Anhang 3
(Ziff. 4.1)

Domänenpolicy blau

1 Grundlagen

[1] Die Domänenpolicy blau legt die Sicherheitsanforderungen und -vorgaben an die blaue Domäne fest.

[2] Grundlagen für die "Domänenpolicy blau" sind die Sicherheitsvorgaben nach Anhang 2 der WIsB.

2 Zuständigkeiten

[1] Der Informatikrat des Bundes ist Inhaber der blauen Domäne. Er nimmt die Pflege des Domäneninhalts bzw. die Delegation dieser Aufgabe im Rahmen von IRB- oder A-IS-Beschlüssen vor.

[2] Das Informatikstrategieorgan des Bundes (ISB**)** ist im Rahmen seiner Aufgaben für den Ausschuss Informatiksicherheit (A-IS) zuständig für:

a) vorbereitende und begleitende Arbeiten zu den in dieser Policy genannten Anträgen von Organisationseinheiten;
b) begleitende Aufgaben nach der Erteilung von Bewilligungen, beispielsweise das Vorlegen bestehender Bewilligungen zur erneuten Beurteilung durch den A-IS bei relevanten Änderungen von Rahmenbedingungen;
c) die Verwaltung des Domäneninhalts der blauen Domäne, beispielsweise das Führen der Liste aller blauen Netze und aller Firewalls im Rahmen dieser Domäne.

3 Domänenpolicy

3.1 Domänenbezogene Massnahmen

Ein System gilt als blau-kompatibel, wenn eine der beiden folgenden Bedingungen erfüllt ist:

a) Das System erfüllt die in diesen Weisungen festgelegten minimalen Sicherheitsanforderungen an die blaue Domäne.
b) Das System wurde gemäss diesen Weisungen einer Schutzbedarfsanalyse unterzogen, die entsprechenden Massnahmen wurden umgesetzt und die Systemverantwortung ist klar geregelt.

3.2 Firewallbedingungen

[1] Authentifikationen, die durch eine Firewall vorgenommen werden, unterteilen sich in Personen- und Prozessauthentifikationen.

[2] Eine Personenauthentifikation muss die folgenden Bedingungen erfüllen:

a) Auf dem anrufenden System besteht eine Echtzeit-Interaktion zwischen dem anrufenden Prozess (Client-Applikation) und einer berechtigten Person.
b) Diese Echtzeit-Interaktion muss während der gesamten Lebensdauer der Kommunikation bestehen bleiben.
c) Die benutzten Credentials (Zertifikate, Benutzername/Passwort etc.) sind dieser Person zugeordnet.
d) Die Authentifikation wird bei der authentifizierenden Firewall als Personenauthentifikation erkannt.

[3] Eine Prozessauthentifikation muss die folgenden Bedingungen erfüllen:

a) Auf dem anrufenden System authentifiziert sich direkt ein Prozess, es ist keine Person involviert.
b) Die authentifizierte Kommunikation wird durch die Firewall spätestens nach einer definierten Lebensdauer beendet.
c) Die benutzten Credentials (Zertifikate, Hostname/Passwort etc.) sind diesem Prozess bzw. dem anrufenden System zugeordnet.
d) Die Authentifikation wird bei der authentifizierenden Firewall als Prozessauthentifikation erkannt.
e) Die Prozessauthentifikation darf keine Personenauthentifikation ersetzen; sie ist für den Batch-Betrieb reserviert.

[4] Bestimmte Credentials dürfen jeweils nur für Prozess- oder für Personenauthentifikationen, nie jedoch für beide eingesetzt werden.

[5] Firewallübergreifende Kommunikationen, bei denen das anrufende System in einem Fremdnetz und mindestens ein angerufenes System in einem blauen Netz liegt, müssen folgende Bedingungen erfüllen:

a) Die Kommunikation durchläuft eingangs auf der Firewall eine Personen- bzw. eine durch den A-IS bewilligte Prozessauthentifikation.
b) Die zugreifende Person bzw. der zugreifende Prozess ist dem Firewallbetreiber bekannt und wurde von ihm autorisiert, auf die in der blauen Domäne liegenden angerufenen Systeme zuzugreifen.

[6] Die Firewall muss sicherstellen, dass die Authentifikation mindestens folgende Vorgaben nach Anhang 2 Ziffer 5.3, Abs. 4 erfüllt:

a) starke Authentifikation;
b) Verbindungs- oder Kryptokontext.

[7] Personenauthentifikationen sind die Regel. Eine Prozessauthentifikation ist nur zugelassen, falls der A-IS sie bewilligt hat. Die Bewilligung erfolgt auf Antrag des oder der Anwendungsverantwortlichen der in der blauen Domäne liegenden Anwendung, auf die zugegriffen werden soll. Ein solcher Antrag muss mindestens die folgenden Informationen beinhalten:

a) die Domäne, aus der zugegriffen werden soll (i.d.R. die rote Domäne);
b) die Anwendung, auf die zugegriffen werden soll, und deren Systeme;
c) die Authentifikationsmethode;
d) die maximale Lebensdauer der Kommunikationen, nach deren Überschreitung die Firewall die Kommunikation unterbricht.

