Richtlinien des Fachausschusses

für Netzwerke der KIT zur

gesicherten Anbindung an

Fremdnetzwerke

"AFNW Richtlinien"

Teil A - Organisation

B u n d e s m i n i s t e r i u m f ü r ö f f e n t l i c h e L e i s t u n g u r

Richtlinien des Fachausschusses für Netzwerke der KIT zur gesicherten Anbindung an Fremdnetzwerke

"AFNW - Richtlinien"

Teil A - Organisation

2000-9-1

---

1. Reduktion des Gefahrenpotentials durch Einzelanbindung

Durch die Vernetzung der Dienststellen der öffentlichen Verwaltung bestehen ressortübergreifende Verbindungen der

EDV-Systeme.

Bei der Anbindung an das Internet sind daher folgende Gesichtspunkte zu beachten:

* EDV-Systeme, welche zeitweise oder dauernd an Produktions-Netze angeschlossen sind, dürfen nur unter Verwendung ausreichender Sicherheits-einrichtungen (z.B. Firewalls") mit Fremdnetzwerken verbunden werden.

  Die betroffenen Einrichtungen sollten ggf. zusätzlich durch Netzsegmentierung geschützt werden.

* Diese Sicherheitseinrichtung besteht aus einem zwei- oder mehrstufigen System (im folgenden als "Firewall" bezeichnet), welches zumindest die unter "Wichtige Punkte eines Pflichtenhefts" angeführten Kriterien erfüllt.

* Die Firewall muß während des laufenden Betriebs gewartet und seine Logfiles sollten täglich (mindestens jedoch zwei mal pro Woche) kontrolliert werden.

2. Interne und externe Benutzerprofile, allgemeine Sicherheitspolitik

Internet-Sicherheitspolitik stellt IT-Systemsicherheits-politik im Sinne des ITSiHb Teil 1 dar und muß daher

- die grundlegenden Vorgaben und Leitlinien zur Sicherheit bei der Kommunikation mit dem Internet definieren

- Details über die ausgewählten Dienste und Sicherheitsmaßnahmen (z.B. Firewall) beschreiben

- die Gründe für die Auswahl der Sicherheitsmaßnahmen darlegen

- mit der organisationsweiten IT-Sicherheitspolitik der Behörde kompatibel sein

Die Erstellung der Internet-Sicherheitspolitik umfaßt im wesentlichen folgende Schritte:

- Festlegung der Sicherheitsziele
z.B.
Schutz gegen Zugriffe von außen
Schutz der Einrichtung gegen Angriffe von außen
Schutz der Einrichtung gegen Manipulationen von innen
Schutz der gespeicherten Daten

- Auswahl der Kommunikationsanforderungen
z.B.
welche Kommunikationsanforderungen dürfen nach außen

welche Kommunikationsanforderungen dürfen nach außen bzw. innen durchgelassen werden
welcher Datendurchsatz ist zu erwarten
welche Zugänge werden benötigt

- Diensteauswahl
z.B.
alle Dienste, die nicht explizit zugelassen sind, werden verboten
welche Dienste werden für welche Benutzer / Rechner zugelassen
Dienste für interne bzw. externe Benutzer werden unterschieden

- organisatorische Regelungen
z.B.
Verantwortliche für die Erstellung, Umsetzung und Einhaltung der Kontrolle werden benannt
Festlegung der Protokollierung

Die Entscheidung darüber, zu welchen Diensten ein Bediensteter im Internet Zugang erhalten kann, hängt auch von seinem dienstlichen Aufgabenbereich, seinem Problembewußtsein und der Qualität der Firewall ab.

Bei der Erstellung eines Benutzerprofils für Bedienstete des Bundessind daher folgende Kriterien zu beachten:

* Der Benutzer benötigt Dienste zur Erfüllung und qualitätsmäßigen Verbesserung seiner dienstlichen Erledigungen (z. B. telnet, wenn regelmäßig in

Datenbanken recherchiert wird, Email, oder ähnliche Dienste).

