ConSecur
GmbH

IT-Sicherheitsmanagement

Einführung von Intrusion-Detection-Systemen

Leitfaden für die Einführung

31. Oktober 2002

Version 1.0

Inhaltsverzeichnis

1 Zusammenfassung

Die Internet-Interaktion mit internen Systemen (z. B. im Rahmen von eCommerce- und eBusiness-Anwendungen) führt zu einer Zunahme von Risiken und Missbrauchsmöglichkeiten.

Bei der Kopplung interner Netze an das Internet oder an andere Fremdnetze hat sich die Absicherung des Netzübergangs durch Firewall-Systeme etabliert. Anforderungen, resultierend aus dem steigenden Kommunikationsbedarf neuer Anwendungen sowie interaktiver Internet-Anwendungen in den Bereichen eCommerce und eBusiness, führen dazu, dass interne Serversysteme und Datenbanken immer mehr in die Interaktion mit einbezogen werden. Diese Systeme stellen häufig einen hohen Wert für das Unternehmen dar und weisen einen entsprechend hohen Schutzbedarf auf. Die Internet-Interaktion mit diesen Systemen bedingt dabei eine Erhöhung der Risiken und Missbrauchsmöglichkeiten insbesondere gegenüber Angriffen, die aus dem Internet initiiert werden. Zudem wird durch die erhöhte Funktionalität von Internet-Angeboten und deren Kopplung mit internen Systemen auch deren Attraktivität als Angriffsziel erhöht. Dies ist unter anderem daran erkennbar, dass täglich neue Angriffe bekannt werden, die Sicherheitslücken in Systemen und Anwendungen ausnutzen.

Der Schutz durch Firewall-Systeme ist als alleinige Maßnahme in vielen Fällen nicht mehr ausreichend.

Technisch erfordert die Interaktion mit internen Systemen eine erweiterte Öffnung bestehender Firewall-Systeme nach innen. Daneben kann auch die Dienstkonformität des Datenflusses durch Firewall-Systeme aufgrund verschlüsselter oder getunnelter Kommunikation häufig nicht hinreichend sichergestellt werden. Ihre Schutzwirkung wird dadurch verringert und ist in vielen Fällen als alleinige Maßnahme nicht mehr ausreichend.

Intrustion-Detection-Systeme können Angriffe und Sicherheitsverletzungen zeitnah erkennen. Auf dieser Basis können Verfügbarkeit und Integrität von Systemen und Diensten erhöht werden.

Intrusion-Detection-Systeme (kurz IDS) können dazu dienen, die aus den erhöhten Kommunikationsanforderungen und der verringerten Schutzwirkung der Firewall-Systeme resultierenden, zusätzlichen Risiken wieder zu vermindern. IDS erlauben die Überwachung des Netzverkehrs, der Systeme und Anwendungen auf Angriffe und Sicherheitsverletzungen. Die zeitnahe Erkennung von Angriffen, angriffsvorbereitenden Aktivitäten und Sicherheitsverletzungen bildet dabei die Voraussetzung dafür, Schäden zu verhindern, zu begrenzen oder zumindest zeitnah zu beheben. Hierdurch lassen sich die Verfügbarkeit und Integrität von Systemen, Anwendungen und auf diesen basierender Dienste erhöhen. Dies setzt jedoch voraus, dass die Auswirkungen erkannter Angriffe zeitnah untersucht werden und auf diese angemessen reagiert wird. IDS können zwar grundsätzlich auch automatisch Gegenmaßnahmen einleiten, in den meisten Fällen kann auf eine manuelle Prüfung der Auswirkungen des Angriffs aber nicht verzichtet werden. Dies liegt darin begründet, dass IDS einerseits nicht frei von Fehlalarmen sind und andererseits die Auswirkungen des Angriffs nur begrenzt durch das IDS erfasst werden können. Über die eigentliche Erkennung und Meldung von Angriffen hinaus bieten IDS Funktionen zur Auswertung aufgezeichneter Ereignisse. Diese können zur Visualisierung der Angriffslast, zur Ermittlung von Angriffskontexten und ggf. zur Rückverfolgung von Angreifern dienen. In vielen Fällen ermöglicht das Erkennen von Verhaltensweisen, die erst durch den IDS-Einsatzes sichtbar werden, auch die Verbesserung von Systemkonfigurationen.

Der vorliegende Leitfaden dient als Hilfsmittel bei der Einführung von Intrusion-Detection-Systemen.

Aufgrund der zunehmenden Integration des Internets in Geschäftsprozesse und den damit gestiegenen Kommunikationsanforderungen hat sich der Einsatz von IDS in den letzten Jahren verbreitet und mit ihm das Angebot an marktverfügbaren IDS. Inzwischen gibt es eine Vielzahl entsprechender Produkte, die - wenn auch in unterschiedlichem Maße - Marktreife erlangt haben. Es besteht nunmehr konkreter Unterstützungsbedarf bei der Einführung von IDS. Diesem wird durch den vorliegenden Leitfaden Rechnung getragen, der speziell die Einführung von IDS zur ergänzenden Absicherung von Netzübergängen zum Internet unterstützt. Ein Großteil der bereitgestellten Hilfsmittel und Vorgehensweisen ist jedoch direkt auf andere Einsatzweisen von IDS übertragbar.

Der Leitfaden unterstützt sowohl die Klärung, ob ein IDS-Einsatz in der vorliegenden Situation sinnvoll ist, als auch den Prozess der IDS-Einführung.

Der Leitfaden richtet sich an Mitarbeiter im Unternehmen bzw. der Organisation, die für die IT-Sicherheit des Netzübergangs zum Internet verantwortlich sind. Er unterstützt zunächst bei der Klärung, ob ein IDS-Einsatz unter den gegebenen Randbedingungen sinnvoll ist oder nicht. Bei der Entscheidung für einen IDS-Einsatz wird der Anwender zu den einzelnen Einführungsschritten angeleitet. Grundlagenkenntnisse zu IDS und zu berücksichtigende rechtliche Aspekte beim Einsatz von IDS werden in separaten, zum Leitfaden gehörigen Dokumenten bereitgestellt.

Der Leitfaden berücksichtigt sämtliche Phasen der IDS-Einführung und des IDS-Einsatzes, von der Konzeption über die Integration bis zum Betrieb und der Revision von IDS.

Diese Phasen werden in Kapitel 2 im Überblick erläutert und sind nachfolgend im Zusammenhang aufgezählt.

In der Phase *Bedarfsfeststellung* wird zunächst ermittelt, ob der Einsatz eines IDS unter den gegebenen Randbedingungen sinnvoll ist und welchen Zielsetzungen er dienen soll. Falls der Einsatz eines IDS als sinnvoll erachtet wird, wird in der Phase *Grobkonzept und Anforderungsanalyse* untersucht, in welcher Weise ein IDS in die bestehende IT-Infrastruktur zu integrieren ist und welche Anforderungen es erfüllen muss, um die Zielsetzungen zu erreichen. Anschließend wird im Rahmen der Erstellung einer *Entscheidungsvorlage* die Machbarkeit des Ansatzes geprüft und es erfolgt eine Abschätzung entstehender Kosten und Aufwände. Falls auf dieser Basis die grundsätzliche Entscheidung für einen IDS Einsatz getroffen wird, schließen sich die *Feinkonzeption* des IDS-Einsatzes und die *Produktauswahl* an. Aufbauend darauf erfolgt die *Integration* des IDS. Diese umfasst sowohl technische Aspekte, wie die Inbetriebnahme des IDS und dessen Kalibrierung, als auch organisatorische Aspekte, wie insbesondere die Integration des IDS in das Incident-Handling. Auch sind im Rahmen der Integration bereits sämtliche Aspekte des nachfolgenden *Betriebs* des IDS zu klären. Der Leitfaden schließt mit der Phase *Revision* ab, in der Vorgehensweisen für die Revision von IDS erläutert werden.

Vorgehensweisen für die einzelnen Phasen werden erläutert und es werden unterstützende Hilfsmittel bereitgestellt.

Jeder der Phasen ist in Kapitel 3 ein dedizierter Abschnitt zugeordnet, in dem Arbeitsschritte und Inhalte der Phase detailliert beschrieben werden. Die Phasen werden durch Hilfsmittel (wie etwa Kriterienlisten oder Anwendungsbeispiele) ergänzt, welche die Durchführung der Arbeitsschritte unterstützen. Diese sind im Anhang (Kapitel 4) aufgeführt.

2 Übersicht über die Phasen der IDS-Einführung

Die einzelnen Phasen der Einführung eines IDS sind im nachstehenden Phasenplan dargestellt:

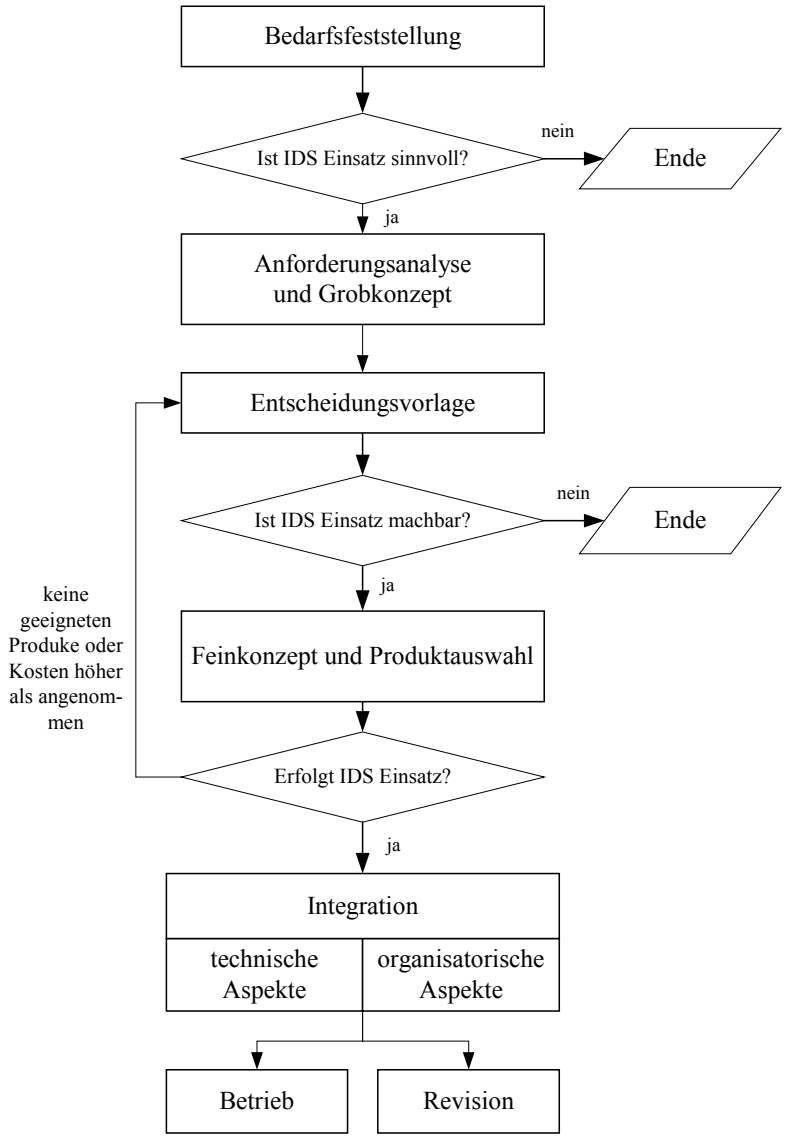

Abbildung 2-1: Phasenplan IDS-Einführung

Die Phasen werden nachstehend kurz erläutert:

1. **Bedarfsfeststellung**

   Im Rahmen der Bedarfsfeststellung wird geklärt, in wie weit der Einsatz von IDS zur ergänzenden Absicherung des Netzübergangs zum Internet grundsätzlich sinnvoll ist. Nutzenaspekte – insbesondere der sicherheitstechnische Zusatznutzen – werden analysiert und mit einem IDS-Einsatz verbundene Zielsetzungen werden ermittelt. Eine Analyse der Kosten erfolgt später bei der Erstellung der Entscheidungsvorlage.

2. Grobkonzept und Anforderungsanalyse

Im Rahmen des Grobkonzepts und der Anforderungsanalyse wird beantwortet, in welcher Weise ein IDS in die bestehende technisch-organisatorische Infrastruktur zu integrieren ist und welche Anforderungen das einzusetzende IDS erfüllen muss, um die Zielsetzungen zu erreichen.

3. Entscheidungsvorlage

In der Entscheidungsvorlage wird auf Basis der Vorüberlegungen die Machbarkeit verifiziert. Es wird untersucht, ob IDS-Lösungen am Markt verfügbar sind, die den Anforderungen entsprechen. Daneben wird abgeschätzt, welche Kosten Anschaffung, Integration und Betrieb eines IDS verursachen. Dabei ist es sinnvoll, Kosten und Nutzen für unterschiedliche Lösungsansätze gegenüberzustellen. Verschiedene Lösungsansätze können sich dabei z. B. in unterschiedlichen Ausbaustufen eines IDS-Einsatzes oder in der Betrachtung von Produkten mit voneinander abweichender Funktionalität unterscheiden.

In der Privatwirtschaft findet bei der Erstellung der Entscheidungsvorlage typischerweise bereits eine Produktvorauswahl statt. Teilweise orientiert sich die Darstellung von Lösungsalternativen bereits an konkreten Produkten, so dass mit der Entscheidung für eine Lösungsalternative die Produktentscheidung weitgehend vorweggenommen wird.

Auf Basis der Entscheidungsvorlage entscheidet das Management, ob finanzielle Mittel und personelle Ressourcen für Einführung und Betrieb eines IDS bereit gestellt werden sollen und welche der dargestellten Lösungsalternativen verfolgt werden soll.

4. Feinkonzept und Produktauswahl

Grobkonzept und Anforderungsanalyse werden dem verabschiedeten Lösungsansatz angepasst und verfeinert. Es wird ein IDS-Produkt ausgewählt, das eingesetzt werden soll.

Falls bei der Produktauswahl deutlich wird, dass es keine marktverfügbaren Produkte gibt, die die Anforderungen abdecken, oder der Kostenrahmen sich deutlich von den zuvor abgeschätzten Kosten unterscheidet, ist die Entscheidungsvorlage entsprechend zu überarbeiten.

5. Integration

Die Integration umfasst sowohl technische Aspekte, wie das Vorgehen zu Rollout, Inbetriebnahme und Konfiguration des IDS, als auch organisatorische Aspekte, wie die Personalplanung und die Einbettung der IDS-Alarmierung in die Incident-Handling-Prozesse.

6. Betrieb

Diese Phase umfasst den Betrieb des IDS. Sämtliche betriebsrelevanten Aspekte sind dabei in einem Betriebshandbuch zu regeln. Im Leitfaden werden die hierbei zu berücksichtigenden Punkte aufgeführt. Der Anwender wird zur Erstellung eines Betriebshandbuchs angeleitet.

7. Revision

Die Ordnungsmäßigkeit des IDS-Betriebs ist regelmäßig durch eine geeignete Revision zu prüfen. Im Leitfaden werden Hinweise zur Revision von IDS gegeben. Diese umfassen typische Fragestellungen und Prüfmethoden.

3 Die Phasen im Einzelnen

Die einzelnen Phasen der IDS-Einführung werden in den nachfolgenden Abschnitten erläutert.

3.1 Bedarfsfeststellung

Im Rahmen der Bedarfsfeststellung wird geklärt, in wie weit der Einsatz eines Intrusion-Detection-Systems zur ergänzenden Absicherung des Netzübergangs zum Internet in einer Organisation bzw. einem Unternehmen sinnvoll ist. Adressaten dieser Phase sind das IT-Sicherheitsmanagement bzw. der Verantwortliche für den Netzübergang zum Internet.

Zur Bedarfsfeststellung wird folgendes Vorgehen empfohlen:

- Ist-Aufnahme der Einflussfaktoren für den Einsatz von IDS, insbesondere der sicherheitsrelevanten Aspekte am Netzübergang zum Internet
- Ermittlung, ob der Einsatz eines IDS in der Organisation sinnvoll ist
- Festlegung der Ziele, die mit dem Einsatz eines IDS erreicht werden sollen

Falls der Einsatz eines IDS als grundsätzlich sinnvoll erachtet wird, ergeben sich folgende weitere Aktivitäten:

- Sensibilisierung der Entscheider für das Thema Intrusion-Detection
- Bereitstellung von Ressourcen zur Erstellung einer Entscheidungsvorlage

3.1.1 Ist-Aufnahme für Einsatz und Einführung von IDS-relevanten Faktoren

Einflussfaktoren für Intrusion-Detection und die Auswahl technischer Hilfsmittel leiten sich aus der umgebenden Organisation sowie der zugrundeliegenden Infrastruktur inklusive bereits verwendeter Schutzmaßnahmen ab. Als typische Einflussfaktoren sind zu berücksichtigen:

- Risikobereitschaft und Risk-Management der Organisation,
- Infrastruktur und Schutzmaßnahmen der Organisation (Gebäudemanagement, Verteilung, Objektschutz),
- Organisation und Infrastruktur am Netzübergang zum Internet (Policy, Aufbau, Dienste, Auswertung),
- Art und Verwendung der angebotenen Kommunikationsdienste am Internetübergang.

3.1.1.1 Risikobereitschaft der Organisation

Die individuelle Risikobereitschaft einer Organisation spielt eine entscheidende Rolle bei der Gestaltung des IT-Sicherheitsmanagements. Hierin äußert sich die Abwägung, ob und in welcher Stärke auf protektive Maßnahmen gesetzt werden soll und in welcher Intensität Risiken getragen bzw. durch reaktive Maßnahmen abgefedert werden.

Protektive und reaktive Maßnahmen

Es wird unterschieden zwischen „protektiven“ Maßnahmen, die Gefährdungen abwehren und vor deren Eintreten schützen und „reaktiven“ Maßnahmen, mit deren Hilfe das Eintreten von Schadensereignissen erkannt, gemeldet und darauf reagiert werden soll, bis hin zur Schadensbehebung.

Protektive und reaktive Maßnahmen ergänzen sich. Es ist nicht möglich durch Konzentration auf Maßnahmen der einen, Art Maßnahmen der jeweils anderen Art völlig vernachlässigbar zu machen. Zum Beispiel beinhaltet die Aussage: „Es gibt keinen 100%-igen Schutz.“, dass es immer zu Schadensfällen kommen kann, auf die zu reagieren ist.

Intrusion-Detection ist eine reaktive Maßnahme und dient zur Erkennung von eintretenden Schadensfällen oder erster Anzeichen dafür. Es dient explizit nicht zur Abwehr oder Verhinderung des Eintretens von Schadensereignissen. Dennoch ist Intrusion-Detection eine wichtige Voraussetzung für die Alarmierung (Eskalation) und Reaktion (Schadensbegrenzung) auf eintretende Ereignisse.

Beispiele unterschiedlicher Risikobereitschaft

Der Bereich Datenschutz ist ein Beispiel für geringe Risikobereitschaft. Zum Schutz personenbezogene Daten sind protektive Maßnahmen das geeignete Mittel. Reaktive Maßnahme können dabei lediglich ergänzend dienen. Dies liegt insbesondere darin begründet, dass erfolgte Vertraulichkeitsverletzungen grundsätzlich nicht wieder rückgängig gemacht werden können.

In eCommerce- und eBusiness-Applikationen erfolgt bewusst eine Öffnung interner Datenbanken und Geschäftsprozesse zum Internet. Aufgrund des hierdurch erhöhten Risikos, spiegelt das Anbieten entsprechender Dienste eine höhere Risikobereitschaft wieder. Erfolgte Verletzungen der Verfügbarkeit oder Integrität können dabei durch reaktive Maßnahmen zeitnah erkannt werden. Derartige Maßnahmen bilden die Voraussetzung für eine zeitnahe Wiederherstellung der Verfügbarkeit bzw. Integrität.

3.1.1.2 Ist-Aufnahme der Infrastruktur und Schutzmaßnahmen der Organisation

Die Aufnahme - auch der physischen - Infrastruktur und bestehender Schutzmaßnahmen einer Organisation hat Relevanz für die Einschätzung,

- ob Externe die Firewall-Infrastruktur auf physikalischem Wege überbrücken können (etwa durch Einbruch, Ankoppeln an Netzverteiler oder Nutzung von WLANs),
- ob Interne unberechtigt weitere Netzübergänge schaffen und die Firewall überbrücken können (etwa durch Installation von Modems, WLANs, etc.),
- ob IT-Systeme, Server und Firewall-Komponenten zugangsgeschützt aufgestellt sind,
- ob weitere Netzübergänge ins Internet, etwa von externen Liegenschaften aus, existieren, durch deren Nutzung der betrachtete Internet-Übergang umgangen werden kann. Dies betrifft auch VPN-Verbindungen oder „Standleitungen“.

3.1.1.3 Ist-Aufnahme der Organisation und Infrastruktur des Internet-Übergangs

Durch die Ist-Aufnahme der Infrastruktur des Internet-Übergangs soll ermittelt werden, ob und in welcher Stärke bereits Schutzmaßnahmen realisiert sind. Hierzu sind sicherheitsrelevante technische und organisatorische Aspekte des Internet-Übergangs zu erheben.

Für die Bedarfsfeststellung relevante und zu beantwortende Fragestellungen in diesem Zusammenhang sind:

- Welche Komponenten werden eingesetzt? (Router, Switches, Firewall, Server in der DMZ, zugrundeliegende Plattformen, etc.)
- Durch welche Prozesse werden Konfigurationsänderungen am Schutzkomponenten (Router, Switches, Firewall) flankiert?
- Welche der Komponenten sind – trotz bestehender Schutzmaßnahmen - Gefährdungen aus dem Internet in besonderer Weise ausgesetzt?

Insbesondere fallen hierunter Serverkomponenten, bei denen entweder keine angemessene Datenflusskontrolle durch bestehende Schutzkomponenten gegeben ist oder bei denen aufgrund der Funktionalität des Dienstes erhöhte Restrisiken bestehen, wie z. B. bei der Nutzung eines Webservers.

Um einen Überblick über die technische Infrastruktur zu erhalten, ist die Darstellung der Komponenten und ihrer Kommunikationsverbindungen in einem Architekturdiagramm hilfreich und sinnvoll.

