

# WhiteList-Konzept

## Wie weit kommt man ohne die tiefe Analyse der vorhandenen IT ?

### Ergänzendes Material zum Papier IT-Sicherheit an Hochschulen

Erarbeitet durch den AK-„IT-Sicherheit“ von Herbst 2004 bis Sommer 2005  
Version 1.0 - Stand Oktober 2005

Um die Rahmenrichtlinie der IT-Sicherheit einführen und Dienste, die diese implementieren, entwerfen zu können, ist zunächst erforderlich, die technische Infrastruktur und organisatorische Prozesse, welche zu schützen sind, zu erfassen. Basierend auf dieser Information kann eine Kategorisierung nach Anforderungen an der Infrastruktur, den angebotenen Diensten sowie den beherbergenden Systemen vorgenommen werden. An Hochschulen werden IT-Systeme jedoch meist nach den DFG-Richtlinien verteilt administriert, so dass sich eine Erfassung und Kategorisierung der Gesamtstruktur als sehr schwierig erweisen kann. Dieses Papier beschreibt einen Ansatz, eine Erfassung durchzuführen, die diesen Randbedingungen Rechnung trägt und das Design von Basisdiensten zum Schutz des IT-Verbundes ermöglicht.

## 1 Erfassung des IT-Verbundes - Situation

In klassischen Modellen zur Einführung von IT-Sicherheit wird davon ausgegangen, dass der Betreiber die volle Kontrolle über die gesamte IT-Infrastruktur hat und daher Information zu allen eingesetzten Server- und Endsystemen sowie vorhandenen Netzkoppelementen zur Verfügung hat. Diese Information wird zu einem strukturierten Netzplan zusammengefasst und mit der Information über die Anforderungen an die Funktionalität und den angebotenen Diensten zusammengeführt. Daraus lässt sich der Schutzbedarf ableiten und eine Normalisierung des Verbundes durchführen.

An Hochschulen stellt sich die Situation anders dar. Gemäß der Richtlinien der DFG werden u.U. große Teile des Netzes verteilt administriert. Hochschulen sind in zentrale Einrichtungen, Fakultäten und Institute, z.T. noch weiter in Abteilungen gegliedert. An vielen Hochschulen existieren noch sogenannte An-Institute, die netztechnisch wie Einrichtungen der Hochschule behandelt werden; diese stellen ein gesondertes Problem dar.

Die IT-Infrastrukturen dieser Einheiten werden z.T. zentral durch das Rechenzentrum der Hochschule (oder dessen Äquivalent) oder dezentral durch Mitarbeiter der Einheiten administriert. I.A. existiert keine zentral verfügbare Informationsbasis, die alle Systeme und Netzkoppelemente des Verbundes vollständig beschreibt und an welche die verschiedenen Administratoren ihre Information liefern. Eine Erfassung all dieser Daten stellt eine nicht triviale Aufgabe dar, da die Erfahrung zeigt, dass die einzelnen Administratoren sehr unterschiedliche Verfahren anwenden und sich auch Wissens- und Kenntnisstände der Verwalter deutlich unterscheiden. Daher ist auch die Dokumentation der vielen verschiedenen Verbünde von sehr unterschiedlicher Qualität, die von exzellenten Konzepten bis zur fast völligen Unkenntnis sowohl der technischen Grundlagen als auch des jeweils verwalteten Teil des Netzes (Institutsnetz) reicht. Nicht unüblich sind auch "alleingelassene" Benutzer, die ihre Systeme selbst verwalten müssen, dazu aber weder befähigt sind, noch die erforderliche Qualifikation besitzen - z.B. Dekanatssekretärinnen, deren Systeme nicht von einem Institut mitbetreut werden.

Der Ansatz, den gesamten Verbund durch eine zentrale Stelle (z.B. dem Rechenzentrum) zu erfassen, wird daher in vielen Fällen nicht oder nicht rasch zu einem befriedigenden Ergebnis führen. Insbesondere in Fällen, in denen die Etablierung eines organisatorisch fest verankerten Sicherheitsmanagements nicht leicht erfolgen kann, sind alternative Wege zur Erhöhung der Sicherheit gefragt.