* Dem Benutzer sollte Fortbildung auch mittels geeigneter Internet-Dienste ermöglicht werden (z.B. durch News).
* Jeder Benutzer sollte Zugang zu E-Mail erhalten (entspricht den E-Mail Empfehlungen der KIT).
* Jeder Internetdienst bzw. Dienst eines Fremdnetzwerkes birgt Gefahren, welche nicht auf technischer Ebene durch einen Firewall abgefangen werden können.

  Durch Schulung sind daher dem Benutzermögliche Risken aufzuzeigen bzw. ist sein Problembewußtsein dadurch zu fördern.
* Die Frage der Internetzugänge und der erlaubten Services sollte den jeweiligen dienstlichen Aufgaben angemessen gehandhabt werden.

  Umgehungsversuche und ihre Folgen führen in der Regel für den Dienstgeber zu erheblichen Risken und Kosten.
* Die organisatorisch und technisch reglementierenden Instanzen der betroffenen Installationen sowie deren Vertretungen müssen definiert werden.
* Firewalls können nur von Institutionen sinnvoll gemeinsam betrieben werden, wenn dieseüber eine gemeinsam getragene Sicherheitspolitik verfügen.
* Diese Sicherheitspolitik legt u.a. fest, auf Grund

Diese Sicherheitspolitik legt dar, auf Grund welcher Kriterien eine "trusted" / "untrusted" bzw. Freund / Feind"-Einstufung zu erfolgen hat. Für alle als "Feind" eingestuften Kommunikationspartner im Netz gelten die gleichen einzuhaltenden Sicherheitsziele.

Da die Einhaltung der Richtlinien für die Anbindung an Fremdnetzwerke bei der großen Zahl an Teilnehmern in einem behördenweiten Netz kaum zu überprüfen undauch nicht durchzusetzen ist, wird dringend empfohlen, zwischen verschiedenen Organisationen innerhalb der Verwaltung (wie etwa Bundesdienststellen, Ländern) ebenfalls über Sicherheitseinrichtungen zu kommunizieren.Die Auswirkung eventueller Sicherheitsmängel im Netzwerk wird so möglichst begrenzt.

* Es darf keine anderen Verbindungen aus dem -sicheren Bereich (sowohl hinaus als auch herein) als über die Sicherheitseinrichtung bzw. Firewall geben.

  Wählleitungsmodems stellen prinzipiell ein erhöhtes Sicherheitsrisiko dar; sie sind daher nur über

Firewalls oder äquivalente Sicherheitsmaßnahmen in das Netz einzubinden.

* Jede Sicherheitspolitik muß konzeptionell auf bestmögliche Reduktion des eventuellen Schadensfalles ausgelegt sein (Betrieb von Teilnetzen, Firerooms", großzügiger Einsatz von Routern).

  In diesem Zusammenhang ist auch der Raum, in welchem der Firewall betrieben wird, zusammen mit den Netzwerkeinrichtungen wie Routern einer besonderen Zugangskontrolle zu unterwerfen (siehe auch ITSiHb Teil 2, Kap 1).

* Es ist zu entscheiden, ob besonders sensible Daten auf Servern im Netzwerk besser bzw. kostengünstiger durch organisatorische als durch technische Maßnahmen geschützt werden können.

* Sicherheitspolitik muß Validierung (Überprüfung eines nicht nach dem Vier-Augen-Prinzip installierten Firewalls), Screening (periodische oder ad hoc-Überprüfung eines validierten Firewalls) und Revision (Überprüfung der Behebung der an einem Firewall festgestellten Mängel) zwingend beinhalten.

* Sicherheitspolitik muß sich permanent an Betriebserfahrungen des Firewalls sowie aktuellen Entwicklungen der Organisation, Hardware und Software sowie der Kenntnis neuer Angriffsmethoden orientieren.

Es ist absehbar, daß auch EDV-Anwender aus Fremdnetzwerken Zugriff auf Daten erhalten werden müssen, die im Intranet der Behörden liegen. Dies sollte in die Sicherheitspolitik bereits einfließen.