3.1.1.4 Ist-Aufnahme des Zwecks und der Art von Kommunikationsdiensten am Internet-Übergang

Für die Bedarfsfeststellung relevante und zu beantwortende Fragestellungen in diesem Zusammenhang sind:

- Welche physischen und logischen Kommunikationsverbindungen bestehen zwischen den Komponenten?
- Welchem Zweck dienen die am Internet-Übergang angebotenen Kommunikationsdienste (E-Mail, Webzugriff, Webserverangebot, E-Business-Angebot, etc.)?
- Welche Anforderungen an Verfügbarkeit und Integrität bestehen für die Dienste?

3.1.2 Ist der Einsatz eines IDS grundsätzlich sinnvoll?

Grundsätzlich ist der Einsatz von IDS nur dann sinnvoll[1], wenn

1. sich aus dem Einsatz des IDS ein sicherheitstechnischer Zusatznutzen ergibt und
2. ein höherer sicherheitstechnischer Zusatznutzen nicht mit vergleichbarem (oder geringerem) Aufwand durch andere Maßnahmen erzielbar ist.

Ein sicherheitstechnischer Zusatznutzen ist dann gegeben, wenn der Schutz am Netzübergang verbessert wird bzw. bestehende Restrisiken vermindert werden. Im Vordergrund steht dabei der Schutz eigener IT-Systeme vor unberechtigtem Zugang aus dem Internet.

Bei der Absicherung eines Internet-Übergangs sollte grundsätzlich darauf geachtet werden, zunächst die Einsatzmöglichkeiten „protektiver“ Maßnahmen (Firewall-Systeme, Authentisierungsverfahren, etc.) auszuschöpfen, da „reaktive“ Maßnahmen erst in Verbindung damit ihre volle Wirkung entfalten können.

Der Einsatz eines Firewall-Systems an einem Netzübergang zum Internet ist daher eine grundlegende Voraussetzung dafür, den Einsatz eines IDS in Erwägung zu ziehen. Aus diesem Grund wird im Folgenden davon ausgegangen, dass der Netzübergang zum Internet bereits durch ein Firewall-System geschützt ist.

Das nachstehend beschriebene Vorgehen zur Ermittlung, ob der Einsatz eines IDS sinnvoll ist, orientiert sich an der Darstellung von Faktoren, von denen der sicherheitstechnische Zusatznutzen eines IDS abhängt. Dabei wird der Zusatznutzen durch das IDS im Vergleich zum Zusatznutzen alternativer Maßnahmen betrachtet. Solche Faktoren sind unter anderem

- die Architektur und Einsatzweise des bestehenden Firewall-Systems,
- die Verfügbarkeits- und Integritätsanforderungen an gefährdete Komponenten,
- der Grad der Interaktion mit internen Systemen bei Zugriffen aus dem Internet.

[1] An dieser Stelle wird von „grundsätzlich sinnvoll“ gesprochen, da erst an späterer Stelle beantwortet wird, ob der Einsatz von IDS auch unter Kosten-Nutzen-Aspekten sinnvoll ist.

Relevante Einflussfaktoren sind in Anhang 4.1.2 dokumentiert. Zu jedem Einflussfaktor ist dabei angegeben, wie sich der jeweilige Ist-Zustand auf den IDS-Bedarf auswirkt.

Zur Ermittlung, ob der Einsatz eines IDS grundsätzlich sinnvoll ist, sind die beschriebenen Einflussfaktoren durchzugehen. Für jeden Einflussfaktor ist die Frage zum Ist-Zustand zu beantworten. Aus der zugehörigen Bewertung und Stellungnahme ergibt sich,

- ob ein IDS-Einsatz hinsichtlich des betreffenden Einflussfaktors und dessen konkreter Ausprägung in der Ist-Situation sinnvoll ist und
- welchen Zwecken ein IDS-Einsatz dabei dienen kann.

Im Einflussfaktor E9 wird zudem die Relevanz der Nutzenaspekte von IDS abgefragt.

Auf eine Gewichtung der einzelnen Einflussfaktoren wurde verzichtet, da ihre Ausprägung im konkreten Einzelfall sehr unterschiedlich sein kann. Die beschriebenen Einflussfaktoren dienen insofern als Hilfestellung zur Ermittlung, ob und zu welchem Zweck ein IDS-Einsatz sinnvoll ist[2].

Aus der Ist-Situation und den zugehörigen Stellungnahmen zu den Einflussfaktoren ist abzuleiten, ob der Einsatz eines IDS grundsätzlich sinnvoll ist oder ob durch andere Maßnahmen mit vergleichbarem Aufwand ein höherer Zusatznutzen erreicht werden kann.

Eine Begründung dafür, weshalb der Einsatz eines IDS grundsätzlich sinnvoll ist, kann erstellt werden, indem die angegebenen Stellungnahmen unter Berücksichtigung der Ist-Situation entsprechend umformuliert werden.

Die Anwendung des beschriebenen Verfahrens ist in Anhang 4.1.3 für unterschiedliche Szenarien der Nutzung von Internet-Übergängen beschrieben.

3.1.3 Sensibilisierung der Entscheider für das Thema Intrusion-Detection

Die Entscheiderebene sollte darüber informiert werden, dass sich das IT-Sicherheitsmanagement bzw. die für den Internet-Übergang verantwortliche Stelle mit dem Thema IDS beschäftigt. Das Interesse der Entscheider für IDS sollte durch eine motivierende Heranführung an das Thema geweckt werden.

Anhang 4.1.1 kann als Vorlage für eine Management-Einführung in IDS dienen. Die Vorlage sollte unter Berücksichtigung der zuvor erhobenen Einsatzziele konkretisiert und ggf. um die Begründung erweitert werden, weshalb ein IDS-Einsatz sinnvoll ist.

3.1.4 Bereitstellung von Ressourcen zur Erstellung einer Entscheidungsvorlage

Falls der Einsatz eines IDS als grundsätzlich sinnvoll erkannt wurde, sind die nächsten Schritte die

- Grobkonzeption eines möglichen IDS-Einsatzes,
- die Klärung der Anforderungen an ein einzusetzendes IDS und die
- Erstellung einer Entscheidungsvorlage unter Berücksichtigung von Kosten-Nutzen-Aspekten.

Die hierzu erforderlichen Ressourcen sind bereitzustellen.

Abhängig vom jeweiligen organisatorischen Umfeld, ist hierzu ggf. die Beantragung eines internen Projekts und dessen Beauftragung erforderlich.

---

[2] Die Einflussfaktoren stellen jedoch keinen „Algorithmus“ zur Berechnung des Nutzens dar.

Es wird empfohlen Grobkonzept, Anforderungen und Entscheidungsvorlage mit verantwortlichen Vertretern folgender Bereiche abzustimmen:

- Systemadministration und Systembetrieb,
- IT-Strategie und IT-Planung,
- Revision,
- Datenschutzbeauftragter und
- Personalvertretung (Betriebsrat, Personalrat)[3].

Ein geeignetes Vorgehen ist z. B. die Ausarbeitung des Grobkonzepts, der Anforderungen und der Entscheidungsvorlage unter Leitung des IT-Sicherheitsmanagements im Rahmen eines Projekts, das von einem Kernteam mit Vertretern der aufgeführten Bereiche gesteuert und begleitet wird.

[3] Der Datenschutzbeauftragte und die Personalvertretung sind zu berücksichtigen, da ein IDS im Rahmen der Netz- und Systembeobachtung ggf. auch Daten aufzeichnet, die personenbezogenen Charakter aufweisen oder zur Arbeitsüberwachung genutzt werden könnten.

3.2 Grobkonzept und Anforderungsanalyse

Im Rahmen des Grobkonzepts und der Anforderungsanalyse wird beantwortet, in welcher Weise ein IDS in die bestehende technisch-organisatorische Infrastruktur zu integrieren ist und welche Anforderungen das einzusetzende IDS erfüllen muss, um die Zielsetzungen zu erreichen. Der Leitfaden richtet sich in dieser Phase an das IT-Sicherheitsmanagement bzw. das zur Ausarbeitung von Grobkonzept, Anforderungsanalyse und Entscheidungsvorlage gebildete Projektteam.

Arbeitsschritte zur Grobkonzeption und Analyse der Anforderungen sind:

1. Ist-Aufnahme der technischen Infrastruktur am Netzübergang zum Internet
2. Ist-Aufnahme bestehender Prozesse für die Verfolgung von Sicherheitsvorfällen
3. Festlegung der mit dem Einsatz des IDS verbundenen Zielsetzungen
4. Ableitung von Anforderungen an ein einzusetzendes IDS
5. Festlegung der Platzierung von Sensoren
6. Interne Abstimmung der Zuständigkeiten für die Administration des IDS sowie der Zuständigkeiten für Annahme und Eskalation von Alarmen des IDS
7. Festlegung der Platzierung von Management- und Auswertungsstation
8. Dokumentation der Ergebnisse im Dokument „Grobkonzept und Anforderungsanalyse“

3.2.1 Ist-Aufnahme der technischen Infrastruktur

Um festzulegen, an welchen Stellen Sensoren mit welcher Funktion zum Einsatz kommen sollen, muss zunächst die technische Infrastruktur am Internet-Übergang detailliert erhoben werden. Hierzu ist die Ist-Aufnahme aus Abschnitt zu 3.1.1 zu verfeinern. Zu beantwortende Fragestellungen in diesem Zusammenhang sind unter anderem:

- Welche Funktionen haben die einzelnen Komponenten und wie sind sie aufgebaut?
  - Betriebssystem,
  - Konfiguration,
  - Anwendungssoftware,
  - Versionen der Softwareprodukte.
- Gibt es spezifische Management-Systeme für die Komponenten (z. B. Firewall-Management, System-Management)? Falls ja:
  - Wo sind diese Management-Systeme platziert?
  - Wie erfolgt der Zugriff auf die Management-Systeme?
- Wie ist der Verkehrsfluss zwischen den Komponenten?
  - Welche Protokolle/Dienste werden genutzt?
  - In welcher Richtung erfolgt der Verbindungsaufbau?

Für die anschließende Diskussion unterschiedlicher Sensorplatzierungen ist es sehr hilfreich und empfehlenswert, die Komponenten und ihre Kommunikationsverbindungen in einem Netzwerkdiagramm darzustellen!

3.2.2 Ist-Aufnahme der bestehenden Incident-Response-Organisation

Wenn Schadensereignisse erkannt werden, sollte darauf angemessen reagiert werden. Hierfür definierte Vorgehensweisen werden als Incident-Response bezeichnet und umfassen neben der Schadenserkennung auch die Schadensbegrenzung und -behebung. Zur Reaktion auf IT-spezifische Sicherheitsvorfälle unterhalten einige Behörden und Unternehmen eigene Abteilungen oder Teams, wie z. B. CSIRTs (Computer Security Incident Response Teams), Katastrophenvorsorge-Teams und/oder IT-Krisenstäbe.

Sofern es bereits eine Organisation für das Incident-Response im Unternehmen gibt, sollte der Einsatz des Intrusion-Detection hiermit koordiniert werden. Falls in einigen Bereichen Eskalationsverfahren etabliert sind, sollte untersucht werden, ob und wie die Eskalation bei IDS-Alarmen hiermit verknüpft werden kann. Vorliegende Erfahrungen können zu Synergieeffekten führen. Wenn bislang noch keine Incident-Response-Organisation definiert und etabliert ist, so ist diese im Rahmen der IDS-Einführung festzulegen, um geeignet auf durch das IDS erkannte Sicherheitsvorfälle zu reagieren.

Für die Festlegung einer Incident-Reponse-Organisation für den Betrieb des IDS ist zunächst zu erheben, welche Prozesse es im Hause bereits für die Meldung und Verfolgung von Sicherheitsvorfällen gibt. Zu beantwortende Fragestellungen in diesem Zusammenhang sind beispielsweise:

- Gibt es bereits Vorgehensweisen zur Verfolgung von Problemen und Sicherheitsvorfällen im Unternehmen?
  - Welche Vorgehensweisen sind definiert?
  - An welcher Stelle laufen Problemmeldungen auf?
- Gibt es ein System-Management, auf dessen Basis z. B. der Ausfall von Servern erkannt wird?
  - An welcher Stelle laufen die entsprechenden Alarme auf?
- Gibt es eine zentrale Stelle, bei der Problemmeldungen und Alarme gebündelt auflaufen?
  - Zu welchen Zeiten ist diese Stelle besetzt?
  - Über welche technischen Medien (Ticketing-System, E-Mail) erfolgen Alarmierungen und Problemmeldungen bislang?

3.2.3 Konkretisierung der Ziele des IDS-Einsatzes

Im Rahmen der Bedarfsfeststellung wurde bereits die Relevanz der Nutzenaspekte eines IDS-Einsatzes ermittelt. An dieser Stelle werden die mit dem Einsatz eines IDS verbundenen Zielsetzungen konkretisiert. Hierzu sind im Anhang 4.2.1 Fragestellungen zu den einzelnen Zielsetzungen angegeben, die möglichst detailliert beantwortet werden sollten.

3.2.4 Anforderungsanalyse

Auf Basis der Zielsetzungen und der Ist-Situation sind Anforderungen an das IDS abzuleiten und zu dokumentieren. Das Vorgehen umfasst

- die Festlegung einer Gewichtung,
- die Ableitung von Anforderungen aus der Ist-Situation und den Zielsetzungen sowie
- die Dokumentation der Anforderungen.

Festlegung einer Gewichtung

Zunächst sind mögliche Gewichte für die Anforderungen festzulegen. Dabei sollten mindestens die vier nachstehend angegebenen Gewichtungen unterschieden werden. Bei Bedarf können weitere Gewichtungen vorgesehen werden.

Ausschluss- / k.o.-Kriterium:	Das einzusetzende IDS muss die Anforderung erfüllen.
Soll-Kriterium:	Das IDS soll die Anforderung erfüllen.
Wunsch-Kriterum:	Die Anforderung wird als „nice-to-have“ eingestuft.
Irrelevantes Kriterium:	Die Erfüllung der Anforderung ist für die Ziele und Ist-Situation nicht relevant.

Ableitung und Dokumentation von Anforderungen

Die Abhängigkeiten zwischen Ist-Situation und Zielsetzungen sowie die an das IDS zu stellenden Anforderungen sind in Anhang 4.2.4 beschrieben. Die Beschreibung orientiert sich an Fragestellungen zur Ist-Situation und den Zielsetzungen. Zur Ableitung der Anforderungen sind die Fragen durchzugehen.

Zur Dokumentation der Anforderungen und ihrer Gewichtung ist in Anhang 4.2.5 eine Vorlage angegeben. Diese enthält nicht nur Anforderungen, die von Ist-Situation und Zielsetzungen abhängen, sondern auch Basisanforderungen, die von IDS allgemein erfüllt werden sollten. Vor jeder Anforderung ist dabei ein Feld zur Angabe des Gewichts der Anforderung vorgesehen.

3.2.5 Sensortypen und Sensorplatzierung

Basis für die Diskussion möglicher Sensorplatzierungen bildet das Netzwerkdiagramm des Internet-Übergangs. Die Vorgehensweise zur Ermittlung sinnvoller Platzierungen ist in der nachstehenden Abbildung dargestellt.

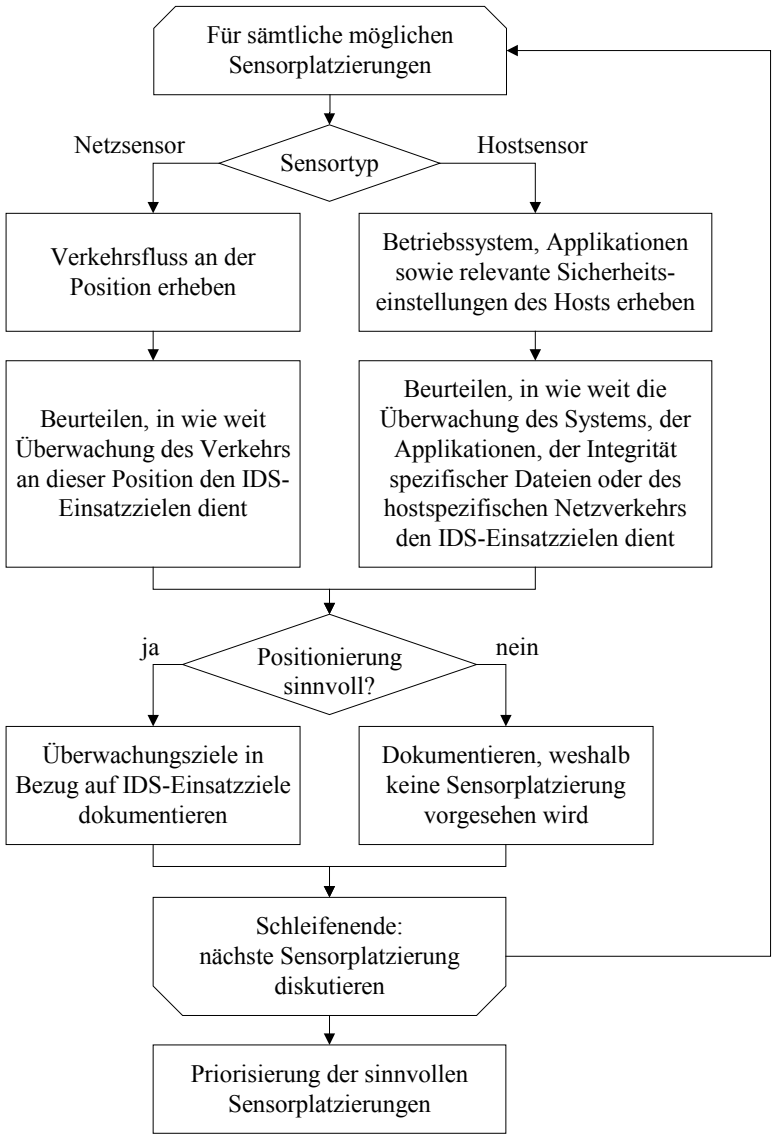

Abbildung 3-1: Vorgehen zur Ermittlung sinnvoller Sensorplatzierungen

Für sämtliche möglichen Sensorpositionen ist zu diskutieren, ob eine Platzierung an der jeweiligen Position sinnvoll ist.

Platzierung von Netzsensoren

Mögliche Platzierungen von Netzsensoren werden in Anhang 4.2.2 beispielhaft für den vom BSI empfohlenen 3-stufigen Internet-Übergang diskutiert.

Bei der Priorisierung der sinnvollen Sensorpositionen ist zu überlegen und zu dokumentieren, an welchen Punkten eine Sensorplatzierung besonders wichtig ist und an welchen sie weniger wichtig ist. Zu berücksichtigen ist bei der Priorisierung

- wie weit die jeweilige Platzierung zum Erreichen der IDS-Einsatzziele beiträgt,

- durch welche Platzierungen sich Synergieeffekte ergeben (z. B. kann derselbe Verkehrsfluss ggf. an unterschiedlichen Positionen durch Netzsensoren abgegriffen werden) und
- ob eine Überwachung des Netzverkehrs an der jeweiligen Position effizient möglich ist. Dabei sind die in Anhang 4.2.2 aufgeführten Grundsätze zu beachten.

Platzierung von Hostsensoren

Mögliche Platzierungen für Hostsensoren sind die verschiedenen Serversysteme der IT-Infrastruktur am Netzübergang. Im Rahmen der Konkretisierung der Ziele des IDS-Einsatzes wurde bereits geklärt, für welche Systeme und Applikationen eine Überwachung besonders wichtig ist.

Hostsensoren werden immer auf dem zu überwachenden System installiert und betrieben. Bei der Diskussion, ob ein Hostsensor auf einem bestimmten System platziert werden soll, sind zuständige System- bzw. Applikationsverantwortliche mit einzubinden. Diese können konkret darüber Auskunft geben, welche Logdaten das System bzw. die Applikation liefert und ob deren Überwachung sinnvoll ist. Eine weitere Voraussetzung für die Platzierung eines Hostsensors ist, dass Kapazitäten (CPU, Speicher) zum Betrieb des Sensors auf dem zu überwachenden Host vorhanden sind. Dabei sollte von einer Systembelastung von bis zu 5% der CPU-Last durch den Sensor ausgegangen werden.

Für die Platzierung von Hostsensoren ist des Weiteren zu prüfen, ob bestehende Wartungsverträge die Installation eines Sensors auf dem System zulassen[4].

Priorisierung der Platzierungen

Die Priorisierung vereinfacht die Spezifikation von Lösungsansätzen mit einer geringeren Anzahl von Sensoren, die z. B. im Rahmen der Entscheidungsvorlage Alternativlösungen darstellen können. Des Weiteren dient die Priorisierung bei der späteren Inbetriebnahme der Sensoren als Richtschnur für die Reihenfolge der Inbetriebnahme.

3.2.6 Festlegung einer geeigneten Organisation

Für die Festlegung einer geeigneten Organisation wird zunächst eine generisches Rollenmodell beschrieben, dass dann auf die konkrete Organisation abzubilden ist.

Es ist zu entscheiden, welchen internen Stellen (Mitarbeitern, Abteilungen, Bereichen) die Rollen bzw. Zuständigkeiten und Verantwortlichkeiten zugewiesen werden.

Generisches Rollenmodell

Für den Betrieb des IDS wird zwischen folgenden Rollen unterschieden:

- **IDS-Manager**
  Der IDS-Manager vertritt die Belange des IDS gegenüber der Entscheidungsebene.
- **IDS-Administration**
  Die IDS-Administration kümmert sich um sämtliche Aufgaben im Zusammenhang mit der Verwaltung, Wartung und Konfiguration des IDS[5]. Sie kalibriert das IDS und wertet regelmäßig die Meldungen des IDS aus.
- **IDS-Monitoring**
  Die Alarme des IDS laufen beim IDS-Monitoring auf. Das IDS-Monitoring initiiert die entsprechende Eskalation an das IDS-Incident-Response.

---

[4] Falls eine Platzierung des Sensors auf dem System nicht zulässig ist, kann eine eingeschränkte Überwachung der Logdaten ggf. über einen zusätzlich zu betreibenden Logserver erfolgen.

