identifiziert werden.

Die von der Internet Society (ISOC) ins Leben gerufene MANRS-Initiative zielt folglich darauf ab, dass Netzbetreiber*innen im eigenen Betriebsbereich (ihrem „Autonomous System", kurz AS) so gut wie möglich für Netzhygiene sorgen.



Auszug aus den Routing-Statistiken für Österreich

Die Grafik links zeigt den Anteil der bei der Internet Routing Registry (IRR) registrierten Routen am gesamten Datenverkehr. Im Jänner 2019 lag dieser bei 98%, im Jänner 2020 bei 99%.

Die Grafik rechts zeigt die Entwicklung der mittels Resource Public Key Infrastructure (RPKI) gesicherten Routen.
Jänner 2019: 24% gültig, 67% unbekannt, 9% ungültig
Jänner 2020: 45% gültig, 55% unbekannt, 0% ungültig

(Quelle: **https://observatory.manrs.org/#/history**)

MANRS I: Paketfilter

Der beste Ansatzpunkt für eine Überprüfung der Quelladresse ist das sogenannte Default Gateway – also der allererste Router, an dem ein von einem Computer abgesendetes Datenpaket auf seinem Weg durch das Internet vorbeikommt. Dieser Router weiß genau, welches Netzsegment an ihn angeschlossen ist, und kennt seinen eigenen Adressbereich. Am Default Gateway können ungültige Quelladressen mit einem Filter auf Paketebene leicht erkannt und verworfen werden.

MANRS II: Routing-Filter

Ein weiterer Ansatz für eine bessere Netzhygiene greift auf Ebene der Routing-Informationen: Router im Internet „erzählen" ihren jeweiligen Nachbar-Routern, für welche Adressbereiche sie sich zuständig fühlen. Diese Adressbereiche sollten zudem auch überprüfbar registriert sein (siehe Infobox rechts). Wenn jeder Router korrekt weitergibt, was er weiß, und selbst nur verifizierte Routen annimmt, dann funktioniert das Internet.

ACOnet als Netzbetreiber muss sicherstellen, dass seine Backbone-Router von den Teilnehmer-Routern nur verifizierte Adressbereiche „lernen". Um den mitunter fatalen Auswirkungen von Irrtümern und Fehlkonfigurationen im Routing-Bereich vorzubeugen, werden an allen Teilnehmerschnittstellen, wo das Routingprotokoll BGP zum Einsatz kommt, ungültige Routen automatisch ausgefiltert.

MANRS III: Kontaktdaten

Auch die besten Sicherheitsvorkehrungen können das Risiko, dass etwas schiefgeht, nur verringern – passieren kann dennoch immer etwas. In diesem Fall ist es wichtig, möglichst schnell jemanden zu erreichen, der das Problem beheben kann.

Daher ist ein weiteres wichtiges Kriterium für die MANRS-Konformität, valide Kontaktdaten zu hinterlegen, damit im Ernstfall möglichst wenig Zeit verloren geht.

Dokumentation von Netzressourcen

- Offiziell vergebene Adressbereiche und die dazugehörigen Rechtspersonen sind in internationalen, weltweit lesbaren Datenbanken dokumentiert. Für die Region Europa und etwas darüber hinaus ist die RIPE-Datenbank zuständig (**https://apps.db.ripe.net/db-web-ui/query**).
- In der RIPE-Datenbank sind auch die IP-Adressbereiche und AS-Nummern von ACOnet-Teilnehmern gespeichert, sofern diese global eindeutige Ressourcen beantragt und zugeteilt bekommen haben.
- Teilnehmerorganisationen, die ACOnet-Ressourcen („Provider Aggregatable" IP-Adressen und „private" AS-Nummern) verwenden, benötigen keine eigenen Einträge in der RIPE-Datenbank.

Erfüllt man die von MANRS vorgegebenen Kriterien, kann man sich in die Liste der MANRS-Teilnehmer aufnehmen lassen. ACOnet hat ohne Änderungen im Betriebsablauf die Basisvoraussetzungen erfüllt und ist daher seit Sommer 2019 auf **www.manrs.org/isps/participants/** gelistet.

Verbesserungen sind dennoch immer möglich. Die ACOnet-Router versuchen zwar, Datenpakete mit ungültigen Quelladressen auszufiltern; die dabei verworfenen Pakete haben aber oft schon einen langen Weg hinter sich. Hier hilft es, wenn alle ACOnet-Teilnehmer Filter so nahe wie möglich an den Endgeräten betreiben. So kann man „Datenmüll" vermeiden und (geeignete Logmechanismen vorausgesetzt) Fehler deutlich schneller aufspüren.

Harald Michl

ACOnet
Betriebskoordination

Services

IPv4-Adresspool erschöpft:

Die IPv6-Ära rückt näher

Bei der Vergabe von IP-Adressen muss sichergestellt sein, dass die Adressen weltweit eindeutig sind. Die Vergabe wird deshalb ausschließlich über insgesamt fünf Regional Internet Registries (RIRs) abgewickelt. Für Europa übernimmt diese Funktion das RIPE NCC. Wie zuvor schon bei anderen RIRs sind nun auch beim RIPE NCC die IPv4-Adressen zur Neige gegangen. An IPv6 führt somit bald kein Weg mehr vorbei.

Bereits 2012 erhielt das RIPE NCC einen letzten /8-Adressblock (das sind knapp 17 Millionen IPv4-Adressen – siehe Glossar auf Seite 27) zur Vergabe an die europäischen Local Internet Registries (LIRs). Schon damals war klar, dass in absehbarer Zeit alle IPv4-Adressen verteilt sein werden. Daher wurde von der RIPE-Community mittels Policy beschlossen, die Vergabe zu limitieren und nur noch einen /22-Adressblock pro LIR zu vergeben.

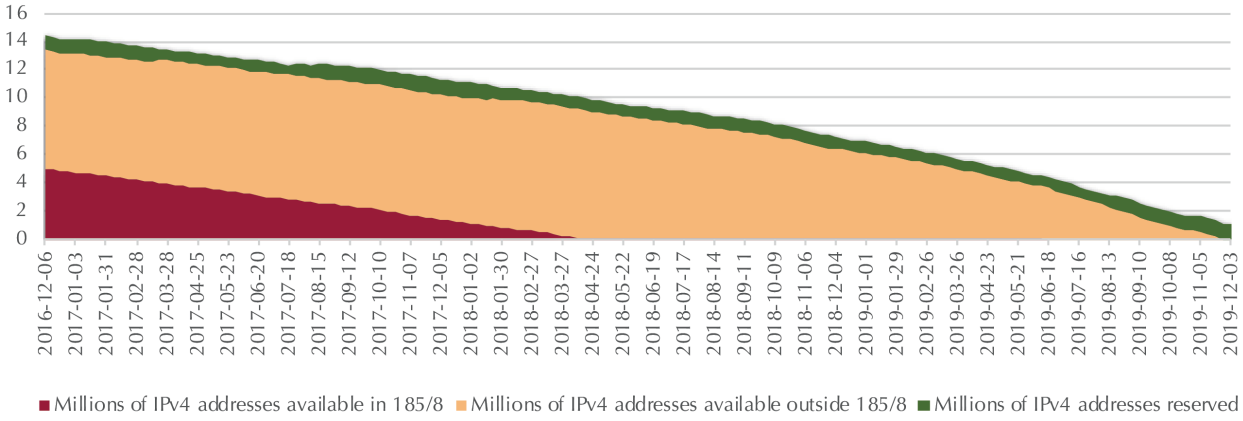
Ab diesem Zeitpunkt wurden zudem auch keine PI-Adressen mehr zugeteilt – alles mit dem Ziel, mit dem bestehenden Adresspool so lange wie möglich das Auslangen zu finden. Auch ACOnet als LIR hat unter dieser Policy noch einmal einen /22-Adressblock beantragt und zugewiesen bekommen. Weil die Gründung einer Local Internet Registry die einzige Möglichkeit war, weitere IP-Adressen zu erhalten, stieg die Zahl der LIR-Gründungen in den letzten Jahren stark an.

Das Ende des Vorrats

Am 25. November 2019 verkündete das RIPE NCC schließlich den „Run Out" von IPv4-Adressen – die letzten Reserven werden für die noch offenen LIR-Gründungsanträge benötigt. Allerdings erhält das RIPE NCC weiterhin IPv4-Adressen zurück (z. B. durch Vertragsauflösungen), sodass immer wieder Adressen verfügbar werden. Deshalb wurde

RIPE NCC IPv4 Pool – Last 36 Months

Aktuelle Version mit Erläuterungen: **www.ripe.net/manage-ips-and-asns/ipv4/ipv4-pool** (© RIPE NCC)



eine Warteliste für neue LIRs implementiert. Jede LIR auf der Liste erhält einen /24-Adressblock, sobald ein solcher zur Verfügung steht.

Kauf & Verkauf von Ressourcen

Da die Anzahl der Rückläufe nicht vorhersehbar ist, lässt sich auch die Wartezeit auf dieser Liste nicht abschätzen. Ein dringender Bedarf an zusätzlichem Adressraum kann somit nur noch über ein Broker-Service bedient werden. Das ist quasi ein Marktplatz, bei dem Broker die Vermittlerrolle zwischen kaufenden und verkaufenden Personen bzw. Organisationen übernehmen.

Wenn man ein solches Broker-Service in Anspruch nimmt, gilt es darauf zu achten, dass alle Transaktionen im Rahmen der RIPE-Policies abgewickelt werden. Zudem ist auch immer mit einem gewissen Risiko in Bezug auf die „Vergangenheit" des Netzblocks zu rechnen (z. B. Blacklisting).

Generell sollte beim Handel mit IP-Adressen stets mit Sorgfalt vorgegangen werden. IPv4-Adressen gelten aktuell als wertvolles Gut. Es ist schwer vorhersehbar, wie sich die Situation und der Bedarf weiter entwickeln werden. Derzeit empfehlen wir daher, von einem Verkauf Abstand zu nehmen.

IPv4-Adressen im ACOnet

Als LIR verfügt ACOnet noch über einen kleinen Vorrat an IPv4-Adressen, die wir im Rahmen der geltenden RIPE-Policies an unsere Teilnehmer zuweisen können. Damit sehen wir uns imstande, den Adressbedarf der ACOnet-Community noch einige Jahre lang zu decken.

Michael Perzi

ACOnet
Ansprechpartner LIR

Glossar zur IP-Adressvergabe

- **RIPE NCC**
  Réseaux IP Européens Network Coordination Centre – zentrale europäische Vergabestelle für Internet-Ressourcen mit Sitz in Amsterdam.
- **RIR**
  Regional Internet Registry – ein regionaler Verwalter von Internet-Ressourcen. Weltweit gibt es fünf RIRs, das RIPE NCC ist eine davon.
- **LIR**
  Local Internet Registry – jeder Provider (auch ACOnet), der an seine Teilnehmer Ressourcen weiterverteilt, die er von einer RIR erhalten hat.
- **IPv4**
  Internet Protocol Version 4 – basiert auf 32-Bit-Adressen, die in Dezimalform notiert werden (z. B. 193.170.0.0/15).
- **IPv6**
  Internet Protocol Version 6 – basiert auf 128-Bit-Adressen, die in Hexadezimalform notiert werden (z. B. 2001:628::/29).
- **PI-Adressen**
  Provider-Independent-Adressen – sind einem Teilnehmer direkt zugewiesen und können bei einem Providerwechsel mitgenommen werden; eine Umnummerierung ist nicht erforderlich.
- **PA-Adressen**
  Provider-Aggregatable-Adressen – gehören der LIR und werden für die Dauer der Vertragsbeziehung „verliehen", müssen also im Fall eines Providerwechsels zurückgegeben werden.
- **Adressblöcke: /8, /22, /24**
  Eine IPv4-Adresse besteht aus 32 Bit. Die Zahl nach dem Slash besagt, wie viele davon zur Adressierung dieses Netzbereichs genutzt werden. Der Rest bleibt für die Adressierung der Hosts in diesem Netz: Bei /24 bleiben 8 Bit übrig, das entspricht 256 Adressen. Bei /22 sind es 10 Bit bzw. 1024 Adressen; bei /8 sind es 24 Bit bzw. knapp 17 Millionen Adressen. In IPv6 wird entsprechend auf 128 Bit aufgerechnet.