Der Zurverfügungstellung von Internet-Diensten bzw. Diensten von Fremdnetzwerken im Netzwerk sollte aufgrund des damit verbundenen Aufwandes der Wartung der Sicherheitseinrichtung eine entsprechende Kosten-/Nutzen Analyse vorausgehen. Bei dieser sollten auch Alternativen

zum Internet bzw. zur Netzwerkeinbindung wie etwa multicast berücksichtigt werden.

3. Vorgangsweise bei der Installation

Bei der Installation eines Firewalls sind daher folgende Schritte aus Kap. 2 in angegebener Reihenfolge zu setzen:

1. Festlegen der Sicherheitspolitik sowie der Benutzerordnung durch organisatorisch und technisch Verantwortliche in Zusammenarbeit mit Benutzervertretern, orientiert an den bestehenden Richtlinien der IT-Koordination
2. Bestimmung der technischen und der organisatorischen Sicherheitsverantwortlichen
3. Definition der angebotenen und anzufordernden Dienste auf Basis des Intranet-Konzeptes"
4. Analyse der Hard- und Softwarevoraussetzungen im internen Netz
5. Auswahl geeigneter Produkte
6. Installation und Konfiguration der Firewall - Installation. Der administrative Zugang zur Sicherheitseinrichtung darf nur über einen gesicherten Weg möglich sein
7. Überprüfung der Installation durch Querlesen der Definitionen und Funktionskontrolle
8. Dokumentation der Installation zum Zweck der Nachvollziehbarkeit, der Wartung und der Validierung
9. Laufende Beobachtung und Wartung
10. Periodische Sicherheitsüberprüfung durch befugte Externe zu nicht angekündigten Zeitpunkten mindestens einmal im Quartal (Screening") sowie Weitermeldung der erhobenen Fakten an die Vorgesetzten
11. Revision der Behebung der bei den Sicherheitstests erhobenen Mängel
12. Weitergabe von relevanten Projekterfahrungen an den Fachausschuß für Netzwerke der KIT. Ihr Zweck ist die Aktualisierung der gegenständlichen Richtlinien.
13. Aus- und Weiterbildung des administrierenden Personals.

Alle Schritte außer 12 und 13 sind unter Anwendung des

Alle Schritte außer 12 und 13 sind unter Anwendung des Vier-Augen-Prinzips durchzuführen.

Dies bedeutet, daß für Spezifikation und Überprüfung der Installation andere als die für die eigentliche Konfiguration des Firewall-Rechners eingesetzten Personen heranzuziehen sind. Interessensverflechtungen beider Gruppen sind durch geeignete Maßnahmen zu vermeiden.

Bei der Aufgabenteilung ist folgende Vorgangsweise einzuhalten:

Schritte 1 bis 5, 7 und 8 werden durch die Firewall-Administration und Vertreter der Benutzer in Zusammenarbeit mit**einer** Gruppe durchgeführt, während Schritt 6 durch**eine andere** Gruppe abgewickelt wird, die auch bei Punkt 8 assistiert.

Dadurch soll gewährleistet werden, daß die konfigurierende Gruppe Unklarheiten in der vorher erstellten Analyse und Spezifikation erkennen kann, während die analysierende Gruppe Fehler in der Konfiguration aufdecken sollte.

Punkt 9 wird durch die Firewall-Administration abgedeckt.

Punkt 10 und 11 werden durch eine näher zu bestimmende Sicherheitsinstanz abgedeckt (Screening"). Die entstehenden Kosten sind als Betriebskosten der Firewall-Installation durch dessen Betreiber zu tragen.

AlsBeispiel für eine bereits eingeführte Benutzerverordnung mit Internet-Bezug (welche im Detail dem jeweiligen Umfeld anzupassen sein wird) liegt diesen Richtlinien die Benutzerordnung des **UNET** der Universität Wien bei.

Ein weiteres Beispiel - das Konzept der ÖSTAT-internen Benutzerrichtlinien - findet sich unter 'Begleitende Maßnahmen' im Erfahrungsbericht zur Firewall-Installation des **ÖSTAT** .