[8] Nach Erteilung der Bewilligung müssen Änderungen der im Antrag angegebenen Elemente dem A-IS gemeldet werden. Der A-IS kann eine einmal erteilte Bewilligung wieder aufheben.

3.3 Bilaterale Vereinbarungen

[1] Bilaterale Vereinbarungen mit Partnerdomänen sind von dem oder der Informatiksicherheitsbeauftragten des Departements beziehungsweise der Bundeskanzlei dem A-IS zur Genehmigung vorzulegen (mit Eskalationsmöglichkeit beim IRB).

[2] Folgende Minimalvorgaben sollten enthalten sein:

a) Die Firewallbedingungen in der Domänenpolicy der Partnerdomäne müssen für deren Netzwerkübergänge in analoger Weise mindestens gleich restriktiv sein wie die Firewallbedingungen der blauen Domänenpolicy.
b) Die Partnerdomäne darf keine bilaterale Vereinbarung mit einer nicht-blauen Domäne abschliessen.
c) Die Partnerdomäne darf Subdomänen bilden. Die blaue Domäne muss jedoch vorab darüber informiert werden, und alle Policies sind offen zu legen. Der blauen Domäne steht es insbesondere zu, bei Meinungsverschiedenheiten über Subdomänen die bilaterale Vereinbarung neu zu verhandeln oder zu kündigen.

[3] Es wird speziell auf folgende Punkte hingewiesen:

a) Im Einzelfall entscheidet der A-IS beziehungsweise der IRB, ob eine bilaterale Vereinbarung abgeschlossen wird oder nicht. Es besteht kein Automatismus. In begründeten Fällen kann er die oben empfohlenen Elemente durch gleichwertige ersetzen, etwa im Fall von Management-Domänen eines Betreibers blauer Netze.
b) Der A-IS beziehungsweise der IRB kann eine bilaterale Vereinbarung unter den dort definierten Rahmenbedingungen neu verhandeln oder kündigen. Dies gilt natürlich auch für die Gegenseite.
c) Bilaterale Vereinbarungen machen Firewalls zwischen den Partnern nicht überflüssig. Sie definieren lediglich (individuell) erleichterte Netzübergänge und ermöglichen damit weniger restriktive Firewalls. Netze der beiden Domänen dürfen aber in der Regel trotzdem nicht direkt verbunden werden.

3.4 Subdomänen

Die blaue Domäne unterstützt keine Subdomänen.

4 Firewallbetrieb

4.1 Bewilligung zum Betrieb einer Firewall

[1] Eine Firewall zum Schutz blauer Netze gegenüber Fremdnetzen muss die folgenden Bedingungen erfüllen:

a) Die Firewall wird entweder durch die beantragende Organisationseinheit direkt oder durch einen Dritten im Auftrag der beantragenden Organisationseinheit betrieben.
b) Der A-IS hat dieser Organisationseinheit den Betrieb der Firewall zum Schutz blauer Netze gegenüber Fremdnetzen bewilligt.

[2] Eine Bewilligung läuft nach folgendem Schema ab:

a) [Optionaler Schritt:] Die Organisationseinheit hat die Möglichkeit, dem A-IS eine konsultative Anfrage zum Betrieb einer Firewall zu stellen. Die Anfrage legt die

Bedürfnisse der Organisationseinheit dar und ist von einer Stellungnahme der oder des Informatiksicherheitsbeauftragten der für die Anfrage zuständigen Departemente begleitet.

b) [Nur falls Schritt a erfolgte:] Können die Bedürfnisse nicht durch eine bereits existierende Firewall einfacher erfüllt werden, befindet der A-IS über die Anfrage und erteilt der Organisationseinheit im positiven Fall die Empfehlung, eine detaillierte Systembeschreibung der Firewall auszuarbeiten und dem A-IS zur Bewilligung vorzulegen. Der A-IS kann dafür eine Frist setzen. In diesem Fall muss er die Konsequenzen einer Fristüberschreitung und das Vorgehen für eine mögliche Fristverlängerung definieren.

c) Die Organisationseinheit erarbeitet eine detaillierte Systembeschreibung der Firewall und legt diese dem A-IS als Antrag zum Betrieb der Firewall vor. Die Vorlage erfolgt durch die Informatiksicherheitsbeauftragten der zuständigen Departemente, welche eine erste grobe Beurteilung über die Zweckmässigkeit abzugeben haben. Der Antrag kann durch den A-IS nur dann verweigert werden, wenn eine der folgenden Bedingungen zutrifft:
    1. Der A-IS wurde vorgängig nicht konsultiert, das heisst, die Schritte a und b fanden nicht statt.
    2. Der A-IS lehnte es in Schritt b ab, eine Empfehlung auszusprechen.
    3. Die Terminvereinbarungen wurden verletzt.
    4. Die Rahmenbedingungen haben sich grundlegend geändert.
    5. Die Systembeschreibung ist unvollständig oder unklar.
    6. Der A-IS akzeptiert die für das Audit vorgesehene Stelle nicht.

