Universität Zürich[UZH]

Weisung

Weisung über die Netzwerksicherheit (WNS)

(vom …)
Aktuelle Version, welche für die Zentrale Informatik seit 1.10.2020 in Kraft ist

Die Zentrale Informatik,

gestützt auf § 6 Abs. 1 des Reglements über den Einsatz von Informatikmitteln an der Universität Zürich vom … (REIM),

erlässt folgende Weisung:

1 Grundsätzliches

Die Weisung über die Netzwerksicherheit (WNS) legt Minimalstandards für Netzwerke und für den Anschluss von Systemen an diese fest und regelt die Planung und Umsetzung von entsprechenden Massnahmen.

1.1 Geltungsbereich

Diese Weisung gilt für alle Organisationseinheiten der UZH und alle verbundenen externen Einheiten, welche selbständig Netzwerke oder Netzwerksegmente betreiben oder durch externe Anbieter betreiben lassen. Organisationseinheiten der UZH, welche ihre Netzwerke vollumfänglich durch die Zentrale Informatik betreiben lassen, müssen lediglich die im REIM ausgeführten Vorgaben berücksichtigen.

1.2 Begriffe

Die in dieser Weisung gewählten Begriffe haben die gleiche Bedeutung wie die in der Verordnung über die Informationsverwaltung und -sicherheit (IVSV) des Kanton Zürich; deren Bestimmungen bleiben unberührt.

1.3 Netzwerkdienstleistungen gegenüber Dritten

Die Erbringung von Netzwerkdienstleistungen gegenüber Dritten ist untersagt. Davon ausgenommen ist die Zentrale Informatik.

1.4 Verantwortlichkeiten von Netzwerkbetreibern

Netzwerkbetreiber haben folgende Verantwortlichkeiten und Aufgaben sicherzustellen:

- Definieren von Regelwerken, Funktionen und Verantwortlichkeiten im Bereich der Netzwerksicherheit
- Definieren eines Netzwerkmanagements
- Implementieren von Sicherheitszonen gemäss Vorgaben der IT-Sicherheit der Zentralen Informatik
- Pflegen der Kontaktdaten von Netzwerkverantwortlichen / IT-Verantwortlichen

Universität Zürich[UZH]

2 Organisatorische und technische Vorgaben

Nachfolgende Kapitel beschreiben detaillierte organisatorische und technische Vorgaben zur Sicherstellung der Netzwerksicherheit.

2.1 Verbindungen mit fremden Netzwerken

- Verbindungen mit universitätsfremden Netzwerken, wie Mietleitungen oder Tunnelverbindungen von ausserhalb der Universität ins Netzwerk der Universität, die nicht an einem entsprechenden Dienst der Zentralen Informatik enden, wie z.B. Remote Access VPN-Dienst, sind in jedem Fall bewilligungspflichtig.

- Verbindungen zu Netzwerken anderer Organisationen (z.B. anderer Hochschulen, Spitäler, kantonaler Netze) in organisationsübergreifenden Einheiten (z.B. gemeinsame Forschungseinrichtungen, gemeinsame Institute, Kliniken mit Forschung) sind in jedem Fall bewilligungspflichtig.

- Bei bewilligten Verbindungen ist die Bewilligungsempfängerin verpflichtet, ein Sicherheitssystem wie z.B. eine Firewall nach Vorgaben der Zentralen Informatik zu betreiben, ein Sicherheitskonzept zu erstellen und verlangte Audits durchzuführen.

- Alternative Pfade zum Internet von am Netzwerk der Universität Zürich (NUZ) angeschlossenen Geräten ausserhalb des offiziellen Internet-Zugangs der UZH sind nicht erlaubt.

- Ein IP-basierter Zugriff auf das interne Netz muss über einen sicheren Kommunikationskanal erfolgen und auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden. Derartige VPN-Gateways sollten in einer DMZ realisiert werden. Es sollte beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über den VPN-Gateway authentisierten Zugriffe ins interne Netz müssen mindestens die interne Firewall durchlaufen.

- Zugriffe aus dem Internet auf das interne Netzwerk müssen immer über eine DMZ erfolgen.