4. Wichtige Kriterien für Pflichtenheft und Leistungsbeschreibung

Bei der Erstellung eines Pflichtenhefts für Firewalls sind zumindest folgende Punkte zu berücksichtigen:

* Welche Informationsflüsse sind zu erwarten?

* Welche Internet-Dienste werden von wie vielen Benutzern wie oft benötigt bzw. von außen in Anspruch genommen (Diensteprofil, Ports)?
* Wie sensibel sind die Daten im zu schützenden Netz? (Erstellung eines Risikokatalogs)
* Wie sind interaktive Zugänge von außen abzusichern, falls solche erforderlich sind?
* Welche Dienste werden nach außen angeboten´?
* Welche Hard- und Software wird intern verwendet?
* Wird Verschlüsselung bzw. Authetizierung im Verkehr zu anderen Internet- bzw. Fremdnetzteilnehmern benötigt?
* Wie und von wem wird der Firewall gewartet?
* Welche Art von IP-Adressen wird intern verwendet?
* Muß man sich gegen interne Angriffe schützen? Im Normalfall: ja!
* Welche Logs und welches Accounting werden benötigt?
* Wie wird der Administrator der Sicherheits-einrichtung alarmiert?
* Wie sieht die Entscheidungskette Firewall-Administrator -> Führungsebene aus? Ist sie durchgängig? Wurden Vertretungen bestellt?
* Auf Grund welcher Abnahmekriterien wird abgenommen?

5. Sicherer Betrieb - laufende Wartung

Nach der Installation einer Sicherheitseinrichtung ist es erforderlich, daß diese fachgemäß administriert wird.

Dabei sind die im folgenden dargestellten Punkte organisatorisch, technisch und budgetär zu berücksichtigen.

Es bedarf mindestens zweier Personen, welche die angeführten Aufgaben erfüllen und zu deren Durchführung berechtigt sind:

* Anlegen und Entfernen von Benutzern, Profilen, Filtern etc.
* Ändern von Berechtigungen, Funktionen etc. (siehe auch ITSiHb Kap. 2.1, PER 1.2 bis PER 1.5)

* Kontrolle und Analyse der Logfiles
* Einschränken und Beenden des Internetzugangs
* Weiterleitung sicherheitsrelevanter Beobachtungen an die in der Sicherheitspolitik definierten Instanzen
* Benachrichtigung der zuständigen Instanzen bei

Benachrichtigung der zuständigen Instanzen bei Entdeckung von Angriffen aus dem Internet

* Verfolgen der aktuellen Entwicklungen im Bereich Sicherheit (z.B. durch Lesen der entsprechenden Newsgroups) sowie entsprechende Weiterbildung

Für die qualitativ ausreichende Betreuung einer Firewall-Installation ist mit einem Aufwand von mindestens zwei bis drei Personenstunden pro Tag zu rechnen.

Die getroffenen organisatorischen Regelungen sind regelmäßig auf ihre Einhaltung zu überprüfen.

6. Regelmäßige technische Überprüfung (Screening, Audit)

Zusätzlich zu den regelmäßigen Wartungsaktivitäten ist es erforderlich, einen bereits validierten Firewall mindestens einmal pro Quartal durch eine geeignete Instanz kontrollieren zu lassen.

Zusätzlich erfordern sicherheitsrelevante Änderungen unbedingt "ad hoc" Kontrollmaßnahmen auf evtl. unbekannte Seiteneffekte.

Die "geeignete Instanz" ist nach strengen Qualitäts-anforderungen auszuwählen. Sie muß den Vorgang der Überprüfung schriftlich protokollieren und sich zu **Verschwiegenheit und Schutz der erhobenen Daten** verpflichten.
Eine derartige Überprüfung ist wie folgt innerhalb eines eng begrenzten Zeitraumes (z.B. einer Woche) durchzuführen:

* Studium des Ausgangsmaterials inkl. Begehungen, Interviews, Messungen, Auswertungen der Logdateien
* Interne Überprüfung der Sicherheitspolitik
* Interne Überprüfung der Konfiguration
* Überprüfung der für ein Neuaufsetzen der Einrichtung notwendigen gesicherten Datenbestände (z.B. Access-Listen)auf Aktualität und Schutz gegen Verfälschung

