|  |  |  |
| --- | --- | --- |
| IT Services Support | Werftestrasse 4, Postfach 2969, CH-6002 Luzern  T +41 41 228 21 21  hslu.ch/helpdesk, informatikhotline@hslu.ch | |
|  |
| Luzern,  Seite 1/6 | | |
| Richtlinien und Vorgaben Laborzonen EEE | |

|  |  |
| --- | --- |
| Kurzbeschrieb: | Die vorliegende Dokumentation beschreibt die Richtlinien und Vorgabe für die EEE Laborzonen.  Hinweis für PHLU-Kunden: In dieser Dokumentation wird der Begriff *Benutzerkonto* gleichbedeutend mit *PHLUnet-Account* verwendet. |

|  |  |
| --- | --- |
| Klassifikation: | IT intern  Public  Andere |
| Kundengruppe: | HSLU  PHLU  Andere |
| Rolle: | Mitarbeitende / Doz.  Studierende  Andere |
| Geräteverwaltungstyp: | HSLU/PHLU Geräte  private Geräte  Andere |
| Betriebssystem: | Windows  OS X  Andere |
| Publikation:  Support: | hslu.ch/helpdesk  Intranet  Andere  Web: hslu.ch/helpdesk  E-Mail: informatikhotline@hslu.ch  Tel: 041 / 228 21 21  Portal: helpdesk.hslu.ch |

Änderungsverzeichnis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Datum | Status | Änderungen und Bemerkungen | Bearbeitet von |
| Nr. 1.0 | 03.06.2014 |  | Überführung CD/CI | mih |
| Nr. 1.1 | 13.08.2014 | Überarbeitet | Web12 | enp |

Inhaltsverzeichnis

[1. Allgemein 3](#_Toc396379085)

[2. Generelle Anforderungen für HSLU Labors 3](#_Toc396379086)

[3. Zusätzliche Rahmenbedingungen für „Simple“ Labors 4](#_Toc396379087)

[4. Zusätzliche Rahmenbedingungen für „Advanced Labors“ 5](#_Toc396379088)

[5. Schlussbestimmungen 5](#_Toc396379089)

# Allgemein

An der Hochschule Luzern betreiben verschiedene Labors eigene Netzwerke. Diese Netzwerke werden in einem Experimental Enterprise Environment-Netzwerk (EEE) zusammengefasst. In diesem Dokument werden die Vorgaben und die Rahmenbedingungen für die Betreiber der Labors zusammengestellt.

Bei der Gestaltung des Konzeptes für die EEE-Integration wurde darauf geachtet, dass die einzelnen Labors möglichst unabhängig von anderen Labors und von IT Services betrieben werden können. Dies hat aber zur Folge, dass IT Services nur im Bereich der Connectivity Support leisten kann.

Ein Anschluss an das EEE-Netzwerk hat folgende Vorteile:

* Die Labors können untereinander kommunizieren
* Rechner im HSLU-Netzwerk können auf die Ressourcen im Labor zugreifen
* Im EEE-Netzwerk werden einige Services für die Labors zur Verfügung gestellt:
  + Microsoft KMS Lizenz-Server
  + DNS-Server für Namensauflösung im Internet und die Labors
  + Zeitserver
  + Root CA

Es wird zwischen „Simple“ und „Advanced“ Labor-Integrationen unterschieden. Betreiber von

„Simple“-Labors bekommen einen Netzwerk-Anschluss für den Zugriff auf die EEE-Dienste und das Internet. „Simple“-Labors sind aber vom Internet her nicht erreichbar.

Bei „Advanced“-Labors können Labor-Ressourcen auch vom Internet her erreicht werden. Bei

„Advanced“ Labors sind die Betreiber für alle Sicherheitsbelange selbst verantwortlich. Das Internet wird ungefiltert in die Laborinfrastruktur geführt. Diese Labors müssen daher zwingend eine ausreichende Firewall-Infrastruktur betreiben. In diesem Dokument sind die wichtigsten Rahmenbedingungen für die Betreiber von „Advanced“ Labors zusammengestellt.

Wenn das EEE Segment genutzt wird, gelten automatisch die folgenden Richtlinien:

# Generelle Anforderungen für HSLU Labors

Für EEE-Laborintegration gelten die folgenden gemeinsamen Rahmenbedingungen:

* Es kann über IPv4 und IPv61 laborintern, laborübergreifend und ins Internet kommuniziert werden
* Vom HSLU Netzwerk ist ein Zugriff auf Labor-Ressourcen über IPv4 möglich. Sobald im HSLU Netzwerk IPv6 unterstützt wird, wird auch eine Verbindung über IPv6 möglich sein.