Der VIX wird „NIS-fit“

IT-Security war im Betriebsteam des Vienna Internet eXchange (VIX) schon immer gelebte Realität. Nun wurde der VIX offiziell als wesentlicher Dienst im Sinne der EU-weit gültigen NIS-Richtlinie klassifiziert. Für das VIX-Team – das im Wesentlichen mit dem ACOnet-Team identisch ist – bedeutet das einen spürbaren Mehraufwand, der sich aber lohnt.

Ein hohes Sicherheitsniveau ist für den Betrieb von Internet Exchange Points (IXPs) eine unabdingbare Voraussetzung. Die Sicherheitsmaßnahmen, die am VIX zum Einsatz kommen, sind dementsprechend über Jahre hinweg gewachsen und wurden stets mit Bedacht geplant und umgesetzt, in enger Abstimmung mit einem internationalen Umfeld von Exchange Points. Nun ist dieses hohe Sicherheitslevel auch gesetzlich verankert: 2019 wurde der VIX als wesentlicher Dienst im Sinne der EU-NIS-Richtlinie eingestuft. NIS steht dabei für „Network Information Security“ bzw. „Netz- und Informationssystemsicherheit“.

Die NIS-Richtlinie der EU vom 6. Juli 2016 wurde in Österreich mit dem NIS-Gesetz 2018 und der zugehörigen NIS-Verordnung 2019 in nationales Recht umgesetzt. Beide Texte definieren Exchange Points ab 100 Teilnehmern als wesentliche Dienste und verpflichten sie, durch technische und organisatorische Maßnahmen ein Sicherheitsniveau zu gewährleisten, das „zur Beherrschung der Risiken für die Netzsicherheit geeignet ist“.

Aus Vorgesprächen zwischen dem Bundeskanzleramt (welches die nationale Umsetzung der NIS-Richtlinie koordiniert) und allen potentiellen Betreibern kritischer Infrastruktur war bereits 2018 absehbar, dass der VIX als wesentlicher Dienst eingestuft werden wird. Das VIX-Team bereitet sich daher schon länger gezielt darauf vor, die mit der NIS-Richtlinie verbundenen Vorgaben sukzessive zu erfüllen.

Ein eigens eingesetztes „Information Security Management Team“ (ISM-Team) widmet sich intensiv der Standardisierung und Dokumentation bestehender Sicherheitsvorkehrungen sowie der Implementierung weiterer Maßnahmen, um den gesetzlichen Bedingungen zu entsprechen. Dabei orientieren wir uns am ISO-27001-Standard (Information Security Management Systems). Das erleichtert eine eventuelle Zertifizierung und stellt sicher, dass künftig auch ACOnet von den gewonnenen Erfahrungen profitieren kann.

Romana Cravos

Vienna Internet eXchange
ISM-Team

Vienna Internet eXchange (VIX)

Der VIX ist ein hochverfügbarer, neutraler Internet Exchange Point mit nationalen und internationalen Teilnehmern (Wissenschaftsnetze, Internet Service Provider, Content Provider, ...). Große und kleine Netzbetreiber nutzen solche Exchange Points, um regionalen Datenverkehr zwischen ihren Netzen auf kurzem Wege direkt auszutauschen.

Der Vienna Internet eXchange wurde 1996 an der Universität Wien für anfangs fünf Teilnehmer (darunter ACOnet) installiert. Er wird bis heute vom Zentralen Informatikdienst der Universität betrieben. Mittlerweile hat der VIX bereits drei Standorte in Wien und rund 150 Teilnehmer.

Alle Infos: **www.vix.at**

TCS: Die nächste Runde

Über das Trusted Certificate Service (TCS) können ACOnet-Teilnehmer seit vielen Jahren digitale Zertifikate unentgeltlich und in unlimitierter Anzahl beziehen. Der Rahmenvertrag wird von GÉANT, dem europäischen Dachverband der nationalen Wissenschaftsnetze, regelmäßig neu ausgeschrieben – zuletzt im Jahr 2019.

Was war: GlobalSign, Comodo, DigiCert

Das Zertifikats-Service startete 2006 unter dem Namen SCS (Server Certificate Service) mit der Firma **GlobalSign** als ausstellender CA (Certification Authority). Damals war es weit aufwendiger, an Zertifikate zu kommen: Für jedes Zertifikat (verfügbar waren anfangs nur Server- und E-Mail-Zertifikate) bzw. für jede Domain mussten Formulare ausgefüllt und per Fax an das ACOnet-Team gesendet werden. Wir kümmerten uns dann als Registration Authority (RA) um die Validierung und Registrierung. Die tatsächliche Beantragung und der Bezug des Zertifikats lief über ein von ACOnet betriebenes Portal; die Zustellung erfolgte per Mail.

2009 wechselte man zu **Comodo** als CA, und das Service wurde auf TCS umbenannt (das T stand bis 2014 für TERENA, eine der Vorläuferorganisationen von GÉANT). Verfügbar waren diverse Arten von Server-Zertifikaten, Code-Signing-Zertifikate sowie persönliche Zertifikate zur Signierung von E-Mails und Dokumenten. Alle Zertifikate konnten über Webportale bezogen werden, die teils von ACOnet, teils föderiert von TERENA betrieben wurden. Einige RA-Aufgaben blieben noch bei ACOnet und wanderten erst 2013 zu Comodo, als sich aufgrund verschärfter Richtlinien die Formalitäten änderten und DCV (Domain Control Verification) als zusätzlicher Kontrollmechanismus eingeführt wurde.

Nach sechs Jahren mit Comodo gewann der Anbieter **DigiCert** die nächste Ausschreibung. Der Wechsel wurde Mitte 2015 vollzogen. Seither wurden persönliche Zertifikate über ein föderiertes Portal und alle anderen Zertifikatstypen über von DigiCert betriebene Portale ausgestellt.

TCS-Nutzung im ACOnet (2019)

- **16691** Persönliche Zertifikate
- **3665** Organisation Validated Server-Zertifikate
- **1417** Extended Validation Server-Zertifikate
- **73** andere Zertifikate

Mit **insgesamt 21846** ausgestellten Zertifikaten lag ACOnet 2019 bei der Nutzung des Trusted Certificate Service europaweit im Spitzenfeld.

Was kommt: Sectigo

Da der Vertrag mit DigiCert Ende April 2020 ausläuft, stand 2019 ganz im Zeichen der Ausschreibung für das künftige TCS. In einem mehrstufigen Verfahren wurde zum Jahresende **Sectigo** als jene CA ermittelt, über die ab Mai 2020 Zertifikate bezogen werden können. Die Firma Sectigo ist in New Jersey (USA) beheimatet, hat aber auch Niederlassungen in Großbritannien und Kanada. Sie entstand aus der 2017 von Francisco Partners übernommenen Comodo und fungiert u. a. als CA für Internet2, das Wissenschaftsnetz der USA. Nach intensiver Suche haben wir also einen in unserem Sektor erfahrenen Anbieter gefunden, mit dem wir das Service wieder einige Jahre erfolgreich weiterführen können.

Kurt Bauer

ACOnet
Ansprechpartner TCS

DNS over TLS vs. DNS over HTTPS

Das Domain Name System (DNS) regelt die Zuordnung von Hostnamen zu IP-Adressen und ist für die Adressierung im Internet unverzichtbar. Die im Hintergrund laufenden DNS-Anfragen der Benutzerrechner gehen standardmäßig allerdings unverschlüsselt über das Netz. Aktuell gibt es zwei Lösungsansätze, um DNS-Anfragen vor heimlichem Mitlesen zu sichern: DNS over TLS (DoT) und DNS over HTTPS (DoH).

Das Domain Name System (DNS) basiert auf Netzwerkprotokollen, die aus einer Zeit stammen, wo Security und Privacy im Netz noch kein großes Thema waren. Im Rahmen der Überlegungen, das DNS sicherer zu machen, konnten im Laufe der Zeit etliche Problembereiche durch Erweiterungen (z. B. DNSSEC) verbessert bzw. gelöst werden. Ein elementares Problem ist aber nach wie vor offen: Auf jedem Benutzerrechner stellt jede Applikation, die mit dem Internet kommuniziert, im Hintergrund laufend Anfragen an einen DNS-Server, um das jeweils benötigte Service im Internet lokalisieren und ansprechen zu können. Diese DNS-Anfragen gehen unverschlüsselt über das Netz.

Eine der relevantesten Anwendungen in diesem Kontext ist das Browsen von Websites („Surfen"). Es liegt in der Natur der Sache, dass dabei zahllose DNS-Anfragen generiert werden, aus denen sehr viel Information gewonnen werden kann. Werden diese Anfragen mitgelesen und analysiert, so lässt sich nachvollziehen, welche Webseiten jemand besucht hat. Daraus kann man – wie bei diversen Targeting-Methoden – ein Benutzerprofil erstellen und aus diesem wiederum leicht auf eine bestimmte Person rückschließen. Das ermöglicht Eingriffe in die Privatsphäre; in manchen Situationen oder Ländern können solche Informationen auch reale Gefahr bedeuten.

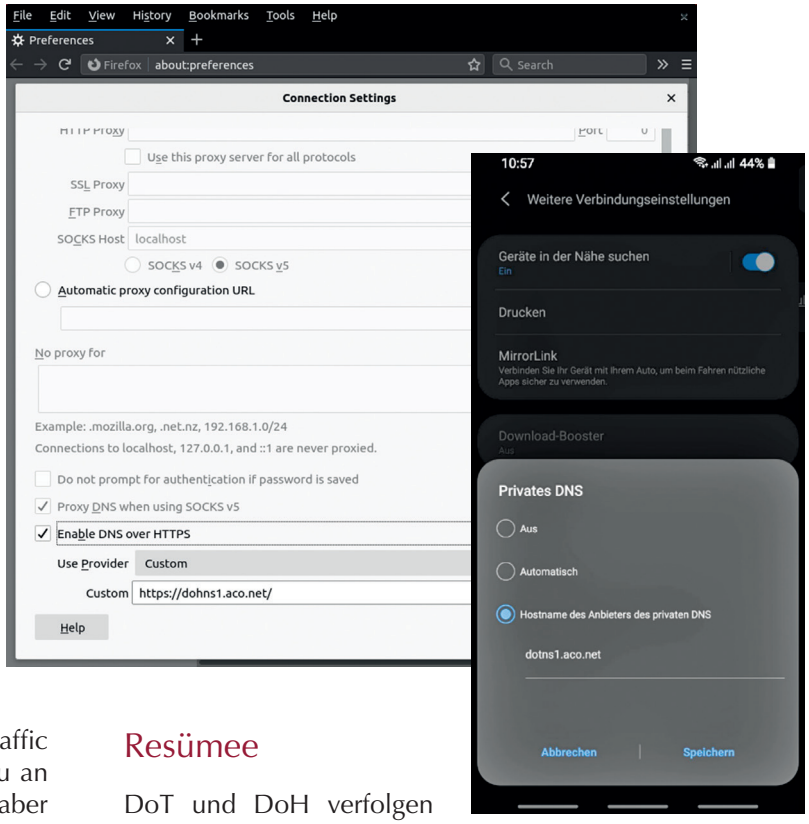
Der Wunsch ist daher, den DNS-Verkehr verschlüsselt über das Netz zu transportieren, so wie es viele andere Netzwerkprotokolle bereits tun (auch der Inhalt von Webseiten wird meist verschlüsselt vom Webserver zum Browser übertragen). Um dieses Ziel zu erreichen, wurden bislang zwei Lösungen erarbeitet, die von komplett unterschiedlichen Ansätzen ausgehen.

DNS over TLS (DoT)

Diese Lösung basiert auf bestehenden Konzepten. TLS (Transport Layer Security) ist eine weit verbreitete Technologie, die bereits bei zahlreichen Netzwerkprotokollen zum Einsatz kommt. Beispielsweise erfolgt auch die Transport-Verschlüsselung von Web-Traffic mit TLS, sofern HTTPS anstelle von HTTP verwendet wird. Es ist naheliegend, auch den DNS-Traffic über eine TLS-gesicherte Verbindung abzuwickeln. Verändert wird dabei nicht das DNS, sondern nur der darunterliegende Transport. Alle Vor- und Nachteile (d. h. Einschränkungen) von TLS gelten somit auch für DNS over TLS.