[5] Im Fall des Betriebs hostbasierter Sensoren sind die Zuständigkeiten für deren Betrieb und Kalibrierung zwischen IDS-Administration und den jeweiligen System- bzw. Anwendungsverantwortlichen abzustimmen.

- **IDS-Incident-Response**
  Das IDS-Incident-Response ist zuständig für eine zeitnahe und angemessene Reaktion auf Alarme sowie eine ggf. erforderliche, weitere Eskalation. Es ermittelt Ursachen und Auswirkungen des gemeldeten Ereignisses und leitet ggf. schadensreduzierende oder -behebende Maßnahmen ein.

Das Zusammenspiel der Rollen ist in der nachstehenden Abbildung skizziert.

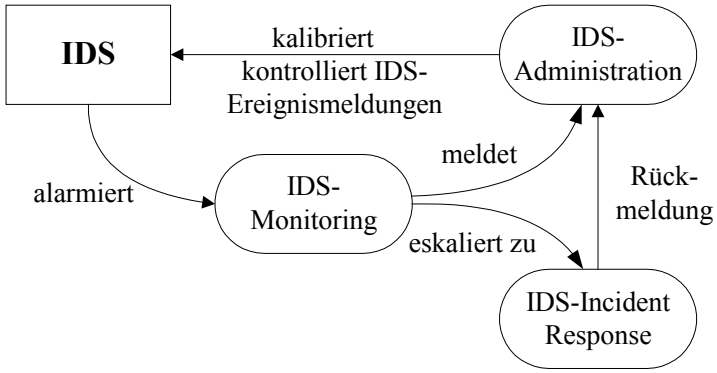

Abbildung 3-2: Zusammenspiel der IDS-Rollen (Skizze)

Eine personelle Trennung der Rollen ist nicht erforderlich. Es ist vielmehr sinnvoll, dass die Rollen des IDS-Monitoring und IDS-Incident-Response – soweit möglich – während der üblichen Arbeitszeit von der IDS-Administration wahrgenommen werden.

Es ist festzulegen, wer die oben angesprochenen Rollen wahrnehmen soll.

IDS-Manager

Als IDS-Manager eignet sich z. B. ein Mitarbeiter des IT-Sicherheitsmanagements. Prädestiniert für dieses Aufgabe ist der Leiter des aktuellen Projekts zur IDS-Einführung.

Zur Wahrnehmung seiner Aufgaben benötigt der IDS-Verantwortliche Kenntnisse über die Funktionalität und Grenzen des eingesetzten IDS. Er sollte sämtliche bereichsübergreifenden und technisch nicht detaillierten Fragestellungen zum IDS und dessen Einsatzweise beantworten können. Die Kenntnisse sollten folgende Punkte beinhalten:

- Einsatzzweck, Nutzen und Grenzen des IDS,
- Sensorarten des IDS sowie kontrollierbare Netze und Systeme,
- Einsatzweise des IDS (insbesondere Sensorplatzierungen),
- Organisation des Incident-Handling/Notfallbearbeitung sowie
- Datenschutz und rechtliche Aspekte des IDS-Einsatzes.

IDS-Administration

Ein IDS ist ein komplexes, technisches Werkzeug, dessen Administration tiefgehende Kenntnisse sowohl über die zu schützende IT-Infrastruktur als auch über Angriffe und Sicherheitsverletzungen erfordert. Als IDS-Administratoren eignen sich grundsätzlich sowohl Administratoren bestehender Schutzkomponenten am Internet-Übergang mit Hintergrundwissen im Bereich IT-Sicherheit als auch technisch versierte Mitarbeiter des IT-Sicherheitsmanagements.

Die IDS-Administration sollte grundlegende Kenntnisse aufweisen, über

- die überwachten Netze, Betriebssysteme, Anwendungen und
- Techniken (Firewall, Router) zur Netzabsicherung.

Bei der Einführung, der Kalibrierung und dem Betrieb des IDS benötigt die IDS-Administration darüber hinaus detaillierte Kenntnisse über

- den Ist-Zustand der Infrastruktur (vgl. Kapitel 3.2.1), insbesondere
  - zulässige und nicht zulässige Kommunikationsbeziehungen sowie
  - aktuelle Informationen zur Konfiguration geschützter Systeme (Versionen, Patchlevel, etc.), sowie über
- Angriffe, Sicherheitsverletzungen und Maßnahmen, die im Fall erkannter Angriffe oder Sicherheitsverletzungen zu ergreifen sind.

Aus Gründen des Datenschutzes ist der IDS-Administrator darauf zu verpflichten, die Protokolldaten des IDS nur für die mit den Einsatzzielen des IDS verbundenen Zwecke zu nutzen.

IDS-Monitoring

Es ist festzulegen, welche Stelle bzw. welche Stellen wann (während welcher Zeiten) für die Annahme von IDS-Alarmen zuständig sind.

Hierzu ist zunächst auf Grundlage der mit dem IDS-Einsatz verbundenen Zielsetzungen zu überlegen, zu welchen Zeiten die Annahme und Weiterverfolgung von IDS-Alarmen erforderlich ist:

- Annahme und Weiterverfolgung der IDS-Alarme während der Kernarbeitszeit sind ausreichend.
- IDS-Alarme sollen in erweiterten Arbeitszeiten (z. B. Mo-Fr 7:00 - 19:00 Uhr, Sa 8:00-14:00 Uhr) entgegengenommen werden.
- IDS-Alarme müssen rund um die Uhr entgegengenommen werden.

Abhängig von den Anforderungen an die Annahme von Alarmen kann es sinnvoll sein, die Zuständigkeit für die Annahme auf unterschiedliche Stellen zu verteilen (z. B. User-Help-Desk von 8:00-18:00 Uhr, Wachdienst/Gebäudeschutz außerhalb dieser Zeiten).

Das IDS-Monitoring muss über keine IDS-spezifischen Kenntnisse verfügen. Durch geeignete Hilfsmittel (IDS-Eskalationsplan, siehe Kapitel 3.6.6) muss es in die Lage versetzt werden, abhängig vom Alarm die festgelegte Eskalation auszulösen.

Aus Gründen des Datenschutzes ist das IDS-Monitoring darauf zu verpflichten, die Protokolldaten des IDS nur für die mit den Einsatzzielen des IDS verbundenen Zwecke zu nutzen.

IDS-Incident-Response

Wer für die Reaktion auf Alarme des IDS zuständig ist, kann im Einzelfall vom spezifischen Alarm abhängen. Die Verantwortung für unterschiedliche Systeme und Anwendungen kann bei unterschiedlichen Personen bzw. Rollen liegen, die abhängig vom konkreten Alarm zu benachrichtigen sind.

Die Festlegung der Zuständigkeiten im Alarmfall erfolgt daher später im Rahmen der Integration des IDS.

Die angemessene Reaktion auf IDS-Alarmierungen verlangt

- technische Kenntnisse über das eingesetzte IDS und die überwachten Systeme bzw. Netze zur detaillierten Beurteilung von IDS-Meldungen,
- Kenntnisse über mögliche Angriffe auf Netze und Systeme,
- das Vermögen zur realistischen Einschätzung gemeldeter, sicherheitsrelevanter Ereignisse sowie
- Kenntnis der rechtlichen Rahmenbedingungen des Incident-Response.

Aus Gründen des Datenschutzes sind die Mitarbeiter des IDS-Incident-Response darauf zu verpflichten, die Protokolldaten des IDS nur für die mit den Einsatzzielen des IDS verbundenen Zwecke zu nutzen.

3.2.7 Platzierung der Management- und Auswertungsstation

Bei der Platzierung der Management- und Auswertungsstation ist zu beachten, dass die folgenden Anforderungen an die Kommunikation bestehen[6]:

- Kommunikation mit den Netz- und Hostsensoren insbesondere zur Konfiguration der Sensoren und Meldung von Ereignissen.
- Kommunikation mit IT-Systemen für das Intrusion-Response (z. B. Mailserver für das Versenden von E-Mail oder Systemmanagementsysteme als Empfänger von SNMP-Traps).
- Kommunikation mit Clients im internen Netz, die remote auf die Management- und Auswertungsstation zugreifen.

Für die Platzierung der Management- und Auswertungsstation gibt es verschiedene Möglichkeiten:

1. Die Management- und Auswertungsstation wird in einer bestehenden DMZ oder im internen Netz platziert. Für die Kommunikation werden bestehende Übertragungsstrecken genutzt.
2. Für die IDS-Kommunikation wird ein physikalisch separates IDS-Netz eingerichtet, in dem die Management- und Auswertungsstation betrieben wird. Alle Übergänge ins IDS-Netz werden dabei geeignet geschützt.
3. Die Management- und Auswertungsstation wird in einem zusätzlichen Teilnetz betrieben, das am bestehenden Firewall-System eingerichtet wird (separate DMZ, Management-Teilnetz).

Die unterschiedlichen Platzierungen werden im Anhang 4.2.3.3 diskutiert. Welche Platzierung gewählt wird, hängt letztlich vom zu erreichenden Sicherheitsniveau und vom zur Verfügung stehenden Budget ab.

3.2.8 Dokumentation der Ergebnisse

Der Aufbau eines Dokuments „Grobkonzept und Anforderungsanalyse“ lehnt sich eng an die vorangegangenen Arbeitsschritte an. Ein Dokumentenrahmen ist in Anhang 4.2.6 angegeben.

[6] In diesem Abschnitt wird vereinfachend von einer Management- und Auswertungsstation ausgegangen. Kommen mehrere Stationen zum Einsatz oder erfolgen Management und Auswertung separiert, sind die beschriebenen Überlegungen für jede der zum Einsatz kommenden Stationen unter Berücksichtigung ihrer jeweiligen Kommunikationsanforderungen durchzuführen.

3.3 Entscheidungsvorlage

Im Rahmen der Erstellung der Entscheidungsvorlage wird die Machbarkeit des IDS-Einsatzes verifiziert. Die erforderlichen finanziellen und personellen Aufwände für Einführung und Betrieb eines IDS werden abgeschätzt. Adressaten dieser Phase sind das IT-Sicherheitsmanagement bzw. das mit der Ausarbeitung der Entscheidungsvorlage beauftragte Projektteam.

Arbeitsschritte zur Erstellung der Entscheidungsvorlage sind:

1. Marktsichtung
2. Darstellung von Lösungsalternativen (inklusive Kostenabschätzung)
3. Erstellung der Entscheidungsvorlage

3.3.1 Marktsichtung

Im Rahmen der Marktsichtung wird ermittelt, ob und in wie weit die zuvor festgelegten Anforderungen durch marktverfügbare IDS-Produkte erfüllt werden können.

Um einen Überblick über IDS-Produkte, deren Funktionalitäten und zugehörigen Hersteller zu erhalten, empfiehlt es sich, zunächst Testberichte von IDS-Produkten zu studieren. Produkttests von IDS-Produkten sind im Internet von zahlreichen Magazinen und Analysten veröffentlicht. Im Anhang 4.3.1 ist eine Auswahl von Links angegeben.

Um zu eruieren, ob und in wie weit die zuvor ermittelten spezifischen Anforderungen von marktverfügbaren Produkten abgedeckt werden, empfiehlt es sich, einen Fragebogen zusammenzustellen, in dem die Anforderungen in Form von Fragen formuliert sind, und auf dessen Basis Informationen von Herstellern über deren IDS-Produkte einzuholen.

Neben der Erfüllung der Anforderungen sollten im Fragebogen auch Preise und Aufwandsabschätzungen abgefragt werden:

- Preise der IDS-Komponenten: Netz-/Hostsensoren, Management- und Auswertungskomponenten sowie ggf. erforderliche Zusatzsoftware
- Wartungskosten: Kosten für Signatur- und Softwareaktualisierungen
- Kosten der Herstellerunterstützung (z. B. für Installation und Erstkalibrierung)
- Erfahrungswerte für den Aufwand bei Installation, Inbetriebnahme und Kalibrierung

Auf Basis der erhaltenen Informationen wird ersichtlich, ob es geeignete Produkte am Markt gibt und welche Teilmengen der Anforderungen praktisch abgedeckt werden können.

3.3.2 Darstellung von Lösungsansätzen

Auf Grundlage der vorliegenden Informationen sind realisierbare und sinnvolle Lösungsansätze darzustellen. Dabei sollten vorliegende Randbedingungen, wie Budgetobergrenzen oder verfügbare personelle Kapazitäten für Einführung und Betrieb des IDS, bereits berücksichtigt werden.

Unterschiedliche Lösungsansätze können sich unter anderem aus folgenden Gründen ergeben:

- Die Anforderungen werden von IDS-Produkten oder Produktgruppen nur teilweise und in unterschiedlichem Maße erfüllt.

- IDS-Produkte ähnlicher Funktionalität werden in unterschiedlicher Weise eingesetzt.
- Es werden unterschiedlich viele Sensoren vorgesehen. Für die Sensorplatzierung ist dabei die im Grobkonzept erfolgte Priorisierung zu berücksichtigen.

Des Weiteren ist zu berücksichtigen, dass der Integrationsaufwand von Hostsensoren deutlich höher ist als der Integrationsaufwand von Netzsensoren, da Netzsensoren im Gegensatz zu Hostsensoren im Wesentlichen unabhängig von der bestehenden IT-Infrastruktur integriert und betrieben werden können.

Falls es am Markt keine geeigneten Produkte gibt, ist zu prüfen, ob Basisanforderungen durch Entwicklung geeigneter Software oder durch „manuelle Ereigniserkennung“ sinnvoll erfüllt werden können.

Für die unterschiedlichen Lösungsansätze sind die zu erwartenden Kosten und Aufwände abzuschätzen. Beim Einsatz eines marktverfügbaren IDS fallen typischerweise folgende Arten von Aufwänden und Kosten an:

- Kosten für IDS-Produkte, Einführungsunterstützung, Wartung, ggf. HW/SW-Plattformen und ggf. erforderliche Zusatzsoftware,
- Personelle Aufwände für die IDS-Beschaffung und IDS-Einführung (Installation, Integration, Inbetriebnahme, Konfiguration und Kalibrierung),
- Personelle Aufwände für den IDS-Betrieb (IDS-Administration, IDS-Monitoring[7]).

Eine grobe Abschätzung typischer Kosten und Aufwände ist in Anhang 4.3.2 gegeben.

Das Verhältnis zwischen verfügbarem Budget und verfügbaren personellen Ressourcen kann dabei die Entscheidung zwischen dem Kauf eines IDS oder dem Einsatz von Open Source Software (z. B. Snort) beeinflussen: Falls interne personelle Ressourcen eng begrenzt sind, jedoch finanzielle Mittel zu Verfügung stehen, empfiehlt sich der Kauf eines IDS-Produkts inklusive Herstellerunterstützung. Falls umgekehrt finanzielle Mittel sehr begrenzt sind, jedoch IT-Personal verfügbar ist, kann der Einsatz von Open Source Software eine sinnvolle Alternative darstellen. Im Vergleich zur Einführung kommerzieller IDS-Produkte ist beim Einsatz von Open Source Software von zusätzlichen Aufwänden für die Anpassung und Erweiterung der Software auszugehen, um ein in der jeweiligen Einsatzumgebung sinnvoll einsetzbares IDS zu erhalten.

3.3.3 Erstellung der Entscheidungsvorlage

Die Entscheidungsvorlage dient dem Management (Entscheidungsebene) als Basis zur Entscheidung über Einführung und Betrieb eines IDS.

Mit der Entscheidungsvorlage sind dem Management alle notwendigen Informationen bereitzustellen, um über das weitere Vorgehen hinsichtlich Einführung und Betrieb von IDS entscheiden zu können. Die Darstellung hat prägnant und auf die wesentlichen Informationen reduziert zu erfolgen.

Wesentliche Inhalte sind

- die Beschreibung der mit dem Einsatz eines IDS verbundenen Zielsetzungen,
- die Skizzierung und Diskussion von Lösungsalternativen inklusive Kosten-Nutzen-Analysen sowie
- die abschließende Empfehlung einer der dargestellten Lösungsalternativen inklusive der zu erwartenden Aufwände.

Ein Dokumentenrahmen für eine Entscheidungsvorlage ist in Anhang 4.3.3 angegeben.

[7] Die Aufwände für die Reaktion auf IDS-Meldungen (CSIRT) lassen sich nur schlecht abschätzen, da sie vom jeweiligen Vorfall abhängen. Sie werden daher an dieser Stelle nicht berücksichtigt.

3.4 Managemententscheidung

Auf Basis der Entscheidungsvorlage entscheidet das Management, ob und welcher der beschriebenen Lösungsansätze weiterverfolgt werden soll. Hiermit ist im Allgemeinen die Freigabe der abgeschätzten finanziellen Mittel sowie der personellen Ressourcen verbunden. Zusätzlich zur Entscheidung des Managements ist die Zustimmung des Betriebs- bzw. Personalrats und des Datenschutzbeauftragten zu dem ausgewählten Lösungsansatz und den damit verbundenen Zielsetzungen einzuholen.

3.5 Feinkonzept und Produktauswahl

Nach der Managemententscheidung ist geklärt, ob und in welcher Weise ein IDS-Einsatz erfolgen soll. Jetzt sind weitere Einzelheiten zum IDS-Einsatz festzulegen. Anschließend ist ein geeignetes IDS-Produkt auszuwählen und zu beschaffen. Diese Phase des Leitfadens richtet sich an das IT-Sicherheitsmanagement bzw. an Mitarbeiter (Projektteam), die mit der Feinkonzeption und Produktauswahl beauftragt wurden.

Arbeitsschritte dieser Phase sind:

1. Feinkonzeption
2. Produktauswahl
3. Produktbeschaffung

3.5.1 Feinkonzeption

In der Phase „Grobkonzept und Anforderungsanalyse“ wurden Soll-Anforderungen und Soll-Einsatzweise für ein einzusetzendes IDS beschrieben. Im Rahmen der Entscheidungsvorlage ausgearbeitete Lösungsansätze können hiervon abweichen, falls z. B. marktverfügbare IDS-Produkte nur eine Teilmenge der Anforderungen erfüllen, eine Spezialentwicklung jedoch aus Kostengründen abgelehnt wird. Bei der Feinkonzeption sind daher zunächst Zielsetzungen, Anforderungsanalyse und Grobkonzept dem im Rahmen der Managemententscheidung verabschiedeten Lösungsansatz anzupassen.

Im Rahmen des Feinkonzepts sind die Einzelheiten zum IDS-Einsatz festzulegen, die unabhängig davon sind, welches IDS-Produkt letztlich eingesetzt wird[8]. Hierzu zählen:

- Ggf. für den Einsatz des IDS erforderliche Änderungen an der bestehenden Netzinfrastruktur.
- Festlegung der Art des Abgriffs des Netzverkehrs beim Einsatz von Netzsensoren. Unterschiedliche Möglichkeiten (TAP, Hub, Switch) werden in Anhang 4.4.1 kurz erläutert.
- Ermittlung der Komponenten, die zusätzlich für die technische Integration des IDS benötigt werden (Hub, TAPs, Switches, ggf. Router, zusätzliche Interfaces für bestehende Rechner).
- Klärung, ob und welche Konfigurationsänderungen an bestehenden Komponenten erforderlich sind.

Falls Komponenten lastverteilt oder im Standby betrieben werden, sind folgende weitere Punkte im Rahmen des Feinkonzepts zu klären:

- Lastverteilung:

  Es ist festzulegen, in welcher Weise ein Abgriff des Netzverkehrs und ein Einsatz von Netzsensoren zu erfolgen hat, damit der Netzverkehr vollständig überwacht wird. Unterschiedliche Ansätze hierzu sind in Anhang 4.4.2 angegeben.

- Multicast-Betrieb[9]:

  Multicast ist eine häufig genutzte Form der Lastverteilung, bei der mehrere Systeme unter derselben Adresse (z. B. IP- und MAC-Adresse) angesprochen werden und die Verarbeitung eingehender Daten/Verbindungen zwischen den Systemen verteilt wird. Dabei entsteht die Problematik, den zu

---

[8] Viele Einzelheiten des IDS-Einsatzes sind jedoch produktabhängig und können daher erst nach der Produktauswahl festgelegt werden. Dies betrifft z. B. die Kommunikation zwischen den IDS-Komponenten sowie die Konfiguration des IDS.

[9] Gemeint ist hier nicht ein IP-Multicast, bei dem mehrere Rechner mit unterschiedlichen IP-Adressen Datenpakete mit einer bestimmten IP-Zieladresse (aus dem Multicast-Adressbereich) annehmen und verarbeiten.

überwachenden Netzverkehr einerseits vollständig und andererseits nur genau einmal abzugreifen. Problematik und Lösungsmöglichkeiten werden in Anhang 4.4.3 näher erläutert.

- Standby-Betrieb:

  Es ist zu entscheiden, ob auch im Standby-Fall eine Überwachung erfolgen soll. Falls ja, müssen zusätzliche Netz- und Hostsensoren vorgesehen werden, um die im Standby-Fall genutzten Übertragungswege und IT-Systeme in die Überwachung einzubeziehen. Gegen die Überwachung im Standby-Fall spricht, dass dieser im Allgemeinen selten eintritt und nur von kurzer Dauer sein sollte. Daher steht dem Zusatzaufwand ein eher geringer Zusatznutzen gegenüber.

Da die IDS-Administration für wesentliche Aufgaben der nachfolgenden Phase „Integration“ zuständig ist, ist bereits jetzt festzulegen und im Feinkonzept zu dokumentieren, welche Mitarbeiter die Rolle der IDS-Administration übernehmen sollen.

Die Zuständigkeit für die Administration von Hostsensoren ist dabei zwischen IDS-Administration und dem Verantwortlichen, der für das vom Hostsensor überwachte System bzw. die überwachte Anwendung zuständig ist, abzustimmen. Folgende Aufgabenteilung wird dabei vorgeschlagen:

- Der System- bzw. Anwendungsverantwortliche legt die Kalibrierung des Hostsensors fest, d. h. er gibt vor, was der Hostsensor erkennen soll und wie das IDS hierauf reagieren soll. Diese Aufgabe sollte der System- bzw. Anwendungsverantwortliche deshalb übernehmen, da er sich mit Details des zu überwachenden Systems bzw. der zu überwachenden Anwendung auskennt und er den Nutzen aus dem Einsatz des Hostsensors zieht.
- Die IDS-Administration setzt die Vorgaben des System- bzw. Anwendungsverantwortlichen um. Diese Aufgabe sollte die IDS-Administration deshalb übernehmen, da sie sich mit der Konfiguration und Bedienung des IDS auskennt und die IDS-Konfiguration auf wenige Mitarbeiter konzentriert bleibt.