[4] Die konsultative Anfrage zum Betrieb einer Firewall umfasst mindestens folgende Punkte:

a) detaillierte Darlegung des Bedürfnisses und Untersuchung alternativer Szenarien mit entsprechenden Kostenabschätzungen und Risikobeurteilungen durch den Antragsteller;

b) konzeptionelle Beschreibung, wie die Firewallbedingungen der Domänenpolicy technisch umgesetzt werden;

c) alle zu diesem Zeitpunkt absehbaren Firewallbedingungen, die der Domänenpolicy voraussichtlich nicht genügen. Werden solche Firewallbedingungen erst im Antrag bekannt gegeben, kann die Bewilligung verweigert werden;

d) effektiver Betreiber und Rahmenbedingungen der existierenden oder geplanten Vereinbarungen mit ihm, falls der Betrieb nicht direkt durch den Antragsteller erfolgen soll. Wird ein Betrieb durch Dritte erst im Antrag bekannt gegeben, kann die Bewilligung verweigert werden.

[5] Die Systembeschreibung der Firewall umfasst mindestens folgende Punkte:

a) Nachweis, dass das Firewallsystem als solches gemäss diesen Weisungen einer Schutzbedarfsanalyse unterzogen wurde und dass die relevanten Massnahmen umgesetzt sind;

b) Firewallpolicy;

c) Betriebskonzept;

d) Angaben über einen Betrieb durch Dritte, falls ein solcher vorgesehen ist;

e) detaillierte Darlegung des Bedürfnisses und Untersuchung alternativer Szenarien mit entsprechenden Kostenabschätzungen und Risikobeurteilungen durch den Antragsteller, sofern dies nicht bereits im Rahmen einer konsultativen Anfrage erfolgte;

f) Angabe einer unabhängigen Stelle, welche spätestens 6 Monate nach Inbetriebnahme der Firewall ein Auditing vornimmt.

[6] Die Firewallpolicy umfasst mindestens folgende Punkte:

a) Beschreibung, wie die zu authentifizierenden Objekte ihre Authentifikations-Credentials (meistens Zertifikate) bekommen, etwa durch Verweis auf akzeptierte PKIs;
b) Beschreibung, wie die Firewallbetreiber die Autorisierungs-Informationen über zu autorisierende Objekte bekommen, z.B. durch Auftrag vom Inhaber von Datensammlungen;
c) Beschreibung aller Firewallbedingungen, die über die Domänenpolicy hinausgehen;
d) Beschreibung aller Firewallbedingungen der Domänenpolicy, welche nicht umgesetzt werden;
e) Beschreibung aller Firewallbedingungen, die von denjenigen der Domänenpolicy abweichen;
f) Angaben über Kooperationsvereinbarungen mit anderen Firewalls, die blaue Netze schützen;
g) Liste aller genutzten Transitnetze anderer Domänen mit Referenz auf eventuelle Transitabkommen;
h) Liste aller blauen Transitnetze, die in Zusammenarbeit mit der Firewall Fremdnetzen Transitdienste zur Verfügung stellen.

[7] Firewallbedingungen, welche der Domänenpolicy nicht genügen, dürfen nur in begründeten Ausnahmefällen aufgenommen werden. Wenn sie nicht bereits in der konsultativen Anfrage bekannt gegeben wurden, sind sie im Antrag zu deklarieren. Sie können zur Verweigerung der Bewilligung führen.

[8] Das Betriebskonzept einer Firewall umfasst mindestens folgende Punkte:

a) Organisation und Verantwortlichkeiten des Firewallbetriebs;
b) Angaben über die Verfügbarkeit und Safety-Massnahmen;
c) technische Verfahren zur Umsetzung aller Punkte der Firewallpolicy;
d) Angaben zur Umsetzung der Anforderungen, welche aus der Schutzbedarfsanalyse der Firewall gemäss diesen Weisungen hervorgehen.

[9] Neu bewilligte Firewalls müssen spätestens 6 Monate nach Inbetriebnahme einem Audit durch eine unabhängige Stelle unterzogen werden. Der Antragsteller der Firewall gibt diese Stelle in der bewilligungspflichtigen Systembeschreibung bekannt.

