ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D-MAVT

D-MAVT Standards für Verantwortlichkeiten und Systempflege

Gültig ab 1.11.2003

ISG MAVT

Daniel Richard
V1.0
Last saved: 11.11.2003
Print: 11.11.03

Index

1. D- MAVT Standards für Verantwortlichkeiten und Systempflege

1.1 Einleitung

Per 6.02.2003 hat der Vizepräsident für Forschung und Wirtschaftsbeziehungen der ETH Zürich die *Standards für Verantwortlichkeiten und Systempflege* definiert und in Kraft gesetzt. Darin sind bestimmte Verantwortlichkeiten und Massnahmen im IT Bereich definiert. Allerdings sind diese allgemein gehalten und es benötigt weitere Definitionen die für ein Departement speziell sind. Daher ist dieses Papier eine Ergänzung mit speziell für das D-MAVT zugeschnittenen Regeln die oben erwähntes Regelset ergänzt und diesem untergeordnet ist. Diese Regeln gelten sowohl für Administratoren als auch für die Benutzer der entsprechenden Infrastruktur.

Im Folgenden ist die Verordnung 1:1 wiedergegeben **und mit Fett gedruckten Zusätzen ergänzt.** Wo nötig wurden zusätzliche Artikel eingefügt.

Anzumerken ist hierbei noch, dass es keine aktive Überwachung der Rechner geben darf, ebenso keine Aufzeichnung irgendwelcher Daten der Benutzer. Sollte auf Grund eines bestimmten Verdachts ein Benutzer überwacht werden müssen, so ist dieser vorgängig zu informieren und die Überwachung hat mit dem Datenschutzgesetz konform zu sein.

1.2 Verordnung

Art. 1 Gegenstand

Diese Verordnung bezweckt, dass im Falle eines Angriffs auf ein System* oder ausgehend von einem System der ETH Zürich die zuständige Person identifiziert und erreicht werden kann. Ausserdem bezweckt sie die zeitgerechte Beseitigung bekannter Schwachstellen, um die Verletzlichkeit des Gesamtsystems zu verringern.

Art. 2 Grundsatz

1 An der ETH Zürich dürfen nur Geräte an das Datennetzwerk angeschlossen werden, welche die Standards gemäss dieser Verordnung erfüllen.

2 Die Informatikdienste überprüfen durch Stichproben regelmässig die Einhaltung der Standards.

Art. 3 Verantwortlichkeiten

1 Jede Organisationseinheit **(Institut, Laboratorium oder Professur)** benennt folgende Verantwortliche:

a. Systemverantwortliche/r:

Für jedes Gerät innerhalb oder ausserhalb des Campus' der ETH Zürich, welches mit dem Datennetz verbunden wird, gibt es eine zuständige Person. Diese sorgt unter anderem für das Aufsetzen der Netzwerkanbindung, ist für die Systempflege und die Datensicherheit verantwortlich und regelt die Zugriffspolitik so, dass systemrelevante Vorgänge rekonstruierbar sind und einer Person zugeordnet werden können.

Damit ist eine Person gemeint, die als Verantwortliche für eine gesamte Organisationseinheit definiert worden ist und diese internen systemrelevante Vorgänge bei Bedarf überwacht und bei Vorfällen einschreitet. Diese Person trägt die Verantwortlichkeit für alle ETH Rechner. Die Benutzer der einzelnen Rechner sind jedoch aufgerufen verantwortungsbewusst mit deren Geräten umzugehen und allfällige Auffälligkeiten umgehend dem Administrator zu melden.

Geräte von ausserhalb des Campus der ETH stehen in der Verantwortung des jeweiligen Gerätebesitzers. Dieser hat sich den Regeln der ETH konform zu verhalten und ist für die Sicherheit des Rechners verantwortlich. Ein Anschliessen solcher Geräte darf nur mit Einverständnis des Netzanschlussverantwortlichen erfolgen.

*** Unter einem *System* ist z.B. ein Computer, eine Netzwerkkomponente wie ein Router etc. zu verstehen.**

b. Netzanschlussverantwortliche/r:

Diese Person

- leitet alle Tätigkeiten betreffend das Anschliessen von Geräten an das Datennetz der Organisationseinheit,
- ergänzt die von den Informatikdiensten vorgegebenen Netzwerkrichtlinien entsprechend der zugehörigen Organisationseinheit und kommuniziert diese,
- legitimiert Geräte für den Netzanschluss,
- ist verantwortlich für alle netzwerkrelevanten Registrierungen,
- ist verantwortlich für die Aktivierung der Datenanschlussdosen,
- verwaltet die von den Informatikdiensten zugeordneten Nummernbereiche,
- organisiert den Netzzugriff,
- ordnet den Geräten IP- Nummern zu und
- dient bei Netzwerkproblemen als Ansprechpartner innerhalb und ausserhalb der Organisationseinheit.