3.5.2 Produktauswahl

Auf Basis der Anforderungen ist ein geeignetes IDS-Produkt auszuwählen.

Im öffentlichen Bereich erfolgt hierzu typischerweise eine Ausschreibung auf Grundlage der Anforderungen und der im Feinkonzept dokumentierten Einsatzweise für ein IDS. Falls der Kreis der möglichen Produkte im Rahmen der Marktsichtung und Machbarkeitsermittlung bereits sinnvoll eingegrenzt werden konnte, ist dabei eine entsprechende Beschränkung der Ausschreibung sinnvoll.

Bei der Ausschreibung sind neben dem eigentlichen IDS-Produkt folgende Punkte zu berücksichtigen:

- Einführungsunterstützung durch den Auftragnehmer/Lieferanten.
- Produktwartung inklusive regelmäßiger Signatur-Updates.
- Erforderliche HW/SW-Plattformen.
- Ggf. erforderliche Zusatzsoftware. Manche IDS erfordern den Einsatz von Zusatzsoftware (wie etwa Webserver oder Datenbanken), die zusätzliche Kosten verursachen.
- Mitarbeiterschulung bzw. -einweisung.

Die Ausschreibung kann dabei einen unterschiedlichen Umfang aufweisen:

- In jedem Fall sollten IDS-Produkte, Einführungsunterstützung (inklusive Mitarbeitereinweisung) und Wartung für das IDS ausgeschrieben werden. Für Produkte, die zum Einsatz des IDS erforderlich sind (z. B. TAPs, Webserver, HW/SW-Plattformen) ist zu prüfen, ob sie sinnvoller und kostengünstiger direkt beschafft werden können (z. B. aufgrund bestehender Rahmenverträge) oder ob sie mit ausgeschrieben werden, um eine Komplettlösung aus einer Hand zu erhalten.
- Darüber hinaus kann die Ausschreibung die vollständige Integration des IDS in die Einsatzumgebung inklusive Erstkalibrierung des IDS umfassen. Voraussetzung hierfür ist jedoch, dass die

Einsatzziele des IDS so konkret beschrieben sind, dass sie als Abnahmekriterien für eine erfolgreiche IDS-Integration dienen können.

- Alternativ kann neben der Integration auch der IDS-Betrieb mit ausgeschrieben werden. Neben den zuvor genannten Punkten sind dabei zusätzlich die Argumente pro und contra eines IDS-Outsourcing zu beachten (vgl. Kapitel „Outsourcing“ im Grundlagendokument). Sicherheitsrelevante Bedingungen für ein Outsourcing sind in die Ausschreibung aufzunehmen.

Im privatwirtschaftlichen Bereich ist häufig bereits mit der Entscheidung für einen Lösungsansatz im Rahmen der Entscheidungsvorlage auch eine Produktentscheidung gefallen. In diesem Fall werden der Hersteller oder Lieferanten direkt angesprochen und um ein Angebot gebeten. Falls sich mehrere Produkte im Rahmen der Marktsichtung für den ausgewählten Lösungsansatz als gleichwertig herausgestellt haben, werden typischerweise auf Basis der Anforderungen und des Feinkonzepts Angebote von mehreren Herstellern bzw. Lieferanten eingeholt.

Falls bei der Produktauswahl festgestellt wird, dass entweder keine Produkte am Markt verfügbar sind, welche die Anforderungen hinreichend abdecken, oder die anzusetzenden Kosten deutlich von den in der Entscheidungsvorlage abgeschätzten Kosten abweichen, ist eine Überarbeitung der Entscheidungsvorlage erforderlich.

Die Zustimmung des Betriebs- bzw. Personalrats und des Datenschutzbeauftragten zum Einsatz des ausgewählten IDS-Produkts in der im Feinkonzept spezifizierten Weise ist einzuholen.

3.5.3 Produktbeschaffung

Die Produktbeschaffung umfasst insbesondere die Beschaffung der gesamten für den Einsatz des IDS erforderlichen Technik inklusive Wartung. Zusätzlich wird ggf. personelle Unterstützung für die Integration des IDS eingekauft.

Es wird empfohlen, vor dem Einkauf eines IDS-Produkts dessen technische Integrierbarkeit und Funktionalität hinsichtlich der Zielsetzungen im Rahmen eines Testbetriebs zu verifizieren. Am aussagekräftigsten ist hierzu ein Test des IDS in einer eigenen Testumgebung, die technisch weitgehend mit der Produktionsumgebung übereinstimmt.

3.6 Integration

In diesem Abschnitt wird das Vorgehen zur technischen und organisatorischen Integration des IDS beschrieben. Ziel des Leitfadens ist es, den Anwender bei der Vervollständigung des Feinkonzepts und bei der Realisierung und Integration des ausgewählten IDS auf der Grundlage der Vorgaben des Feinkonzepts zu unterstützen. Adressaten dieser Phase sind das IT-Sicherheitsmanagement bzw. das IDS-Projektteam, die IDS-Administration und die Systemadministration.

Die Integration und Konfiguration des IDS erfolgt zusammen mit der Systemadministration und der IDS-Administration. Folgende Arbeitspakete sind zu berücksichtigen:

- Vorbereitung der technischen Infrastruktur auf die Integration
- Integration und Inbetriebnahme des IDS
- Kalibrierung der Sensoren
- Aufnahme der Überwachungsziele in den Sicherheitsstandard (Policy)
- Zuweisung von IDS-Funktionen an Organisationseinheiten
- Festlegung der Eskalation bei IDS-Alarmen
- Schulung der IDS-Funktionsträger
- Vereinbarungen über den IDS-Betrieb mit dem Betriebs- bzw. Personalrat
- Integration in das Change-Management
- Festlegung von Verfahrensweisen zur Prüfung der Funktionsfähigkeit der Sensoren

3.6.1 Vorbereitung der technischen Infrastruktur auf die Integration

Als Voraussetzung für die Integration des IDS sind zunächst die für die Kommunikation zwischen den IDS-Komponenten erforderlichen Kommunikationsbeziehungen im Detail zu spezifizieren und im Feinkonzept zu dokumentieren[10]. Dies betrifft insbesondere verwendete Portnummern und IP-Adressen.

Darauf folgend ist die technische Infrastruktur gemäß der Vorgaben aus dem Feinkonzept für die Integration des IDS vorzubereiten. Dies umfasst die folgenden Schritte:

1. Installation und Konfiguration der für das IDS benötigten Hardware- und Systemplattformen, sofern keine Appliances zum Einsatz kommen.
2. Integration (oder Anpassung) von Komponenten zum Abgriff des Netzverkehrs (Hub, Switch, TAP) an den zu überwachenden Positionen.
3. Integration der Plattformen für die IDS-Komponenten in die Infrastruktur. Damit verbunden ist auch die ggf. erforderliche Integration weiterer Komponenten (wie z. B. zusätzliche Paketfilter zur Entkopplung eines IDS-Netzes vom Produktionsnetz).
4. Durchführung der notwendigen Konfigurationsänderungen an Switches, Paketfiltern und Applikations-Gateways zur Freigabe der erforderlichen Kommunikationsbeziehungen. Dies betrifft
   - die IDS-Kommunikation zwischen Sensoren und Management- und Auswertungsstation,
   - den Remote-Zugriff von internen Clients auf die Management- und Auswertungsstation sowie

[10] Details der Kommunikationsbeziehungen können erst jetzt festgelegt werden, da sie von IDS zu IDS verschieden sind.

- die für Intrusion-Response-Funktionen erforderlichen Kommunikationsbeziehungen (z. B. Versenden von E-Mail durch die Auswertungsstation).

Falls die durchgeführten Aktivitäten die im Feinkonzept beschriebenen Vorgaben verfeinern oder ergänzen, ist das Feinkonzept entsprechend anzupassen.

3.6.2 Integration und Inbetriebnahme des IDS

Auf Basis der vorbereiteten technischen Infrastruktur können jetzt die IDS-Komponenten integriert und in Betrieb genommen werden. Die Integration umfasst folgende Schritte:

1. Installation und Inbetriebnahme der Management- und Auswertungsstation

   Dabei sind folgende Punkte zu beachten:

   - Die Installation und Inbetriebnahme umfasst auch ggf. erforderliche weitere Komponenten wie Datenbank oder Webserver.
   - Marktverfügbare IDS-Produkte weisen im Allgemeinen keine Benutzer- und Rechteverwaltung auf. Falls diese erforderlich ist, kann sie ggf. beschränkt auf Systemebene oder - bei webbasierten Oberflächen - im Webserver realisiert werden.
   - Sofern erforderlich ist der Remote-Zugriff auf die Management- und Auswertungsstation zu realisieren.
   - Die Intrusion-Response-Funktionen sind einzurichten und zu konfigurieren.

2. Schrittweise Installation und Inbetriebnahme der Sensoren

   Die Installation und Inbetriebnahme sollten Sensor für Sensor erfolgen. Dabei sollten zunächst Netzsensoren und danach Hostsensoren installiert und in Betrieb genommen werden, da die Integration von Netzsensoren unabhängig von bestehenden Systemen und daher typischerweise unproblematischer ist, als die Integration von Hostsensoren.

   Als Reihenfolge für die Inbetriebnahme der Netzsensoren empfiehlt sich ein Vorgehen von innen nach außen. Dies liegt darin begründet, dass weiter innen (zum internen Netz hin) bereits viele Angriffe durch vorgeschaltete Schutzkomponenten (Paketfilter, Applikations-Gateway) ausgefiltert wurden und für dort platzierte Netzsensoren daher sowohl die zu erwartende Anzahl gemeldeter Ereignisse geringer ist als auch die erkannten Ereignisse mit höherer Wahrscheinlichkeit sicherheitskritisch sind.

   Für jeden Sensor sind folgende Schritte durchzuführen:

   2.1. Installation des Sensors.

   2.2. Anbindung des Sensors an die Management- und Auswertungsstation sowie Registrierung des Sensors bei der Management- und Auswertungsstation.

   2.3. Es wird empfohlen, zu testen, ob der Sensor Zugriff auf die zu überwachenden Daten (Netzverkehr, Logdaten) hat. Ebenfalls sollte verifiziert werden, dass die Managementstation den Ausfall des Sensors sowie dessen erneute Aktivierung automatisch erkennt.

   2.4. Kalibrierung des Sensors.

3.6.3 Kalibrierung der Sensoren

Im Rahmen der Kalibrierung wird für jeden Sensor festgelegt, was der Sensor erkennen soll und wie er - bzw. das IDS - auf das erkannte Ereignis reagieren soll. Das Erreichen der Einsatzziele hängt daher wesentlich von der Kalibrierung des IDS ab.

Einzelne Aktivitäten zur Kalibrierung sind detailliert in Anhang 4.5.2 aufgeführt. Da eine vollständige Kalibrierung grundsätzlich die Berücksichtigung jeder Signatur[11] erfordert und die Anzahl der Signaturen heutiger IDS sehr hoch ist (bis zu einigen 1000), ist eine vollständige Kalibrierung des Sensors im Rahmen der Inbetriebnahme äußerst aufwändig.

Empfohlen wird daher ein zweistufiges Vorgehen, bestehend aus einer **Basiskalibrierung** im Rahmen der Inbetriebnahme und der **Verfeinerung der Kalibrierung** im laufenden Betrieb.

Art und Möglichkeiten der Festlegung von Reaktionen auf erkannte Ereignisse unterscheiden sich von IDS zu IDS. Für die Beschreibung eines generalisierten Vorgehens zur Kalibrierung wird an dieser Stelle zwischen folgenden IDS-Reaktionen (Intrusion-Response) unterschieden:

- Alarmierung

  Eine Alarmierung ist für Signaturen vorzusehen, bei denen die zugrunde liegenden Ereignisse mit hoher Wahrscheinlichkeit schadenverursachend sind. Für die Signaturen sind dabei Alarmlevel festzulegen.

- Protokollierung zur Nachverfolgung

  Ereignisse werden zur Nachverfolgung protokolliert, falls die Auswirkungen des der Signatur zugrunde liegenden Ereignisses bislang nicht geklärt wurden, das Ereignis abhängig von Randbedingungen sehr unterschiedliche Auswirkungen haben kann oder die Signatur eine hohe Wahrscheinlichkeit von Fehlalarmen aufweist.

- Protokollierung für Auswertungszwecke

  Das der Signatur zugrunde liegende Ereignis hat keine schädlichen Auswirkungen, wird jedoch für Auswertungszwecke protokolliert.

- Deaktivierung

  Eine Signatur wird vollständig deaktiviert, wenn die durch die Signatur erkannten Ereignisse nachweislich unschädlich und auch für Auswertungszwecke nicht relevant sind.

- Protokollierung als „Unbearbeitet“

  Für Signaturen, deren zugrunde liegenden Ereignisse bislang nicht bewertet bzw. eingestuft wurden, sollte eine spezifische Kennzeichnung bei der Protokollierung vorgesehen werden.

Basiskalibrierung

Im Rahmen der Basiskalibrierung wird die Reaktion des IDS insbesondere für Signaturen festgelegt, die besonders relevant für die Einsatzziele des IDS sind. Hierzu kann auch die Parametrisierung bestehender Signaturen oder die Programmierung neuer Signaturen erforderlich sein. Des Weiteren werden die Signaturen des IDS deaktiviert, die zum Erreichen der Einsatzziele irrelevant sind.

- Für Signaturen, bei denen die zugrunde liegenden Ereignisse mit hoher Wahrscheinlichkeit schadenverursachend sind, ist eine Alarmierung vorzusehen. Beispiele:
  - Ein interner Client oder Server reagiert auf einen Netbus Scan aus dem Internet, d. h. der Angreifer ist im Begriff, die Kontrolle über den betreffenden Rechner zu übernehmen.
  - Ein Telnet-Request aus dem Internet auf ein geschütztes System ist unkritisch und ggf. zu Auswertungszwecken zu protokollieren. Alarmiert werden sollte, wenn das geschützte System mit einem Acknowledge reagiert.
- Signaturen, bei denen die zugrunde liegenden Ereignisse nachweislich keine Schadenswirkung auf die zu schützende IT-Infrastruktur haben, können deaktiviert werden. Für Auswertungszwecke kann es dennoch sinnvoll sein, auch diese Ereignisse zu protokollieren. Beispiele:

[11] Unter Signatur wird hier allgemein - unabhängig von der Verfahrensweise - ein Mechanismus zur Erkennung eines bestimmten Ereignisses verstanden.

- Falls ein Apache Webserver eingesetzt wird, können Angriffssignaturen, die speziell für den Microsoft Internet Information Server vorgesehen sind, deaktiviert werden.
- Falls auf einem Webserver lediglich statische Web-Seiten bereitgestellt werden, sind Angriffe, die auf Schwächen von CGI-Scripten basieren, nicht relevant. Die entsprechenden Signaturen können deaktiviert werden.
- Falls in einem zu schützendem Teilnetz ausschließlich UNIX-Systeme betrieben werden, können sämtliche Windows-spezifischen Angriffssignaturen deaktiviert werden.
- Falls sämtliche zu schützenden Server-Systeme aufgrund installierter Security-Patches gegen einen bestimmten Angriff resistent sind, kann die zugehörige Signatur deaktiviert werden.

- Für alle sonstigen Signaturen wird zunächst die Protokollierung als „Unbearbeitet“ vorgesehen.

Verfeinerung der Kalibrierung

Im Verlauf des IDS-Betriebs erfolgt die Verfeinerung der Kalibrierung. Die möglichen und realen Auswirkungen gemeldeter Ereignisse werden untersucht. Auf dieser Basis werden die zugehörigen Signaturen neu bewertet.

Ein Beispiel für den typischen zeitlichen Verlauf der Kalibrierung ist in Abbildung 3-3 dargestellt. Dabei wurde davon ausgegangen, dass im Rahmen der Basiskalibrierung ca. 10% der Signaturen deaktiviert wurden, für ca. 3% eine Alarmierung vorgesehen wurde und der Rest zur Verfolgung eingestuft wurde[12]. Anfänglich besteht deshalb ein hoher Aufwand zur Nachverfolgung der IDS-Meldungen und Verfeinerung der Kalibrierung. Mit der Zeit wird für mehr und mehr Signaturen geklärt, ob die zugrunde liegenden Ereignisse sicherheitskritisch sind, ob eine Protokollierung (für Auswertungszwecke) ausreicht oder ob die Signatur ganz deaktiviert werden kann. Parallel wächst die Menge der Erfahrungen der IDS-Administration und der im Mittel erforderliche Zeitaufwand für die manuelle Analyse zu verfolgender Ereignisse nimmt ab. Im Beispiel reduziert sich der Anteil der Signaturen, die eine Nachverfolgung bzw. Reaktion erfordern, schließlich auf ca. 25% (15% Verfolgung und 10% Alarmierung). Hierdurch entsteht für die IDS-Administration ein zeitlicher Freiraum, der z. B. zur Kalibrierung weiterer Sensoren genutzt werden kann.

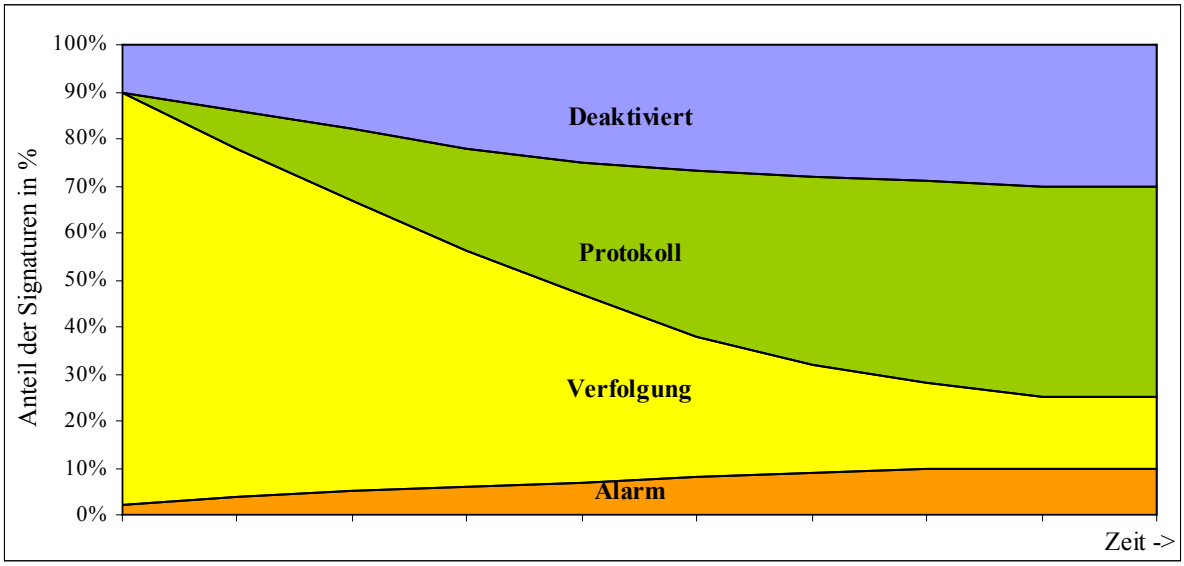

Abbildung 3-3: Beispiel eines typischen zeitlichen Verlaufs der Kalibrierung

[12] Unter den zur Verfolgung eingestuften Signaturen befinden sich zunächst auch die als „unbearbeitet“ markierten Signaturen, die in der Abbildung nicht separat dargestellt sind.

Grundsätze für die Kalibrierung

- Es empfiehlt sich, zurückhaltend mit der Festlegung von Alarmen umzugehen. Falls das IDS einige Male alarmiert und sich die zugrunde liegenden Ereignisse als ungefährlich herausstellen, stumpft die Sensibilität des Incident-Response-Personals schnell ab und mit ihr die Akzeptanz des IDS als relevantes Instrument zur Erkennung von Sicherheitsverletzungen.
- Je detaillierter die Einsatzziele des IDS formuliert wurden und je genauer spezifiziert ist, was erkannt werden soll, desto einfacher gestaltet sich die Kalibrierung.
- Für Ereignisse, die gemäß Konfiguration anderer Sicherheitskomponenten oder vorgegebener Richtlinien nicht auftreten sollten, können die zugehörigen Signaturen aktiviert werden. Ihr Auftreten stellt eine Anomalie dar und weist möglicherweise auf die Fehlkonfiguration anderer Komponenten oder auf sicherheitsgefährdende Aktivitäten hin.
- Vor der Festlegung automatischer aktiver Reaktionen, wie etwa der Unterbrechung von Kommunikationsverbindungen oder der temporären Rekonfiguration einer Firewall, sind deren Auswirkungen im Fall von Fehlalarmen genau zu prüfen. Aktive Reaktionen des IDS können ggf. von Angreifern durch Herbeiführen von Fehlalarmen provoziert werden. Es ist sicherzustellen, dass von den festgelegten Reaktionen auch in diesem Fall keine Gefährdung ausgeht.
- Die Festlegung aktiver Reaktionen ist für solche Signaturen sinnvoll, durch die entstandene Schäden erkannt werden und bei denen eine Schadensbehebung oder -eingrenzung durch die Reaktion möglich ist. Ein Beispiel hierfür ist die automatische Rekonstruktion einer sensitiven Datei, nachdem eine Integritätsverletzung dieser Datei erkannt wurde.

3.6.4 Aufnahme der Überwachungsziele in den Sicherheitsstandard (Policy)

Sicherheitsstandards im Sinne einer Policy, die von der konkreten Technik und Organisation abstrahieren, spiegeln Sicherheitsziele und Leitsätze des Unternehmens wieder. Auf dieser Ebene sollte der Einsatz des IDS als Überwachungsinstrument zur Verbesserung des Schutzes am Netzübergang zum Internet verankert werden. Hierdurch wird die Entscheidung des Managements, IDS zu den beschriebenen Zwecken einzusetzen, dokumentiert und im Unternehmen kommuniziert.