## 2 Alternatives Vorgehen

Ein Ansatz, der sich in der Praxis bewährt hat, ist die Unterteilung des Verbundes in den zentral administrierten Teil und die vielen delegierten Bereiche, die formal als verteilt administrierter Teil (auch "delegierte Netze") bezeichnet werden. Maßnahmen können leicht auf den zentral administrierten Bereich angewendet werden, während dies im verteilt administrierten Teil nicht so einfach ist. Daher wird der Schutz der gesamten Infrastruktur zunächst durch die Implementierung von Maßnahmen im zentraladministrierten Bereich erhöht, die so eingeführt werden, dass weder der Betrieb unterbrochen, noch die Administratoren der delegierten Netze überfordert werden. In Fällen, in denen das trotzdem vorkommt, müssen die entsprechenden Administratoren bei der Umsetzung unterstützt werden.

## **Erfassung der zentralen und dezentralen Verbünde – Gemeinsamkeiten**

Die vollständige Erfassung erfasst alle:

- Netzkoppelemente, die im Verantwortungsbereich administriert werden
- an hochschulfremde Institutionen delegierte Netzbereiche
- Systeme (Server, Pools, Arbeitsplätze etc.)
- Adressen, die an die o.g. Systeme vergeben sind
- Ansprechpartner, verantwortliche sowie kompetente Personen (Administratoren und Vorgesetzte)
- Dokumentation der Abbildung Adresse → Verantwortlicher

Ziel ist die konsistente Dokumentation der Netze und Systeme in dem Sinne, dass mindestens die Übergänge vom zentral administrierten Netz zu den delegierten Bereichen und die verantwortlichen und kompetenten Ansprechpartner bekannt sind. Auch hier gilt: Bereits aus Gründen des Routings ist eine Planung der Vergabe von Adressbereichen erforderlich, die auch für die Erfassung o.g. Information sehr wertvoll ist.

Sofern diese Planung nicht erfolgt ist, müssen jetzt Überlegungen zu ihrer Einführung angestellt werden. Eine Dokumentation, welche die Verantwortung für Adressen (idealerweise Adressbereiche) beschreibt, muss auf jeden Fall angelegt werden. Weiterhin müssen dokumentierte Verfahren die Neuvergabe von Adressen regeln. Die Dokumentation ist aktuell zu halten, alle eingesetzten Verfahren sind mit den Dokumentationsverfahren zu koppeln. Es ist anzuraten, Dokumentation sowohl in maschinenles- und -verarbeitbarer als auch in menschlich leicht lesbarer Form vorzuhalten (letztere Form kann aus ersterer erzeugt werden).

## **Erfassung der zentralen und dezentralen Verbünde - Unterschiede**

Der zentrale Verbund besteht aus der IT-Infrastruktur, die von einer zentralen Einrichtung aus – i.A. dem Rechenzentrum – administriert wird.

Die dezentrale (verteilt administrierte) Verbund besteht aus der IT-Infrastruktur, die außerhalb der zentralen Administration dezentral von Fakultäten, Instituten und weitere, nachgeordneten Einheiten sowie anderen Einrichtungen administriert wird. Diese verwenden dabei Adressen, die der Hochschule zugerechnet werden, sodass diese dadurch zunächst in die Haftung für Aktivitäten gerät, die von diesen Adressen ausgehen.

## **3 Sicherheitsmanagement**

Um die diversen Sicherheitsbelange adressieren zu können, ist ein Team aus technisch qualifizierten Mitarbeitern zu bilden, die sowohl tiefen Einblick in die Verwaltung komplexer Netze als auch die Administration von Endsystemen besitzen. Die Kommunikation mit den entsprechenden Abteilungen zum Betrieb der Infrastruktur muss sehr eng sein, um aktuell auftretende Schwachstellen und andere Bedrohungen rasch und fundiert bewerten zu können.

Neben der Bewertung potentieller Bedrohungen ist dieses Team mit der Bearbeitung von Sicherheitsvorfällen betraut. Dies umfasst sowohl die Incident Response (IR) und die Vulnerability Response (VR) als auch das Abuse-Handling.

Dieses Team muss organisatorisch mit den entsprechenden Befugnissen ausgestattet werden, um in Notfällen Maßnahmen ergreifen zu können, die den Betrieb des betroffenen Systems ggf. einschränkt, um die Sicherheit der nicht betroffenen Systeme zu gewährleisten.