Weisung für die Protokollierungen von Systemvorgängen (Logfile Policy)

(vom 27.10.2006, Stand 5.11.2024[1])

Die Zentrale Informatik,

gestützt auf § 6 Abs. 2 Bst. d des Reglements über den Einsatz von Informatikmitteln an der Universität Zürich vom 29.11.2022, Stand 5.11.2024 (REIM),

erlässt folgende Weisung:

1 Grundsätzliches

Die Logfile Policy legt Minimalstandards für die Protokollierungen von Systemvorgängen auf Informatikmitteln der UZH fest.

1.1 Geltungsbereich

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

Ausnahmen von dieser Weisung bedingen ein alternatives Sicherheitskonzept gemäss REIM §13.

1.2 Begriffe

1) Die im Reglement über den Einsatz von Informatikmitteln (REIM) definierten Begriffe gelten analog.
2) Log-Dateien, Logs: Mit genauer Zeitangabe verknüpfte elektronische Aufzeichnungen von Ereignissen in Computer-Systemen und -Netzwerken.
3) Technische Fachbegriffe (DHCP, VPN-Tunnels, ssh) sind ergänzende Erklärungen für Fachleute und werden von diesen verstanden.

2 Organisatorische und technische Vorgaben

Nachfolgende Kapitel beschreiben detaillierte organisatorische und technische Vorgaben zur Protokollierung von Systemvorgängen auf Informatikmitteln der UZH.

2.1 Aufzeichnungs- und Sammel-Pflicht

1) Folgende Aufzeichnungen müssen gesammelt und aufbewahrt werden:

[1] Die Weisung wurde per 5.112024 ins neue UZH Corporate Design überführt und an die Struktur der Weisung über die Netzwerksicherheit (WNS) angeglichen. Inhaltlich wurden keine Änderungen vorgenommen.

a. Alle temporären oder festen Zuteilungen von IP-Nummern zu Personen (Netzwerkfreischaltung, VPN-Tunnels, ssh-Tunneldienst) oder Maschinen (DHCP). Sie müssen so festgehalten werden, dass entweder die Person oder die Maschine im Nachhinein gefunden werden kann.

b. 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.

c. Die für die E-Mail beim Durchgang durch die Mailserver anfallenden Logs.

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

2.2 Zweck der Log-Dateien

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

a. Bei der Behandlung von Reklamationen über das Verhalten einer Maschine oder deren Benutzer im Internet.

b. Bei der Abklärung von auffälligem oder störendem Verhalten von Maschinen im Internet.

c. Für die Information über Ergebnisse von Sicherheitsüberwachungen an die Betroffenen.

d. Für die Anordnung von Notmassnahmen oder die Mitteilung von getroffenen individuellen Notmassnahmen bei Hacker- und Viren-Problemen.

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

2.3 Aufbewahrungsfrist

1) 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.)

2) 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.

3) Gemäss dem Datenschutzgesetz müssen diese Daten nachher gelöscht werden.

2.4 Vorschriften für andere Log-Dateien

1) 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 eine umschriebene personenbezogene Auswertung notwendig ist oder wenn die Löschung nicht zumutbar ist.

2) 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.

2.5 Log-Dateien der Zentralen Informatik

1) Die Log-Dateien der Zentralen Informatik gemäss Ziffer 2.1 müssen dem IT Security Officer auf einem zentralen System zur Verfügung gestellt werden.

2) 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.

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

2.6 Ausnahmen

1) 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.

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

2.7 Weitere Bestimmungen

3) Log-Dateien mit Personendaten nach Ziffer 2.1 und 2.4 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.

4) 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-Geräte sollten mindestens bei jeder Inbetriebnahme sowie mindestens einmal täglich synchronisiert werden.

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

3 Schlussbestimmungen

3.1 Inkrafttreten

Die Weisung über die Protokollierungen von Systemvorgängen (Logfile Policy) ist seit 27.10.2006 in Kraft und ist bis auf Widerruf gültig.

3.2 Übergangsfrist

Für Umsetzung und Einhaltung dieser Weisung besteht eine Übergangsfrist von 12 Monaten ab Inkrafttreten.