- Ausgehende Kommunikation aus dem internen Netz zum Internet muss über ein Sicherheits-Gateway geführt werden

2.2 «Defence in Depth»-Prinzip

- Die Implementierung mehrerer Sicherheitsstufen und Kontrollpunkte, welche die Umsetzung von Sicherheitskonfigurationen durchsetzen, muss für jede Zone sichergestellt werden. Direkte, uneingeschränkte Verbindungen von Systemen aus Netzwerkzonen mit nicht gleichwertigen Trustlevels müssen verhindert werden.

2.3 Nachvollziehbarkeit benutzter Netzwerkadressen

- Es sind die notwendigen Vorkehrungen zu treffen, dass jede benutzte Netzwerkadresse der UZH jederzeit auf die dahinter agierende Person zurückgeführt werden kann.

Es gibt dazu folgende Modelle:

- Dezentrale Verantwortlichkeit: Die Zentrale Informatik delegiert die Verantwortlichkeit für bestimmte IP-Bereiche an eine andere organisatorische Einheit. Bei der Zentralen Informatik werden in einer Datenbank

die Zuordnung IP-Bereich – organisatorische Einheit – Kontaktperson(en) gespeichert. Die registrierten Kontaktpersonen werden bei Ereignissen informiert. Die Kontaktpersonen und letztlich die organisatorische Einheit sind für die Behandlung der Ereignisse verantwortlich. Die interne Weitergabe der Verantwortlichkeit innerhalb der organisatorischen Einheit obliegt der organisatorischen Einheit.

- Die Zentrale Informatik stellt durch geeignete technische Massnahmen sicher, dass eine direkte Zuordnung zwischen IP-Adresse und einzelnem/r Nutzer/in möglich ist. Diese/r wird im Fall eines Ereignisses direkt angesprochen.

2.4 Adressübersetzung (NAT)

- Werden bei einem Netz- oder Sicherheitssystem die IP-Adressen übersetzt, typischerweise zwischen auf der Aussenseite öffentlichen Adressen und auf der Innenseite privaten Adressen, so muss in jedem Fall jede einzelne Adressübersetzung geloggt werden. Zweck dieser Massnahme ist die Nachvollziehbarkeit, welcher Host zu welchem Zeitpunkt welche öffentliche IP-Adresse benutzt hat.

- Das Loggen muss auf einem Server des Betreibers der Adressumsetzung geschehen. Die geltenden rechtlichen Bestimmungen des Datenschutzes sind dabei einzuhalten. Die Logdatei muss über die letzten sechs Monate Auskunft geben können.

2.5 Automatische Adresszuweisung mit DHCP-Server

- Werden die IP-Adressen den Hosts automatisch mittels eines zentralen Servers, typischerweise mit dem Verfahren DHCP, zugewiesen, so muss in jedem Fall jede einzelne Adresszuteilung geloggt werden. Zweck dieser Massnahme ist die Nachvollziehbarkeit, welcher Host zu welchem Zeitpunkt welche IP-Adresse benutzt hat.

- Das Loggen muss auf einem Server des Betreibers der automatischen Adresszuweisung geschehen. Die geltenden rechtlichen Bestimmungen des Datenschutzes sind dabei einzuhalten. Die Logdatei muss über die letzten drei Monate Auskunft geben können. Zudem ist die Logfile Policy der UZH zu berücksichtigen.

2.6 Client-Server-Segmentierung

- Clients und Server müssen in unterschiedlichen Sicherheitssegmenten platziert werden. Die Kommunikation zwischen diesen Segmenten muss mindestens durch eine Firewall kontrolliert werden.

- Es ist zu beachten, dass mögliche Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Sicherheitssegment zu positionieren, in den entsprechenden anwendungs- und systemspezifischen Sicherheitsanforderungen in einem separaten Sicherheitskonzept geregelt werden.

- Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, müssen dedizierte Sicherheitssegmente eingerichtet werden.

2.7 Fernwartungszugänge

Fernwartung über externe Netze oder durch Dritte ist besonders kritisch. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung, wenn immer möglich, zu verzichten. Ist dies nicht möglich, so sind folgende Punkte zu beachten:

- Bei einer Fernwartung über externe Kommunikationsverbindungen müssen die Zugänge und die Verbindungen abgesichert werden. Das Fernwartungspersonal muss sich authentisieren und die übertragenen Daten müssen verschlüsselt werden. Beispielsweise kann die Anbindung per VPN oder exklusiv genutzte Verbindungen realisiert werden.

- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden. Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-how oder die Kapazität nicht verfügbar ist, kann das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten über die Vorgänge sollte lokale IT-Experten sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.

- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.

- Alle Remote-Administrationsvorgänge müssen aufgezeichnet werden. Dabei sind zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

- Entsprechend sind auch mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

- Es ist ein Sicherheitskonzept zu erstellen, welches die Risiken sowie allfällige kompensierende Massnahmen aufzeigt.

2.8 Netztrennung in Sicherheitszonen

2.8.1 Allgemein

- Das Gesamtnetz muss mindestens in folgende drei Netzwerkzonen separiert sein:
  - internes Netz,
  - demilitarisierte Zone (DMZ) und
  - Aussenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze).

- Zonenübergänge müssen durch eine Firewall abgesichert werden.

2.8.2 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).

2.8.3 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).

- Es dürfen nur Endgeräte in einem Sicherheitssegment positioniert werden, die einem ähnlichen Sicherheitsniveau der Netzwerkzone entsprechen.

- Durch ein VLAN darf keine Verbindung zwischen einer Zone vor der DMZ bzw. den Sicherheits-Gateway und dem dahinterliegenden internen Netz geschaffen werden. Generell muss sichergestellt werden, dass Zonen nicht überbrückt werden können, wenn VLANs eingesetzt werden. Ausnahmen können nur mit einem Sicherheitskonzept beantragt werden.

2.8.4 Sicherheitszonen und Trustlevel

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

2.8.5 Separation von Sicherheitszonen

- Sicherheitszonen müssen durch ein Sicherheitssystem wie z.B. eine Firewall separiert werden.

- Für jede Sicherheitszonen-Verbindung muss ein Set von Basis-Kommunikationsregeln definiert werden. Die Standardisierung reduziert den Aufwand für die Etablierung und Änderung von Netzwerkverbindungen.

2.8.6 Logische und physische Trennung

- Auf virtualisierten Netzen und IT-Systemen dürfen Sicherheitszonen unterschiedlicher Trustlevel nebeneinander ohne Trennung der Hardware betrieben werden, solange Verbindungen nur an den erwünschten, kontrollierten Übergängen möglich sind. Es sind die einschlägigen Best Practices und Herstellerempfehlungen zu berücksichtigen. Insbesondere sind in diesem Umfeld ohne Verzögerung Security Advisories, unter Berücksichtigung des operativen IT-Risikos, umzusetzen und alle identifizierten, verfügbaren sicherheitsrelevanten Systemupdates einzuspielen.

- Existieren physische Trennungen (wie z.B. die Institutszone im Datacenter), so dürfen (logische) Netzwerkzonen diese nicht überschreiten. Konkret bedeutet dies im genannten Beispiel, dass Netze der physischen Institutszone nicht im restlichen Teil des Datacenters oder Netze der anderen logischen Zonen der Zentralen Informatik nicht in der Institutszone verbreitet werden dürfen.

2.9 WLAN-Sicherheit

- Das drahtlose Netz wird durch die Zentrale Informatik und verschlüsselt betrieben, und die Clients müssen sich mit ihren Benutzer-Credentials anmelden.

- Folgende Punkte müssen zudem bezüglich «denial-of-service», «man-in-the-middle attacks» sowie allgemein «over-the-air security threats» berücksichtigt werden:

    - An wichtigen Punkten können drahtlose Intrusion Detection Systeme (WIDS – Wireless Intrusion Detection System) eingesetzt werden, um drahtlose Geräte zu identifizieren, sowie Angriffsversuche und erfolgreiche Kompromittierung zu erkennen. Zusätzlich zu WIDS sollte jeder drahtlose Verkehr von WIDS überwacht werden, da der Verkehr in das kabelgebundene Netzwerk übergeht.

    - Zur Authentisierung in drahtlosen Netzwerken bedarf es Authentifizierungsprotokollen wie z.B. das Extensible Authentication Protocol-Transport Layer Security (EAP / TLS), welche u.a. den gesamten Authentisierungs-Vorgang in genügendem Masse schützen.