2 Alle IP-Nummern mit den entsprechenden verantwortlichen Personen (und ihrer Email Adressen) sind von den Netzanschlussverantwortlichen in einer zentralen Datenbank einzutragen. Wo vorgängig keine Zuordnung einer IP-Nummer zur systemverantwortlichen Person möglich ist, wird diese Information fallweise aus dafür vorgesehenen Logfiles abgeleitet.

Solange die zentrale Datenbank der ID nicht zur Verfügung steht, erstellt jeder Verantwortliche eine Datenbank oder Tabelle, auf der alle nötigen Informationen enthalten sind. Dies sind im Minimum: IP Adresse, Hostname, Benutzer, Standort sowie Subnetz. Die Liste ist mindestens einmal monatlich zu aktualisieren und an den Informatik-Koordinator (ISL) des D-MAVT zu senden. Dieser hält somit ein zentrales Register aller am Departement sich im Einsatz befindlichen Geräte. Sobald die zentrale Datenbank zur Verfügung steht, werden alle Rechner nur noch dort eingetragen.

3 Um die Erreichbarkeit im Ereignisfall zu gewährleisten, müssen alle Verantwortlichen über vordefinierte Adressen erreichbar sein. Die Verantwortlichen oder ihre Stellvertretung müssen innerhalb eines Arbeitstages erreichbar sein.

Die Verantwortlichen einer Organisationseinheit geben dem ISL Ihre Erreichbarkeit im Büro sowie für Notfälle eine weitere Erreichbarkeit an. Gleiches gilt für deren Stellvertreter. Der ISL führt, bis die zentrale Datenbank verfügbar ist zentral im Departement eine Erreichbarkeitsliste aller Informatikverantwortlichen. Diese darf an die Departementsleitung sowie auszugsweise an die Informatikdienste ausgehändigt werden. Gemäs Datenschutzgesetz hat jedermann des Departements Einsichtsrecht. Diese Listenlösung ist zu vernichten nachdem die offizielle Lösung der ETH verfügbar wird. Die Daten der Liste sind dann entsprechend der Bedürfnisse in die neue Lösung zu übertragen.

4 Die Datenbank muss für alle Angehörigen der ETH Zürich zugänglich und lesbar sein.

Art. 4 Systempflege

1 Geräte, die an das Netzwerk der ETH Zürich angeschlossen werden, müssen gegen bekannte Verletzlichkeiten geschützt sein.

Es muss auf allen Geräten mindestens ein Virenschutzprogramm installiert sein. Dieses muss so konfiguriert sein, dass die neusten Virensignaturen mindestens einmal pro Woche aktualisiert werden. Empfohlen wird, den Online Scanner eingeschaltet zu haben, das Update täglich sowie mindestens einmal pro Woche einen Vollscan des Gerätes durchzuführen.

Der Administrator ist dafür verantwortlich, sich regelmässig über die Verfügbarkeit von Security-Updates für sämtliche im Einsatz befindlichen Betriebssysteme zu erkundigen. Entsprechend untenstehenden Terminen sind die entsprechenden Patches mindestens auf den am Netzwerk im Einsatz stehenden Rechnern zu applizieren. Einen Hinweis auf Updates sowie Tools für deren Applizierung gibt die Webseite der Network Security Group (http://www.kom.id.ethz.ch/netsec/).

2 Die Informatikdienste führen eine nach Priorität und Dringlichkeit geordnete, laufend nachgeführte und ETH Zürich-weit zugängliche Liste der für die ETH Zürich relevanten Verletzlichkeiten. Zu den aufgeführten Verletzlichkeiten wird nach Möglichkeit ein Test bereitgestellt, mit dem geprüft werden kann, ob ein bestimmtes Gerät verletzlich ist. Bei Geräten, die alleine hinter einem Firewall stehen, wird nicht das Gerät, sondern das Gesamtsystem betrachtet.

3 Je nach Art der Verletzlichkeit und deren Ausnutzung, gelten folgende Fristen zur Behebung:

- 1 Arbeitstag: Die Verletzlichkeit wird aktiv ausgenutzt indem andere Systeme direkt angegriffen werden, oder es gehen andere schädliche Aktivitäten davon aus.
- 5 Arbeitstage: Die Verletzlichkeit wird aktiv ausgenutzt, aber es gehen noch keine schädlichen Aktivitäten davon aus.
- 20 Arbeitstage: Die Verletzlichkeit ist bekannt und nachvollziehbar und es sind keine Fälle bekannt, wo diese aktiv ausgenutzt wird.

