DIGITALE HOCHSCHULE NRW

Datum:25.10.2019

Antrag für fördergestützte Kooperationsvorhaben

Diesem Antrag sind als Anlagen ausschließlich beizufügen:

1. **Votum der thematisch einschlägigen Input-Gruppe(n)**
2. **Letter of Intent der Kooperationspartner**
3. **Finanzierungsplan**
4. **Meilensteinplanung**

Bitte beachten Sie die Hinweise zu Skizzen, Anträgen und Vorschlägen von Förderlinien an die DH.NRW unter: www.dh.nrw.de/foerderung

Titel des Kooperationsvorhabens

Kooperationsvorhaben sind in der Nomenklatur „Projekttitel.nrw" zu bezeichnen.

„Anti-Spam-Cluster NRW" asc.nrw

Antragstellende/Konsortialführende Hochschule

Bezeichnung und Adresse des öffentlich-rechtlichen Mitglieds der Digitalen Hochschule NRW

Rheinische Friedrich-Wilhelms-Universität Bonn

Regina-Pacis-Weg 3

53113 Bonn

Ansprechpartner/Projektverantwortliche

Dr. Rainer Bockholt, Direktor des Hochschulrechenzentrums

[redacted]

Beteiligte Hochschulen des Konsortiums

Ausschließlich öffentlich-rechtliche Hochschulen, die Mitglied in der Digitalen Hochschule NRW sind, und Einrichtungen des Landes

Universität Bonn (Konsortialführer)
Technische Universität Dortmund
Universität Siegen
RWTH Aachen
Ruhr-Universität Bochum
Universität zu Köln

WWU Münster
Fernuniversität in Hagen
DSHS Köln
Fachhochschule Aachen
Technische Hochschule Köln
Hochschule Ruhr West
Westfälische Hochschule
Hochschule Bonn-Rhein-Sieg
Hochschule Rhein-Waal
Hochschule für Musik und Tanz Köln
Hochschule Hamm-Lippstadt
IUK NRW

Involvierte Inputgruppe(n)

Welche Inputgruppe(n) unterstützen das Kooperationsvorhaben?
Eine Übersicht der Inputgruppen finden Sie in § 2 Abs. 3 der Verfahrensordnung der DH.NRW.

Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren in Nordrhein-Westfalen ARNW

Laufzeit des Kooperationsvorhabens

[redacted]

Gesamtförderbedarf

Angabe der Gesamtsumme sowie Aufteilung auf die Haushaltsjahre

[redacted]

Bankverbindung (ggf. Verwendungszweck)

Universitätskasse Bonn

Sparkasse KölnBonn
Konto-Nr. 576 95
BLZ 370 501 98
IBAN: DE08 3705 0198 0000 0576 95
BIC: COLSDE33

Ust-IdNr. DE 122 119 125

Verwendungszweck: „Anti-Spam-Cluster.NRW“

Kurzbeschreibung des Vorhabens

Max. ½ Seite

Die Abwehr von E-Mails mit schädlichem Inhalt, sogenannte Spammail, ist eine dauernde Herausforderung zur sicheren Nutzung des Mediums E-Mail. Bis zu 90% der Anzahl von Zustellversuchen von E-Mails sind Spammails, so dass zur Abwehr leistungsfähige Systeme, sogenannte Appliances, erforderlich sind. Heute sind an 16 NRW-Hochschulen und der IuK NRW Hardware Appliances (Appliance = Kombination aus physischem Gerät, Betriebssystem und darauf laufender Applikation) im erfolgreichen Dauereinsatz und schützen so etwa 360.000 Mailboxen. Neue technische Entwicklungen erlauben es nun, diese als sogenannte virtuelle Appliances mittels „Cloud-Technologie" zu betreiben. Losgelöst von Hardware vor Ort können diese in virtuellen Cloudumgebungen betrieben werden und darüber hinaus losgelöst von der jeweilig nutzenden Einrichtung. Die Diensterbringung eines Anbieters für einen Abnehmer erfolgt quasi transparent, Betriebskompetenz muss nicht mehr in allen Einrichtungen vorgehalten werden und trägt somit zur Entlastung vor Ort bei. Darüber hinaus sind komplexe „Katastrophenfall"-Szenarien auch über Weitverkehrsverbindungen möglich und sorgen so für eine sehr hohe Verfügbarkeit. Die Anti-Spam-Cluster integrieren sich dank der verwendeten Cloud-Technologie nahtlos als weiterer Dienst in die Hochschulcloud.nrw. Sie unterstützen dabei ausdrücklich auch andere Vorhaben der DH.NRW wie die „AcademicGroupware.nrw" oder ergänzen sich gegenseitig mit „security.nrw"