DNS over HTTPS (DoH)

DoH geht einen ganz anderen Weg: Hier werden die DNS-Anfragen nicht mehr getrennt von anderem Traffic transportiert, sondern direkt in ein „artfremdes" Protokoll gepackt – nämlich in gesichertes HTTP, also HTTPS. Von außen ist dabei nicht feststellbar, ob der verschlüsselte HTTPS-Traffic reinen Web-Content oder eben auch DNS-Anfragen enthält. Das ist ein kompletter Paradigmenwechsel, der die Eigenständigkeit von (Anwendungs-)Protokollen aufweicht.



Konfiguration von Firefox (links) und Android (rechts) mit ACOnet-Nameservern als DoH- bzw. DoT-Provider:
– dohns1.aco.net (DoH)
– dotns1.aco.net (DoT)

Beide Nameserver laufen derzeit im Testbetrieb. Bei Interesse bitten wir um Voranmeldung per E-Mail an noc@aco.net.

DNS over HTTPS kommt ausschließlich bei Webbrowsern zum Einsatz. Alle anderen Anwendungen wickeln ihre DNS-Anfragen weiterhin über das Betriebssystem ab und sind von DoH nicht betroffen. Das bedeutet, dass eine bestimmte Anwendung auf einem Rechner – der Webbrowser – in Bezug auf DNS aus der Reihe tanzt: Er schickt seine Anfragen nicht (wie alle anderen Applikationen) an einen DNS-Server, sondern an einen in der Browser-Konfiguration definierten DoH-Provider. Dieser extrahiert die DNS-Anfragen aus dem Web-Traffic und leitet sie ins „normale“ DNS über. Genau an dieser Schnittstelle können die DNS-Anfragen aber weiterhin aufgebrochen, mitgelesen oder manipuliert werden.

Damit verschiebt sich die Vertrauensabhängigkeit von den klassischen DNS-Providern zu den neuen DoH-Providern. Die aktiven Player sind hier aktuell die großen Content-Provider, allen voran Cloudflare. Daraus ergibt sich einer der großen Kritikpunkte an DoH, nämlich dass sich die in den DNS-Anfragen enthaltenen Informationen in der Hand der großen Provider konzentrieren würden. Ein weiterer Kritikpunkt ist, dass klassische Betriebskonzepte (Einsatz von Firewalls, Problemanalyse an einem Benutzerrechner etc.) bei Verwendung von DoH nicht mehr gelten. So könnten z. B. zwei verschiedene Webbrowser – von denen einer DoH unterstützt, der andere nicht – beim Aufruf derselben Webadresse auf demselben Rechner zwei unterschiedliche Ergebnisse (Webseiten) anzeigen, weil die DNS-Auflösung auf zwei verschiedenen Servern erfolgt bzw. der DoH-Provider die Anfragen nachträglich umleitet.

Diesen Schwächen steht gegenüber, dass das Konzept auch neue technische Möglichkeiten bietet, um nicht nur das Verhalten und die Geschwindigkeit eines Webbrowsers zu verbessern, sondern auch das subjektive Sicherheitsempfinden – sofern der jeweilige Content-Provider vertrauenswürdiger erscheint als der lokale DNS-Provider, was in manchen Staaten durchaus der Fall sein kann.

Resümee

DoT und DoH verfolgen unterschiedliche Konzepte, um den DNS-Verkehr zwischen einem Benutzerrechner und der DNS-Infrastruktur verschlüsselt abzuwickeln. Zum gegenwärtigen Zeitpunkt lässt sich noch nicht sagen, welche dieser Lösungen größere Verbreitung finden wird. Vermutlich werden beide Verfahren – allerdings in unterschiedlichen Szenarien – zum Einsatz kommen. Beide könnten weitreichende betriebliche Herausforderungen zur Folge haben. Speziell bei DoH werden sich Dienstleister, Firmen und Provider Gedanken darüber machen müssen, wie man mit dieser neuen Technologie umgeht, da sie auch auf die Konfiguration der Webbrowser Einfluss nimmt.

Jedenfalls wird in beiden Fällen zwar der Transport verschlüsselt, doch an jenem Punkt, wo die Namensauflösung tatsächlich erfolgt, ist es weiterhin möglich, zentral Daten zu sammeln. Es ist daher individuell zu entscheiden, ob man einem lokalen Service-Provider oder einem global agierenden Content-Provider mehr Vertrauen schenken will.

Gerhard Winkler

Teamleiter
Internet Domain Administration

No Risk, no Fun?

Was waren im Jahr 2019 die größten Herausforderungen für die Sicherheit der IT-Infrastruktur im ACOnet? Eine kurze Zusammenfassung aus Sicht des Computer Emergency Response Teams (ACOnet-CERT).

Confluence-Sicherheitslücke

Im Frühjahr 2019 wurden mehrere kritische Sicherheitslücken in Atlassians Confluence-Software bekannt, die als „Wiki" zum Wissensmanagement häufig eingesetzt wird. Nicht nur an österreichischen Universitäten, sondern europaweit wurden Confluence-Instanzen reihenweise gehackt und übernommen. Überraschend ist, in welcher Geschwindigkeit Schwachstellen nach ihrem Bekanntwerden mittlerweile ausgenutzt werden. In diesem Zusammenhang können wir nur empfehlen, Betriebssysteme und Software laufend zu aktualisieren und vor allem Sicherheitsupdates zeitnah einzuspielen. Hilfreich sind auch die Mailinglisten von CERT.at, in denen täglich die wichtigsten Sicherheitswarnungen zusammengefasst werden: **https://cert.at/de/services/mailinglisten/**

Phishing-Mails

Das beherrschende Thema im Kontext von Bildungseinrichtungen und damit auch im ACOnet waren gezielte Phishing-Kampagnen. Phishing-Mails sind Nachrichten, die versuchen, die Empfänger*innen durch Vortäuschung falscher Tatsachen zur Herausgabe von Passwörtern zu bringen. Dabei werden Anmeldemasken gefälscht und User-Accounts missbraucht, um weitere Phishing-Mails zu verbreiten. Als ACOnet-CERT haben wir hier gute Erfahrungen gemacht, wenn wir URLs bei Google Safe Browsing melden. Zudem kontaktieren wir die Betreiber der betroffenen (oft kompromittierten) Webseiten, auf denen die gefälschten Login-Masken untergebracht sind. Andere Maßnahmen – wie z. B. den Versand von E-Mails geografisch und zeitlich einzuschränken oder Multi-Faktor-Authentisierung – können nur auf Ebene der einzelnen Einrichtungen umgesetzt werden.

Emotet

„Emotet ist der König der Schadsoftware", heißt es vom Präsidenten des BSI in Deutschland. Kleine und mittelständische Unternehmen werden von der Software ebenso geplagt wie der IT-Verlag Heise, der Emotet im Frühjahr 2019 zum Opfer fiel, und etliche deutsche Hochschulen (im Herbst wurde u. a. die Medizinische Hochschule Hannover von Emotet befallen, im Winter die Justus-Liebig-Universität Gießen). Fälle wie diese zeigen, dass hier die gesamte IT-Infrastruktur eines Unternehmens oder einer Bildungseinrichtung in Gefahr sein kann.

Emotet wurde bereits 2014 entdeckt und ändert seine Vorgehensweise häufig. Ursprünglich als Verschlüsselungstrojaner konzipiert, hat sich die Software weiterentwickelt und operiert derzeit mit einem Schadsoftware-Auslieferungs-Modell als Dienstleistung für Dritte. Besonders gefährlich ist, dass Emotet authentisch wirkende E-Mails automatisiert erzeugen kann.

Wie operiert Emotet? Zuerst werden mit Hilfe von Phishing-Kampagnen Logindaten zu Mailboxen ausgespäht. Bei den betroffenen Accounts wird dann die Inbox ausgelesen. Die Kolleg*innen vom deutschen CERT-Bund berichteten am 11. 04. 2019 via Twitter: „Seit Ende 2018 späht Emotet aus Outlook-Postfächern nicht nur die Kontaktbeziehungen, sondern auch die ersten 16 kB jeder E-Mail aus. Diese ausgespähten E-Mails werden nun verwendet, um mit vermeintlichen Antworten die Schadsoftware weiter zu verbreiten." In Folge werden die ausgelesenen Bausteine genutzt, um spezielle E-Mails zu gestalten. Diese werden an Empfänger*innen versendet, mit denen der betroffene User bereits in Kontakt war. Die authentisch wirkenden E-Mails sind oft mit Schadsoftware (z. B.

Verschlüsselungstrojanern) oder einem Link zu einer Phishing-Seite versehen. Wird Schadsoftware nachgeladen, kann das verheerende Folgen haben, da sie sich im internen Netz ausbreiten und die lokale Infrastruktur kompromittieren kann. Das kann fatal enden, wenn z. B. die Windows-Domäne übernommen wird. Dann hilft oft nur ein kompletter Neu-Aufbau der IT-Infrastruktur.

Aus den vielen Empfehlungen und Ratgebern zum Umgang mit Emotet haben wir die folgende Liste aus „Lessons Learned" und Vorsichtsmaßnahmen zusammengestellt:

- Microsoft Office: Makros und OLE-Objekte deaktivieren, signierte Makros verwenden
- Emotet Spam-Mails blockieren (Spamfilter und AV-Lösung)
- bekanntermaßen mit Emotet in Verbindung stehende IP-Adressen blockieren
- Botnet-Kommunikation zu bekannten Emotet „Command and Control"-Servern blockieren
- SMB-Schwachstellen im internen Netzwerk identifizieren und absichern („Eternal Blue")
- Netzwerk segmentieren
- direkte Verbindungen zwischen Clients in einem Netzwerk mittels Firewall unterbinden
- Nutzer*innen sensibilisieren
- von Herstellern bereitgestellte Sicherheitsupdates zeitnah installieren
- zentral administrierte AV-Software verwenden
- regelmäßig mehrstufige Datensicherungen (Backups) durchführen
- regelmäßiges manuelles Monitoring von Logdaten, idealerweise ergänzt um automatisiertes Monitoring mit Alarmierung bei schwerwiegenden Anomalien
- Application Whitelisting verwenden (Windows AppLocker)
- Windows Script Host einschränken bzw. deaktivieren
- Zwei-Faktor-Authentisierung zur Anmeldung an Systemen verwenden (als Maßnahme gegen erbeutete Credentials)
- Dateiendungen standardmäßig im Betriebssystem anzeigen lassen
- Plain Text („Nur Text") statt HTML für E-Mails verwenden (größte Schutzwirkung!)
- E-Mails mit ausführbaren Dateien wie .exe, .scr, .chm, .bat, .com, .msi, .jar, .cmd, .hta, .pif, .scf, ... im Anhang (auch in Archiven wie .zip!) blockieren oder in Quarantäne verschieben

Ausblick

Für das Jahr 2020 erwarten wir, dass sowohl konventionelle Phishing-Kampagnen als auch Kampagnen wie Emotet weiter zunehmen werden. Universitäten und Bildungseinrichtungen sind aufgrund mehrerer Faktoren – wie z. B. ihrer offenen Netze und ihrer großen User-Zahl – besonders gefährdet. Obwohl die Zahl der Fälle noch gering ist, scheint es, als würden akademische Einrichtungen auch zunehmend in den Fokus gezielter Angriffe (im Gegensatz zu unspezifischen Bedrohungen wie durch Emotet) geraten. Zwar ist der Forschungs- und Bildungssektor schwerlich als finanziell attraktiv anzusehen; er verfügt aber häufig über eine hochperformante und weit offene IT-Infrastruktur mit guter Reputation in z. B. Firewalls. Die Abwägung zwischen Freiheit und Offenheit als Erfolgsfaktor für wissenschaftliche Arbeit einerseits und Kontrolle und Abschottung zum Schutz derselben andererseits wird längerfristig immer wieder neu zu diskutieren und zu definieren sein.