3.6.5 Zuweisung der IDS-Funktionen an Organisationseinheiten

Im Rahmen des Grobkonzepts wurde bereits überlegt, welche Organisationseinheiten/Rollen bzw. Mitarbeiter die Funktion von IDS-Administration, IDS-Monitoring und IDS-Verantwortlichem übernehmen sollen. Diese Zuordnung ist jetzt auf Grundlage der konkretisierten Informationen zu überprüfen und bei Bedarf anzupassen.

Die Aufgabenbeschreibungen der für die Übernahme der Funktionen vorgesehenen Stellen sind um die entsprechenden Aufgaben, Zuständigkeiten und Verantwortlichkeiten zu erweitern[13]. Ein Überblick über die zuzuordnenden Aufgaben, Zuständigkeiten und Verantwortlichkeiten ist in Anhang 4.5.1 gegeben.

3.6.6 Festlegung der Eskalation bei IDS-Alarmen

Wie auf IDS-Alarme zu reagieren ist wird im Rahmen eines Eskalationsplans festgelegt. Ein Beispiel für solche Festlegungen ist in Anhang 4.4.4 angegeben.

[13] Die Zuordnung ist erst jetzt sinnvoll, da vor der Produktauswahl nicht feststand, ob ein IDS-Einsatz erfolgt.

Zweck des IDS-Eskalationsplans

Der IDS-Eskalationsplan dient dazu, Mitarbeitern mit begrenzten technischen Kenntnissen (IDS-Monitoring), die Alarme entgegennehmen, dazu anzuleiten, wie sie bei Eintritt der Alarme zu reagieren haben. Der Plan muss so gestaltet sein, dass mit seiner Hilfe zu einem gegebenen Alarm in einfacher Weise die auszuführenden Eskalationsschritte ermittelt werden können.

Typischerweise dienen dabei vom IDS angezeigte Alarmlevel zur Einordnung des Alarms. Es kann jedoch auch die Festlegung ereignisspezifischer Eskalationen erforderlich sein.

Des Weiteren kann im Rahmen des Eskalationsplans festgelegt werden, unter welchen Bedingungen vom IDS-Incident-Response weiter zu eskalieren ist (etwa zum Abteilungsleiter).

Erstellung, Aktualisierung und Inhalt des IDS-Eskalationsplans

Verantwortlich für die Erstellung und regelmäßige Aktualisierung des IDS-Eskalationsplans ist der IDS-Manager. Er legt in Abstimmung mit dem IDS-Incident-Response und der IDS-Administration die jeweils erforderliche Eskalation fest. Im Rahmen der Kalibrierung ist für jede Signatur, für die eine IDS-Alarmierung vorgesehen wird, durch die IDS-Administration ein Alarmlevel einzustellen. Es ist zu prüfen, ob die im Eskalationsplan vorgesehen Eskalation geeignet ist. Bei Bedarf ist der Eskalationsplan anzupassen.

3.6.7 Schulung der IDS-Funktionsträger

Die Mitarbeiter, die in den IDS-Rollen wie IDS-Administration, IDS-Monitoring und IDS-Incident-Response tätig werden, sind in ihre Aufgabenstellungen einzuweisen und zu schulen. Die erforderlichen Kenntnisse der Funktionsträger wurden bereits in Kapitel 3.2.6 aufgeführt. Im Folgenden werden kurz für die Schulung und Einweisung relevante Punkte zu den unterschiedlichen Rollen aufgeführt.

IDS-Administration

Die Vermittlung der erforderlichen Grundlagen der Anwendung des IDS kann direkt im Rahmen der Hersteller- oder Integrator-Unterstützung bei der Installation und Inbetriebnahme des IDS erfolgen, die von den Mitarbeitern der IDS-Administration begleitet wird. Details zur Anwendung des IDS, wie insbesondere die Interpretation der Meldungen des IDS und Einzelheiten zur Kalibrierung, werden im Verlauf des IDS-Einsatzes erlernt. Wichtig ist, dass die IDS-Administration zu Beginn des IDS-Einsatzes die Grundlagen und Voraussetzungen dazu erlernt, wie das IDS im Betrieb als Werkzeug zu nutzen und den jeweiligen Zielsetzungen anzupassen ist. Die Grundlagen hierzu umfassen Kenntnisse darüber,

- wie das IDS zu bedienen ist (Kalibrierung, Auswertung des Ereignisprotokolls, etc.),
- wie ermittelt werden kann, wie die Ereigniserkennung durch die Signatur im Detail erfolgt,
- wie Signaturen verfeinert oder neue Signaturen erstellt werden können,
- wo Informationen über Angriffe und Sicherheitslücken abgefragt werden können.

IDS-Monitoring

Nach Fertigstellung einer ersten Version des IDS-Eskalationsplans sind die Mitarbeiter des IDS-Monitoring in dessen Anwendung einzuweisen. Dies betrifft die Ableitung der durchzuführenden Eskalationsschritte aus IDS-Alarmen (wer ist mit welcher Dringlichkeit zu benachrichtigen). Die Einweisung kann durch die IDS-Administration vorgenommen werden.

IDS-Manager

Der IDS-Manager kann sich die für ihn erforderlichen IDS-spezifischen Kenntnisse von der IDS-Administration erläutern lassen. Diese umfassen Nutzen und Grenzen des eingesetzten IDS, unterstützte Sensorarten sowie kontrollierbare Netze und Systeme. Kenntnisse über die Einsatzweise und Einsatzziele des IDS sowie der Organisation des Incident-Response erhält der IDS-Manager im Rahmen seiner Tätigkeit.

IDS-Incident-Response

Die angemessene Reaktion auf IDS-Alarmierungen verlangt das Vermögen zur realistischen Einschätzung der vom IDS gemeldeten Alarme.

Dies setzt Basiskenntnisse in der IDS-Bedienung voraus, z. B. zur Abfrage von Kontextinformationen zu Angriffen. Die Einweisung in die IDS-Bedienung kann durch die IDS-Administration erfolgen. Daneben sind jeweils aktuelle Kenntnisse über relevante Angriffe und Sicherheitslücken sowie über die Möglichkeiten des IDS zu deren Erkennung erforderlich. Um diese Kenntnisse aktuell zu halten, ist eine regelmäßige Abstimmung bzw. ein regelmäßiger Informationsaustausch zwischen IDS-Administration und IDS-Incident-Response notwendig.

3.6.8 Vereinbarungen über den IDS-Betrieb mit dem Betriebs- bzw. Personalrat

Die von IDS aufgezeichneten Daten sind teilweise personenbezogen bzw. lassen die Zuordnung von Personen zu bestimmten Aktivitäten zu. Beispiele hierfür sind

- die Aufzeichnung unberechtigter Zugriffsversuche auf Daten,
- die Aufzeichnung unberechtigter Zugangsversuche zu Anwendungen,
- die Aufzeichnung der IP-Adressen oder Domain-/Rechnernamen, von denen aus Angriffe oder Angriffsversuche gestartet wurden.

Da IDS über weitgehende Protokollierungs- und Auswertungsfunktionen verfügen, können sie des Weiteren dazu missbraucht werden, Verhaltensweisen von Mitarbeitern zu kontrollieren.

Beim Einsatz von IDS ist daher darauf zu achten, dass rechtliche Anforderungen sowohl des Datenschutzes als auch der Arbeitnehmer-Mitbestimmung berücksichtigt werden. Es wird empfohlen, hierzu geeignete Anforderungen zum IDS-Betrieb mit dem Betriebs- bzw. Personalrat sowie dem Datenschutzbeauftragten abzustimmen und umzusetzen. Entsprechende Anforderungen sind beispielhaft in Anhang 4.5.3 aufgeführt.

Eine Übersicht über die zu berücksichtigenden rechtlichen Vorgaben ist im Dokument „Einführung von Intrusion-Detection-Systemen - Rechtliche Aspekte beim Einsatz von IDS“ angegeben.

3.6.9 Integration des IDS in das Change-Management

Bei der Integration des IDS in das Change-Management ist zu beachten, dass es für ein IDS besonders wichtig ist, Aktualisierungen zeitnah durchzuführen, da die Überwachungsfunktionalität des IDS wesentlich von dessen Aktualität abhängt. Dies betrifft insbesondere die folgenden Änderungen bzw. Aktualisierungen, die bereits in der Aufgabenbeschreibung der IDS-Rollen berücksichtigt wurden (siehe Anhang 4.5.1):

- Zeitnahes Einspielen von Signatur-Updates und Konfiguration bzw. Kalibrierung der neuen Signaturen.

- Zeitnahes Einspielen vorliegender Software-Patches für das IDS.
- Zeitnahe Anpassung des IDS bei Änderungen der zu schützenden IT-Infrastruktur. Relevant sind dabei insbesondere folgenden Änderungen:
  - Änderungen der Konfiguration zu schützender Systeme und Anwendungen,
  - Änderungen der überwachten Netz-Infrastruktur,
  - Änderungen der Konfiguration von anderer Schutzkomponenten (Firewall, Paketfilter, etc.).

3.6.10 Prüfung der Funktionsfähigkeit der Sensoren

Bereits bei der Integration des IDS sollte darüber nachgedacht werden, wie zukünftig im Betrieb des IDS die Funktionsfähigkeit der Sensoren geprüft werden kann. Dies gilt insbesondere für Sensoren, die aufgrund ihrer Platzierung und Kalibrierung im Normalfall kaum Ereignisse melden.

Die Funktionsfähigkeit von Sensoren, die häufig Angriffsversuchen ausgesetzt sind, ist implizit dadurch verifizierbar, dass sich Anzahl und Art der Ereignismeldungen normal verhalten. Ob das Verhalten normal ist oder nicht, entscheidet dabei die IDS-Administration auf Basis von Erfahrungswerten. Eine explizite Funktionsprüfung des Sensors sollte durchgeführt werden, falls signifikant weniger Ereignisse vom Sensor gemeldet werden als normal.

Für Sensoren, die aufgrund ihrer Platzierung und Kalibrierung im Normalfall kaum Ereignisse melden, sind regelmäßig explizite Funktionsprüfungen vorzusehen, z. B. durch das Einspielen von Angriffsmustern, die durch den Sensor gemeldet werden sollten.

Eine Möglichkeit die Funktion eines solchen Sensors zu prüfen, besteht darin, den Sensor so zu kalibrieren, dass er einige für die IT-Infrastruktur unkritische Ereignisse meldet, und diese Ereignisse zur Funktionsprüfung zu nutzen. Diese Ereignisse können dann auch zur Automatisierung der Funktionsprüfung eingesetzt werden, indem sie - z. B. skriptgesteuert - regelmäßig automatisch eingespielt werden. Es ist zu beachten, dass diese Prüfung lediglich die grundsätzliche Funktionsfähigkeit des Sensors nachweist, jedoch nicht, dass der Sensor insgesamt wie spezifiziert arbeitet.

3.7 Betrieb des IDS

Vor der Aufnahme des regulären IDS-Betriebs sind sämtliche betriebsrelevanten Punkte zu klären und in einem IDS-Betriebshandbuch zu dokumentieren. Das Vorgehen hierzu wurde bei der Integration von IDS im Kapitel 3.6 beschrieben. Ein Dokumentenrahmen für ein Betriebshandbuch ist im Anhang 4.6.1 angegeben.

Als wesentliche betriebsrelevante Prozesse und Aktivitäten sind insbesondere zu betrachten:

- Verfeinerung der IDS-Kalibrierung
- Nachverfolgung von Ereignissen
- Reaktion auf IDS-Alarme
- Aktualisierung der IDS-Signaturen
- Aktualisierung des IDS
- Begleitung der IT-Planung und Entwicklung
- Anpassung des IDS bei Änderungen der zu schützenden IT-Infrastruktur
- Datensicherung des IDS

Diese sind Anhang 4.6.2 beschrieben.

3.8 Revision

In diesem Kapitel werden Vorgehensweisen für die Revision des IDS-Einsatzes beschrieben. Es wendet sich an das IT-Sicherheitsmanagement bzw. das IDS-Projektteam und an für die Revision zuständige Mitarbeiter. Für den Einsatz des IDS als ergänzende Schutzmaßnahme am Netzübergang zum Internet wird empfohlen, die Revision des IDS und der Firewall-Systeme am Netzübergang gemeinsam durchzuführen.

Die Häufigkeit und Tiefe der Prüfungen richtet sich nach dem zu erreichenden Sicherheitsniveau. Auch für diese Parameter wird empfohlen, sie an die Revision des Firewall-Systems anzulehnen.

Den Ausgangspunkt und die Grundlage für die Revision des IDS bilden die Dokumente, in denen die Einsatzweise und der aktuelle Stand des IDS beschrieben sind. Diese sind

- der IDS-Eskalationsplan,
- das Betriebshandbuch des IDS und
- die Dokumentation der Softwareversionen und Aktualisierungen.

Grundlegende Revisionsschritte

Bei der Revision des IDS können grundsätzlich drei aufeinander aufbauende Schritte unterschieden werden:

1. Prüfung der Dokumentation

   Bei der Prüfung der Dokumentation wird geprüft, ob die zuvor aufgeführten Dokumente vorliegen und inhaltlich vollständig sind. Eine Basis zur Kontrolle der Vollständigkeit können die im vorliegenden Leitfaden enthaltenen Beschreibungen bilden. Konkrete Fragestellungen und Prüfmethoden sind in Anhang 4.7.1 angegeben.

2. Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs

   Bei ordentlicher Dokumentation ist zu prüfen, ob der IDS-Einsatz und Betrieb gemäß dieser Dokumentation erfolgt. Hierzu ist die technische Einsatzweise des IDS zu verifizieren und die Umsetzung organisatorischer Maßnahmen im Umfeld des IDS zu prüfen. Konkrete Fragestellungen und Prüfmethoden sind in Anhang 4.7.2 angegeben.

3. Prüfung der Wirksamkeit des IDS und des Incident-Handling

   Die Prüfung der Wirksamkeit des IDS beinhaltet sowohl eine Kontrolle der Konfiguration und Kalibrierung des IDS als auch eine praktische Kontrolle der Wirksamkeit des IDS durch geeignete Penetrationstests. Es wird untersucht, ob die IDS-Sensoren Angriffe und Sicherheitsverletzungen erkennen und ob in der festgelegten Weise technisch und organisatorisch reagiert wird. Konkrete Fragestellungen und Prüfmethoden sind in Anhang 4.7.3 angegeben.

Unterschiedliche Vorgehensweisen für die Revision

Im Rahmen einer Revision lediglich die Dokumentation zu prüfen, ist nicht sinnvoll[14]. Aus diesem Grund wird zwischen zwei Vorgehensweisen mit verschiedenen Revisionstiefen unterschieden, die sich deutlich im Aufwand und in den notwendigen Kenntnissen des Revisors unterscheiden. In beiden Vorgehensweisen erfolgt keine vollständige Kontrolle sämtlicher zu prüfender Punkte. Vielmehr wird stich-

[14] Bei der Beschränkung der Prüfung auf die Dokumentation würde beispielsweise nicht geprüft, ob überhaupt ein IDS eingesetzt wird.

probenhaft ermittelt, ob der Einsatz des IDS und die flankierende Organisation den vorgegebenen, dokumentierten Anforderungen genügt.

- **Vorgehen 1: Prüfung der Rahmenbedingungen**

  Bei der Prüfung der Rahmenbedingungen werden alle Voraussetzungen für einen wirksamen IDS-Einsatz verifiziert, ohne die Wirksamkeit des IDS direkt zu prüfen. Die Prüfung der Rahmenbedingungen umfasst die o. g. Schritte der Prüfung der Dokumentation und der Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs.

  Die Prüfung erfordert vom Revisor lediglich grundlegende Kenntnisse über die eingesetzten Systeme und Netze. Sie wird mit Unterstützung der IDS-Administration durchgeführt.

- **Vorgehen 2: Vollständige Prüfung**

  Bei der vollständigen Prüfung wird über die Rahmenbedingungen hinaus auch die Wirksamkeit des IDS und Incident-Handlings geprüft. Sie umfasst die drei o. g. Revisionsschritte.

  Die Wirksamkeit des IDS wird dabei durch einen Penetrationstest verifiziert. Im Rahmen der vollständigen Prüfung ist es vorteilhaft, diesen Penetrationstest vor der Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs durchzuführen. Bei der Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs kann dann direkt geprüft werden, ob die im Rahmen der Penetration versuchten Angriffe und Sicherheitsverletzungen vom IDS gemeldet wurden.

  Die vollständige Prüfung des IDS erfordert vom Revisor ähnlich tiefgehende Kenntnisse wie die der IDS-Administration. Die Prüfung setzt Kenntnisse in folgenden Gebieten voraus:

  - Kenntnisse über die überwachten Netze, Systeme und Anwendungen
  - Kenntnisse über Techniken (Firewall, Router) zur Netzabsicherung
  - Aktuelle Kenntnisse über mögliche Angriffe auf Netze und Systeme
  - Kenntnisse über das eingesetzte IDS

  Sofern Mitarbeiter der Revision auf diesen Gebieten nicht über die entsprechenden Detailkenntnisse und Erfahrungen verfügen, wird empfohlen, die Revision durch einen Sicherheitsexperten begleiten zu lassen, der über die notwendigen Kenntnisse und Erfahrungen verfügt.

Revisionsrichtlinie

Richtlinien für die Revision des IDS sollten in einer Revisionsrichtlinie dokumentiert werden. Ein Dokumentenrahmen für eine Revisionsrichtlinie ist in Anhang 4.7.4 angegeben.

4 Anhang

4.1 Hilfsmittel für die Bedarfsfeststellung

4.1.1 Vorlage für Management-Einführung in das Thema IDS

Im Bereich infrastruktureller Maßnahmen ist der Einsatz von Alarmanlagen gängige Praxis. Auch wenn Sicherheitsbereiche bereits durch Wände, einbruchshemmende Türen und Fenster gut geschützt sind, wird auf den zusätzlichen Einsatz von Alarmanlagen im Allgemeinen nicht verzichtet.

Abgebildet auf die Ebene der IT-Kommunikation übernehmen IDS in vielerlei Hinsicht die Funktion von Alarmanlagen. Sie können Angriffe und Angriffsversuche im Netzverkehr aufspüren und Sicherheitsverletzungen in Systemen und Anwendungen feststellen.

Ihr Internet-Übergang ist sicherlich durch ein Firewall-System geschützt. Aber haben Sie auch schon eine Alarmanlage, die Ihnen mitteilt, wenn trotz Firewall Angriffe nach innen durchdringen oder Einbrüche in kritische Serversysteme erfolgen? Die Überwachung erfolgt dabei durch Sensoren, die entweder als eigenständige Systeme den Netzverkehr überwachen (Netzsensoren) oder als Agenten auf den zu überwachenden Systemen betrieben werden (Hostsensoren). Die Auswertung der gemeldeten Ereignisse und das Management der Sensoren erfolgen typischerweise über zentralisierte Konsolen.

Ein Firewall-System filtert den Datenfluss gemäß vorgegebener Regeln. Es lässt nur den zulässigen Verkehr passieren und bietet somit eine aktive Sicherheit. Die nachfolgenden Beispiele demonstrieren Grenzen von Firewall-Systemen, bei denen IDS nutzbringend eingesetzt werden können.

- **Überwachung der Funktion und Konfiguration der Firewall**

  Die IT-Komponenten des Firewall-Systems sind selbst Angriffen ausgesetzt. Des Weiteren sind gerade bei komplexen Kommunikationsanforderungen Fehlkonfigurationen der Firewall nicht auszuschließen. Mit einem IDS kann kontrolliert werden, ob die Firewall gemäß ihrer Policy arbeitet oder sicherheitskritischer Verkehr ins interne Netz gelangt.

- **Überwachung nicht ausreichend kontrollierter Dienste**

  Im allgemeinen prüft die Firewall zwar, wer mit wem über welche Ports kommuniziert, sie kann jedoch häufig nicht den Netzverkehr auf Ebene der Anwendung kontrollieren[15]. Gerade auf dieser Ebene finden jedoch viele Angriffe statt, die durch ein IDS erkannt werden können. Des Weiteren kann die Firewall getunnelte oder verschlüsselte Kommunikation nicht analysieren. Auch hier bieten IDS verbesserte Möglichkeiten zur Überwachung.

- **Erkennung von Angriffen über sonstige Zugänge**

  Firewall-Komponenten kontrollieren den Verkehr nur an einem bestimmten Punkt. Sie können nur Angriffe abwehren, die über sie laufen. Mit einem IDS können hingegen Angriffe unabhängig davon erkannt werden, über welchen Zugang sie erfolgen (z. B. auch Angriffe aus dem internem Netz).

Unabhängig von den Grenzen von Firewall-Systemen können IDS praktisch zu folgenden Zwecken genutzt werden:

[15] Eine Kontrolle auf Ebene der Anwendung würde den Einsatz von Applikations-Gateways erfordern, die im Allgemeinen nicht für sämtliche Dienste verfügbar sind.

- **Frühwarnfunktion bei der Erkennung von Angriffen**

  IDS können dazu eingesetzt werden, angriffsvorbereitende Aktivitäten zu erkennen. Dies bildet die Voraussetzung dafür, rechtzeitig Maßnahmen zur Angriffsabwehr einzuleiten.

- **Erkennung allgemeiner Systemstörungen**

  IDS können dazu dienen, allgemeine Systemstörungen zeitnah zu erkennen.

- **Erhöhung der Verfügbarkeit kritischer Systeme**

  Auf Basis der zeitnahen Erkennung von Angriffen, Sicherheitsverletzungen und Systemstörungen durch ein IDS können Ausfallzeiten verkürzt und resultierende Schäden verringert werden.

- **Rückverfolgung und Identifizierung von Angreifern**

  Mit einem IDS können detaillierte Kontextinformationen zu Angriffen aufgezeichnet werden, die eine Rückverfolgung von Angreifern erleichtern.

- **Automatische Reaktion bei erkannten Angriffen**

  IDS bieten zum Teil die Möglichkeit, bei erkannten Angriffen automatisch Gegenmaßnahmen einzuleiten.

- **Darstellung der Gefährdungssituation**

  Durch die Aufzeichnung von Angriffen und Angriffsversuchen kann die Gefährdungssituation des Internet-Übergangs dargestellt werden.