Darstellung des Landesinteresses

asc.nrw wird einen wesentlichen Beitrag nicht nur zur E-Mailsicherheit sondern darüber hinaus zur gesamten IT-Sicherheit der NRW Hochschulen leisten. Ohne eine wirksame Spam-Abwehr ist weder eine zuverlässige Nutzung dieses Kommunikationsmediums möglich, noch sind die Auswirkungen der über Spam verteilten Schadsoftware unter Kontrolle zu halten.
Das Land NRW und seine Hochschulen werden für die gesamte Laufzeit des Vorhabens maßgeblich von der Absicherung einer zuverlässigen elektronischen Kommunikation profitieren. Darüber hinaus trägt das Vorhaben maßgeblich zur Konsolidierung und Standardisierung (alle NRW-HS mit allen ihren Mitglieder sind nutzungsberechtigt) für eine digitale Servicestruktur bei.

Das Vorhaben könnte ohne die Förderung des Landes nicht im erforderlichen Umfang durchgeführt werden

☒ **ja** ☐ **nein (Subsidiarität)**

1. **Kooperation**

Weist das Vorhaben einen hochschul(arten)übergeifenden Bezug auf?

ja ☒ **nein** ☐

2. **Programmatischer Bezug**

Weist das Vorhaben einen Bezug zum „Positionspapier der Digitalen Hochschule NRW zu den Handlungsfeldern Studium und Lehre sowie Administration und Infrastruktur" vom März 2018 auf?

ja ☒ **nein** ☐

3. **Einschlägiges Handlungsfeld**

In welchem bzw. welcher der Handlungsfelder der DH.NRW ist das Vorhaben seinem Schwerpunkt nach zu verorten?

☐ **Studium & Lehre**

☐ **Administration**

☒ **Digitale Infrastruktur**

4. **Skalierung**

Wie viele Mitgliedshochschulen werden bei Realisierung des Vorhabens an der vorgeschlagenen Lösung potentiell partizipieren?

☐ **2 – 10** ☐ **> 10** ☒ **alle 42**

Welche Hochschularten werden von dem Vorhaben potentiell profitieren?

☒ **Kunst- und Musikhochschulen**

☒ **Fachhochschulen**

☒ **Universitäten**

5. **Art des Vorhabens**

☒ **Vorschlag einer zeitlich begrenzten Maßnahme**

☐ **Vorschlag eines dauerhaften Service**

Beschreibung des Kooperationsvorhabens

Die Beschreibung des Kooperationsvorhabens sollte maximal 36.000 Zeichen inkl. Leerzeichen (ca. 12 Seiten) umfassen. Auf die den Hinweisen zu Anträgen beigefügten Bewertungskriterien 4 bis 14 ist einzugehen.

