Vereinbarung zur Filterung unerwünschter Inhalte beim Browsen im Internet

an der Stiftung Tierärztliche Hochschule Hannover

§ 1 Präambel[1]

(1) Zunehmend stammen Bedrohungen des TiHo - Netzwerks aus internen Quellen, wenn Beschäftigte unbewusst auf Webseiten surfen, die Schadsoftware wie Viren, Trojaner, Spyware oder Würmer enthalten, welche das Hochschulnetzwerk infizieren könnten. Diese Schadsoftware befindet sich überproportional häufig auf Internetseiten, deren Inhalte unerwünscht (im Sinne der Benutzungsordnung für das Datennetz und die angeschlossenen Rechenanlagen der Stiftung Tierärztliche Hochschule Hannover §2 Abs. 7) sind. Dies kann in Folge dazu führen, dass Externe Zugriffe auf dienstliche, vertrauliche Daten erlangen und/oder die Verfügbarkeit von PCs oder Netzwerkdiensten in Mitleidenschaft gezogen werden.

(2) Zum Schutz der TiHo - Infrastruktur und zum Schutz der Anwenderdaten betreibt die TiHo-IDS eine Inhaltsfilterung von Internet-Seiten die die Zugriffe auf “malwareverdächtige“ und/oder „unerwünschte“ Webseiten überwacht und unterbindet.

(3) Die Details dieser Filterung werden durch eine Vereinbarung zwischen der TiHo – IDS mit Personalrat und Datenschutzbeauftragtem wie folgt geregelt:

§ 2 Art der Filterung

Unterbunden werden sollen Zugriffe auf Websites, die durch einen kommerziellen Dienst in die folgende Kategorien eingestuft werden:

- adult (= Verbreitung von Pornographie)
- hacking (=Malware, um PCs zu kompromittieren)
- malware (=Verbreitung von Malware)
- questionable (Verbreitung Hass/Rassismus und Illegales [z.B. gecrackte Software]
- phishing (=Methoden zum Identitätsdiebstahl)

§ 3 Zugriff auf eine gesperrte Webseite

(1) Wenn Benutzer den Zugriff auf eine Website anfordern, für die der Zugriff blockiert wird, erhalten sie eine Verweigerungsbenachrichtigung.

(2) Um einer „falsch positiven“ Kategorisierung einer an der TiHo dienstlich benötigten Website zu widersprechen, wird ein Meldevorgang eingerichtet, um diese Klassifikation für die TiHo zu korrigieren.

[1] Aus Gründen der besseren Lesbarkeit wird für Amtsbezeichnungen und Personen nur die männliche Sprachform verwendet. Sie soll jeweils die weibliche Sprachform mit umfassen.

§ 4 Protokollierung der Zugriffe auf gesperrte Webseiten

Es erfolgt keine gesonderte Protokollierung der Zugriffe auf gesperrte Web - Seiten. Die Webzugriffe aus dem TiHo – Netz werden mit Personenbezug grundsätzlich auf einem sog. Proxy-Server gespeichert. Auf diese Liste haben nur die Mitarbeiter im Arbeitsbereich Server / Speichersysteme der IDS Zugriff. Der Zugriff erfolgt grundsätzlich nicht mit dem Zweck einer gezielten Verhaltenskontrolle, sondern ausschließlich aus folgenden Gründen:

(1) Im Zuge der Ermittlung von Strafverfolgungsbehörden

(2) Nach einer Supportanfrage eines Mitarbeiters oder einer Gruppe von Mitarbeitern, z. Bsp. wenn es Zugriffsprobleme bei bestimmten Webseiten gibt, deren Klärung die Nutzung dieser Logs erfordert.

(3) Zur Beseitigung von generellen Störungen im Netzverkehr, zur Erkennung oder Beseitigung von Performance-Problemen oder zur Aufdeckung einer konkreten Sicherheitsbedrohung, z. Bsp. um einen kompromittierten PC zu identifizieren. In diesen Fällen ist der Personalrat vorher zu beteiligen und kann diesen beiwohnen, sofern diese Beteiligung nicht zu einer derartigen Verzögerung führen würde, dass der Zweck der Maßnahme zunichte gemacht würde, z. Bsp um einen Bot – Netz kompromittierten PC so schnell wie möglich zu eliminieren.

Die übrigen Mitarbeiter der IDS haben nur Zugriffe auf Proxyprotokolle, bei denen der Personenbezug irreversibel „unsichtbar“ gemacht wurde.

§ 5 In-Kraft-Treten

Diese Benutzungsordnung tritt nach der Unterzeichnung in Kraft. Änderungen des Verfahrens z. Bsp. hinsichtlich der Art der Filterung werden zeitnah mit dem Personalrat abgestimmt und den Beschäftigten zur Kenntnis gebracht.

Hannover, den

für die TiHo - IDS

für den Personalrat