Diesen Einsatzzwecken stehen folgende Grenzen von IDS gegenüber:

- **IDS reagieren erst nach dem Angriff**

  IDS schützen nicht vor dem Eintreten von Angriffen. Sie können Angriffe und Sicherheitsverletzungen nicht aktiv abwehren, sondern sie lediglich erkennen und melden.

- **IDS erkennen nur Angriffe, auf die sie programmiert wurden**

  Wie auch Virenscanner müssen IDS daher regelmäßig aktualisiert werden. Des Weiteren müssen IDS so konfiguriert werden, dass sie genau die Angriffe erkennen, die für den jeweiligen Einsatzzweck relevant sind.

- **IDS erlauben keine exakte Angriffserkennung**

  IDS sind niemals frei von Fehlalarmen. Eine manuelle Untersuchung und Interpretation gemeldeter Ereignisse ist im Allgemeinen erforderlich. Daher ist die Einleitung automatischer Gegenmaßnahmen durch das IDS häufig nicht sinnvoll.

- **IDS erfordern ein Incident-Handling**[16]

  IDS sind nur dann nutzbringend, wenn auf die gemeldeten Ereignisse auch angemessen und zeitnah reagiert wird. Hierzu ist eine geeignete Organisation vorzuhalten.

Der Aufwand zum Aufbau und Betrieb eines IDS hängt stark von Art und Anzahl der eingesetzten Sensoren sowie der zu überwachenden IT-Infrastruktur ab[17].

[16] Incident-Handling = Maßnahmen zur Verfolgung von Sicherheitsvorfällen

[17] Eine grobe unverbindliche Abschätzung zur ergänzenden Absicherung eines 3-stufigen Internet-Übergangs durch ein IDS mit 2-3 Netzsensoren: 50 T€ Investitionen für Hard- und Software, 2 Personenmonate Konzeptions- und Integrationsaufwand sowie 5-8 Personentage monatlicher Betriebsaufwand (vgl. Kapitel 4.3.2).

4.1.2 Bewertete Einflussfaktoren

Nachstehend sind Faktoren aufgeführt, von denen es abhängt, ob der Einsatz eines IDS sinnvoll ist oder nicht.

- Architektur und Anzahl der Stufen des Netzübergangs
- Betriebsumgebung des Firewall-Systems
- Sonstige Übergänge zum Internet
- Anzahl und Kontrolle eingehend freigeschalteter Dienste
- Konfiguration des Firewall-Systems und flankierender Prozesse
- Regelmäßige Aktualisierung gefährdeter Komponenten
- Interaktion mit internen Systemen (betrifft insbesondere WWW-Applikationen)
- Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten
- Relevante Nutzenaspekte von IDS

Zu den Einflussfaktoren ist das Nutzenpotenzial von IDS hinsichtlich des jeweiligen Faktors unter Berücksichtigung alternativer Maßnahmen beschrieben und bewertet (von gering □□□□ bis hoch ■■■■).

E1. Architektur und Anzahl der Stufen des Netzübergangs

Wie viele Stufen hat der Netzübergang zum Internet?

☐ 1-Stufig		■■□□
☐ 2-Stufig		■■□□
☐ 3-Stufig		■■■■
☐ mehr als 3		■■■■

Bevor die Entscheidung für den Einsatz eines IDS gefällt wird, ist abzuwägen, ob nicht durch

- ein Änderung der Architektur des Netzübergangs,
- dem Einsatz weiterer aktiver Kontrollkomponenten und/oder
- der Einrichtung zusätzlicher Stufen im Netzübergang

die Sicherheit sinnvoller verbessert werden kann als durch Einführung eines IDS. Insbesondere betrifft dies Internet-Übergänge mit weniger als drei Stufen. Dabei ist zu beachten, dass IDS lediglich Angriffe und Sicherheitsverletzungen erkennen, ihre Möglichkeiten zur aktiven Abwehr von Angriffen jedoch äußerst begrenzt sind.

Die Funktionalität von Schutzkomponenten (Paketfilter, Applikations-Gateway) am Netzübergang kann z. B. durch

- unbeabsichtigte und unbemerkte Fehlkonfiguration von Komponenten,
- den Ausfall von Komponenten oder
- deren Beeinflussung durch Angreifer (etwa Ausnutzen von Implementierungsfehlern)

beeinträchtigt werden. Daher ist es für die Sicherheit eines Netzübergangs bedeutend, dass auch bei Fehlfunktion einer Komponente kein freier Internet-Zugriff auf interne Ressourcen gegeben ist (Fail-Safe). Durch eine Reihenschaltung mehrerer Komponenten lässt sich die Widerstandsfähigkeit des Internet-Übergangs erhöhen. Für den Übergang zum Internet wird ein dreistufiger Netzübergang empfohlen (siehe BSI-Empfehlung [BSI 1-02]). Falls es einem Angreifer gelingt, eine der Komponenten zu überwinden, ist so durch die verbleibenden Komponenten immer noch zumindest ein gewisser Schutz gegeben. Um dem gezielten Ausnutzen von Fehlern in Komponenten einzelner Hersteller vorzubeugen ist darüber hinaus zu empfehlen, Komponenten unterschiedlicher Hersteller zu verwenden.

E2. Betriebsumgebung des Firewall-Systems

Werden die Komponenten des Firewall-Systems in einer gesicherten Umgebung betrieben?

☐ Nein	Der Betrieb der Firewall-Komponenten in einer gesicherten Umgebung ist grundlegend für die Sicherheit des Netzübergangs. Z. B. ist sicherzustellen, dass Unberechtigte nicht in einfacher Weise Firewall-Komponenten physikalisch überbrücken können. Gleiches gilt auch für den Betrieb eines IDS.	☐☐☐☐
☐ Ja	Bei Einsatz eines IDS sollten auch die IDS-Komponenten in einer gesicherten Umgebung betrieben werden, so dass Manipulationen durch Unberechtigte weitgehend ausgeschlossen sind.	■■■■

E3. Sonstige Übergänge zum Internet

Besteht die Möglichkeit, dass es sonstige Netzübergänge ins Internet gibt?

Sonstige Übergänge könnten z. B. verursacht werden, durch

- **den Einsatz von Modems,**
- **die Verwendung von WLANs,**
- **weitere Internet-Übergänge z. B. an externen Liegenschaften.**

☐ Ja	Andere Übergänge sind möglich. In diesem Fall ist die zusätzliche Überwachung nur des betrachteten Internet-Übergangs durch ein IDS lediglich begrenzt sinnvoll. Ein IDS-Einsatz sollte im erweiterten Rahmen erfolgen und sämtliche Übergangsmöglichkeiten zum Internet berücksichtigen.	■■☐☐
☐ Nein	Es gibt keine sonstigen Übergänge in das Internet.	■■■■

Falls die Erkennung von Angriffen aus dem Internet eine wesentliche Zielsetzung darstellt, ist zu beachten, dass hierzu sämtliche möglichen Internet-Übergänge zu berücksichtigen sind. Falls neben dem betrachteten Internet-Übergang andere Übergänge möglich oder gegeben sind, hat dies in jedem Fall Auswirkungen auf die Einsatzweise des IDS (Platzierung von Sensoren, etc.). Ggf. ist das Ziel einer vollständigen Überwachung nicht erreichbar und ein IDS-Einsatz damit nur bedingt sinnvoll.

E4. Anzahl und Kontrolle eingehend freigeschalteter Dienste

Wie viele Dienste sind zwischen internem Netz und Internet freigeschaltet?

☐ Keine	Es kann überwacht werden, dass keine eingehenden Internet-Verbindungen über den Netzübergang oder auf anderen Wegen aufgebaut werden.	■■□□
☐ Wenige	Es sind lediglich die für Bürokommunikation üblicherweise genutzten Dienste freigeschaltet (eingehend: E-Mail, ausgehend: E-Mail, DNS, HTTP/HTTPS). Es kann überwacht werden, dass die freigeschalteten Dienste nicht missbräuchlich eingesetzt werden und dass keine spezifischen anderen Dienste genutzt werden.	■■■■
☐ Viele	Weitreichende Kommunikationsanforderungen erfordern die Freischaltung einer Vielzahl von Diensten. Es kann überwacht werden, dass die freigeschalteten Dienste nicht missbräuchlich eingesetzt werden und dass keine spezifischen anderen Dienste genutzt werden.	■■■■

Wie werden die Dienste durch das Firewall-System kontrolliert?

☐ Die meisten Dienste werden lediglich durch Paketfilter kontrolliert.	Falls es für eingehende Dienste praktische Möglichkeiten zur Verbesserung der Datenflusskontrolle gibt (z. B. durch ein Applikations-Gateway) sollten diese ausgeschöpft werden.	□□□□
	Falls Komponenten zur Verbesserung der Datenflusskontrolle für eingehende Dienste nicht marktverfügbar oder aus anderen Gründen nicht sinnvoll einsetzbar sind, kann die begrenzte Datenflusskontrolle durch Einsatz von IDS reaktiv verbessert werden.	■■■■
☐ Eingehende Internet-Dienste werden über Applikations-Gateways kontrolliert.	Durch den Einsatz von Applikations-Gateways ist bereits ein hoher Schutz gegeben. Verbleibende Restrisiken können durch den zusätzlichen Einsatz eines IDS verringert werden. Der Bedarf hängt vom konkreten Schutzbedarf ab.	■■■□
☐ Die Dienstnutzung erfolgt anonym	Falls die Einführung eines Authentisierungsverfahrens praktisch sinnvoll möglich ist, sollte dies Vorrang gegenüber der Einführung eines IDS haben.	□□□□
	Falls ein Einsatz von Authentisierungsverfahren praktisch nicht sinnvoll möglich ist, können die anonym aufgebauten Verbindungen durch das IDS überwacht werden.	■■■■
☐ Die Dienstnutzung erfordert eine Authentisierung.	Eine sichere Authentisierung bietet bereits hohen Schutz gegen Angreifer ohne Zugangsrechte. Verbleibende Restrisiken können durch den zusätzlichen Einsatz eines IDS verringert werden. Der Bedarf hängt vom konkreten Schutzbedarf ab.	■■■□

Grundsätzlich gilt: Je höher die Anzahl eingehend freigeschalteter Dienste und je schlechter deren Kontrolle, desto höher ist die Wahrscheinlichkeit, dass über einen der Dienste ein Einbruch erfolgt (z. B. durch Ausnutzen ggf. vorhandener Designfehler in einem der Protokolle oder von Implementierungsfeh-

lern in betroffenen Komponenten). Auch wächst mit der Anzahl konfigurierter Kommunikationsbeziehungen (Firewall-Regeln) die Wahrscheinlichkeit von Fehlkonfigurationen des Firewall-Systems.

Vor dem Einsatz eines IDS sollten zur Verfügung stehende Möglichkeiten zur Verbesserung der Datenflusskontrolle eingehender Dienste und zur Authentisierung der Dienstnutzer ausgeschöpft werden, um den aktiven Schutz zu optimieren. Danach verbleibende Restrisiken können durch die zusätzliche Kontrolle des Verkehrs durch ein IDS weiter reduziert werden.

Das IDS kann dabei zu unterschiedlichen Zwecken eingesetzt werden:

- Policy-Kontrolle:

  Gerade bei komplexen Kommunikationsanforderungen kann das IDS sinnvoll dazu eingesetzt werden, sicherheitsgefährdende Kommunikationsverbindungen, die eigentlich durch die Firewall unterdrückt werden sollten, zu erkennen, bei ihrem Auftreten zu alarmieren oder sie ggf. direkt zu unterbrechen.

- Erkennung von Angriffen im Netzverkehr:

  Die Erkennung von Angriffen im Netzverkehr ist insbesondere für die Verbindungen relevant, bei denen der Verkehr nicht durch ein Applikations-Gateway kontrolliert wird. Die verminderte „aktive“ Datenflusskontrolle in Diensten, für die kein Applikations-Gateway verfügbar ist, kann dabei teilweise durch die „reaktive“ Erkennung von Angriffen und Sicherheitsverletzungen ausgeglichen werden.

E5. Konfiguration des Firewall-Systems und flankierende Prozesse

Wie oft ändert sich die Konfiguration des Firewall-Systems?

☐ Eher selten	Die Konfiguration ändert sich eher selten.	■■□□
☐ Oft (wöchentlich)	Die Konfiguration ändert sich oft (wöchentlich).	■■■■

Erfolgt vor Konfigurationsänderungen eine Analyse des damit verbundenen Risikos?

☐ Ja	Konfigurationsänderungen erfordern eine interne Freigabe auf Basis einer vorhergehenden Abschätzung des mit der Konfigurationsänderung verbundenen Risikos.	■■■■
☐ Nein	Wichtige Kommunikationsanforderungen sind häufig ad-hoc einzurichten. Eine Risikoanalyse findet nicht statt.	■■□□

Werden nicht mehr benötigte Dienste erkannt und gesperrt?

☐ Ja	Es wird regelmäßig geprüft, welche Dienste genutzt werden.	■■■■
☐ Nein	Prozesse zur Erkennung nicht mehr benötigter Dienste sind nicht explizit definiert.	■■□□

Wird die Wirksamkeit des Firewall-Systems regelmäßig geprüft?

☐ Ja	Es erfolgen z. B. regelmäßig Penetrationstests.	■■■■
☐ Nein	Es wird davon ausgegangen, dass das Firewall-System korrekt konfiguriert ist und entsprechend funktioniert.	■■□□

Sämtliche negativen Faktoren erhöhen die Wahrscheinlichkeit dafür, dass das Firewall-System offener konfiguriert ist als erforderlich. In dieser Situation kann durch die Verbesserung der organisatorischen Rahmenbedingungen des Firewall-Einsatzes mit deutlich weniger Aufwand eine Verbesserung der Sicherheit des Internet-Übergangs erreicht werden, als durch zusätzlichen Einsatz eines IDS. Es ist zu beachten, dass der Betrieb eines IDS typischerweise deutlich mehr organisatorischen Aufwand erfordert, als der Betrieb einer Firewall.

Falls die beschriebenen Möglichkeiten zur Reduzierung der Wahrscheinlichkeit von Fehlkonfigurationen des Firewall-Sysems bereits weitgehend umgesetzt sind, kann durch den Einsatz von IDS zusätzlich verifiziert werden, dass keine sicherheitskritischen Dienste genutzt werden.

E6. Regelmäßige Aktualisierung gefährdeter Komponenten

Wird für Komponenten, die einer starken Gefährdung gegenüber Angriffen aus dem Internet unterliegen (insbesondere Firewall, Webserver), regelmäßig geprüft, ob neue, sicherheitsrelevante Software-Patches vorliegen?

☐ Ja	Typischerweise sind Signaturen zur Erkennung von Angriffen verfügbar, bevor Software-Patches zu deren Abwehr entwickelt worden sind. Ein geringer Zusatznutzen durch den Betrieb eines IDS ergibt sich für den entsprechenden Übergangszeitraum dadurch, dass mit dem IDS bereits die jeweiligen Angriffe erkannt werden können, bevor entsprechende Patches verfügbar sind. Dies setzt jedoch eine regelmäßige Aktualisierung des IDS voraus.	■■□□
☐ Nein	IDS können relevante Angriffe lediglich erkennen, während durch geeignete Software-Patches eine Resistenz der Komponenten gegen die Angriffe erreicht werden kann. Durch eine regelmäßige Aktualisierung kann daher mit weniger Aufwand eine qualitativ deutlich besserer Schutz erreicht werden, als durch den Betrieb eines IDS.	□□□□

E7. Interaktion mit internen Systemen (betrifft insbesondere WWW-Applikationen)

In wie weit erfolgt bei Zugriffen aus dem Internet eine Interaktion mit internen Systemen?

☐	Statische Bereitstellung	Auf Web- oder FTP-Servern werden Daten bereitgestellt. Die Bereitstellung erfolgt manuell und damit kontrolliert.	□□□□
☐	Asynchroner Datenaustausch	Es erfolgt ein automatischer Datenaustausch zwischen internen Systemen und Systemen in der DMZ. Es erfolgt jedoch kein Aufbau von Verbindungen aus der DMZ zu internen Systemen (z. B. Edifact, Batchverarbeitung).	■■□□
☐	Synchroner Datenaustausch	Aus der DMZ heraus werden automatisch Verbindungen zu internen Systemen aufgebaut und in diesen Transaktionen ausgeführt (z. B. Online-Banking). Die automatische Interaktion mit internen Systemen verlangt einerseits die Öffnung der Firewall von außen nach innen. Andererseits steigt gerade hierdurch die Gefährdung interner Systeme gegenüber Angriffen aus dem Internet. In dieser Situation können IDS sinnvoll ergänzend eingesetzt werden, wenn Maßnahmen zur aktiven Sicherheit bereits angemessen umgesetzt sind (siehe Einflussfaktoren E1 - E6). Der Einsatz von IDS kann dazu dienen, durch die frühzeitige Erkennung von Angriffen und Sicherheitsverletzungen und durch eine zeitnahe Reaktion, ggf. die Schadensausbreitung zu stoppen, bevor interne Systeme betroffen sind, oder zumindest das Schadensmaß gering zu halten.	■■■■

Je höher und automatisierter der Grad an Interaktion von außen nach innen ist, desto gefährdeter sind grundsätzlich interne Systeme.

E8. Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten

Gibt es Komponenten, die trotz des Schutzes durch das Firewall-System gegenüber Angriffen aus dem Internet gefährdet sind? Welche Anforderungen an Verfügbarkeit und Integrität bestehen für diese Komponenten?

☐	Nein	Die IT-Infrastruktur ist gegenüber Angriffen aus dem Internet durch das Firewall-System angemessen geschützt. Bestehende Restrisiken sind bekannt und werden akzeptiert.	☐☐☐☐
☐	Ja, geringe Anforderungen	Es gibt zwar Komponenten, die trotz Firewall gefährdet sind. Verfügbarkeits- und/oder Integritätsverletzungen dieser Komponenten beeinträchtigen die Aufgabenerbringung jedoch nur in geringem Maße und führen höchstens zu geringfügigen finanziellen Schäden.	■■☐☐
☐	Ja, hohe Anforderungen	Es gibt Komponenten, die trotz Firewall gefährdet sind. Eine Beeinträchtigung der Verfügbarkeit oder eine Manipulation dieser Komponenten kann zu einem Imageverlust des Unternehmens und zu gravierenden finanziellen Auswirkungen führen.	■■■■

Der Einsatz eines IDS kann dazu dienen, sowohl Angriffe auf gefährdete Komponenten als auch Sicherheitsverletzungen und Systemstörungen der Komponenten zeitnah zu erkennen. Hierdurch kann frühzeitig auf entsprechende Ereignisse reagiert werden. Ausfallzeiten können so reduziert und das Schadensmaß kann gering gehalten werden. Insbesondere können mit IDS auch Denial-of-Service Angriffe erkannt werden. IDS sind daher eine Maßnahme, auf deren Basis die Verfügbarkeit von Internet-Angeboten erhöht werden kann.

Ob die Überwachung durch ein IDS sinnvoll ist hängt davon ab, welche Restrisiken hinsichtlich relevanter Gefährdungen für die zu schützende Komponente bestehen. Dies hängt konkret von weiteren Faktoren ab, wie etwa

1. die Funktionalität der Komponente (z. B. sind Mailserver typischerweise weniger gefährdet als Webserver),
2. dem eingesetzten Produkt (der Microsoft Internet Information Server ist z. B. häufiger Ziel von Angriffen als der iPlanet Webserver),
3. die Konfiguration der Komponenten und Betriebssysteme. (z. B. kann durch das IDS der Zeitraum überbrückt werden, in dem ein neuer Angriff bereits bekannt ist, jedoch noch keine zugehörigen Software-Patches verfügbar sind, um die betreffende Komponente gegen den Angriff resistent zu machen. Durch den Einsatz des IDS kann der Angriff in diesem Zeitraum zumindest erkannt werden.)

E9. Relevante Nutzenaspekte von IDS

Wie relevant sind die in der nachstehenden Tabelle angegebenen Nutzenaspekte für ihre konkreten Zielsetzungen?