Zielesetzung(en)

Z.B. Steigerung der Qualität der Lehre, Verbesserung der Forschungssituation, Steigerung der Effizienz von Verwaltungsabläufen

E-Mail ist nach wie vor das meistgenutzte Kommunikationsmedium, häufig sogar verpflichtend für die Kommunikation der jeweiligen Hochschule mit ihren Studierenden und Mitarbeitenden und vice versa. Die sichere Nutzung ist nur möglich, wenn es den Betreibern der E-Mailsysteme gelingt, diese vor Spam-Mail zu schützen. Mittels virtueller Appliances wird dieser Schutz vor Spam-Mail erreicht. Darüber hinaus werden Cluster aus den Appliances aufgebaut. Diese sowohl als reine Hosting-Lösung (der Anbieter überlässt dem Nachfrager eine virtuelle Maschine, auf der der Nachfrager seine eigene virtuelle Appliance betreibt) als auch als „Full Service": der Anbieter übernimmt den kompletten Betrieb der virtuellen Appliance für den Nachfrager.
In verschiedenen Kombinationen wird die gesteigerte Ausfallsicherheit erprobt: Redundanz an einem Standort, Redundanz über zwei oder mehrere Standorte und Redundanz über Weitverkehrsstrecken für echten „K-Fall"-Schutz.

[redacted] Wesentliche Vorarbeiten zu diesem Fernziel werden in diesem hier vorliegenden Antrag adressiert, erarbeitet und auf Praxistauglichkeit hin überprüft, so dass am Ende der Laufzeit konkrete Empfehlungen für die Umsetzung der Anti-Spam-Center stehen werden.

Zielgruppen

Z.B. Studierende, Lehrende, Forschende, Verwaltung

Alle Mitglieder aller staatlichen Hochschulen in NRW

Ausführliche Beschreibung des Vorhabens

Inkl. Organisation des Konsortiums, Darstellung der Arbeitspakete und des Qualitätsmanagements

E-Mail ist als Kommunikationsmedium auch perspektivisch in der Unternehmenskommunikation nicht zu ersetzen. Insbesondere weite Verbreitung, hohe Standardisierung und einfache Bedienbarkeit machen es auch auf viele Jahre hinaus zum asynchronen Kommunikationsmedium Nummer eins. Neben den vielen Vorteilen von E-Mail gibt es durchaus auch Nachteile, die im Wesentlichen der zeitlich sehr frühen Entwicklung des E-Maildienstes im Kontext elektronischer Kommunikation geschuldet sind. Die „Schwächen" des E-Mailsystems werden von verschiedensten „Interessengruppen" auch massiv zur Verteilung von Schadsoftware, sogenannter Spam-Mails, ausgenutzt. Dem relativ günstigen Stückpreis von E-Mail ist es zuzuschreiben, dass heute bis zu 90% der Einlieferungsversuche auf E-Mailservern schadbelastet sind. Um dauerhaft eine zuverlässige Nutzung des E-Mailsystems sicherstellen zu können, sind zuverlässige Abwehrmaßnahmen erforderlich. Unter anderem durch gesetzliche Vorgaben (Telekommunikationsgesetz) dürfen Betreiber von E-Mailschutzsystemen nicht in die jeweilige E-Mail „hineinschauen", sondern müssen geeignete Filterparameter auf die jeweilige E-Mail „von außen" anwenden. Dabei ist die eigentliche Erkennungsrate ein wichtiger Parameter. Noch wichtiger allerdings ist die Quote der sogenannten

„false positives", also sauberer E-Mails, die irrtümlich als schlecht deklariert werden: nur wenn diese Quote sehr niedrig ist, erreicht das System eine gute Akzeptanz und Nutzbarkeit.

BEDARF:

Das „Spamgeschäft", es sind in der Regel (kriminelle) kommerzielle Anbieter die Spamdienste anbieten, bewegt sich seit Jahren auf einem konstant hohen Niveau. Im langjährigen Mittel schwankt der schadbehaftete Anteil von Mail-Zustellversuchen im Bereich um die 90%, d.h. dass insgesamt nur etwa jede zehnte E-Mail eine Nutzmail ist. Hochgerechnet auf die NRW-Hochschulen ergeben sich pro Tag viele Millionen Zustellversuche von Spam-Mail, mit dem vollen Risikopotential dahinter: nur ein einziger unbedacht geöffneter E-Mailanhang mit Schadsoftware kann massive Schäden im gesamten internen Netz einer Hochschule anrichten. Um dieser Bedrohung effektiv entgegenzutreten, betreiben heute alle NRW-Hochschulen einen E-Mailschutz auf verschiedener technischer Basis. Das größte, aus 16 Hochschulen und IuK bestehende Konsortium in diesem Bereich ist die „Internet Security NRW" unter Konsortialführerschaft der Universität Bonn. Dieses Konsortium setzt seit Jahren erfolgreich sogenannte Appliances, also eine Kombination aus Hardware, Betriebssystem und Applikation, [redacted] ein. Die Betriebserfahrungen mit den Appliances sind umfassend positiv: beste Erkennungsrate, nicht messbare false positives und hohe Systemstabilität. Nachteilig ist bislang, dass die Hardware an jeder Standorthochschule betrieben werden muss: damit müssen zum ausfallsicheren Betrieb jeweils mindestens zwei, bei größeren Installationen auch mehr, Appliances vorgehalten und betreut werden.

IMPLEMENTIERUNG:

Technische Entwicklungen erlauben es heute, dass die Appliances nicht mehr auf Hardwarebasis betrieben werden müssen, sondern dass sie auch als sogenannte virtuelle Appliances basierend auf Cloud-Technologie zur Verfügung stehen. Damit eröffnen sich ganz neue Möglichkeiten in der kooperativen Diensterbringung. Interne Mechanismen der Hostsysteme, die die virtuellen Appliances beherbergen, tragen zu einer verbesserten Betriebsstabilität bei, da diese per se auf Ausfallsicherheit ausgelegt sind. Perspektivisch sind hier auch Dienste wie Infrastructure as a Service nutzbar, [redacted] Eine Kopplung verteilter virtueller Appliances über Weitverkehrsstrecken (WAN: Wide Area Network) bringt signifikante Ausfallsicherheit, selbst im sogenannten Katastrophen-Fall.

Neben der verbesserten und vereinfachten Betriebsstabilität ist auch die Bildung von Hochschulclustern möglich: ein Anbieter und Betreiber von virtuellen Appliances kann dies transparent auch für Abnehmer tun und so deutlich zur Entlastung vor Ort beitragen: Betriebskompetenz muss im Wesentlichen nur noch bei den Anbietern vorgehalten werden und nicht bei jeder nutzenden Hochschule. Mit Blick auf andere intendierte Vorhaben der DH-NRW [redacted] können auch diesem kommenden System virtuelle Appliances vorgeschaltet werden, ohne dass man sich damit heute schon auf ein Groupware-Produkt festlegen muss.

Durch die aktive Hochschul-Community zur „Internet Security NRW" und die dortigen Erfahrungen ist eine Implementierung der neuen Technologie in kurzer Zeit, [redacted] möglich.

Geeignete Hosts für virtuelle Appliances stehen in vielen NRW Hochschulen zur Verfügung und können von dort Kooperationspartnern auch angeboten werden.

KONSORTIALSTRUKTUR:

Aufgrund der Vorerfahrungen mit der „Internet Security NRW" ist die Universität Bonn bereit, die Konsortialführerschaft für asc.nrw zu übernehmen. Neben den Verhandlungen mit den Anbietern und der eigentlichen Beschaffung wird der Konsortialführer sich um die Identifizierung der Cluster bemühen, also sowohl Anbieter als auch Abnehmer der virtuellen Appliances zu identifizieren und zu koordinieren, [redacted]

Darüber hinaus ist eine flache Konsortialstruktur geplant, [redacted] Bedarfsgerechte Erfahrungsaustausche werden vom Konsortialführer organisiert, ebenso technische Workshops, diese vor allem in der Einführungsphase, in Abstimmung mit dem Hersteller.

Die Teilnahme am Konsortium steht allen NRW-Hochschulen initial und auch während der Laufzeit offen, eine möglichst umfassende Teilnahme ist ausdrücklich erwünscht. In den Anbietergesprächen wird auch darauf ausdrücklich hingearbeitet. Allein schon durch die initial teilnehmenden HS sind schon zu Projektbeginn 360.000 Mailboxen geschützt; durch eine angestrebte Vereinheitlichung [redacted] ist zu erwarten, dass diese Anzahl in der Laufzeit noch wesentlich ansteigt.

