Standards für Verantwortlichkeiten und Systempflege

vom 6.02.2003

Der Vizepräsident für Forschung und Wirtschaftsbeziehungen der ETH Zürich,

gestützt auf Art. 3 Abs. 2 Bst. c Detailorganisationsverordnung ETH Zürich vom 9. Juni 1998,

verordnet:

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 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 Zugriffpolitik so, dass systemrelevante Vorgänge rekonstruierbar sind und einer Person zugeordnet werden können.

[*] 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 E-Mail 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.

[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.

[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.

[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.

Art. 6 Inkrafttreten

Diese Verordnung tritt am 6. Februar 2003 in Kraft.

6. Februar 2003 Prof. Dr. U. Suter