2.10 IT-Sicherheit in Netzen

2.10.1 Eingrenzung und Behebung kritischer Situationen

- Stellt die IT-Sicherheitsstelle oder der Netzbetreiber eine kritische Situation im Datennetz fest, so treffen sie unverzüglich Massnahmen zur deren Eingrenzung und Behebung. Eine kritische Situation kann beispielsweise bei der Beobachtung eines Einbruchs, bei der Feststellung aktiver Malware, bei einer Betriebsstörung durch Benutzerfehlverhalten oder bei anderen ähnlichen Umständen gegeben sein.

- Wird eine Ursache im Verantwortungsbereich einer organisatorischen Einheit festgestellt, so informieren die IT-Sicherheitsstelle oder der Netzbetreiber die bei der Zentralen Informatik registrierte Kontaktperson. Dabei leistet die Zentrale Informatik soweit möglich Unterstützung.

2.10.2 Separierung der Infrastrukturdienste

- Server, die grundlegende Dienste (bspw. Jumphosts / Backup / NAS / generell administrative Zugänge zu produktiven Services etc.) für die IT-Infrastruktur bereitstellen, sind in einem dedizierten Sicherheitssegment zu positionieren. Die Kommunikation mit ihnen sollte durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

2.11 Netzmanagement

2.11.1 Ausfallsicherheit und Verfügbarkeit

- Das Datennetz ist grundsätzlich nicht redundant aufgebaut. Für eine besonders hohe Verfügbarkeit sind das Core-Netz und die Netze in den zentralen Datacentern redundant aufgebaut. Dienste mit hohen Verfügbarkeitsanforderungen müssen deshalb innerhalb dieser Umgebung integriert werden.

- Für die Alarmierung, welche Personen, bedeutende Sachwerte oder wesentliche immaterielle Werte betrifft, muss ein vom Netz unabhängiger Backup-Weg existieren.

- Gebäudesteuer- und Schliesselemente dürfen durch einen Ausfall des Netzes während der Nacht oder während dem Wochenende in keinen Zustand geraten, der Menschen, bedeutende Sachwerte oder wesentliche immaterielle Werte gefährdet.

- Die Perimeter-Infrastruktur muss robust, zuverlässig und stabil gegen Ausfälle geschützt sein, um interne wie externe Verbindungen sicherzustellen und Ausfällen vorzubeugen. Zu berücksichtigen sind insbesondere Verbindungen zu wichtigen Diensten mit Verbindungen vom und zum Internet bezüglich Stabilität und Robustheit gegenüber DDoS-Angriffen (richtet sich nach den Möglichkeiten des Internet Service Providers).

2.11.2 Sicherheitssysteme

- Sicherheitssysteme müssen dem aktuellen Stand der Technik entsprechen.

- Ein Sicherheitssystem kann ein Stand Alone-System wie z.B. eine Firewall, aber auch eine ins Netzwerk integrierte, dienstbasierte Sicherheitslösung sein.

2.11.3 Einspielen von Updates und Patches

- Die verantwortlichen Mitarbeiter müssen sich regelmässig über bekannt gewordene Schwachstellen der eingesetzten Netzmanagement-Lösungen informieren und sicherheitsrelevante Updates und Patches so schnell wie möglich einspielen. Nicht sicherheitsrelevante Updates dürfen nicht die Sicherheit und Stabilität der Netzmanagement-Lösung beeinträchtigen.

2.11.4 Regelmässige Datensicherung

- Alle eingesetzten Netzmanagement-Lösungen müssen ins Datensicherungskonzept der organisatorischen Einheit eingebunden werden. Dabei müssen alle spezifischen Daten für das Netzmanagement berücksichtigt werden. Es müssen mindestens die Systemdaten für die Einbindung der zu verwaltenden Komponenten bzw. Objekte, Ereignismeldungen, Statistikdaten sowie vorgehaltene Daten für das Konfigurationsmanagement gesichert werden.

2.11.5 Absicherung der Netzmanagement-Kommunikation

- Erfolgt die Netzmanagement-Kommunikation über die produktive Infrastruktur, müssen dafür sichere Protokolle verwendet werden.

2.11.6 Beschränkung der SNMP-Kommunikation

- Grundsätzlich dürfen im Netzmanagement keine unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Werden dennoch unsichere Protokolle verwendet und nicht über andere sichere Netzprotokolle (z. B. VPN oder TLS) abgesichert, muss ein isoliertes Managementnetz genutzt werden. Grundsätzlich sollte über SNMP nur mit den minimal erforderlichen Zugriffsrechten zugegriffen werden. Die Zugangsberechtigung sollte auf dedizierte Management-Server eingeschränkt werden.