Der Hersteller des Anti-Spam-Produktes [redacted] hat in Vorgesprächen zugesagt, technische Workshops in der erforderlichen Anzahl zur bestmöglichen Implementierung ohne Zusatzkosten durchzuführen.

QUALITÄTSMANAGEMENT

Ein dediziertes Qualitätsmanagement ist für das Vorhaben asc.nrw nicht erforderlich, da eine wirklich permanente Überprüfung durch die Anwender sattfindet: bei nur kleinen Störungen des Systems werden die Auswirkungen sofort für viele Nutzer sichtbar, so dass Spam ggf. in Massen zugestellt wird. Das Konsortium wird jeweils alle erforderlichen Maßnahmen ergreifen, um höchste Qualität und damit Nutzerzufriedenheit sicherzustellen. Die erforderliche Kompetenz dazu ist bei den Konsortialteilnehmern vorhanden.

NACHHALTIGKEIT:

Das Vorhaben ist auf zunächst [redacted] ausgelegt. Die Erfahrungen, die während der Laufzeit gewonnen werden, können auch nach dem Ende der Laufzeit weiterverwendet werden. Perspektivisch ist gut vorstellbar, dass sich die NRW Hochschulen in einer nächsten Förderperiode auf zwei oder drei Anti-Spam-Cloud-Cluster verteilt über das Land konzentrieren; damit wäre die maximale Synergie erreicht, es müssen aber umfangreiche technische und vor allem administrativ/rechtliche Randbedingungen geprüft werden. In einer Förderperiode [redacted] anschließend wäre dies sicher möglich.

MEILENSTEINPLANUNG

1) Identifizierung und Vorklärung der „use cases“ [redacted]

2) Erarbeitung der technischen, organisatorischen und rechtlichen Voraussetzungen für Hosting, Full Service und WAN-Kopplung: [redacted]

3) Exemplarische Umsetzung und Erprobung mit Pilotpartnern für Housing, Full Service und WAN-Kopplung [redacted]

4) Sukkzessive Überführung der use cases in den Produktivbetrieb aller Konsortialpartner [redacted]

5) Sukkzessive Aufnahme von „Noch-Nicht-Konsortial-Teilnehmern“ [redacted]

6) Vorarbeiten zu einer weiteren Konsolidierung der Anti-Spam-Cluste [redacted]

Finanzierungsplan

Das Vorhaben hat eine Laufzeit von [redacted] Die Lizenzgebühren für die virtuellen Appliances und der Anti-Spam-Software betragen inklusive aller Updates in der Zeitspanne [redacted] Dabei ist die Anzahl der virtuellen Appliances nicht beschränkt, das Konsortium kann jederzeit die Anzahl den jeweiligen Bedarfen ohne zusätzliches Entgelt anpassen. [redacted] Ein Beitritt weiterer Konsortialteilnehmer ist jederzeit möglich und ausdrücklich erwünscht.

Professionalität des Konsortiums

Erläuterung, warum das jeweilige Konsortialmitglied für die Erbringung des jeweiligen Arbeitspaketes geeignet ist.

Das Konsortium asc.nrw basiert auf den jahrelangen Betriebserfahrungen des Konsortiums „Internet Security NRW". Verteilt auf fast zwanzig NRW-Hochschulen ist so über die Zeit höchste und beispiellose Kompetenz zu E-Mailsicherheitsfragen entstanden. Die Kommunikation und der Austausch zu allen Fragen in diesem Zusammenhang (rechtlich, betrieblich, technisch) sind etabliert und werden auf hohem Niveau weitergeführt. Das Konsortium kann alle anstehenden Arbeiten und Aufgaben bestens erfüllen.

Ort, Datum

Unterschrift der gemäß § 18 Abs. 1 HG oder § 18 Abs. 1 KunstHG ermächtigten Person