Christoph Campregher

ACOnet-CERT

Alexander Talos-Zens

Teamleiter
ACOnet-CERT

Community

Meetings & Workshops

12. – 13. März
Peering Days 2019

16. April
18. KUKIT-Stammtisch

9. – 10. Mai
12. ArgeStorage-Meeting

Vortrag bei den Peering Days (© Marko Iglic)

Peering Days 2019

12. – 13. März 2019
Zagreb/Kroatien

2019 fanden die jährlichen Peering Days in Zagreb statt. Mehr als 200 internationale Gäste nahmen an der zweitägigen Konferenz teil, die mit einem RIPE-Workshop zum Thema RPKI (Resource Public Key Infrastructure) startete. Das weitere Programm bot – wie immer – neben anregenden Vorträgen und Diskussionen auch ausreichend Zeit für bilaterale Meetings und Networking. Den krönenden Abschluss bildete ein hochinteressanter Vortrag von Richard Tang, Gründer des britischen Providers Zen Internet, zum Thema „Our AI Future".

Peering Days

- Die **Fachtagung** wird seit 2013 einmal jährlich veranstaltet und richtet sich primär an Internet Service Provider aus dem zentral- und osteuropäischen Raum.
- Der **Teilnehmerkreis** besteht großteils aus Personen, die in den Bereichen Peering-Koordination, Cloud-Administration und Netzwerk-/Datacenter-Betrieb tätig sind.
- Das **Programm** ist eine Kombination aus technischen Workshops, professionellen Präsentationen und Networking.
- Alle Infos: **www.peeringdays.eu**


Bilaterale Meetings bei den Peering Days (© Marko Iglic)

16. – 17. Mai
39. ArgeSecur-Meeting

28. Mai
DNSSEC-Workshop

5. Juni
DNSSEC-Workshop

6. – 7. Juni
59. TBPG-Sitzung

KUKIT – Kunst, Kultur & IT

18. KUKIT-Stammtisch

16. April 2019
Weltmuseum, Wien

19. KUKIT-Stammtisch

10. Dezember 2019
Schloss Schönbrunn, Wien

Beide KUKIT-Stammtische im vergangenen Jahr waren demselben Thema gewidmet: der Entwicklung einer gemeinsamen Schnittstelle für die Ticketsysteme österreichischer Kunst- und Kulturinstitutionen. Diese Idee wurde im April 2019 im Weltmuseum Wien erstmals präsentiert. Für viele Teilnehmer*innen war der 18. KUKIT-Stammtisch zugleich eine wunderbare Möglichkeit, das ethnografische Museum durch die Ausstellung „Nepal Art Now" kennenzulernen. Das verbindende Element Kunst vor allem sinnlich zu erfassen ist Teil des KUKIT-Konzepts. Direktor und Kurator Dr. Christian Schicklgruber hat diesen Ansatz in seiner Führung mehr als bestätigt. Vielen Dank!

Von der Idee zur Umsetzung: Beim 19. KUKIT-Stammtisch im Dezember wurden bereits konkrete Strategien für die Realisierung einer dezentralen Schnittstelle vorgestellt. Das Ziel: Die Buchungsprozesse für Ticketanbieter und Besucher*innen zu vereinfachen sowie kleinere und innovative Vertriebskonzepte zu ermöglichen. Mittlerweile ist das Projekt weit fortgeschritten (siehe Seite 46).

Nähere Informationen zu KUKIT finden Sie unter **www.aco.net/kukit-stammtisch**.

ArgeStorage

12. ArgeStorage-Meeting

9. – 10. Mai 2019
Alpen-Adria-Universität, Klagenfurt

13. ArgeStorage-Meeting

22. – 23. November 2019
nic.at, Wien

Das Frühjahrsmeeting 2019 der ArgeStorage fand im sonnigen Süden Österreichs – an der Alpen-Adria-Universität in Klagenfurt – statt. Den 19 Teilnehmer*innen wurden sechs Vorträge geboten. Neben den üblichen Themen wie Ceph, Seafile und iSCSI gab es diesmal auch Neues zu NVMe. Darüber hinaus wurde der gewohnte Themenkreis der ArgeStorage um den Bereich „Verarbeitung von Datenströmen" anhand der Open-Source-Software Apache Kafka erweitert. Der externe Gastvortrag kam von der Firma Pure Storage.

Das Herbstmeeting 2019 wurde bei nic.at in Wien abgehalten. 42 Teilnehmer*innen kamen in den Genuss von sieben Vorträgen. Die Präsentationen behandelten einerseits bekannte Produkte wie IBM Spectrum Scale, andererseits aber auch neue Storage-Konzepte wie z. B. LINBIT's LINSTOR oder Red Hat Stratis. Eine Fortsetzung fand zudem der Vortrag zu Apache Kafka vom Frühjahrsmeeting. In Wien gab es keinen Gastvortrag, dafür jedoch ein wenig Neues zum Thema Cloudstrategie, was für besonders angeregte Diskussionen sorgte.

Wir bedanken uns herzlichst bei unseren Gastgeber*innen und allen Vortragenden!

10. – 11. Oktober
40. ArgeSecur-Meeting

7. – 8. November
60. TBPG-Sitzung

22. – 23. November
13. ArgeStorage-Meeting

10. Dezember
19. KUKIT-Stammtisch

DNSSEC-Workshops

28. Mai 2019
nic.at, Wien

5. Juni 2019
Bundeskanzleramt, Wien

Bei einem DNSSEC-Vortrag von Arsen Stasic beim GovCERT im April 2019 kam der Wunsch nach weiteren Workshops zum Thema auf. Diese wurden kurzfristig in Wien organisiert und gemeinsam mit zwei Experten abgehalten: Norbert Stubenvoll vom Magistrat Wien behandelte das Thema Monitoring von DNSSEC; Wolfgang Breyha von der Universität Wien beleuchtete die Bereiche DANE und Mailing und wie diese mit DNSSEC zusätzlich abgesichert werden können. Herzlichen Dank an beide! In zwei ganztägigen Workshops wurden insgesamt 51 Personen geschult.

In den DNSSEC-Workshops wird nicht nur theoretisches Wissen vermittelt, sondern auch großes Augenmerk auf die Praxis und den täglichen Betrieb gelegt. Daher konfigurieren alle Teilnehmer*innen selbständig einen BIND-Nameserver und richten diesen mit einer eigenen Schulungsdomain ein. Sie erhalten auch Tipps bezüglich Monitoring und Überwachung sowie Hinweise zu den Risiken und möglichen Problemen von DNSSEC.

Da mittlerweile sowohl .ac.at als auch .gv.at mittels DNSSEC gesichert sind, können nun alle Domains im .at-Namensraum (außer .priv.at) signiert werden. Ende 2019 gab es unter .ac.at und unter .gv.at jeweils vier DNSSEC-signierte Domains.

Technische Betriebs- und Planungsgruppe

59. TBPG-Sitzung

6. – 7. Juni 2019
Anton Bruckner Privatuniversität, Linz

60. TBPG-Sitzung

7. – 8. November 2019
Universität für Bodenkultur, Wien

Themenschwerpunkt beim TBPG-Treffen in Linz war einer der jüngsten ACOnet-Standorte: jener in St. Johann / Pongau beim Zentralen Ausweichsystem des Bundes (ZAS). Nach der Vorstellung des Standorts durch Vertreter des Bundeskanzleramtes berichteten ACOnet-Teilnehmer (Österreichische Nationalbibliothek, Zentralanstalt für Meteorologie und Geodynamik, Statistik Austria) über ihr Setup am ZAS. Die Universität Klagenfurt zeigte, wie man noch zu IPv4-Adressen kommen kann, bevor sie zur Neige gehen. Gerade noch rechtzeitig, denn seit 25. November 2019 ist der Pool an verfügbaren IPv4-Adressen leer (siehe Seite 26).

Im Herbst 2019 fand die TBPG-Sitzung erstmals an der traditionsreichen Universität für Bodenkultur in Wien statt. Neben den üblichen Berichten des ACOnet-Teams über Neuigkeiten im Backbone- und Servicebereich präsentierten ACOnet-Teilnehmerorganisationen Lösungsansätze zur Konzeption und Implementierung neuer WLAN-Infrastruktur sowie verschiedene Möglichkeiten zur Automatisierung von Abläufen bei der Netzwerkkonfiguration und Statistikauswertung.

Kunst & Kultur im ACOnet

Zwei Ideen haben sich in den vergangenen Jahren zu langfristigen und erfolgreichen Projekten entwickelt: Das net:art coordination center und der KUKIT-Stammtisch (siehe Seite 37) leisten auf internationaler und nationaler Ebene vielbeachtete Pionierarbeit.

Ende März 2019 ging die Website **www.netart.cc** online. Das Thema: die Produktion von interaktiven Multi-Site-Performances in Echtzeit. Endlich hatte das net:art coordination center einen Webauftritt, der nicht nur einen dokumentarischen Auftrag erfüllte.

Alle ab 2015 gestalteten Projekt-Webseiten, die unsere komplexen Multi-Site-Produktionen **net:art | near in the distance 1–3** transparent und detailliert darstellen, sind nun gesammelt auf der Website www.netart.cc unter „past shows" zu finden. Durch die freundliche Unterstützung der Firma Kapsch konnten wir die definitiv erste und bisher einzige Website weltweit zum Thema „performing arts over advanced networks" (= net:art) erstellen, die sowohl umfangreich dokumentiert als auch neue Projekte bewirbt und kommuniziert. Videos und Fotogalerien veranschaulichen diese komplexen Produktionen der darstellenden Kunst, die sich mit den Herausforderungen und Möglichkeiten des digitalen Zeitalters beschäftigen – online und offline, auf inhaltlicher und technischer Ebene.

Anfang April 2019 stellten wir die neue Plattform sogleich den internationalen Teilnehmer*innen des Network Performing Arts Production Workshop (NPAPW) in Prag vor. Die Website erwies sich als ideales Werkzeug, um die geplante Projektserie „aaron's law" zu präsentieren und potentielle Kooperationspartner*innen zu interessieren. Aus den nachfolgenden Gesprächen entstand dann das Projekt „komitas vardapet" (**www.netart.cc/new_projects/komitas_vardapet**). Die Kolleg*innen von CESNET waren nicht nur herausragende Gastgeber des NPAPW 2019, sondern sind auch für die Entwicklung der Low-Latency- und Streaming-Technologien UltraGrid und MVTP verantwortlich, die wir in unseren Multi-Site-Produktionen verwenden.

Von Prag zum Ars Electronica Festival

Das New-Media-Team des Poznan Supercomputing and Networking Center (PSNC) war beim NPAPW 2019 in Prag ebenfalls dabei und beeindruckte mit einer begehbaren Ambisonic-Installation aus 24 Lautsprechern: In Zusammenarbeit mit drei polnischen Bands wurden drei Audio/Video-Sessions aufgenommen und als immersive VR/360°-Installation präsentiert, die später im Jahr auch beim Ars Electronica Festival in Linz zu sehen war. Das PSNC zeigte im Deep Space des AEC zudem ein spektakuläres 8K-Realtime-Streaming einer interaktiven Sound/Dance-Performance.

NPAPW Programme Committee

Als Mitglied des Programmkomitees ist ACOnet in die monatelangen Planungsphasen des jährlich (abwechselnd in den USA und Europa) stattfindenden Workshops involviert. Dieses internationale Meeting, das von GÉANT und Internet2 in Kooperation mit lokalen Gastgeber*innen organisiert wird, ist das wichtigste Treffen zum Thema darstellende Kunst innerhalb der transkontinentalen Wissenschaftsnetze (Infos unter **https://npapws.org/**).

Renate Kreil

ACOnet
Kunst- und Kulturkommunikation

Neue ACOnet-Teilnehmer 2019

Land Salzburg Landesinformatik
Institute of Advanced Research in Artificial Intelligence (IARAI) GmbH
Silicon Austria Labs GmbH
Technisches Museum Wien mit Österreichischer Mediathek
Central European University (CEU) GmbH

Beiträge von ACOnet-Teilnehmern

VIENNA SCIENTIFIC CLUSTER

Rechenpower für die Forschung:

Der Supercomputer VSC-4

Der Vienna Scientific Cluster (VSC) ist eine gemeinsame Einrichtung österreichischer Universitäten im Bereich Hochleistungsrechnen (High Performance Computing, HPC). Aktuelle Systeme sind der VSC-3 mit diversen Erweiterungen (siehe ACOnet Jahresbericht 2017, Seite 50) und der VSC-4, der im Sommer 2019 installiert und Anfang Dezember 2019 offiziell in Betrieb genommen wurde.