1. IPv6 kann nur vom EEE-Advanced vom Internet-Adressbereich 147.88.0.0. genutzt werden.

* Es ist kein Zugriff aus dem Labornetzwerk in das HSLU-Netzwerk möglich
* Die Labors verwenden einen Domain-Namen der auf eee.intern endet. Der Präfix wird von IT Service zugewiesen und im DNS-Server konfiguriert.
* IT Services weist den Labors IPv4 IP-Adressen aus dem internen Netzwerkbereich 10.0.0.0/8 und aus dem Internet-Adress-Bereich 147.88.0.0/16 zu. IT Service stellt die Connectivity dieser Adressbereiche sicher. Die Connectivity zwischen Labors wird ausschliesslich über ein Layer 3 Routing gewährleistet.
* Falls weitere laborinterne Netzwerke gebildet werden, sollen andere private Adress-Bereiche (172.0.0.0, 192.168.0.0) verwendet werden. Diese Adressen werden ausserhalb der Labors nicht geroutet.
* Falls IPv6-Adressen verwendet werden, müssen die von IT-Services zugeteilten Adressbereich zwingend eingehalten werden.
* Die Netzwerkwerk-Komponenten (Firewall, interne Switches) werden von den Labors beschafft.
* Aktivierungen von Microsoft-Labor-Rechnern welche von IT Services zur Verfügung gestellt werden, müssen zwingend über den EEE-KMS erfolgen. Für alle anderen Rechner ist die Nutzung des KMS-Servers erlaubt.
* Drucker im HSLU-Netzwerk können nur über das HSLU VPN angesprochen werden
* Zugriff auf Dateiablagen im HSLU-Netzwerk muss zwingend über das HSLU VPN vorgenommen werden.
* Die Labors sind nach Möglichkeit über einen Gigabit-Link angeschlossen. Eine Glasverbindung ist grundsätzlich möglich. Verursacht ein Anschluss per Glasfaser erhöhte Kosten (gegenüber einem Anschluss per Kupfer), so kann dieser an das entsprechende Labor weiter verrechnet werden.
* Grundsätzlich können Labors eigene WLAN Access Points einsetzen. Um eine sichere Identifikation zu ermöglichen und eine Verwechslung zu vermeiden, müssen die SSID von eigenen WLAN’s mit dem String „eee“ beginnen. Die vom Access Point abgestrahlte Leistung muss soweit minimiert werden, dass nur im Laborbereich mit dem WLAN gearbeitet werden kann. WLAN Access Points dürfen ausschliesslich an Labornetzwerke angeschlossen werden. Es ist nicht erlaubt, ein HSLU-Netzwerk aufzuschalten. Falls ein Zugriff auf das Internet möglich ist, ist eine Authentisierung (mindestens WPA2) zwingend.
* Es dürfen keine Multi-Homed Rechnerkonfigurationen (ein Interface im Labor und ein Interface im HSLU-Netzwerk) oder andere Tunneling-Mechanismen in das HSLU Netzwerk implementiert werden.
* Die Labors übernehmen die Verantwortung für den gesamten Netzwerkverkehr ins Internet. Die Labors müssen jederzeit in der Lage sein, über die aktiv verwendeten IP-Adressen Auskunft zu geben.
* Es gibt regelmässige Sitzungen, zwischen EEE-Vertretern der Departemente und IT Services.

Hier werden Erfahrungen und Tipps bezüglich den Netzwerkgeräten ausgetauscht. (Prinzip User-Group)

* In den Labornetzwerken wird eine Root-CA betrieben. Labors können eigene untergeordnete CA’s betreiben.

# Zusätzliche Rahmenbedingungen für „Simple“ Labors

Für die „Simple“ Labors gilt:

* Es kann über alle Ports mit dem Internet kommuniziert werden.
* Ein Zugriff vom Internet her auf die Labor-Infrastruktur ist nur über eine VPN-Verbindung (HSLU VPN) möglich.

# Zusätzliche Rahmenbedingungen für „Advanced Labors“

Für die „Advanced Labors gilt:

* Die Labors haben direkten Internet-Anschluss (schwarzes Netzwerk) und sind selbst für eine ausreichende Sicherung (Firewall) zuständig. Es ist sicherzustellen, dass der IPv4 und der IPv6 Verkehr ausreichend gefiltert wird.
* Die Labors stellen mit geeigneten Sicherheitsmechanismen sicher, dass kein Verkehr aus dem Internet in das interne EEE-Netzwerk weitergeleitet werden kann.
* Pro Labor werden zwei logische (oder physikalische) Ports zur Verfügung gestellt:
  + Ein Port zu der EEE-Infrastruktur (andere Labors, EEE Infrastruktur, HSLU-Netzwerk eingehend)
  + Ein Port zum Internet mit public IPv4 Adressen und IPv6 Connectity
* Falls von einem Labor Services angeboten werden, die vom Internet her zugänglich sind, übernimmt das Labor die Verantwortung für diesen Service. Insbesondere stellen die Labors sicher, dass die Richtlinien von der Stiftung Switch2 und von IT Services eingehalten werden. Es dürfen keine Services angeboten werden, die das Angebot der IT Services konkurrenzieren.

Es sind insbesondere die folgenden Punkte zu beachten:

* + Mail-Services dürfen nur für einen klar eingeschränkten Einsatzbereich (Projektbezug, Lehre) eingesetzt werden. Für Mail-Services gilt insbesondere
    - Es muss sichergestellt werden, dass der Mail-Server nicht für SPAM-Mails missbraucht werden kann.
    - Es dürfen keine Massenmails verschickt werden.
    - Ausgehende Mails müssen über einen Smarthost versendet werden.
  + DNS-Server dürfen nur Ressourcen im Labor auflösen oder Services, die im Rahmen eines Hochschulprojektes angesprochen werden.
* Alle vom Internet her erreichbaren Ressourcen sind gemäss den heute üblichen Schutzmassnahmen zu härten.

2) www.switch.ch

# Schlussbestimmungen

Falls eine oder mehrere Punkte dieses Reglements ganz oder teilweise rechtsunwirksam sind oder werden, ist die Wirksamkeit der übrigen Bestimmungen dieses Reglements davon nicht beeinflusst. Eine entsprechend unwirksame Klausel wird durch eine Klausel ersetzt werden, die dem Zweck der unwirksamen Bestimmung am nächsten kommt; dasselbe gilt im Fall einer Lücke.

Sofern in diesem Dokument keine abweichende Klauseln definiert sind, gelten alle Richtlinien aus dem „allgemeinen Benutzungsreglement für Informatikmittel“ der Hochschule Luzern auch für die EEE-Labore.

Die vorliegende Version dieses Reglements ersetzt alle früheren Versionen.