* Integritätstests der eingesetzten Software inkl. OS
* Überprüfung der Installation von außen
* Überprüfung des Verhaltens der Sicherheitseinrichtung bei Totalausfall bzw. Systemabsturz und Analyse der sicherheitsrelevanten Folgen* Durchführung eventuell nötiger Korrekturen
* Erneute Überprüfung von außen (Revision der Korrekturen")

Periodische externe Kontrolle ist notwendig, da die Gefahr besteht, daß Firewall-Administratoren durch Gewöhnungseffekt" und Routinearbeit bestimmte Sicherheitslücken übersehen, welche externen Beobachtern mit hoher Wahrscheinlichkeit auffallen (Vier-Augen-

Prinzip").

7. Konsequenzen für den Betreiber eines Firewalls bei deutlicher Erhöhung der Benutzerzahl

Ist eine Firewall-Installation über die ursprünglich festgelegte Dimensionierung hinaus zu erweitern, sind folgende Fragen zu beantworten:

* Muß die Sicherheitspolitik angepaßt werden?
* Ist die Hardware ausreichend leistungsfähig, um den zusätzlich entstehenden Verkehr zu bewältigen?
* Ist die Software in der Lage, die neuen Anforderungen abzudecken?
* Hat die Firewall-Administration genügend Resourcen für den steigenden Wartungsaufwand?
* Kann die Firewall-Administration neu hinzukommende Benutzer risikolos abdecken?

  Können Sicherheitsverletzungen nach wie vor ausreichend abgewehrt werden, und ist die Informationsweitergabe gesichert, wenn Benutzer wieder gelöscht werden sollen?
* Die Schulung der neuen Benutzer ist rechtzeitig vorzunehmen

---

8. Distribuierte versus zentralisierte Installation

Einer der wichtigsten Punkte bei der Konzeption eines Firewalls ist es, diesen und den Bereich, welcher geschützt wird, möglichst überschaubar zu halten, um Schäden einer eventuellen Sicherheitsverletzung eng zu begrenzen.

Es gilt das Konzept des "Bauens von Burgen", Firerooms" (großzügiger Routereinsatz, Stockwerk-Netzsegmente etc.).

Aus Sicherheitsgründen ist daher zu empfehlen, eher mehrere klein dimensionierte (ev. verteilte) Sicherheitseinrichtungen als eine sehr groß dimensionierte Installation einzurichten.

Die hinter den jeweiligen Sicherheitseinrichtungen liegenden Netze sind in dieser Variante besonders deutlich und sicher voneinander zu trennen, da eine mangelhaft betriebene oder ausgestattete Sicherheitseinrichtung sonst den Zugang in die anderen separierten Netze eröffnen könnte.

9. Weitergabe von Dokumentation

Jegliche Dokumentation von Firewall-Installationen wird vor ihrer Weitergabe an andere (Fachausschuß Netzwerke der KIT, Ressorts, Firmen etc.) vom jeweiligen ernannten Sicherheitsverantwortlichen in ihrem Umfang und Inhalt auf das für die betroffene Installation verträgliche Sicherheitsrisiko eingeschränkt.

Der Austausch von Projekterfahrungen in dieser Materie auf mündlicher Ebene zwischen verantwortlichen Personen ist der Weitergabe von schriftlicher Dokumentation unbedingt vorzuziehen.

Von einer Übermittlung der Firewall-Dokumentationen und verwandtem Material der öffentlichen Verwaltung über öffentliche Netze (z.B. mittels E-Mail oder Fax) ist unbedingt abzusehen.
Öffentliche Netze" sind dabei nach hier erforderlicher strenger Definition jene Netze, die nicht im secure Bereich" einer Institution liegen.

13

Page 14

Literaturhinweise:

ITSiHb, IT-Sicherheitshandbuch für die öffentliche Verwaltung, www.it-koo.bmols.gv.at

14

Page 15

15