Das neue System VSC-4 ist technisch eine „Lenovo Scalable Cluster Solution" und extrem kompakt aufgebaut. Es benötigt (abgesehen vom Filesystem) 12 Rackschränke und verfügt über 790 Doppelsockel-Knoten vom Typ SD650 mit je 2 Prozessoren und 24 Kernen pro Prozessor. Insgesamt stehen also 37 920 Prozessorkerne zur Verfügung. Damit wird eine LINPACK-Leistung von 2,7 PetaFLOPS erreicht, was in der Top-500-Liste der schnellsten Supercomputer der Welt Platz 82 ergibt (Stand November 2019). Ein einzelner Knoten hat demnach 48 physische oder 96 virtuelle Kerne und erreicht eine LINPACK-Leistung von mehr als 3 TeraFLOPS. In der Grundausstattung verfügt jeder Knoten über 96 GB Hauptspeicher sowie eine SSD mit 480 GB für temporäre Daten. 78 Knoten sind mit je 384 GB und 12 Knoten mit je 768 GB Hauptspeicher ausgerüstet. Für die interne Vernetzung des Clusters wird Intel Omni-Path mit einer Bandbreite von 100 Gbit/s pro Richtung eingesetzt.

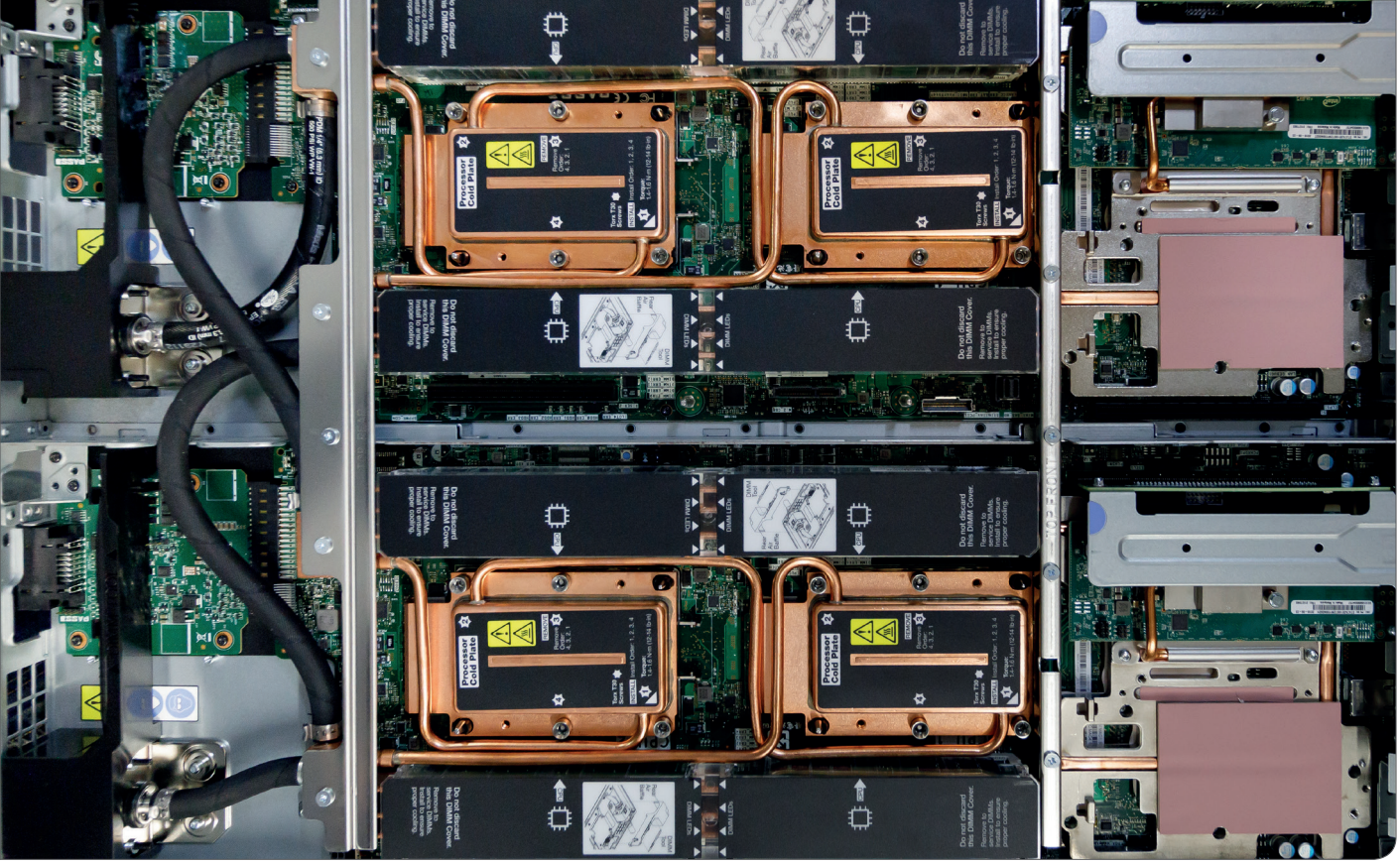
VSC-4: kompakt und leistungsstark (© derknopfdruecker.com)

Die Leistungsaufnahme des Systems beträgt bei normaler voller Auslastung etwa 400 kW und im Extremfall (etwa während eines LINPACK-Benchmarks) 600 kW. Der Großteil von etwa 85–90 % dieser Leistung wird mit Wasserkühlung abgeführt, der Rest über klassische Luftkühlung. Die Wasserkühlung kühlt über ein Netz von dünnen Kupferrohren alle wesentlichen Komponenten jedes einzelnen Knotens. Nur die Netzteile sind luftgekühlt.

Das speziell aufbereitete Kühlwasser hat im Betrieb eine Temperatur von 45–50° C und wird über denselben Sekundärkreislauf rückgekühlt, der auch den VSC-3 kühlt. Die hohe Temperatur ermöglicht ganzjährige Freikühlung ohne Kältemaschinen. Zur Rückkühlung der Luft aus den luftgekühlten Komponenten wird Kühlwasser mit 18° C von der hauseigenen Kälteanlage bezogen, die aus 2 TRANE Turbocor-Systemen mit je 2 Kompressoren besteht.

Infolge der teilweisen Luftkühlung hat das Kühlsystem des VSC-4 gegenüber der Öl-Immersionskühlung des VSC-3 eine deutlich erhöhte Komplexität und eine etwas schlechtere Energieeffizienz. Es hat allerdings andere Vorteile, etwa bei der Wartung von Komponenten.

Das Filesystem ist ein IBM Spectrum Scale (früher GPFS)-System mit 6 Fileservern, die auf 6 Storage-Server und ein IBM FlashSystem 9100 zugreifen.



Einschub mit zwei – von insgesamt 790 – SD650-Doppelknoten des VSC-4 (© derknopfdruecker.com)

Die Storage-Server nutzen je 120 Disks à 12 TB, also insgesamt 720 Disks mit in Summe 8,6 PB brutto. Das FlashSystem bietet NVMe-Devices mit einer Gesamtkapazität von 110 TB zur Speicherung von Inodes und kleinen Files.

Die Finanzierung erfolgt durch das Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) über die Leistungsvereinbarungen der fünf Partneruniversitäten (Universität Wien, Universität Innsbruck, TU Wien, TU Graz, Universität für Bodenkultur Wien) sowie über Projekte. VSC-3 und VSC-4 befinden sich in einem Gebäude der TU Wien im Arsenal, einem Gebäudekomplex im 3. Wiener Gemeindebezirk. Die TU Wien ist auch mit Management und Betrieb der Systeme betraut.

Die VSC-Systeme sind über zwei Leitungen mit jeweils 10 Gbit/s in das ACOnet eingebunden. Der Zugang für Benutzer*innen ist grundsätzlich nur via Netzwerk möglich.

Die Nutzung erfolgt für beide VSC-Systeme über Projekte mit Peer-Review und steht grundsätzlich allen Angehörigen der Partneruniversitäten offen. Für andere Universitäten und wissenschaftliche Einrichtungen wird der Zugang über eine Reihe von Abkommen bzw. über Pay-per-Use-Vereinbarungen ermöglicht.

Die Systeme des VSC werden von ca. 300 laufenden Projekten verschiedenster Fachrichtungen mit insgesamt rund 1200 Anwender*innen genutzt. Die fachliche Vielfalt und die daraus resultierende hohe Zahl verschiedener Anwendungsprogramme stellen für das VSC-Team eine große Herausforderung dar.

Weitere Infos

Falls dieser kurze Abriss Ihr Interesse geweckt hat, laden wir Sie herzlich ein, unsere Homepage **https://vsc.ac.at/** zu besuchen. Dort finden Sie alle Informationen zum Vienna Scientific Cluster, unter anderem auch die verschiedenen laufenden und abgeschlossenen Projekte und die daraus hervorgegangenen wissenschaftlichen Publikationen, die Liste der Institutionen mit Zugang zum VSC sowie aktuelle Hinweise auf Kurse, die auch für Außenstehende zugänglich sind.

Herbert Störi

Leiter des VSC Research Center
herbert.stoeri@tuwien.ac.at

Von der Idee zur Innovation:

Silicon Austria Labs

Silicon Austria Labs (SAL) ist ein europäisches Spitzenforschungszentrum für elektronikbasierte Systeme (EBS) – und seit 2019 ACOnet-Teilnehmer. In Zusammenarbeit mit Partnern aus Wissenschaft und Industrie bietet SAL an drei Standorten „Schlüsseltechnologien" an, die die Stärken aus dem österreichischen EBS-Ökosystem und verschiedenen Forschungsbereichen miteinander verbinden, um Innovation entlang der gesamten Wertschöpfungskette zu schaffen – von der Grundlagen- bis zur anwendungsorientierten Forschung.

Elektronikbasierte Systeme sind Komponenten, Baugruppen und Geräte mit Mikro- und Nanoelektronik sowie eingebetteter Software. Sie sind heute in fast jedem technischen Gerät – ob Smartphone, Tablet oder Fahrzeug – zu finden und bilden das technologische Rückgrat der Digitalisierung. SAL forscht daher an drei Standorten (Graz, Linz, Villach) in den Bereichen Sensor Systems, Power Electronics, RF (Radio Frequency) Systems, System Integration Technologies und Embedded Intelligence. In Eigenforschung und gemeinsam mit Projektpartnern entwickelt SAL Produkte und Prozesse für Technologien der Zukunft.

SAL-Team mit Demonstrator zur Verifizierung von thermischen Simulationen (© Carolin Bohn)

Mit Electronic Based Systems die Zukunft entfalten

Die Sensoren, als Sinnesorgane der Technik, nehmen Informationen auf, messen und analysieren. Die Leistungselektronik sorgt für eine energie- und leistungseffiziente Umsetzung, und mit der Hochfrequenzforschung sollen zukunftsweisende Kommunikations- und Radartechnologien entwickelt werden. Die umfassende Systemintegration stellt dann auf allen Ebenen ein funktionales Gesamtsystem sicher. Somit deckt SAL mit ihren Forschungsschwerpunkten die gesamte EBS-Wertschöpfungskette ab und entwickelt Technologien in den Bereichen Energie, Lifestyle, Gesundheit und Mobilität.

Grundlagenforschung mit österreichischen Universitäten

Für die Grundlagenforschung arbeitet SAL mit Universitäten und Fachhochschulen zusammen, um dort in sogenannten „Uni–SAL Labs" gemeinsame Forschung zu betreiben. An der FH Villach, der TU Graz und der JKU Linz forschen Mitarbeiter*innen von SAL und den jeweiligen Hochschulen bereits gemeinsam an diversen Technologien:

- Im Radio Frequency Front-End Lab (RFFE Lab) in Villach wird an Hochfrequenztechnologien und neuen Lösungen für die drahtlose Kommunikation in 5G und WLAN gearbeitet.

- Das TU Graz–SAL Dependable Embedded Systems Lab (DES Lab) beschäftigt sich mit der Zuverlässigkeit moderner computerbasierter Systeme, das EMCC and Radio InterOp Lab (EMCC Lab) mit der elektromagnetischen Verträglichkeit von elektronikbasierten Systemen.

