Merkblatt 03

Definition von Trustlevels und Sicherheitsmassnahmen für Netzwerkzonen der UZH

1. Allgemeines

- Trust- und Sicherheitszonen-Modell
  - Ein Sicherheitszonenmodell auf Netzwerkebene, welches unterschiedliche sicherheitsrelevante Anforderungen von Daten und Informationen berücksichtigt, muss implementiert werden. Ein Sicherheitszonenmodell beinhaltet Zonen, welche Systeme mit ähnlichen Sicherheitsanforderungen von Daten und Informationen zusammenfasst (z.B. vertrauenswürdige und schützenswerte Informationen in dafür vorgesehenen, sehr sicheren und vertrauenswürdigen Netzwerkzonen, die mit Sicherheitssystemen wie z.B. Firewalls abgetrennt sind).

- Netzwerksegmente und Sicherheitszonen
  - Netzwerksegmente (IP-Netze), welche die Basis für einen Dienst oder eine organisatorische Einheit bilden, und die demzufolge ein einheitliches Mass an Sicherheit erfordern, werden zu einer Netzwerk-Sicherheitszone zusammengefasst. Innerhalb einer Sicherheitszone ist die Kommunikation nicht eingeschränkt. Eine Einschränkung kann aber, sofern notwendig, beantragt werden (siehe Ausnahmeregelung).

- Sicherheitszonen und Trustlevel
  - Sicherheitszonen werden einem Trustlevel zugewiesen. Für unterschiedliche Trustlevels können unterschiedliche Regeln gelten.

- Separation von Sicherheitszonen
  - Sicherheitszonen müssen durch ein Sicherheitssystem wie z.B. eine Firewall separiert werden.
  - Für jede Sicherheitszonen-Verbindung soll ein Set von Basis-Kommunikationsregeln definiert werden. Die Standardisierung reduziert den Aufwand für die Etablierung und Änderung von Netzwerkverbindungen.

2. Logisches Sicherheitszonenmodell

Sicherheitszonen Definition

Gestaltung einer Sicherheitszone:

- Eine netzbasierte Sicherheitszone (im Folgenden kurz Sicherheitszone) ist ein IP-Netzwerk, das aus Sicherheitsgründen von anderen Netzen getrennt wird.
- Die Kommunikation in eine Sicherheitszone hinein oder aus einer Sicherheitszone heraus, wird durch Sicherheitsmaßnahmen kontrolliert. Hierzu werden die Sicherheitszonen durch Sicherheitselemente vernetzt.
- Sicherheitselemente werden je nach Anforderung ausgewählt. Beispiele sind Firewall oder Intrusion Prevention System (IPS) resp. IDS Intrusion Detection Systeme (IDS).
- Innerhalb einer Sicherheitszone wird auf Ebene des Netzes keine weitere Einschränkung der Kommunikation verlangt.
- Ein Sicherheitselement kann an mehrere Sicherheitszonen angebunden werden und eine Sicherheitszone kann ebenso mit mehreren Sicherheitselementen verbunden werden.

Die Netzwerkzonen der UZH sind als Zonen mit unterschiedlich hohen Sicherheitsanforderungen zu betrachten. Jedes Netzwerk muss einem Typen «Sicherheitszone» zugeordnet sein. Das bedeutet, dass mehrere Netzwerke gleicher Art existieren können. Jeder dieser Netzwerke muss aber einem Typen «Sicherheitszone»(Trustlevel) zugeordnet werden (siehe Tabelle unter 2.3.1). Diese Zuordnung stellt sicher das nicht Systeme mit niedrigen Sicherheitsanforderungen zusammen mit Systemen mit hohen Sicherheitsanforderungen in der gleichen Netzwerkzone betrieben werden.

3. Festlegungen zur logischen und physischen Trennung

Wenn Sicherheitszonen durch IP-Netze gebildet werden, muss geregelt werden, unter welchen Rahmenbedingungen eine physische Trennung notwendig ist und wann eine logische Trennung auf Ebene von Netz, Servern und Clients erlaubt ist.

Typen von Sicherheitszonen

Details siehe Merkblatt03_Beilage Zonenkonzept auf der Homepage der IT - Sicherheit

Bezeichnung	Beschreibung	Sicherheitsstufe / Trustlevel
Unsichere Zone	Externe Sicherheitszone, welche nicht vertrauenswürdig ist (Internet)	TL0
Externe vertrauenswürdige Zone	Externe Sicherheitszone, welche vertrauenswürdig ist (z.B. externe Cloud-Dienste / Managed Service Provider / Kooperationen mit externen Partnern)	TL1
Sichere DMZ / halb sichere Zone	Interne Sicherheitszone mit Verbindungen gegen aussen, die als teilweise sicher gilt (z.B. Webdienste, Maildienste, VoIP-Gateway, Remote Access VPN-Dienst, interne Cloud-Dienste)	TL2
Sichere Zone	Interne Sicherheitszone, welche hoch sensitive Informationen/Daten beinhaltet	TL3

4. Sicherheitsstufen-Konzept (Trustlevel)

Die Sicherheitsstufe zeigt an, in welchem Umfang spezifische Sicherheitsmassnahmen umgesetzt werden müssen. Es existieren 4 Sicherheitsstufen:

- Sicherheitsstufe 0
  - Netzwerke, bei denen die Universität keinerlei Sicherheitsmassnahmen und Sicherheitsarchitekturen vorgeben kann. Beispiele: Internet, SWITCHlan, LEUnet.
  -
- Sicherheitsstufe 1
  - Netzwerke, welche durch externe Partner der Universität in Kooperation mit der Universität betrieben werden. Sicherheitsvorgaben müssen von Fall zu Fall und unter den Kooperationspartnern selbst definiert werden. Die Verbindung zum Netz der Universität besteht entweder mittelbar über das Internet bzw. SWITCHlan oder unmittelbar über ein Sicherheitssystem wie z.B. eine Firewall. Eine direkte Anbindung an das Netzwerk der Universität ohne Sicherheitssystem ist nicht erlaubt. Die Verbindung bedarf entsprechender Sicherheitsvorkehrungen und einer

vertraglichen Abmachung zwischen den Kooperationspartner, um die Risiken für die Universität zu minimieren. Die Verbindung wird durch die üblichen Monitoring-Systeme (NetFlow-Daten, SNMP-Parameter) überwacht.

- Sicherheitsstufe 2
  - Netzwerke, welche in diese Sicherheitsstufe eingeordnet werden, sind konform zu den geltenden Vorschriften und Weisungen (Security Policy, RNS, REIM etc.) der Universität. Eine Anbindung ist nur unter Berücksichtigung aller Sicherheitsvorgaben in dieser Weisung erlaubt. Eine Anbindung des UZH an ein Netzwerk mit Sicherheitsstufe 2 muss auf Missbrauch und Anomalien überwacht werden.

- Sicherheitsstufe 3
  - Netzwerkzonen dieser Einstufung sind Sicherheitszonen mit hohen Anforderungen bezüglich CIA (Confidentiality, Integrity, Availability) und müssen nebst den allgemeinen Anforderungen aus den geltenden Vorschriften (Security Policy, RNS, REIM etc.) über eine angemessene Überwachung nicht nur an den Zonenübergängen, sondern auch innerhalb der Zone verfügen. Die System- und Applikationsverantwortlichen dürfen auf Server und Applikationen nur über eine zentral bereitgestellte und kontrollierte Umgebung (z.B. Jumphost) zugreifen. Die Zugriffe müssen aufgezeichnet und in Logdateien (z.B. Syslog, Radiuslog) abgelegt werden. Diese müssen zeitnah (unmittelbar) auf den zentralen Loghost transferiert werden. Details für die Vorgaben zum Logging finden sich in den Vorschriften für die Sammlung von Log-Dateien (Logfile Policy) der UZH.

5. Sicherheitszonen-Verantwortliche / Netzwerkverantwortliche

Für jede Sicherheitszone wird ein/e Verantwortliche/r bestimmt. Er/sie hat folgende Aufgaben:

- Beschreibung der Sicherheitszone inkl. Netzwerkdiagramm.
- Definition einer Verhaltensrichtlinie für die Sicherheitszone (soweit erforderlich).
- Verantwortung für die Konformität der Regeln beim Zonenübergang der Sicherheitszone
- Verantwortung für die der Sicherheitszone zugeteilten Netzwerkadressen.

In den Instituten ist dies mit der Rolle des Netzwerkverantwortlichen / der Netzwerkverantwortliche gleichzusetzen.

6. Datenfluss zwischen Sicherheitszonen

Die Kommunikation zwischen Sicherheitszonen darf nur über Sicherheitssysteme (z.B. eine Firewall) erfolgen. Jede Sicherheitszone ist durch ein Sicherheitssystem zu schützen. Im Weiteren müssen folgende Sicherheitsvorkehrungen implementiert sein:

- Ein Sicherheitssystem zur Durchsetzung und Kontrolle der Kommunikation in eine Sicherheitszone. Folgende Elemente sollen kontrolliert werden können: Protokoll, Quelladresse und -port, Zieladresse und –port, gewisse Applikationsparameter.
- Ein Intrusion Detektion/Prävention-System (IDS/IPS) / SIEM, um den Verkehr von/zu einer Zone auf Anomalien oder Angriffe zu prüfen. Pro Zone wird kein eigenständiges System, sondern die Sonde eines zentralen Systems implementiert.
- Je nach Einstufung einer Sicherheitszone auch Proxy-Technologien oder Filter, um Applikationen mit direktem Internetzugang zu schützen (z.B. gegen Malicous Code Injection). Beispiele: Malware-Überprüfung und RBLs für E-Mail (SMTP), Web Application Firewall (WAF) für Webbrowsing (HTTP/HTTPS) oder RPZs für DNS (DNS-Firewall). Gewisse Filter können bereits bei der Perimeter-Firewall eingesetzt werden, z.B. Web Application Firewall (WAF). Einige dieser Technologien werden nicht beim Zonenübergang, sondern bei den Dienstservern eingesetzt (RBLs, RPZs, evtl. Mailfilter). Für Sicherheitsimplementationen über Osi Layer 4 ist aber der Service- bzw. Systembetreiber verantwortlich.