[10] Mit der Durchführung dieses Audits dürfen ausschliesslich Personen beauftragt werden, welche durch die Fachstelle für Personensicherheitsprüfungen mit positivem Resultat (kein Risiko) geprüft worden sind. Für die Einleitung der Personensicherheitsprüfung ist die Stelle verantwortlich, welche das Audit vornehmen soll.

[11] Das Resultat des Audits wird dem A-IS in Form eines Management-Summary bekannt gegeben.

4.2 Änderungen im Firewallbetrieb nach erfolgter definitiver Bewilligung

[1] Der laufende Unterhalt der Firewallsysteme, wie z.B. Benutzerverwaltung, Aufspielen von Systempatches und Upgrades, Einführung redundanter Systeme, Hardware-Ausbau und

Hardware-Ersatz durch äquivalente Komponenten etc., liegt im Ermessen des Firewallbetreibers und bedarf keiner weiteren Interaktion.

[2] Dem A-IS sind auf dessen Verlangen die jeweils aktuelle Konfiguration und Informationen über geplante Unterhaltsaktionen vorzulegen.

[3] Alle darüber hinausgehenden Änderungen, insbesondere Änderungen der Policy und des Betriebskonzeptes, sind dem A-IS zur Information vorzulegen. Dieser hat ein Einspracherecht.

4.3 Laufende Pflichten der Firewallbetreiber

[1] Der Firewallbetreiber muss den Benutzern seiner Kundennetze Änderungen seiner Firewallpolicy rechtzeitig und auf angemessene Weise mitteilen; das gilt insbesondere, wenn die Policy restriktiver wird.

[2] Der Firewallbetreiber muss die Firewallsysteme sowohl hardware- als auch softwareseitig härten und auf dem aktuellen technischen Stand halten.

[3] Firewalls müssen mindestens alle 3 Jahre einem Audit unterzogen werden. Der Firewallbetreiber hat mindestens ein halbes Jahr vor dem geplanten Termin den A-IS darüber zu informieren, welche Stelle er damit beauftragen will. Der A-IS hat ein Einspracherecht.

[4] Mit der Durchführung dieses Audits dürfen ausschliesslich Personen beauftragt werden, welche durch die Fachstelle für Personensicherheitsprüfungen mit positivem Resultat (kein Risiko) geprüft worden sind. Für die Einleitung der Personensicherheitsprüfung ist die Stelle verantwortlich, welche das Audit vornehmen soll.

[5] Das Resultat des Audits wird dem A-IS in Form eines Management-Summary bekannt gegeben.

4.4 Ausnahmebewilligungen

[1] Der Firewallbetreiber hat die sich aus der Domänenpolicy ergebenden Firewallbedingungen im Rahmen des technisch Machbaren in eigenem Ermessen und in eigener Verantwortlichkeit umzusetzen. Gegebenenfalls kann er beim ISB in Sicherheitsfragen Unterstützung einholen.

[2] Falls der Firewallbetreiber mit Projekten von Organisationseinheiten konfrontiert ist, für welche er keine adäquaten, der Domänenpolicy entsprechenden Massnahmen findet, gelten analog die Regelungen nach Ziffer 4.2 dieses Anhangs.

4.5 Kooperationsvereinbarungen

[1] Firewalls, die blaue Netze schützen, können im Rahmen einer Kooperation betrieben werden. Diese muss in allen Firewallpolicies und Betriebskonzepten aufgeführt und im Rahmen der jeweiligen Firewallbewilligungen durch den A-IS akzeptiert worden sein.

[2] Zusätzliche Kooperationen während der Laufzeit werden als Policy-Änderung gemäss Ziffer 4.2 behandelt. Es spielt dabei keine Rolle, ob die Firewalls durch dieselbe Organisationseinheit betrieben werden oder nicht.

4.6 Transitabkommen

[1] Transitabkommen mit Fremdnetzen oder die Nutzung roter Netze als Transitnetze zur Verbindung geografisch getrennter blauer Netze ist den Firewallbetreibern erlaubt, sofern der

kryptografische Schutz der übertragenen Daten entsprechend ihrer Schutzstufe mittels VPN-Technologie sichergestellt wird. Die Nutzung solcher Transitdienste ist Gegenstand der Firewallpolicy. Kommen Transitdienste im Laufe des Firewallbetriebs hinzu, so werden sie wie Policy-Änderungen gemäss Ziffer 4.2 dieses Anhangs behandelt.

[2] Betreiber blauer Netze dürfen in Zusammenarbeit mit den Firewallbetreibern, die ihre Netze schützen, Fremdnetzen gegenüber Transitdienste anbieten. Dabei müssen alle beteiligten Firewallbetreiber in ihren Firewallpolicies sicherstellen, dass keines der Peer-Systeme der Kommunikation in einem blauen Netz liegt.

Stand 1. November 2007