- In Linz entstehen ein mmWave Lab und eine Testeinrichtung für die nächste Generation von Sensorik und Kommunikation bis zum hohen GHz-Frequenzbereich, während im eSPML Lab gemeinsam an Signalverarbeitung und maschinellem Lernen gearbeitet wird.

Diese „Uni–SAL Labs" bilden die Grundlage für die anwendungsorientierte Forschung, welche in kooperativen Projekten mit Industriepartnern umgesetzt wird.

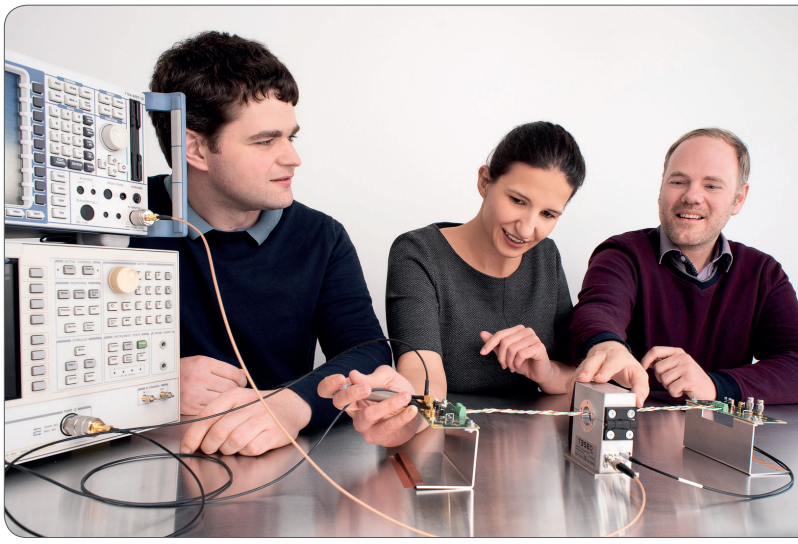
Kooperationsprojekte mit breiter Industriebeteiligung

„Tiny Power Box" ist eines der Vorzeigeprojekte für das Kooperationsmodell der SAL, welches den teilnehmenden Industriepartnern ermöglicht, ihre Kompetenzen zu vereinen und somit eine noch nicht dagewesene Innovationskraft zu schaffen, die ohne Bündelung der Kompetenzen und des Know-Hows nicht möglich wäre. Gemeinsam mit fünf österreichischen Leitbetrieben im Bereich der Leistungselektronik entwickelt SAL im Zuge des Projekts einen bidirektionalen Onboard-Charger, also ein eingebautes Batterieladegerät für E-Autos. Ganz speziell ist die hohe Ladeleistung bei einem geringen Volumen und Gewicht. Der hohe Wirkungsgrad des Gerätes ermöglicht dabei eine effiziente Nutzung der elektrischen Energie.

Mit Mikrospiegel um die Welt

Dass die Produkte heimischer Forschung auch international mitspielen, zeigt sich aktuell im Bereich Sensor Systems, wo SAL das Potenzial von mikroelektromechanischen (MEMS)-Mikrospiegeln für den Einsatz in Automobilsystemen untersucht. Die Vorteile für den Einsatz solcher Systeme liegen

Forscher*innen aus unterschiedlichen Bereichen arbeiten bei SAL gemeinsam an Projekten entlang der Wertschöpfungskette (© Carolin Bohn)



unter anderem in einer vergleichsweise erhöhten Leistung, einem verringerten Platzbedarf sowie einem vereinfachten Herstellungsprozess. Das Projekt wird im Januar 2020 auf der größten MEMS-Tagung in Vancouver einem breiten Fachpublikum präsentiert.

Gelebte wissenschaftliche Exzellenz

Im Forschungsdreieck Linz, Graz, Villach und durch Kooperationen mit (inter-)nationalen Partnern aus Wissenschaft und Industrie will SAL im Bereich EBS Österreich als Wirtschaftsstandort weiter stärken. ACOnet als Hochleistungs-Datennetz bietet hierbei eine hochwertige Stütze für die virtuelle Vernetzung über die Standorte hinaus. 2023 sollen mehr als 300 Top-Forscher*innen bei SAL an Innovationen entlang der EBS-Wertschöpfungskette arbeiten.

Isabella Preuer

Silicon Austria Labs GmbH
Communications & PR
press@silicon-austria.com
www.silicon-austria-labs.com

FIT in die Zukunft

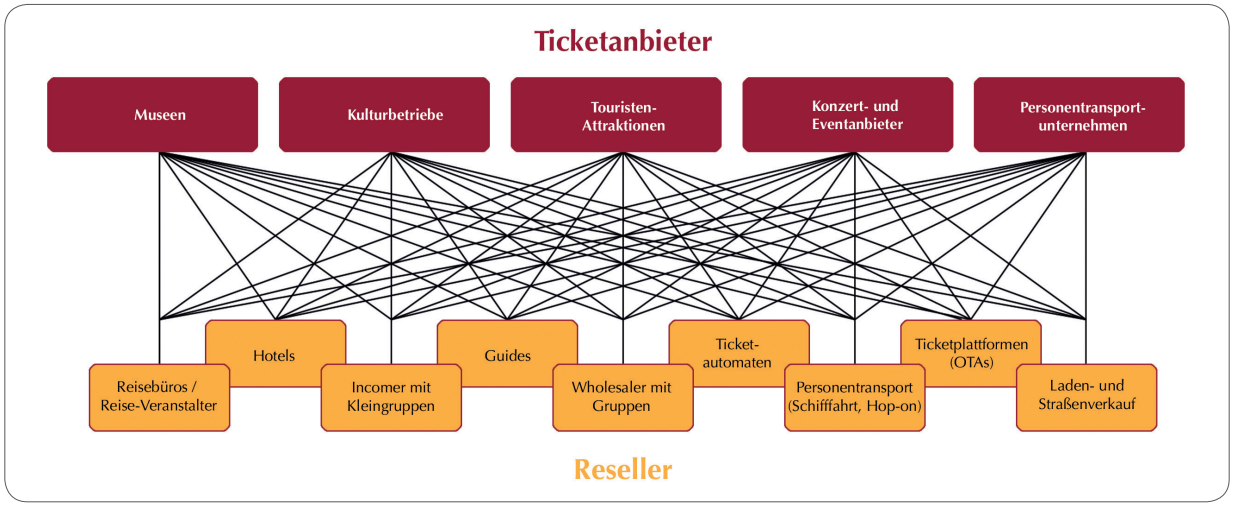
FIT ist eine technische Schnittstellenbeschreibung, die genutzt wird, um den Verkauf von Tickets zwischen Ticketanbietern und Resellern abzuwickeln. Die Idee dazu entstand im Umfeld von KUKIT (Kunst, Kultur und IT, eine Initiative von KHM-Museumsverbund und ACOnet – siehe Seite 37). Sie wurde im Laufe des Jahres 2019 von einem institutionsübergreifenden Projektteam bis zur Marktreife weiterentwickelt. Ihr Name stammt aus der Tourismusbranche: FIT steht dort für „For Individual Travel".

Bis dato müssen Ticketanbieter wie Museen oder Kulturbetriebe jegliche Art von Ticket-Wiederverkäufer*innen („Reseller") über separat einzurichtende Schnittstellen an ihr eigenes Verkaufssystem (Kassen, Warenwirtschaft, Buchhaltung) anbinden. Sollen mehrere Systeme angebunden werden, ist meist für jedes System eine eigene, proprietäre Schnittstelle zu implementieren. Das ist mit mehreren Problemen verbunden:

- hohe Einmalkosten für jede Schnittstelle,
- laufende Betreuung, Wartung bzw. Weiterentwicklung aller Schnittstellen,
- unterschiedliche Standards und Anforderungen an die Sicherheit.

Aufgrund dieser Probleme können oft nur die wichtigsten Anbindungen realisiert werden, da die Kosten einem möglichen Ertrag gegengerechnet werden müssen. Dadurch werden tendenziell nur große Player abgedeckt. Kleine, oft wünschenswerte, Kooperationen und kreative Marktkonzepte können durch den hohen technischen Realisierungsaufwand nicht umgesetzt werden.

Der Markt bietet einen Lösungsansatz durch Unternehmen, die Aggregatoren vertreiben – das sind Systeme, deren Aufgabe es ist, sich an unterschiedliche Systeme anzubinden. Hier entstehen allerdings Extrakosten pro Transaktion bzw. laufende Kosten, die direkt den Gewinn schmälern. Zudem können auch hier oft nur die großen Player angebunden und kreative Vertriebskonzepte nicht realisiert werden, da die Kosten pro Einzelprojekt immer noch erheblich sind.



Geschäftsbeziehungen zwischen Ticketanbietern und Resellern – eine komplexe Situation, derzeit geprägt von Einzellösungen, die durch eine einzige Schnittstelle ersetzt werden könnten (© Wolfgang Handl)

Ein anderer Vertriebsansatz ist die Verwendung von Vouchers (im Gegensatz zu direkt einlösbaren Tickets). Hier wird den Gästen der Tausch gegen eine Eintrittskarte überantwortet, was zu zusätzlichen Wartezeiten führen kann – in jedem Fall ist das Gesamterlebnis getrübt, und der Ticketanbieter muss auch dafür Ressourcen zur Verfügung stellen.

Der FIT-Ansatz

- Alle verwenden dieselbe Schnittstelle.
- Die XML-Schnittstelle ist einmalig zu implementieren (oder wird bereits vom Softwareanbieter bereitgestellt). Kosten für weitere Schnittstellen fallen somit nicht mehr an.
- Es gibt kein zentrales Service / keine Clearingstelle / keinen Man-in-the-Middle, daher entstehen keine ticketbezogenen Kosten.
- Alle könnten untereinander kommunizieren. Einzige Voraussetzung dafür ist ein Vertrag und somit der Wille zur Zusammenarbeit. Technische Hürden sind nicht mehr gegeben.
- Das Ergebnis soll immer ein Ticket sein, das der Gast direkt zum Eintritt verwenden kann. Die Live-Onlinebuchung gewährleistet, dass Zeitaufwand und dadurch Kosten reduziert werden.
- Die Abwicklung der Zahlung obliegt dem Reseller. Eine Abrechnungsmethode festzulegen ist Teil des direkt abzuschließenden Vertrages zwischen Ticketanbieter und Reseller.
- Ticketanbieter können direkt über die Schnittstelle umfangreiche Texte und Multimedia-Elemente als Produktbeschreibung zur Verfügung stellen (sowohl für Reseller als auch für Endkund*innen). Dadurch wird die Weitergabe korrekter Informationen an die Gäste erleichtert.

Mit der Verwendung der FIT-Schnittstelle werden sowohl aufseiten der Ticketanbieter als auch aufseiten der Reseller völlig neue Vertriebskonzepte

Für wen ist FIT interessant?

Ticketanbieter

- Museen, Kulturbetriebe, Touristen-Attraktionen
- Konzert- und Eventanbieter
- Personentransportunternehmen
- alle Anbieter, die Tickets über Vertriebspartner vertreiben
- **Möglichkeiten der Schnittstelle**:
  - Kategorien, Optionen, Größen, Farben denkbar
  - für Einzel- und Gruppentickets möglich
  - Sitzplatzkarten („Bestplatzbuchung“)

Reseller

- Reise-Veranstalter und Reisebüros
- Hotels
- Wholesaler mit Gruppen
- Ticketplattformen / Online Travel Agencies
- Incomer mit Kleingruppen
- eigene Ticketautomaten
- Transportunternehmen (Schifffahrt, Hop-on Hop-off)
- Guides
- Laden- und Straßenverkauf

Kosten für FIT

- Schnittstellenbeschreibung: **kostenfrei**
- Nutzungsgebühren einmalig/laufend: **kostenfrei**
- Programmierbeispiele / Beispiel-Implementation, um die eigenen Implementierungskosten zu reduzieren: **kostenfrei**
- Testsystem, gegen das in der Entwicklungsphase getestet werden kann: **kostenfrei**

möglich. Kooperationen, die bisher aufgrund der technischen Nebenkosten nicht rentabel waren, können realisiert werden. Vertriebswege können ausgetestet werden, ohne ein finanzielles Risiko durch Initialkosten eingehen zu müssen. Häuserübergreifende Kombitickets, die in entsprechende Produkte eingebunden werden, sind realisierbar.