Die aufgeführten Fristen können bei einer akuten Gefährdung der Infrastruktur auch verkürzt werden.

Art. 5 Massnahme bei Nichtbefolgen der Standards

Werden die vorgegebenen Standards nicht eingehalten, sind die Informatikdienste verpflichtet, das entsprechende Gerät vom Datennetz zu trennen, bis die Standards erfüllt werden.

Der ISL ist darüber hinaus befähigt bei Nichterreichung eines System- oder Netzanschlussverantwortlichen, bei Verdachtsfällen und wo nötig in dringenden Fällen bei Gefährdung der Infrastruktur (Nichteinhaltung der verkürzten Frist) ein Trennen vom Netzwerk eines oder mehrerer Geräte bei den Informatikdiensten anzuordnen.

Bei wiederholter Missachtung von Regeln findet eine Meldung an die Leitung der Organisationseinheit statt. Diese kann auch über Disziplinarmassnahmen befinden.

Sollten auf Grund eines bestimmten Verdachts ein Benutzer überwacht werden müssen, so ist dieser vorgängig zu informieren und die Überwachung hat mit dem Datenschutzgesetz konform zu sein.

Art. 6 Zusätzliche Richtlinien am D-MAVT (Ergänzung)

1 Um obige Vorschriften einhalten zu können ist der Gebrauch von DHCP Servern im herkömmlichen Sinn nicht mehr erlaubt. Das heisst, dass ein Gerät nurmehr eine via DHCP Server vergebene IP-Adresse erhalten darf, wenn der Systemadministrator das Gerät kennt und eine Adresse vorreserviert worden ist (per Registrierung der MAC-Adresse). Freie Adressvergaben werden am D-MAVT per 31.12.2003 verboten. Ausnahmen sind mit dem ISL zu besprechen.

In Bereichen wo dies nicht ausreicht, zum Beispiel im Bereich Studentenarbeitsplätze, sind Docking-Arbeitsplätze der ETH Informatikdienste im „public" Subnetz einzurichten. Für das korrekte Vorgehen wenden sich die Systemverantwortlichen an den ISL.

2 Der Betrieb von Serveranwendungen muss zwingend mit dem Systemverantwortlichen der Organisationseinheit abgesprochen werden. Dieser hat das Recht Auskunft darüber zu verlangen warum ein Serverdienst auf einem Clientgerät benötigt wird. Er kann auch darüber bestimmen ob dieser Service betrieben werden darf oder nicht. Der entsprechende Betreiber des Gerätes und des entsprechendes Services hat dafür zu sorgen, dass der Service laufend aktualisiert und gegen Verletzlichkeiten gepatcht wird.

3 Der Betrieb von Peer-to-Peer Diensten ist innerhalb des D-MAVT strikte verboten. Dazu gehört primär der Gebrauch von Tools wie Kaazaa, E-Donkey, WinMX, E-Mule sowie sämtlichen weiteren Tools dieser Art sowie ebenso sämtliche denkbaren Anwendungen die peer-to-peer Funktionalitäten ausnutzen.

4 Das Benutzen von Remote-Control Software ist den Systemverantwortlichen vorbehalten. Muss ein solcher Dienst von einem Mitarbeiter benutzt werden, so hat der Systemverantwortliche davon in Kenntnis gesetzt zu werden.

5 Hackingaktivitäten aller Art sind strengstens verboten und werden von der entsprechenden Organisationseinheit disziplinarisch geahndet. Die ETH entscheidet im Bedarfsfall über eine mögliche Strafverfolgung.

6 Die Benutzung von privaten Rechnern untersteht den Regeln der ETH. Sämtliche Benutzer müssen die Anweisungen der Informatikverantwortlichen strickte befolgen. Die IT Verantwortlichen haben bei Zuwiderhandlung jederzeit das Recht dem User die Benutzung des privaten Rechners im ETH Netzwerk zu verbieten.

7 Die Leiter von Instituten respektive Laboratorien sind angehalten zusätzliche Regeln aufzustellen.

Art. 7 Inkrafttreten

Diese Verordnung tritt per 1.11.2003 mit dem Beschlusses der D-MAVT Departementskonferenz vom 4.11.2003 in Kraft. Die zugrunde liegende Verordnung ist seit 3.2.2003 in Kraft.