universität wien

Zentraler Informatikdienst

Policy

Firewall für Organisationseinheiten

Genehmigt durch Ulf Busch

Gültig ab 25.03.2019

Version 1.0

1. Zweck

Firewalls im Datennetz der Universität Wien reduzieren die Risiken durch Angriffe über das Netzwerk und tragen dazu bei, auftretenden Sicherheitsproblemen besser begegnen zu können.

Diese Policy definiert Rahmenbedingungen und Verantwortlichkeiten, um einen möglichst effektiven Einsatz von Firewalls ohne unnötige Behinderung von nicht sicherheitsrelevantem Datenverkehr an der Universität Wien zu gewährleisten.

2. Anwendungsbereich

Diese Policy gilt für NutzerInnen bzw. deren Geräte, soweit sie das vom Zentralen Informatikdienst (im Folgenden: ZID) betriebene universitäre Datennetz nutzen. Jedes Subnetz der Universität Wien wird über eine vom ZID betriebene Firewall (im Folgenden einfach: Firewall) gemäß dieser Policy an den Universitäts-Backbone angebunden.

3. Grundsätzliches zum Einsatz von Firewalls an der Universität Wien

Das Datennetz der Universität Wien ist in Subnetze gegliedert, die jeweils Organisationseinheiten bzw. anderen Einrichtungen zugewiesen sind. Jeder Datenverkehr zwischen Subnetzen oder zwischen einem Subnetz und anderen Netzen (etwa Internet, Rechenzentrum) muss durch eine Firewall geleitet werden. Für jedes dieser Subnetze ist, sofern nicht mit der Grundkonfiguration der Firewall das Auslangen gefunden wird, wenigstens ein/e EDV-Beauftragte/r als Ansprechpartner/in durch den/die LeiterIn der Einrichtung zu benennen.

Als Leitprinzipien für den Einsatz der Firewalls gelten das Least-Privilege- und das Fail-Safe-Prinzip:

- Least-Privilege-Prinzip: So restriktiv wie möglich, so offen wie nötig. Beispielsweise ist für einen Server, sofern es der Zweck des Dienstes erlaubt, der Freischaltung einzelner IP-Adressen, UserIDs (User Based Rulesets), VPN-Adressen oder des Datennetzes der Universität Wien der Vorzug gegenüber einer internetweiten Freigabe zu geben.

- Fail-Safe-Prinzip: In außergewöhnlichen Betriebssituationen (etwa Störungen, Angriffe) wird Netzverkehr eher abgewiesen als ungesichert weitergeleitet.

Eine Umgehung der Firewalls oder Maßnahmen, die zur Beeinträchtigung ihrer Funktionalität führen, sind ohne Genehmigung des ZID unzulässig.[1] Weiters sind im Subnetz angeschlossene Geräte dem Stand der Technik entsprechend sicher zu betreiben (etwa mittels Virenscanner, Software-Updates).

4. Firewall-Konfiguration

Firewalls werden vom ZID betrieben und administriert. Konfigurationsänderungen und Änderungen des Regelwerks werden dokumentiert, sodass nachvollziehbar bleibt, wann und von wem diese angefordert und durchgeführt wurden.

In der Grundkonfiguration wird grundsätzlich jener Datenverkehr erlaubt, der innerhalb des Subnetzes initiiert wurde. Sonstiger eingehender Datenverkehr wird abgewiesen.

EDV-Beauftragte können innerhalb ihrer Netzbereiche nach Prüfung der Sicherheitsrisiken Regeln zur weitergehenden Einschränkung oder Freischaltung von Verbindungen beantragen.[2] Sollten Bedenken gegen die geplante Konfiguration bestehen, kann der ZID diese ablehnen oder eine schriftliche Verantwortungsübernahme durch die zuständige Leitung verlangen. Die letztgültige Entscheidung trifft der CIO der Universität Wien.

Voraussetzung für eine solche Freischaltung ist, dass die jeweiligen IP-Adressen oder Netzblöcke des geschützten Subnetzes in der IP-Datenbank dokumentiert sind.[3]

Sollte sich nachträglich herausstellen, dass installierte Freischaltungen den Anforderungen nicht oder nicht mehr genügen oder sollte durch sie die Sicherheit oder der Betrieb beeinträchtigt oder gefährdet werden, ist der ZID berechtigt, diese jederzeit anzupassen oder zu entfernen. Die jeweiligen EDV-Beauftragten werden davon unverzüglich in Kenntnis gesetzt.

Der ZID übermittelt den EDV-Beauftragten jährlich eine Aufstellung der aktuellen Regeln ihres Subnetzes bzw. ihrer Subnetze zur Prüfung. Den EDV-Beauftragten obliegt es zu prüfen, ob diese noch aktuell sind, benötigt werden (entsprechend dem Least-Privilege-Prinzip) und die Sicherheitsanforderungen erfüllt sind. Das Ergebnis der Prüfung ist in angemessener Zeit zurückzumelden.