Weitere FIT-Services (in Vorbereitung)

- **Zertifizierungsservice**: Um die technische Zuverlässigkeit sicherzustellen, kann eine Zertifizierung durchgeführt werden. Hierbei wird die eigene Schnittstelle durch eine Zertifizierungsstelle überprüft. Vertragspartner*innen können zwar auf diese Zertifizierung bestehen, grundsätzlich bleibt sie jedoch freiwillig. Die Kosten sind einmalig und werden noch festgelegt.

- **Vertragsplattform**: Um die Kontaktaufnahme mit Vertragspartner*innen zu erleichtern, wird eine kostenfreie Plattform zur Verfügung gestellt.

- **Reseller-Website**: Für Reseller, die die Schnittstelle nicht in ihr eigenes System integrieren wollen oder die gar keine Software besitzen, soll über eine Website der Zugriff auf alle Funktionen sowie eine Buchung durch den Reseller ermöglicht werden. Für die Nutzung dieser Reseller-Website werden laufende Kosten anfallen.

Die FIT-Schnittstelle soll sowohl Ticketanbieter als auch Reseller dabei unterstützen, kosteneffektive Projekte zu realisieren und kreative Vermarktungsmöglichkeiten zu erschließen.

Wolfgang Handl

Schloß Schönbrunn Kultur- und Betriebsges.m.b.H.
Digital Projects Manager
handl@schoenbrunn.at

Eine Cloud-Strategie für die Universität Wien

In Zeiten der Digitalisierung muss sich auch eine 650 Jahre junge Wissensorganisation wie die Universität Wien teilweise neu erfinden und anders denken. Im Zuge dessen wurde eine Initiative geschaffen, um die Entwicklungen von Cloud-Services im Sinne der Alma Mater Rudolphina zu beleuchten.

„Aller Anfang ist nebulös", könnte das Motto lauten, aus dem heraus diese Initiative entstand. In der Vergangenheit konnten viele Fragen rund um das Thema Cloud in Bezug auf Zuständigkeiten oder Kompetenzen nicht geklärt werden. Prinzipiell sollten durch die Initiative technische Kompetenzen in der IT und klare organisatorische Richtlinien an der Universität Wien geschaffen werden.

Hintergrund

Der Zentrale Informatikdienst (ZID) der Universität Wien wurde beauftragt, Empfehlungen für eine Cloud-Strategie und damit zu einem Umgang mit Cloud-Ressourcen zu erarbeiten. Dies wurde notwendig, da die Universität Wien bisher eine No-Cloud-Policy verfolgte, obwohl Angehörige der

Universität Wien längst Cloud-Dienste nutzen und aktuelle Software-as-a-Service(SaaS)-Produkte eine Cloud-Anbindung zwingend benötigen. Eine No-Cloud-Policy ist daher nicht mehr zeitgemäß.

Erkenntnisse

Vor, während und nach dem Projekt wurde innerhalb und außerhalb der Projektgruppe viel diskutiert, um einen Blick über den Tellerrand zu erlangen. Es wurden Schulungen zu Fortbildungszwecken besucht und über das GÉANT „IaaS Cloud Services" Framework Portfolio verschiedene Public-Cloud-Services getestet, um ein Gefühl für die Technik zu bekommen (die öffentliche Dokumentation dazu ist unter **https://wiki.univie.ac.at/display/iaas/** zu finden).

Am Ende des Projekts sind genügend Argumente und Anforderungen für und gegen die Nutzung der kommerziellen Public Cloud im Hochschulsektor zusammengekommen, welche in einem Empfehlungsbericht niedergeschrieben wurden (und auf Nachfrage gerne mit der ACOnet-Community geteilt werden). Trotz der technologischen Möglichkeiten ist jedenfalls zu berücksichtigen, dass die Cloud-Anbieter kommerzielle Unternehmen sind, die nicht nur den wissenschaftlichen Nutzen im Sinn haben, sondern die (Forschungs-)Daten der Universitäten verarbeiten wollen. Gerade diese Daten sind aber die schützenswerten Ressourcen einer Universität, was gegen ihre Auslagerung in eine kommerzielle Cloud spricht.

Überdies war beim Vergleich einer selbstbetriebenen (On-Premise-)Infrastruktur und einer Cloud-Infrastruktur keine konkrete Kosteneinsparung durch eine Cloud-Migration auszumachen. Vielmehr zeigte sich, dass ein in die Cloud ausgelagerter 24/7-Betrieb um ein Vielfaches teurer wäre als der Betrieb einer eigenen Infrastruktur.

Umsetzung

Die Universität Wien muss genau abwägen, ob die Nutzung von Public-Cloud-Services nötig und gewollt ist oder ob die Anforderungen auch mit universitätsinternen Ressourcen umgesetzt werden können. Eines der Ziele der Initiative war es, Know-how aufzubauen, um die Angehörigen der Universität Wien in diesen Fragen qualifiziert beraten zu können.

Konkret sollen in den nächsten drei Jahren folgende Maßnahmen umgesetzt werden:

- Awareness bei den Angehörigen der Universität Wien in Bezug auf ihren Umgang mit Daten schaffen,
- organisatorische Richtlinien erstellen und verabschieden,
- Change-Prozesse begleiten, die sich durch eine Cloud-Nutzung in der Organisation ergeben,
- Charakteristika der Cloud bei der Einführung und Weiterentwicklung von IT-Services berücksichtigen (z. B. Self-Service),
- Forschung und Lehre unterstützen (d. h. Forschungsschwerpunkte zu Cloud Computing, Studierende im Umgang mit Cloud-Plattformen ausbilden).

Die Universität Wien ist mit der Umsetzung einer Cloud-Strategie auf einem guten Weg – jedoch wird dies ein fortlaufender Prozess sein, für den Wissen, Ressourcen und Budget benötigt werden. Zumindest sollte die Initiative genutzt werden, um mit der Entwicklung von Cloud-Services Schritt halten zu können und eine stabile, langfristige Strategie planen zu können.

Christian Kracher

Universität Wien / ZID
Projektmanager
christian.kracher@univie.ac.at

EUROPEAN OPEN SCIENCE CLOUD

Developing EOSC

A view on an ongoing process, as per 31 January 2020

The official launch of the European Open Science Cloud (EOSC) took place during the Austrian EU presidency at the Vienna University Library in November 2018. After extensive co-creation processes and the inclusion of many stakeholders, the Governance is taking shape.

The vision

The goal of the European Open Science Cloud (EOSC) initiative is to offer European researchers a virtual environment with free, open, and seamless services for the storage, management, analysis and re-use of research publications, data and software that are linked to their research activities across borders and disciplines. The model proposed for EOSC is to federate existing and newly developed research data infrastructures under a common governance structure.

The history: EOSC – Not a cloud made in Brussels

What started, at the European level, with a Council conclusion on open, data-intensive and networked research as a driver for faster and wider information in 2015[1)], followed by a Council conclusion on the transition towards an open science system in 2016[2)], supported by the European Parliament by a resolution on the European Cloud initiative, led into a Council conclusion on EOSC in 2018[3)], and in November 2018[4)] finally resulted in the official launch of the European Open Science Cloud and its governance structure by the acclamation of the Vienna Declaration[5)].

The EOSC Governance, 2019–2020

The launch event[6)] marked the start of the first phase of an EOSC Governance within the „Horizon 2020" framework programme. Within a period of two years, the involved boards are expected to develop a model and legal framework in consultation with various stakeholders. The work will eventually result in a sustainable partnership model, clear rules of participation and funding schemes. The current tasks include steering the initial implementation, involving relevant stakeholders from research and infrastructures and enabling the transition to the second stage, EOSC post 2020.

The EOSC Governance Board

The EOSC Governance Board (GB) is an institutional group gathering representatives from the Member States and Associated Countries and from the Commission to ensure effective supervision of the EOSC implementation.

Formally, it is an EOSC Working Group (WG) of the Programme Committee for the specific programme implementing Horizon 2020 – the Framework Programme for Research and Innovation (2014–2020) – strategic configuration. It is tasked with approving

1) http://data.consilium.europa.eu/doc/document/ST-9360-2015-INIT/en/pdf

2) https://data.consilium.europa.eu/doc/document/ST-9526-2016-INIT/en/pdf

3) http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2017)599253

4) http://data.consilium.europa.eu/doc/document/ST-9029-2018-INIT/en/pdf

5) https://eosc-launch.eu/declaration/

6) https://eosc-launch.eu/home/

EOSC launch at the University of Vienna (© derknopfdruecker.com)

the list of the Executive Board members, deciding the strategic orientations for the EOSC (based on the advice of the Executive Board) and approving an annual work plan, assessing the progress of the EOSC implementation, ensuring coordination with relevant Member States/Commission initiatives as well as discussing new activities in support of the EOSC, including its long-term sustainability.

All European Member States and 10 Associated Countries are represented by delegates in the GB. In Austria, the country delegate is Stefan Hanslik from the Austrian Federal Ministry of Education, Science and Research.

The EOSC Executive Board

The Executive Board (EB) is a body of stakeholder representatives to help ensure proper EOSC implementation and accountability. It consists of representatives from the research and e-infrastructures communities, appointed by the European Commission.

The Executive Board is chaired by Karel Luyben (European Association of Universities of Technology – CESAER) and Cathrin Stöver (GÉANT). All Executive Board members are appointed in a personal capacity and represent pan-European organisations of relevance for the EOSC implementation, for example large pan-European research infrastructures, e-infrastructures, public research organisations, universities, public research funding organisations and industry organisations.

The EOSC Working Groups

Five EOSC Working Groups[7)] form an official part of the EOSC Governance structure to ensure a community-sourced approach to the current challenges of the EOSC. The Working Groups include experts from 22 of the EU Member States and Associated Countries and currently work on the following topics:

- Rules of Participation[8)],
- Landscape[9)],
- Sustainability[10)],
- Architecture[11)] and
- FAIR[12)].

7) https://www.eoscsecretariat.eu/eosc-working-groups

8) https://www.eoscsecretariat.eu/working-groups/rules-participation-working-group

9) https://www.eoscsecretariat.eu/working-groups/landscape-working-group

10) https://www.eoscsecretariat.eu/working-groups/sustainability-working-group

11) https://www.eoscsecretariat.eu/working-groups/architecture-working-group

12) https://www.eoscsecretariat.eu/working-groups/fair-working-group

Three more Working Groups are proposed and under preparation. These are:

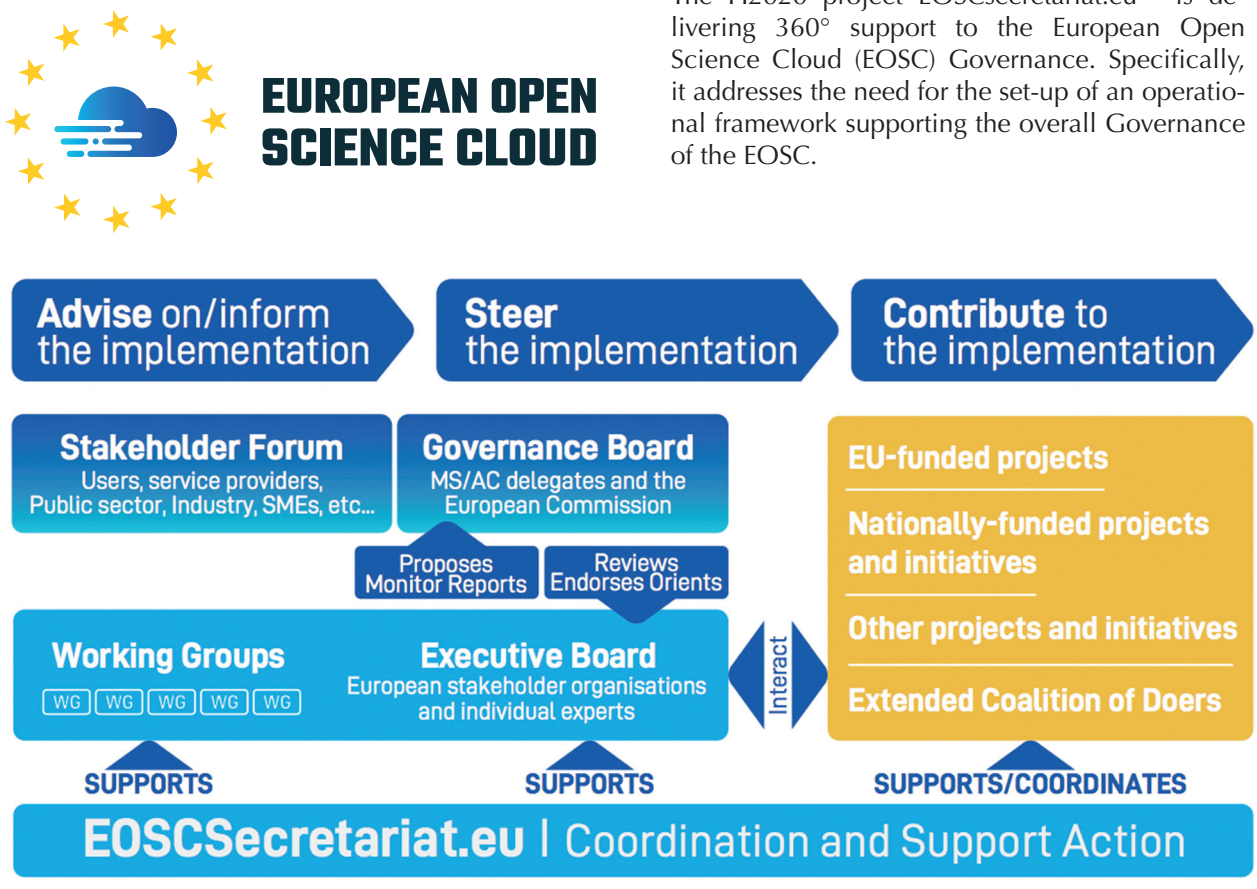
- Communications Task Force (run by EB/EC/Secretariat, tasked with branding, trademark and communications),
- Skills Development WG (proposed to run in 2020) and
- International WG (proposed to run in 2020).