Relevanz			Nutzenaspekte
hoch	mittel	gering	
			Kontrolle der Netznutzung
☐	☐	☐	Erkennung von Angriffen im Netzverkehr Relevant ist die Erkennung von Angriffen im Netzverkehr insbesondere für Systeme in einer DMZ, - deren Schutzbedarf hinsichtlich Integrität und Verfügbarkeit hoch ist und - für die keine angemessene Datenflusskontrolle durch bestehende Schutzkomponenten gegeben ist oder aufgrund der Funktionalität des Dienstes erhöhte Restrisiken bestehen (z. B. HTTP)
☐	☐	☐	Erkennung der unberechtigten Nutzung spezieller Kommunikationsdienste für bestimmte Systeme
☐	☐	☐	Erkennung der Umgehung von Verschlüsslung (z. B. in VPNs) Die Relevanz der Erkennung dieser Ereignisse hängt davon ab, welches Gefährdungspotenzial bei unverschlüsselter Kommunikation gegeben ist und wie wahrscheinlich es unter den gegebenen technischen und organisatorischen Randbedingungen ist, dass eine unverschlüsselte Kommunikation erfolgt.
			Kontrolle der Systemnutzung (Verstoß gegen Nutzungsregelungen)
☐	☐	☐	Erkennung möglicher Sicherheitsverletzungen Beispiele für Sicherheitsverletzungen sind unberechtigte Zugangsversuche zu Systemen oder Anwendungen (z. B. mehrfach fehlgeschlagene Login-Versuche) oder unberechtigte Zugriffsversuche auf Daten (z. B. Passwortdateien). Zu beachten ist, dass die Erkennung auf der Auswertung von Logdateien des Systems bzw. der Anwendungen beruht. Die Erkennungsfunktionalität ist damit prinzipiell auf die Ereignisse begrenzt, die vom System bzw. der Anwendung protokolliert werden können.
☐	☐	☐	Erkennung von Systemstörungen (hohe CPU-Auslastung, geringer verbleibender Festplattenspeicher, etc.) In gleicher Weise wie Sicherheitsverletzungen können durch Hostsensoren auf Basis von Logdaten des Systems oder von Anwendungen auch Störungen dieser erkannt werden. Beispiele hierfür ist die zentrale Warnung bei zu hoher CPU-Auslastung oder zu geringem verbleibenden Plattenspeicher.
☐	☐	☐	Erkennung von Integritätsverletzungen spezifischer Dateien
			Erweiterte Informationserhebung
☐	☐	☐	Erkennung von Ereigniskontexten IDS können dazu eingesetzt werden, Kontextinformationen zu Angriffen, bis hin zum gesamten angriffsspezifischen Netzverkehr aufzuzeichnen. Die Kontextinformationen können zur vertieften Analyse von Angriffen dienen, zur Rückverfolgung und Identifizierung der Angreifer dienen und/oder – bei geeig-

			neten flankierenden organisatorischen Maßnahmen – zu Beweiszwecken eingesetzt werden.
☐	☐	☐	Darstellung der Angriffslast IDS können dazu eingesetzt werden, Anzahl und Art aus dem Internet eingehender Angriffe und Angriffsversuche aufzuzeichnen. Diese Informationen können gegenüber der Entscheiderebene genutzt werden, um die Gefährdungssituation des Internet-Übergangs darzustellen. Daneben kann durch Aufzeichnung und Vergleich der Angriffslast vor und hinter Schutzkomponenten (Paketfilter, Applikations-Gateway) die Funktion der jeweiligen Komponente verifiziert und deren Nutzen dargestellt werden.
☐	☐	☐	Erhöhung der Transparenz Ohne den Einsatz von Überwachungswerkzeugen ist im Allgemeinen unklar, wie Netzverbindungen genutzt werden und wie sich Systeme im einzelnen verhalten. Unabhängig von konkreten Angriffen bieten IDS die Möglichkeit einer umfangreichen und gesteuerten Beobachtung des Verhaltens von Netzen und Systemen sowie aufgezeichnete Daten zu filtern und auszuwerten. Durch Einsatz eines IDS kann die Transparenz der Netznutzung und des Verhaltens von Systemen insgesamt erhöht werden. Dieses Wissen bildet die Grundlage zur Verbesserung und Optimierung des Einsatzes von Systemen, Anwendungen und Netzen.

In der oben angegebenen Tabelle sind die wesentlichen Nutzenaspekte eines Einsatzes von IDS dargestellt. Falls diese Nutzenaspekte nur in einem sehr geringem Maß den Zielsetzungen entsprechen bzw. diesen dienen, ist zu prüfen, ob ein IDS das geeignete Instrument zum Erreichen der Zielsetzungen ist.

Aus den Nutzenaspekten „Darstellung der Angriffslast“ und „Erhöhung der Transparenz“ ergibt sich kein direkter sicherheitstechnischer Zusatznutzen. Sie sollten daher bei der Entscheidung für oder gegen den Einsatz eines IDS im Hintergrund stehen.

4.1.3 Beispielszenarien

Die Bewertung der Einflussfaktoren wird in den nächsten Abschnitten anhand folgender Beispielszenarien für Internet-Übergänge verdeutlicht:

- Allgemeine Informationsbereitstellung über statische Webseiten
- Bürokommunikation mit Internetnutzung
- VPN-Anbindung externer Liegenschaften
- E-Business-Angebot mit individualisierten Transaktionen

Bei den Szenarien wird davon ausgegangen, dass ein IDS-Einsatz nicht deshalb abgelehnt wird, weil zunächst Nachbesserungen an anderen Stellen sinnvoller sind. Konkret wird davon ausgegangen, dass

- ein dreistufiges Firewall-System gemäß BSI Empfehlung eingesetzt wird (vgl. E1),
- das Firewall-System in einer gesicherten Umgebung betrieben wird (vgl. E2),
- es keine sonstigen Übergänge zum Internet gibt (vgl. E3),
- die Komponenten am Internet-Übergang organisatorisch sicher betrieben werden (vgl. E5 und E6).

Die zugehörigen Einflussfaktoren E1, E2, E3, E5 und E6 werden in den Szenarien nicht wiederholt beurteilt.

4.1.3.1 Allgemeine Informationsbereitstellung über statische Webseiten

In diesem Szenario werden auf einem Webserver Informationen zum Abruf über das Internet bereitgestellt. Die Bereitstellung erfolgt über Webseiten, die statisch vorliegen oder durch den Webserver auf Basis minimaler Interaktion mit dem Client zusammengestellt werden. Der Webserver wird dabei typischerweise in einer DMZ betrieben, wobei eine Kommunikation zur Versorgung des Webservers mit Daten nur von Systemen im internen Netz erfolgt. Insbesondere erfolgt kein Aufbau von Kommunikationsbeziehungen aus der DMZ in das interne Netz.

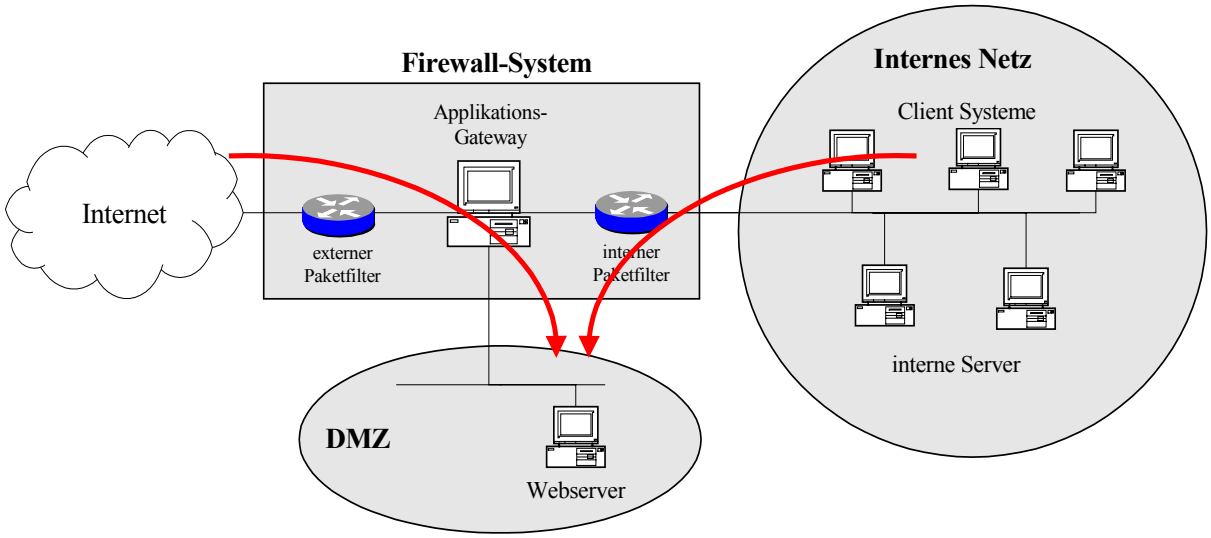

Abbildung 4-1: Internet-Übergang mit Webserver (Beispiel)

Die Betrachtung der Einflussgrößen zeigt, dass in diesem Szenario der sicherheitstechnische Zusatznutzen bei Einsatz eines IDS eher gering ist.

E4	Freigeschaltete Dienste und Dienstkontrolle	Internet-Dienste werden durch einen HTTP-Proxy auf Anwendungsebene kontrolliert. Die Dienstnutzung erfolgt anonym. Bei korrekter Konfiguration der Komponenten ist sichergestellt, dass keine von außen oder aus der DMZ initiierten Verbindungen ins interne Netz möglich sind.
E7	Interaktion mit internen Systemen	Die Daten werden statisch bereitgestellt. Es erfolgt keine automatische Interaktion mit internen Systemen.
E8	Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten	Typische Angriffe auf Webserver nutzen entweder Schwächen der Serverprogramme oder Schwachstellen bei der Realisierung dynamischer Inhalte aus. Bei einer rein statischen Bereitstellung von Daten kann ein angemessener Schutz des Webangebots in der Regel mit bestehenden Mitteln realisiert werden. Bestehende Restrisiken sind auch ohne Einsatz eines IDS tolerierbar.

Der wesentliche Einsatzzweck eines IDS in diesem Szenario würde sich darauf beschränken, die korrekte Konfiguration der Firewall-Komponenten zu kontrollieren. Dies kann jedoch auch durch eine regelmäßige Kontrolle der Firewall-Logs erreicht werden.

Bei der Integration eines IDS wäre außerdem darauf zu achten, dass durch die erforderliche IDS-Kommunikation zwischen Sensoren und Managementstation keine Verbindungen aus der DMZ ins interne Netz aufgebaut würden, denn die Freischaltung von Diensten in das interne Netz hinein würde den durch das Firewall-System gebotenen Schutz reduzieren.

Zusammenfassend ist aufgrund der begrenzten Nutzenaspekte und weiterer erforderlicher Kommunikationsbeziehungen für die IDS-Kommunikation, der Einsatz eines IDS für dieses Szenario nicht oder nur bedingt empfehlenswert.

4.1.3.2 Bürokommunikation mit Internetnutzung

Dieses Szenario betrifft die Kommunikation über E-Mail sowie die Nutzung des WWW von Clientsystemen im internen Netz. Typischerweise erfolgt hierzu eine Kommunikation über einen HTTP-Proxy und smtp-Proxy in der Firewall (siehe Abbildung) bzw. dedizierte Proxy-Server in der DMZ (in der Abbildung nicht dargestellt).

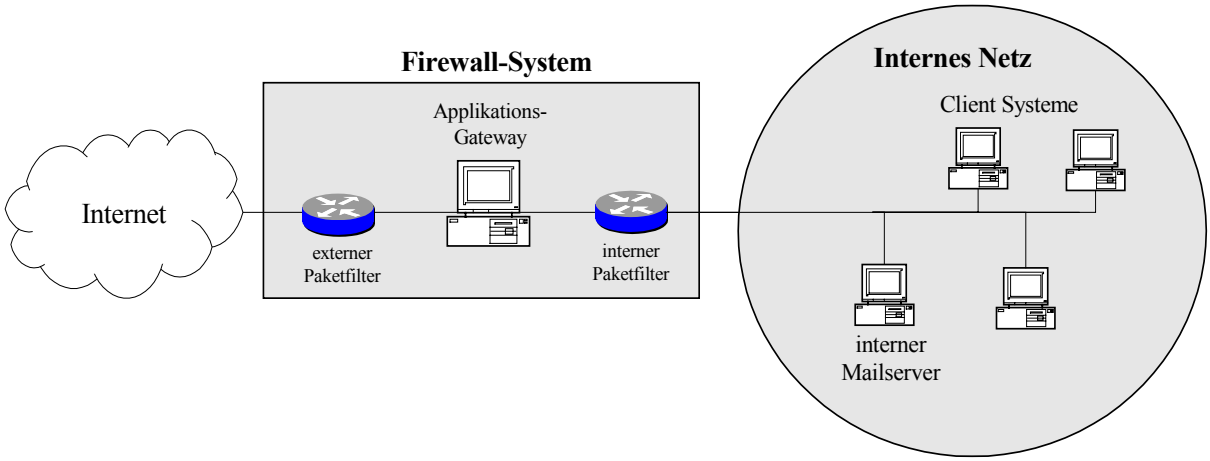

Abbildung 4-2: Internet-Übergang für E-Mail und WWW-Zugriff (Beispiel)

E4	Freigeschaltete Dienste und Dienstkontrolle	Es sind nur wenige Dienste ins interne Netz eingehend freigeschaltet: - E-Mails erreichen den Mailserver im internen Netz über das Protokoll SMTP und werden über den Applikations-Proxy an der Firewall kontrolliert. Ausgehend sind ebenfalls nur wenige Dienste freigeschaltet: - Ausgehende E-Mail vom Mailserver ins Internet über SMTP. - WWW-Verbindungen ins Internet werden über einen HTTP-Proxy an der Firewall kontrolliert. - DNS-Anfragen werden über einen DNS-Proxy auf der Firewall, der typischerweise selbst dem internen Netz gegenüber als DNS-Server auftritt, kontrolliert.
E7	Interaktion mit internen Systemen	Es erfolgt keine automatische Interaktion mit internen Systemen. Stattdessen werden alle von außen nach innen gesendeten Nachrichten am Client manuell weiterverarbeitet.
E8	Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten	Es bestehen mittlere Anforderungen an Verfügbarkeit und Integrität der bereitgestellten Kommunikationsdienste. Eine zeitweise Verzögerung von E-Mail oder WWW-Zugriff kann typischerweise toleriert oder anderweitig überbrückt werden.

Bei korrekter Konfiguration der Komponenten werden die meisten extern initiierten Angriffe ausgeschlossen. Es verbleiben jedoch Risiken dahingehend, dass über die freigeschalteten Dienste versteckte Kommunikationskanäle (bis hin zum Shellzugriff) erfolgen können, z. B. durch Tunneln der Dienste über SMTP, HTTP und DNS. Es sind ebenso Angriffe möglich, bei denen eine Kommunikation von internen Systemen initiiert wird. Dies betrifft z. B. Trojaner, die sich regelmäßig über das HTTP-Protokoll bei einem vom Angreifer kontrollierten Webserver melden.

Ein zusätzlich installiertes IDS kann einen Teil der versteckten Kanäle ausfindig machen und eine Reaktion ermöglichen. Für eine vollständige Abdeckung der genannten Risiken wäre jedoch eine Einbeziehung der Clientsysteme notwendig. Wenn das IDS ausschließlich am Netzübergang installiert werden soll, ist der sicherheitstechnische Zusatznutzen also beschränkt auf die Erkennung offensichtlicher, nicht verschlüsselter Angriffe sowie intern initiierter Angriffe nach außen. Zusätzlich kann das IDS die Konfiguration der Firewall-Komponenten überwachen.

4.1.3.3 VPN-Anbindung externer Liegenschaften

In diesem Szenario wird von einem Internet-Übergang ausgegangen, bei dem ein VPN-Gateway in einer DMZ betrieben wird. Der Netzübergang wird ausschließlich für VPN genutzt. Sämtliche anderen Verbindungen mit dem Internet sind blockiert. Über das VPN-Gateway erfolgt eine verschlüsselte und authentisierte Kommunikation mit externen Liegenschaften, Mitarbeitern in Home-Offices. Daneben wird der VPN-Kanal für Fernwartungszugänge genutzt.

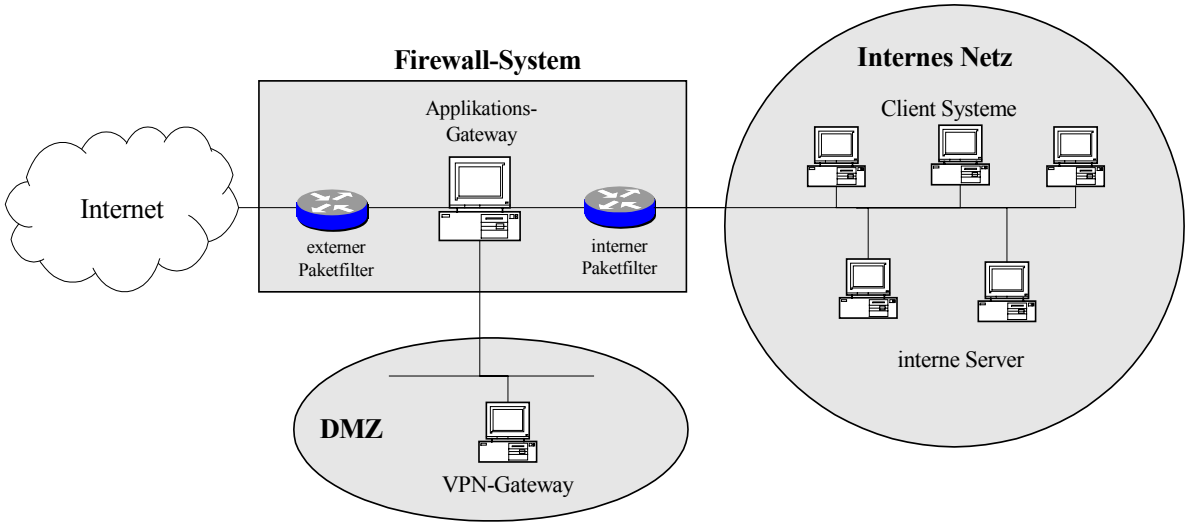

Abbildung 4-3: Internet-Übergang mit VPN-Gateway (Beispiel)

Die Betrachtung der Einflussgrößen zeigt, dass mit dem Firewall-System zwar der Verkehr auf zulässige VPN-Verbindungen beschränkt werden kann, der Datenfluss dieser Verbindungen mit Hilfe der Firewall jedoch nur unzureichend kontrollierbar ist.

E4	Freigeschaltete Dienste und Dienstkontrolle	Über VPN zugreifende Kommunikationspartner werden vom VPN-Gateway authentisiert. Aus dem Internet in die DMZ werden ausschließlich VPN-Verbindungen zugelassen. Aus der DMZ ins interne Netz werden vielfältige Kommunikationsdienste genutzt. Eine Datenflusskontrolle erfolgt im Wesentlichen durch Paketfilter. Applikations-Proxy sind nicht verfügbar bzw. werden nicht eingesetzt.

E7	Interaktion mit internen Systemen	Es erfolgt eine Interaktion zwischen Kommunikationspartnern, die über das Internet angebunden sind, und Systemen im internen Netz. Zulässige VPN-Verbindungen können dabei mißbräuchlich genutzt werden.
E8	Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten	Es bestehen hohe Anforderungen an Verfügbarkeit und Integrität der internen Systeme. Verfügbarkeit und Integrität interner Systeme könnten durch VPN-getunnelte Angriffe oder Sicherheitsverletzungen gefährdet werden.

Bei einer korrekten Konfiguration der Komponenten ist sichergestellt, dass es über die zulässigen VPN-Verbindungen hinaus keine sonstigen Verbindungen aus und ins Internet gibt. Der sicherheitstechnische Zusatznutzen eines IDS ist daher begrenzt auf

- die Überwachung der korrekten Konfiguration der Firewall-Komponenten und des VPN-Gateways sowie
- der Erkennung von Angriffen im VPN-Verkehr.

Eine Überwachung der korrekten Konfiguration kann grundsätzlich auch durch regelmäßige Kontrolle der Komponenten und ihrer Logdaten erfolgen. Hinsichtlich des VPN kann mit dem IDS kontrolliert werden, dass die Kommunikation über das Internet tatsächlich - wie intendiert - verschlüsselt erfolgt.

Der Einsatz eines IDS begründet sich jedoch im Wesentlichen durch die Angriffserkennung in der nicht verschlüsselten Kommunikation zwischen DMZ und internem Netz. Im Vordergrund steht dabei die Erkennung von Angriffen auf interne Systeme, die über VPN-Kanäle erfolgen. Daneben können jedoch auch im ausgehenden Verkehr Angriffe auf Systeme externer VPN-Kommunikationspartner erkannt werden, die von internen Systemen initiiert werden. Der Einsatz eines IDS ist insbesondere dann sinnvoll, wenn nicht sämtliche VPN-Kommunikationspartner als hinreichend vertrauenswürdig für einen unkontrollierten Zugriff eingestuft werden können (wie etwa bei der Fernwartung durch externe Mitarbeiter).

4.1.3.4 E-Business-Angebot mit individualisierten Transaktionen

In diesem Szenario wird der typische Aufbau einer E-Business Architektur betrachtet. Aus dem Internet erfolgt ein Zugriff auf einen Webserver als Frontend-System, auf dem Transaktionen ausgelöst werden können. Über Gateway-Komponenten, die auch in der DMZ oder auf dem Webserver realisiert sind, erfolgt die Umsetzung auf anwendungsspezifische Protokolle und die Kommunikation mit Applikationsservern im internen Netz. Die Applikationsserver führen Transaktionen in den internen Systemen (Hosts, Datenbanken) aus.

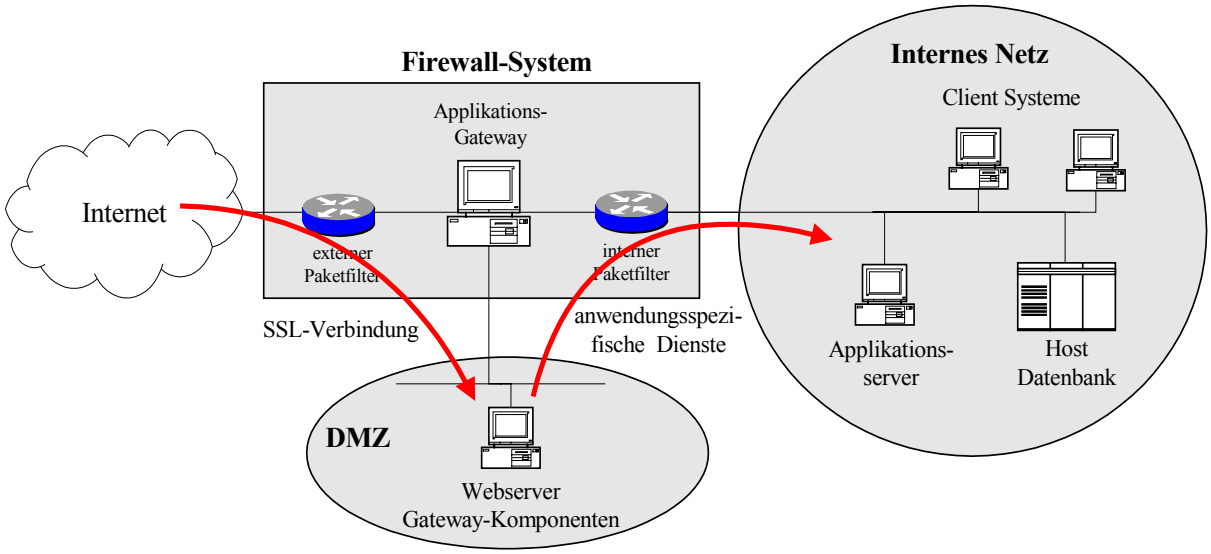

Abbildung 4-4: E-Business Architektur (Beispiel)

Die Betrachtung der Einflussgrößen zeigt, dass der durch das Firewall-System in diesem Szenario gebotene Schutz begrenzt ist und ein deutlicher sicherheitstechnischer Zusatznutzen durch Einsatz eines IDS erreicht werden kann.