2.11.7 Starke Authentisierung des Management-Zugriffs

- Für den administrativen Zugriff auf Netzkomponenten muss eine als sicher geltende Authentisierungsmethode verwendet werden. Die administrativen Zugänge müssen über einen zentralen Authentisierungsserver mittels personalisierter Konten über entsprechend sichere Protokolle authentisiert werden.

- Der Zugriff auf zentrale Netzmanagement-Lösungen und Management-Informationen ist durch eine als sicher geltende Authentisierungsmethode zu schützen. Die Zugänge sollten über einen zentralen Authentisierungsserver mittels personalisierter Konten authentisiert werden.

- Falls von einem Netz ausserhalb der Managementnetze auf Netzmanagement-Werkzeuge zugegriffen wird, müssen als sicher geltende Authentisierungs- und Verschlüsselungsmethoden realisiert werden.

    - Direkte Management-Zugriffe eines Administrators von einem IT-System ausserhalb der Managementnetze auf eine Netzkomponente sollten vermieden werden. Ist ein solcher Zugriff ohne zentrales Management-Werkzeug notwendig, muss die Kommunikation entkoppelt werden. Solche Sprungserver sollten im Management-Netz integriert und in einem getrennten Zugangssegment positioniert sein.

    - Im Rahmen des Netzmanagements sind die Sitzungsdaten aller administrativen Zugriffe zu protokollieren und zu speichern. Dabei sind die datenschutzrechtlichen Bestimmungen einzuhalten.

    - Die Protokollierungsdaten müssen in der Datensicherung ausreichend und gesetzeskonform geschützt werden. Darüber hinaus sollte festgelegt werden, ob und in welchem Umfang Sitzungsdaten für forensische Analysen zu archivieren sind. Wenn Daten archiviert werden, ist darauf zu achten, dass dies gesetzeskonform und revisionssicher durchgeführt wird.

2.11.8 Statusüberwachung der Netzkomponenten

- Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sind automatisch an ein zentrales Management-System zu übermitteln und dort zu protokollieren. Das zuständige IT-Personal sollte zusätzlich automatisch benachrichtigt werden. Das Alarming und Logging muss mindestens folgende Punkte beinhalten:
    - Ausfall bzw. Nichterreichbarkeit von Netz- oder Management-Komponenten,
    - Hardware-Fehlfunktionen,
    - fehlerhafte Anmeldeversuche sowie
    - kritische Zustände oder Überlastung von IT-Systemen.

- Die Logfilepolicy der UZH ist in jedem Fall zu berücksichtigen.

2.11.9 Physischer Schutz der Netzwerkkomponenten

- Die Netz- und Sicherheitssysteme befinden sich in dedizierten Netzwerkräumen, bei welchen die Zentrale Informatik die Hoheit über den Zugang hat.

2.12 Ausnahmeregelungen

Aufgrund technischer oder organisatorischer Gegebenheiten gibt es bei den IT-Systemen und Verfahren der UZH Ausnahmen zu den IT-Sicherheitsvorgaben und IT-Sicherheitsumsetzungsanforderungen. Diese Ausnahmen werden in einem geregelten Prozess entschieden und genehmigt, dokumentiert und nachverfolgt. Der Antrag erfolgt in schriftlicher Form an die IT-Sicherheitsstelle mit folgendem Inhalt:

- Einreichungs- und gewünschtes Umsetzungsdatum
- Verantwortliche Person
- Titel
- Beschreibung
- Anforderung(en) an eine Lösung, welche zur Abweichung der Sicherheitsvorgaben führen
- Begründung, warum die Ausnahme benötigt wird
- Risiko hinsichtlich Auswirkung, wenn die Sicherheitsvorgaben nicht eingehalten werden können
- Kompensierende Massnahmen, welche das Risiko auf ein akzeptables Mass reduzieren

3 Schlussbestimmungen

3.1 Inkrafttreten

Die Weisung über die Netzwerksicherheit (WNS) tritt am … in Kraft und ist bis auf Widerruf gültig.

3.2 Übergangsfrist

Für Umsetzung und Einhaltung dieser Weisung besteht eine Übergangsfrist von 9 Monaten ab Inkrafttreten.