With the support of the Working Groups, a first EOSC iteration is envisioned by the end of 2020:

- Agreed and tested Rules of Participation (Rules of Participation)
- Analysis of the existing national infrastructures and policies (Landscape)
- Financing model, legal entity & post 2020 governance (Sustainability)
- Functioning federated core (Architecture)
- Initial set of EOSC data and services (Architecture)
- EOSC Interoperability Framework (FAIR, Architecture & Rules of Participation)
- Persistent Identifier policy (FAIR & Architecture)
- Metrics for FAIR data and certified services (FAIR)

The H2020 Project „EOSC Secretariat"

The H2020 project EOSCsecretariat.eu[13] is delivering 360° support to the European Open Science Cloud (EOSC) Governance. Specifically, it addresses the need for the set-up of an operational framework supporting the overall Governance of the EOSC.



Composition of EOSC Governance (© EOSCsecretariat.eu)

EOSC explained in few words

EOSC is not a new infrastructure. It is rather a process of making publications, research data and software in Europe accessible to all researchers under the same conditions. Also, it does not start from scratch. It will be built upon existing infrastructures. A lot of investments were already made within the Horizon Europe framework programme. There are good examples of disciplinary research data infrastructures offering research data repositories and services.

The five so called „EOSC cluster projects" (ENVRI-FAIR, EOSC Life, ESCAPE, PaNOSC, and SSHOC) represent infrastructures for the environmental sciences, life sciences, high-energy physics and astronomy, photon and neutron sources, and social sciences and humanities. These projects are disciplinarily focused, EOSC, however, will also foster interdisciplinary and interoperability.

How can we imagine the functioning of EOSC?

Since we write this article for the Austrian NREN ACOnet, we would like to use a metaphor, aligned to one of the main and successful services provided for researchers: eduroam.

This service is well-known, ubiquitous, transparent, free at point of use, is extremely useful, has rules of participation, has system architecture including security, provides a specific (micro-)service, deals with user data and has a governance.

EOSC 2020+: An outlook

In a first phase, EOSC will focus on the deployment of services based on FAIR and open data. Possible „core functions" are at current status defined as follows:

- Develop and govern a federating core
- Manage compliance framework
- Manage trusted certification
- Authentication and authorisation services for allowing access by users. These rules and services have to comply with the EOSC AAI (Authentication & Authorisation Infrastructure) standards.
- Metadata services to allow for discovery
- Manage „EOSC" trademark(s)
- Manage Persistent Identifier (PID) services complying with the EOSC PID policy development
- Outreach to stakeholders
- Contribute to Horizon EU policy
- Monitor services and transactions

EOSC is not a new dedicated infrastructure or software package:[14]

- It is a process of making research data in Europe accessible to all researchers under the same conditions of use and usage.
- It gives a strong push in Europe towards a culture of open research data that are findable, accessible, interoperable and reusable (FAIR).
- It links the existing European data infrastructures, integrating high-capacity cloud solutions, and in due course, will widen the scope of these services to include users from the public sector and industry.
- Efforts are particularly directed on Data Culture, Research Data Services, Federated Architecture and co-Funding.

13) EOSCsecretariat.eu has received funding from the European Union's Horizon Programme call H2020-INFRAEOSC-2018-4, grant Agreement number 831644.

14) Paolo Budroni, Jean-Claude Burgelman, Michel Schouppe: Architectures of Knowledge: The European Open Science Cloud (https://www.degruyter.com/downloadpdf/j/abitech.2019.39.issue-2/abitech-2019-2006/abitech-2019-2006.pdf)

EOSC building processes – The Austrian involvement

Currently several Austrian representatives are directly involved in initiatives intended to shape the EOSC. The most relevant are:

TU Wien is actively involved in the H2020 Project EOSC Secretariat. Main tasks are the monitoring of the co-creation processes (WP2)[15] and the Stakeholders Engagement activities within WP3. Focus is the so called „researchers engagement" which comprises not only the researchers but also universities, university associations and funding bodies. TU Wien is represented in the project through a collaboration within the Faculty of Informatics, the Center for Research Data Management and TU Wien Bibliothek.

University of Vienna – H2020 Project EOSC Pillar: AUSSDA (Austrian Social Science Data Archive), based at Vienna University Library / University of Vienna, is partner in this project. Due to mutual agreements, there are some close links between activities of **Vienna University Library** and **TU Wien Bibliothek** in the fulfillment of some tasks in WP3 of EOSC Pillar. EOSC Pillar coordinates national open science efforts across Austria, Belgium, Germany, France and Italy, and ensures their contribution and readiness for the implementation of the EOSC. The project partners are from the following EU Member States: Austria, Belgium, Germany, France and Italy.

Project SSHOC: Austrian partner is the Austrian Social Science Data Archive (**AUSSDA**) based at **Vienna University Library / University of Vienna**. The project SSHOC aims to provide a full-fledged Social Sciences and Humanities Open Cloud (SSHOC) where data, tools, and training are available and accessible for users of SSH data.

EOSC Café: The EOSC Café is coordinated by the **BMBWF** and was created in the function of an Austrian platform for the exchange of information. It consists of representatives of the Austrian Federal Ministries responsible for science, research and innovation as well as digitalization, various stakeholders from Austrian universities, research infrastructures and funding agencies and of course the Austrian representatives of the EOSC Governance Board, Executive Board, the EOSC Secretariat and the Research Data Alliance (RDA-Austria). The dedicated aim of this group is to communicate and discuss the ongoing process of EOSC implementation by fostering the active participation of Austrian researchers and institutions.

WGs Landscape and Sustainability

The **„Landscape Analysis" Working Group** has the task of providing options allowing a progressive EOSC convergence and alignment of structures and initiatives in Europe including national research infrastructures and e-infrastructures, national open science policies, ESFRI RIs and cluster projects, thematic initiatives and clouds, EOSC-relevant H2020 projects and international Working Groups (such as RDA, etc.). **TU Wien Bibliothek** participates in the Landscaping activities.

The **EOSC Sustainability Working Group** provides a set of recommendations concerning the implementation of an operational, scalable and sustainable EOSC federation after 2020, which will be gradually opening up its user base to the public sector and industry. The Working Group examines

15) EOSCsecretariat.eu retains a high degree of flexibility in its roll-out plan by adopting a co-creation approach and providing budget for all upcoming, foreseen and unforeseen, activities and actions related to the work of the EOSC Secretariat to support the EOSC Governance. https://www.eoscsecretariat.eu/funding-opportunities/co-creation-requests

16) https://youtu.be/qYyliQp5Fkk

17) https://youtu.be/DSVmqH_HrcY

18) https://youtu.be/KbzAfZ80iPs

19) https://www.eoscsecretariat.eu/events/what-do-our-researchers-want-workshop-%E2%80%9Ccollect%E2%80%9D-needs-requirements-and-visions-ideal-future

core aspects related to the business model of EOSC, its governance structure and propose options for the best-fit legal entity to be put in place after 2020. **TU Wien Bibliothek** participates in the Sustainability WG activities.

The results of both Working Groups are expected to be openly available within 2020.

Videos produced by the EOSC Secretariat/TU Wien:
- EOSC What You Need to Know[16)]
- The Backbone of EOSC[17)]
- EOSC A Sustainable Future[18)]

Further steps in QI/QII 2020

Besides the regular meetings of GB, EB, Working Groups, as well as EOSC Secretariat activities (Steering Group and co-creation activities), several events are scheduled for February/March 2020:
- Workshop/Discussion with the members of the Science Europe Working Group on Data Sharing Supporting Infrastructures (WG DSSI).
- Elaboration and release of the findings of a workshop with young European researchers held in Feldkirch, Austria in January 2020. This workshop was about „collecting" needs, requirements and visions on future research environments.[19)]
- Elaboration and release of the findings of a workshop with European Universities Networks and Associations, held in Brussels in January 2020 (Title: „University Networks shaping EOSC" – https://www.eoscsecretariat.eu/events/university-networks-shaping-eosc-workshop).
- Validation Workshop, organised by the EOSC Landscape Working Group in collaboration with the EOSC Secretariat project. The goal of the event is to discuss and validate the Landscape Analysis Report's first draft with experts from GB, EB as well as INFRAEOSC-5B projects, ESFRI research infrastructures, and the other EOSC EB Working Groups.

All announcements are published at: **https://www.eoscsecretariat.eu/news-events-opinion/events**

About the Authors:

Paolo Budroni

paolo.budroni@tuwien.ac.at

Paolo Budroni is member of permanent staff of the University of Vienna (since 1991), and currently on a long-term sabbatical. Since September 2019 he is member of staff of TU Wien Bibliothek, and is in charge of International Projects. Paolo Budroni is E-IRG Chair and is participating in these EOSC building initiatives: EOSC Secretariat, EOSC Pillar, Working Group Landscape Analysis and Working Group Sustainability. He is co-author of the „Vienna Declaration on the EOSC".

Stefan Hanslik

stefan.hanslik@bmbwf.gv.at

Austrian Member of the EOSC Governance Board, coordinator of the EOSC Café, Austrian E-IRG Delegate, co-author of the „Vienna Declaration on the EOSC"

Barbara Sánchez Solís

barbara.sanchez@tuwien.ac.at

Barbara Sánchez Solís, Head of the Center for Research Data Management at TU Wien, is member of the EOSC Secretariat and of the EOSC Secretariat Steering Group. She coordinates co-creation activities within WP2 and participates in Stakeholder Engagement.

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

www.aco.net/jahresberichte

Gastautor*innen

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

- Christian Bösch, FH Vorarlberg
- Peter Gruber, Universität Klagenfurt
- Herbert Störi, VSC Research Center
- Isabella Preuer, Silicon Austria Labs GmbH
- Wolfgang Handl, Schloß Schönbrunn Kultur- und Betriebsges.m.b.H.
- Christian Kracher, Universität Wien
- Paolo Budroni, TU Wien | Stefan Hanslik, BMBWF | Barbara Sánchez Solís, TU Wien

Fotocredits

Cover: © derknopfdruecker.com | Seite 10/11: © Günther Großauer | Seite 12 (unten): © Michael Perzi | Seite 16–17: © FH Vorarlberg
Seite 22: © MANRS | Seite 26: © RIPE NCC | Seite 31: © ACOnet | Seite 36: © Marko Iglic | Seite 42–43: © derknopfdruecker.com
Seite 44–45: © Carolin Bohn | Seite 46: © Wolfgang Handl | Seite 51: © derknopfdruecker.com | Seite 52: © EOSCSecretariat.eu

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