---

[1] Beispiele dafür sind: sogenanntes Multihoming über mehrere VLANs hinweg, Tunnel in Verbindung mit Routing über das Endgerät hinaus. Dies steht dem bestimmungsgemäßen Gebrauch von VPN am Arbeitsplatz zum Zugriff auf beispielsweise eine Forschungseinrichtung nicht entgegen, sofern kein Routing zu anderen Rechnern erfolgt.

[2] Die Eintragung und Entfernung von Regeln wird durch ein formloses E-Mail des/der zuständigen EDV-Beauftragten an firewall.zid@univie.ac.at beantragt. Verbindungen können, soweit es die Hard- und Softwareumgebung erlaubt, aufgrund von IP-Adressen, Port-Nummern, erkanntem Protokoll bzw. Dienst und UserID (etwa bei VPN, WLAN) zugelassen oder abgewiesen werden.

[3] Die Dokumentation erfolgt über die IP-Datenbank net.univie.ac.at und grundsätzlich durch den technischen Kontakt (TECH-C) des jeweiligen Netzblocks. Infrastruktur und Server des ZID sowie vom ZID vergebene dynamische IP-Adressen (etwa für VPN, WLAN) werden vom ZID dokumentiert.

Nicht mehr benötigte Regeln[4] sind unverzüglich, spätestens im Zuge der jährlichen Prüfung, entfernen zu lassen. Der ZID behält sich vor, Freischaltungen zu entfernen, die länger als 12 Monate nicht genutzt wurden.

Darüber hinaus setzt der ZID entsprechend den technischen Möglichkeiten und Gegebenheiten in Abwägung der Betriebserfordernisse der Universität Wien erweiterte Sicherheitsmaßnahmen ein – etwa das Sperren gefährlicher IP-Adressen oder das automatische Blockieren von Verbindungen mit Merkmalen bekannter Angriffe.[5] Diese Maßnahmen werden nur zum Zweck der Sicherheit eingesetzt. Eine inhaltliche Filterung bestimmter Content-Arten ist unzulässig.[6]

4.1. Maßnahmen gegen aktuelle Bedrohungen

Im Fall von akuten Angriffen, Verwundbarkeiten, Störungen, Überlastsituationen und dergleichen ist der ZID jederzeit berechtigt, die zur Schadensvermeidung oder -minimierung gebotenen Gegenmaßnahmen zu ergreifen,[7] auch wenn diese im Einzelfall zu Beeinträchtigungen führen können.

Um die Sicherheit des Datennetzes der Universität Wien und der angeschlossenen Geräte zu sichern, können zeitgemäße Firewall-Funktionen zur Erkennung sowie Abwehr von Schadsoftware und Angriffen eingesetzt werden.[8] Sofern es nach der Sachlage geboten ist, werden die zuständigen EDV-Beauftragten bzw. die betroffenen NutzerInnen automatisch oder persönlich benachrichtigt.

4.2. Verschlüsselte Verbindungen

Der Einsatz von Verschlüsselung, etwa HTTPS, bringt mit sich, dass der Inhalt von Datenverbindungen nicht auf schädliche Inhalte untersucht werden kann. Techniken, die auf ein Entschlüsseln von Verbindungen abstellen, werden an den Firewalls nicht eingesetzt.[9]

Sollten in Netzbereichen mit besonders hohem Bedarf an Schutz vor schädlichem Datenverkehr derartige Maßnahmen benötigt werden, ist vor der Schaffung der technischen Möglichkeiten jedenfalls die Genehmigung des zuständigen Rektoratsmitglieds einzuholen.

---

[4] Besonderes Augenmerk ist darauf zu legen, dass bei Ausscheiden von MitarbeiterInnen oder Änderung ihrer Zuständigkeit für diese angelegte Regeln entfernt bzw. angepasst werden.

[5] Gemäß dem Stand der Technik werden beispielsweise vom Hersteller bezogene Blocklists und Angriffssignaturen zur Deep Packet Inspection eingesetzt.

[6] Mit Content-Arten sind in diesem Zusammenhang Kriterien wie etwa Religion, Politik oder Pornographie gemeint.

[7] Zu diesen Maßnahmen gehören beispielsweise: Umleitung von Phishing-Seiten; Sperre von IP-Adressen, Port-Nummern, Protokollen oder Anwendungen; Entfernen von Regeln.

[8] Diese Merkmale werden allgemein als Malware Protection, Intrusion Detection und Intrusion Prevention bezeichnet.

[9] Das sogenannte Aufbrechen von SSL ist umstritten und insbesondere im organisatorischen Umfeld der Universität Wien nicht allgemein möglich. Davon zu unterscheiden ist das sogenannte TLS Offloading vor Servern im selben Betriebsbereich, das beispielsweise an Load Balancern durchgeführt wird.

5. Inkrafttreten

Diese Policy tritt mit 25.03.2019 in Kraft. Sie ist in der jeweils gültigen Fassung unter zid.univie.ac.at/firewall-organisationseinheiten/ abrufbar. Änderungen werden über die Mailingliste zid-tech@lists.univie.ac.at bekannt gegeben.

Für Subnetze, die dieser Policy noch nicht entsprechen, trifft der ZID mit den Zuständigen die nötigen Vereinbarungen. Ist dies nicht möglich, werden die Firewalls in der Grundkonfiguration aktiviert.