Norm 02

Normen für die Sammlung von Log – Dateien an der UZH

1. Gültigkeit dieser Norm

Dieses Dokument ist eine Ausführungsvorschrift zu den Richtlinien für den Einsatz von Informatikmitteln an der Universität Zürich (REIM) und gilt für dieselben Personen und Anwendungen.

Wenn mit gutem Grund einzelne dieser Normen nicht erfüllt werden, müssen gemäss REIM, vertretbare alternative Sicherheitskonzepte aufgezeigt, festgehalten und umgesetzt werden.

2. Begriffe

Log-Dateien, Logs: Mit genauer Zeitangabe verknüpfte elektronische Aufzeichnungen von Ereignissen in Computer-Systemen und -Netzwerken. Technische Fachbegriffe (DHCP, VPN-Tunnels, ssh) sind ergänzende Erklärungen für Fachleute und werden von diesen verstanden.

3. Aufzeichnungs- und Sammel-Pflicht

Folgende Aufzeichnungen müssen gesammelt und aufbewahrt werden:

- Alle temporären oder festen Zuteilungen von IP-Nummern zu Personen (Netzwerkfreischaltung, VPN-Tunnels, ssh-Tunneldienst trampolin.unizh.ch) oder Maschinen (DHCP). Sie müssen so festgehalten werden, dass entweder die Person oder die Maschine im Nachhinein gefunden werden kann.
- Die temporären oder festen Beziehungen, die von Firewalls, von Servern für Netzwerk-AdressÜbersetzung und von Verbindungen weiter vermittelnden Servern (z.B. Proxies) paarweise zwischen IP-Nummern oder von IP-Nummern zu Login-Namen von Personen erzeugt werden.
- Die für die E-Mail beim Durchgang durch die Mailserver anfallenden Logs.

Da diese Daten zusammen mit anderen Aufzeichnungen zu Persönlichkeitsprofilen verarbeitet werden können, handelt es sich im weitesten Sinne um Personendaten.

4. Zweck der Log-Dateien

Zur Wahrung der Verantwortung, welche die Universität gegenüber dem Internet trägt, müssen die verantwortlichen Personen oder missbrauchte Maschinen gefunden werden, insbesondere:

- Bei der Behandlung von Reklamationen über das Verhalten einer Maschine oder deren Benutzer im Internet.
- Bei der Abklärung von auffälligem oder störendem Verhalten von Maschinen im Internet.
- Für die Information über Ergebnisse von Sicherheitsüberwachungen an die Betroffenen.
- Für die Anordnung von Notmassnahmen oder die Mitteilung von getroffenen individuellen Notmassnahmen bei Hacker- und Viren-Problemen.

Im äussersten Fall werden die Log-Dateien zur richtigen Einweisung von Ermittlungsbehörden gebraucht.

5. Aufbewahrungsfrist

Die Log-Dateien sollen ein halbes Jahr nach der Zuteilung der IP-Nummer aufbewahrt werden. (Obwohl die Universität im Sinne des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BüPF) nicht ein Dienstanbieter ist, übernimmt sie aus praktischen Gründen die Frist.)

Es wird empfohlen, die Dateien während 4-5 Wochen für das autorisierte Personal leicht abfragbar und während weiteren 22-23 Wochen in einem Archiv zu halten.

Gemäss dem Datenschutzgesetz müssen diese Daten nachher gelöscht werden.

6. Vorschriften für andere Log-Dateien

Auch alle anderen Log-Dateien, welche Rückschlüsse auf die Tätigkeit von Personen möglich machen, unterstehen dem Datenschutzgesetz. Sie dürfen nur so lange aufbewahrt werden, wie wie eine umschriebene personenbezogene Auswertung notwendig ist oder wenn die Löschung nicht zumutbar ist.

An der Universität sollen solche auf den Maschinen anfallende Files nach spätestens einem halben Jahr gelöscht oder so umgewandelt werden, dass nur noch anonyme Ergebnisse aufbewahrt werden.

7. Log-Dateien der Informatikdienste

Die Log-Dateien der Informatikdienste gemäss Ziffer 1 müssen dem IT Security Officer auf einem zentralen System zur Verfügung gestellt werden.

Eine Sammlung des Netzwerkverkehrs und dessen inhaltliche Analyse darf nur durch den IT Security Officer und ausschliesslich für die Entdeckung und/oder den Nachweis des Missbrauchs von Maschinen durch unberechtigte Personen oder Programme durchgeführt werden. Andere Erkenntnisse über die Tätigkeit von Personen aus diesen Daten sind zu vermeiden und unterstehen einer absoluten Geheimhaltung (Fernmeldegeheimnis), wo sie dennoch entstehen.

Die maximale Aufbewahrungszeit von Netzwerkverkehrs-Daten, welche mehr als nur die Adressierungselemente enthalten, ist eine Woche.

8. Ausnahmen

Log-Dateien auf Maschinen, auf denen nur eine natürliche Person berechtigt ist, haben keine Vorschriften. Die Sammlung des Netzverkehrs dieser Maschine durch den einzigen Berechtigten ist ebenfalls frei.

Für die Abklärung und Dokumentation technischer Störungen darf der Netzwerkverkehr einzelner Maschinen soweit nötig aufgezeichnet werden.

9. Weitere Bestimmungen

Log-Dateien mit Personendaten nach Ziffer 1 und 4 sind vertraulich zu behandeln. Sie dürfen nur für den direkt betroffenen Personenkreis zugänglich sein. Beigezogene Dritte sind sorgfältig auszuwählen und auf die Vertraulichkeit zu verpflichten.

Log-Dateien müssen akkurate Zeitstempel enthalten. An der Universität sollen alle Server mit den Zeitservern der Universität (time1.unizh.ch, time2.unizh.ch, time3.unizh.ch) synchronisiert werden. Alle Client-Maschinen sollten mindestens bei jeder Inbetriebnahme sowie mindestens einmal täglich synchronisiert werden.

Auszüge aus Log-Dateien und Erkenntnisse aus Log-Dateien, die in Briefwechseln und Untersuchungsberichten vorkommen, können länger aufbewahrt werden. Ebenso Lieferscheinkopien und allfällige Rechnungen.