E4	Freigeschaltete Dienste und Dienstkontrolle	Der SSL-Zugriff auf den Webserver erfolgt anonym. Aufgrund der Nutzung von SSL ist keine Datenflusskontrolle des eingehenden Verkehrs auf Anwendungsebene möglich. Nutzer werden beim Zugang zu Transaktionen authentisiert. Die komplexen Technologien (Sun iPlanet, IBM WebSphere, etc), mit denen E-Business Applikationen realisiert werden, nutzen typischerweise eine Vielzahl von Prozessen, die über proprietäre Protokolle miteinander kommunizieren. Eine angemessene Datenflusskontrolle ist für diese Dienste häufig nicht realisierbar.
E7	Interaktion mit internen Systemen	Es erfolgt eine Interaktion zwischen Kommunikationspartnern, die über das Internet angebunden sind, und Systemen im internen Netz. Falls der Webserver durch einen Angreifer übernommen wird, kann dieser möglicherweise über Gateway-Komponenten Zugang zu internen Systemen erhalten.
E8	Verfügbarkeits- und Integritätsanforderungen gefährdeter Komponenten	Webserver verfügen - insbesondere bei der Bereitstellung dynamischer Seiten - über eine Reihe von Sicherheitslücken, die von Angreifern aus dem Internet ausgenutzt werden können. Andererseits bestehen hohe Anforderungen an Verfügbarkeit und Integrität der internen Systeme sowie mittlere Anforderungen an die Verfügbarkeit des Internet-Angebots.

Durch den Einsatz von IDS kann ein verbesserter Schutz gegen die identifizierten Schwachstellen und Angriffspunkte erreicht werden. Mögliche Angriffe können dadurch schnell erkannt und geeignete Gegenmaßnahmen ausgelöst werden.

In diesem Szenario empfiehlt sich daher der Einsatz eines IDS zu folgenden Zwecken:

- Erkennung von Angriffen auf den Webserver, wie z. B. auch Denial-of-Service Angriffen,

- Erkennung von Angriffen und der unberechtigten Nutzung von Kommunikationsdiensten im Verkehr zwischen dem Webserver und Applikationsservern,
- Überwachung der Integrität und Funktion kritischer Daten und Prozesse auf dem Webserver.

4.2 Hilfsmittel für Grobkonzept und Anforderungsanalyse

4.2.1 Verfeinerung der Zielsetzungen

Z1. Erkennung von Angriffen im Netzverkehr

Relevante Fragestellungen:

- Für welche Systeme ist die Erkennung von Angriffen im Netzverkehr von besonderem Interesse? Für welche Applikationen auf diesen Systemen sind Angriffe zu erkennen?
- Ist die Erkennung von Angriffen am Übergang zum internen Netz relevant?

Z2. Erkennung der unberechtigten Nutzung spezieller Kommunikationsdienste

Relevante Fragestellung:

- Für welche Systeme ist die Nutzung welcher Dienste (mit welchen Parametern) sicherheitskritisch und durch das IDS zu erkennen?

Z3. Erkennung der Umgehung von Verschlüsselung

Relevante Fragestellung:

- Für welche Systeme und Dienste ist sicherzustellen, dass eine Verschlüsselung erfolgt. Welche Klartextmuster sind als Erkennungsmerkmal für eine unverschlüsselte Übertragung geeignet?

Z4. Erkennung von Sicherheitsverletzungen in Systemen/Anwendungen

Relevante Fragestellung:

- Für welche Systeme und Anwendungen ist die log-basierte Erkennung von Sicherheitsverletzungen von besonderem Interesse?

Z5. Erkennung von Integritätsverletzungen an Dateien

Relevante Fragestellung:

- Für welche Dateien auf welchen Systemen ist eine Integritätsüberwachung von besonderem Interesse?

Z6. Erkennung von Störungen

Relevante Fragestellung:

- Für welche Systeme und Applikationen ist die Erkennung allgemeiner Störungen von besonderem Interesse?

Z7. Aufzeichnung von Angriffskontexten

Für die Zielsetzung ist folgendes zu beachten:

- Falls das IDS die Aufzeichnung von Angriffskontexten als automatische Reaktion zulässt, können Kontextinformationen prinzipiell erst ab der Erkennung des Angriffs aufgenommen werden. Insbesondere vorhergehende Kontextinformationen gehen verloren.
- Falls Kontextinformationen allgemein, unabhängig vom konkreten Angriffsfall aufgezeichnet werden sollen, müssen möglichst viele Ereignisse bis hin zum gesamten Netzverkehr aufgezeichnet

werden, da vorab unklar ist, welche Informationen im Fall einer zukünftigen Analyse nutzbringend sind. Dabei fällt eine große Menge zu verwaltender Daten an, welche die Speicherkapazitäten einzelner Sensoren typischerweise innerhalb kurzer Zeiträume übersteigt. Deshalb sind bei dieser Zielsetzung Randbedingungen der Aufzeichnung und Speicherung großer Datenmengen vorab zu klären, wie etwa:

- Über welche Zeitperioden soll eine Aufzeichnung stattfinden?
- Wie detailliert soll die Aufzeichnung sein?
- Wie lange sollen die Daten vorgehalten werden?
- Welche Anforderungen ergeben sich für Speichermedien, Datenbanken und die Datenübertragung?

Z8. Darstellung der Angriffslast

Relevante Fragestellungen:

- Für welche Punkte im Netz ist die Darstellung der Angriffslast relevant?
- Soll die Differenz der Angriffslast (z. B. vor und hinter Schutzkomponenten) ermittelt werden? Falls ja, an welchen Punkten im Netz muss hierzu die Angriffslast ermittelt und verglichen werden?
- Ist eine temporäre Darstellung der Angriffslast ausreichend oder soll die Angriffslast permanent dargestellt werden?

Z9. Erhöhung der Transparenz

Relevante Fragestellungen:

- Gibt es konkrete Zielsetzungen hinsichtlich der Erhöhung der Transparenz?
- Falls ja: An welchen Punkten ist hierzu der Netzverkehr zu beobachten und welche Systeme und/oder Anwendungen sind hierzu zu beobachten?

4.2.2 Diskussion der Platzierung von Netzsensoren

Am Beispiel des vom BSI empfohlenen 3-stufigen Internet-Übergangs werden nachstehend unterschiedliche Sensorplatzierungen diskutiert. Abbildung 4-5 zeigt die betrachteten Sensorplatzierungen.

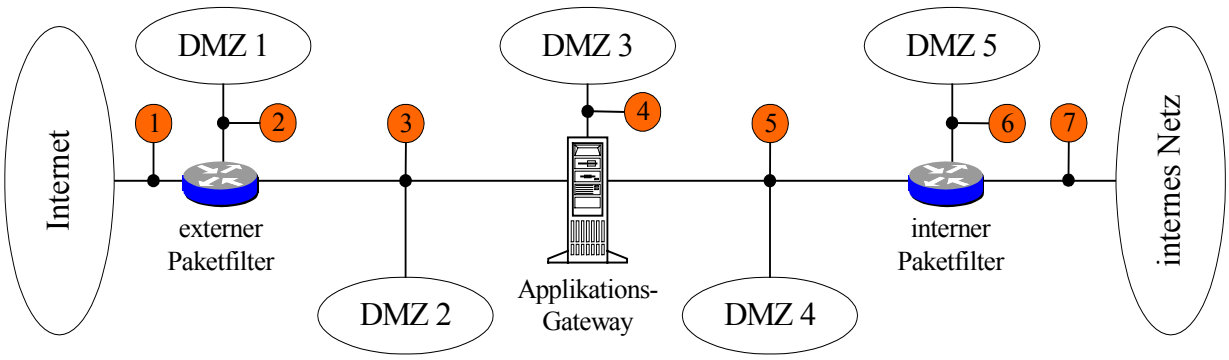

Abbildung 4-5: Mögliche Sensorplatzierungen am 3-stufigen Internet-Übergang

Ein Netzsensors kann prinzipiell nur den Verkehr überwachen, der für ihn sichtbar ist. Dies ist für die einzelnen Sensorplatzierungen in der nachstehenden Tabelle angegeben.

Nr.	Position	Beobachtbarer Netzverkehr
1	Vor dem externen Paketfilter am Übergang zum Internet	Internet ↔ externer Paketfilter
2	Zwischen externem Paketfilter und DMZ 1	Internet ↔ DMZ1 DMZ1 ↔ weiter innen platzierte Systeme
3	Am Knotenpunkt zur DMZ 2	externer Paketfilter ↔ DMZ2 DMZ2 ↔ Applikations-Gateway externer Paketfilter ↔ Applikations-Gateway
4	Zwischen dem Applikations-Gateway und DMZ 3	weiter außen platzierte System ↔ DMZ 3 DMZ 3 ↔ weiter innen platzierte Systeme
5	Am Knotenpunkt zur DMZ 4	Applikations-Gateway ↔ DMZ4 DMZ 4 ↔ interner Paketfilter Applikations-Gateway ↔ interner Paketfilter
6	Zwischen internem Paketfilter und DMZ 5	weiter außen platzierte Systeme ↔ DMZ5 DMZ5 ↔ internes Netz
7	Hinter dem internen Paketfilter am Übergang zum internen Netz	interner Paketfilter ↔ internes Netz

4.2.2.1 Grundsätze zur Sensorplatzierung

Grundsätzliche Aussagen, die für jeden Punkt einer möglichen Sensorplatzierung (1-7) am Netzübergang zum Internet gelten:

1. Die Platzierung an den Positionen 2, 4 bzw. 6 ist nur dann sinnvoll, falls an der jeweiligen Stelle eine DMZ vorhanden ist (DMZ 1, DMZ 3, DMZ 5).
2. Aus dem Internet oder von Komponenten/Systemen, die weiter außen liegen, eingehender Verkehr, ist grundsätzlich als weniger vertrauenswürdig einzustufen. Die Erkennung von Angriffen in diesem Verkehr ist daher grundsätzlich sinnvoll.
3. Von dem überwachten Teilnetz nach innen gehender Verkehr sollte im Gutfall keine Angriffsmuster aufweisen. Falls hier Angriffe oder Sicherheitsverletzungen erkannt werden, könnten sie in einer Kompromittierung von Komponenten/Systemen im überwachten Teilnetz begründet liegen. Die Erkennung von Angriffen in diesem Verkehr wird daher grundsätzlich als sinnvoll eingestuft.
4. Hinsichtlich der Angriffsinitiierung ausgehend von Komponenten im überwachten Teilnetz, ist die Angriffserkennung im nach außen gehenden Verkehr eher von geringerer Relevanz, da erkannte Ereignisse weiter außen liegende Komponenten oder Systeme im Internet betreffen, deren Schutz typischerweise nicht im Vordergrund des IDS-Einsatzes steht. Relevant ist die Überwachung des vom überwachten Teilnetz nach außen gehenden Verkehrs jedoch hinsichtlich der Reaktion von Komponenten im überwachten Teilnetz, die Aufschluss über den Erfolg von Angriffen aus dem Internet geben kann[18].
5. Die Überwachung des Verkehrs von weiter innen liegenden Systemen/Komponenten zum überwachten Teilnetz kann zur Erkennung intern initiierter Angriffsversuche auf Systeme/Komponenten im überwachten Teilnetz dienen. Die Überwachung dieses Verkehr ist grundsätzlich sinnvoll, jedoch weniger relevant als Überwachung von außen nach innen führenden Verkehrs (Fälle 2.+3.).

[18] Ein Beispiel hierfür sind Telnet-Zugangsversuche auf geschützte Komponenten, die dann gefährlich sind, wenn die angesprochene Komponente mit einem Acknowledge antwortet.

6. Je mehr Filterkomponenten zwischen dem Internet und dem Netzsensor vorhanden sind, desto geringer ist die zu erwartende Angriffslast – und umgekehrt.
7. Je weniger Filterkomponenten zwischen dem Netzsensor und dem internen Netz vorhanden sind, desto höher ist die Wahrscheinlichkeit, dass an dieser Position erkannte Angriffe relevante Auswirkungen auf interne Ressourcen haben.

Nachstehend werden die einzelnen Platzierungen kurz diskutiert.

4.2.2.2 Sensor am Übergang zum Internet vor dem externen Paketfilter

Die Platzierung eines Netzsensors an Position 1 erlaubt die vollständige Überwachung des ein- und ausgehenden Verkehrs zum Internet zentral an einem Punkt. Alle vom Internet ausgehenden Angriffsversuche können an diesem Punkt festgestellt werden.

Mit dieser Platzierung kann nicht erkannt werden, ob die vom Sensor beobachteten Ereignisse den externen Paketfilter (und ggf. weitere Schutzkomponenten) passieren oder nicht. Es wird lediglich eine Obermenge der Ereignisse erkannt, welche die Zielsysteme real erreichen.

Die Platzierung ist grundsätzlich auch zur Überwachung des Aufbaus von Internet-Verbindungen durch interne Komponenten geeignet. Dieser Überwachungsansatz ist jedoch eher von untergeordneter Bedeutung, da die Erkennung von Angriffen auf Systeme im Internet im Allgemeinen nicht im Vordergrund des IDS-Einsatzes steht. Es ist jedoch zu beachten, dass zur Erkennung von Angriffen aus dem Internet auch die Beobachtung der Reaktion interner Systeme relevant ist. Der ausgehende Verkehr ist daher in die Überwachung einzubeziehen.

Die Platzierung ist insbesondere für die beiden folgenden Zielsetzungen geeignet:

- Analyse der Bedrohungslage:

  Die Bedrohungslage der Internet-Übergangs gegenüber Angriffen aus dem Internet kann erkannt und dokumentiert werden. Dies kann dazu dienen, Management und Entscheidungsträgern zu verdeutlichen, dass Bedrohungen real vorliegen und deren Bereitschaft fördern, IT-Sicherheitsmaßnahmen zu verbessern.

- Erfassung von Angriffskontexten:

  Netzsensoren, die weiter innen platziert werden, erkennen nur noch einen Teil der Angriffe, da viele Angriffsaktivitäten bereits durch vorgeschaltete Schutzkomponenten abgeblockt werden. Für Ereignisse, die von weiter innen platzierten Netzsensoren erkannt werden, kann durch die Angriffserkennung an Position 1 ermittelt werden, ob sie Bestandteil erweiterter Angriffsaktivitäten sind.

Weiter ist zu beachten, dass an dieser Stelle die Angriffslast am höchsten ist. Es fällt eine große Menge zu verwaltender Daten an, die Speicherkapazitäten einzelner Sensoren typischerweise innerhalb kurzer Zeiträume übersteigt (vgl. Abschnitt 4.2.1, Zielsetzung Z7). Deshalb sind bei dieser Platzierung Randbedingungen der Aufzeichnung und Speicherung großer Datenmengen vorab zu klären, wie etwa:

- Über welche Zeitperioden soll eine Aufzeichnung stattfinden?
- Wie detailliert soll die Aufzeichnung sein?
- Wie lange sollen die Daten vorgehalten werden?
- Welche Anforderungen ergeben sich für Speichermedien, Datenbanken und die Datenübertragung?

4.2.2.3 Sensor zwischen externem Paketfilter und DMZ 1

Die Platzierung des Sensors an Position 2 dient dem ergänzenden Schutz von Systemen/Komponenten in der DMZ 1. Eine Platzierung erscheint dann sinnvoll, wenn für diese Systeme/Komponenten die in Abschnitt 4.2.1 aufgeführten Zielsetzungen Z1, Z2 und/oder Z3 besonderes relevant sind.

4.2.2.4 Sensor zwischen externem Paketfilter und Applikations-Gateway

An Position 3 kann sowohl der Verkehr mit der DMZ 2 als auch der gesamte Internet-Verkehr, der über das Applikations-Gateway erfolgt, gebündelt überwacht werden. Die Platzierung eines Sensors an Position 3 kann unterschiedlichen Zwecken dienen:

1. Kontrolle des Kommunikationsverkehrs mit der DMZ 2 zum ergänzenden Schutz von Systemen/ Komponenten dieser DMZ. Eine Platzierung erscheint dann sinnvoll, wenn für Systeme/Komponenten in der DMZ 2 die in Abschnitt 4.2.1 aufgeführten Zielsetzungen Z1, Z2 und/oder Z3 besonderes relevant sind.
2. Durch die Erkennung spezifischer Kommunikationsdienste, die eigentlich durch den externen Paketfilter blockiert werden müssten, kann die Konfiguration des externen Paketfilters überwacht werden.
3. Da der vom Internet kommende Netzverkehr an Position 3 bislang nur durch den externen Paketfilter gefiltert wurde, kann die Platzierung zur Frühwarnung bei Angriffsversuchen sowie eingeschränkt auch zur Erkennung von Angriffskontexten (Z7) und der Darstellung der Angriffslast (Z8) dienen.

Es ist zu beachten, dass der Netzverkehr durch zusätzliche Schutzkomponenten gefiltert wird, bevor er Systeme/Applikationen in einer weiter innen liegenden DMZ oder im internen Netz erreicht. Ein Netzsensor an dieser Position kann nicht erkennen, ob und welche der Angriffe durch das Applikations-Gateway und ggf. durch den internen Paketfilter blockiert werden. Deshalb ist eine Erkennung von Angriffen auf weiter innen liegende Komponenten effizienter durch Netzsensoren möglich, die weiter innen platziert sind (Positionen 4, 5, 6, 7).

Wie bei der Platzierung an Position 1 ist auch hier zu berücksichtigen, dass eine vergleichsweise große Menge zu verwaltender Daten anfällt. Bei dieser Platzierung sind deshalb Randbedingungen der Aufzeichnung und Speicherung großer Datenmengen vorab zu klären (vgl. Abschnitt 4.2.2.2).

4.2.2.5 Sensor zwischen Applikations-Gateway und DMZ 3

Die Platzierung des Sensors an Position 4 dient dem ergänzenden Schutz von Systemen/Komponenten in der DMZ 3. Eine Platzierung erscheint dann sinnvoll, wenn für diese Systeme/Komponenten die in Abschnitt 4.2.1 aufgeführten Zielsetzungen Z1, Z2 und/oder Z3 besonderes relevant sind.

4.2.2.6 Sensor zwischen Applikations-Gateway und internem Paketfilter

An Position 5 kann sowohl der Verkehr mit der DMZ 4 als auch der gesamte Verkehr zum internen Netz gebündelt überwacht werden. Die Platzierung eines Sensors an dieser Position kann folgenden Zwecken dienen:

1. Kontrolle des Kommunikationsverkehrs mit der DMZ 4 zum ergänzenden Schutz von Systemen/Komponenten dieser DMZ. Eine Platzierung erscheint dann sinnvoll, wenn für Systeme/Komponenten in der DMZ 4 die in Abschnitt 4.2.1 aufgeführten Zielsetzungen Z1, Z2 und/oder Z3 besonderes relevant sind.
2. Durch die Erkennung spezifischer Kommunikationsdienste, die eigentlich durch den internen Paketfilter bzw. durch das Applikations-Gateway blockiert werden müssten, kann die Konfiguration dieser Komponenten überwacht werden.
3. Kontrolle des Netzverkehrs zum Schutz interner IT-Systeme. An dieser Position erkannte Angriffe sind grundsätzlich bereits als sicherheitskritisch einzustufen, da der Netzverkehr nur noch durch den internen Paketfilter kontrolliert wird, bevor er ins interne Netz gelangt.

Aus den aufgeführten Gründen wird die Platzierung eines Netzsensors an dieser Position grundsätzlich als wichtig eingestuft.

4.2.2.7 Sensor zwischen internem Paketfilter und DMZ 5

Die Platzierung des Sensors an Position 6 dient dem ergänzenden Schutz von Systemen/Komponenten in der DMZ 5. Eine Platzierung erscheint dann sinnvoll, wenn für diese Systeme/Komponenten die in Abschnitt 4.2.1 aufgeführten Zielsetzungen Z1, Z2 und/oder Z3 besonderes relevant sind.

4.2.2.8 Sensor zwischen internem Paketfilter und internem Netz

Die Platzierung eines Netzsensors an Position 7 ist zwar grundsätzlich geeignet den Netzverkehr zwischen dem Internet-Übergang und dem internen Netz gebündelt zu überwachen. Die Überwachung an dieser Stelle hat jedoch folgende Nachteile:

- Die Überwachung erfolgt bereits im internen Netz. Abhängig von der Architektur des internen Netzes kann es daher der Fall sein, dass an dieser Position nicht nur der Verkehr zum Internet-Übergang sichtbar ist, sondern auch ein Großteil des Netzverkehrs des internen Netzes, der für den Überwachungszweck irrelevant ist.
- Aus der potentiellen Möglichkeit der Überwachung internen Netzverkehrs ergeben sich grundsätzlich Möglichkeiten zur Überwachung von Mitarbeitern, womit Datenschutzprobleme verbunden sind.

Die Platzierung eines Netzsensors an dieser Position erscheint daher zum Zweck der ergänzenden Absicherung des Netzübergangs[19] nur dann sinnvoll, falls sichergestellt wird, dass ausschließlich der Verkehr zwischen internem Netz und internem Paketfilter für den Sensor sichtbar ist.

4.2.3 Diskussion von Platzierungen der Management- und Auswertungsstation

In den folgenden Abschnitten werden unterschiedliche Platzierungen der Management- und Auswertungsstation sowie zugehörige Kommunikationswege vergleichend diskutiert:

- Platzierung der Management- und Auswertungsstation in einer bestehenden DMZ oder im internen Netz und Nutzung des überwachten Netzes für die IDS-Kommunikation.
- Platzierung der Management- und Auswertungsstation in einem separaten IDS-Netz dass zur IDS-Kommunikation genutzt wird.
- Platzierung der Management- und Auswertungsstation in einer separaten DMZ.

4.2.3.1 IDS-Kommunikation über das überwachte Netz

Die Platzierung der Management- und Auswertungsstation im internen Netz ist beispielhaft in Abbildung 4-6 dargestellt. Es werden bestehende Übertragungswege für die Kommunikation mit der Management- und Auswertungsstation genutzt.

[19] Für andere Einsatzzwecke, wie z. B. zur Überwachung des internen Netzes, kann die Platzierung uneingeschränkt sinnvoll sein.

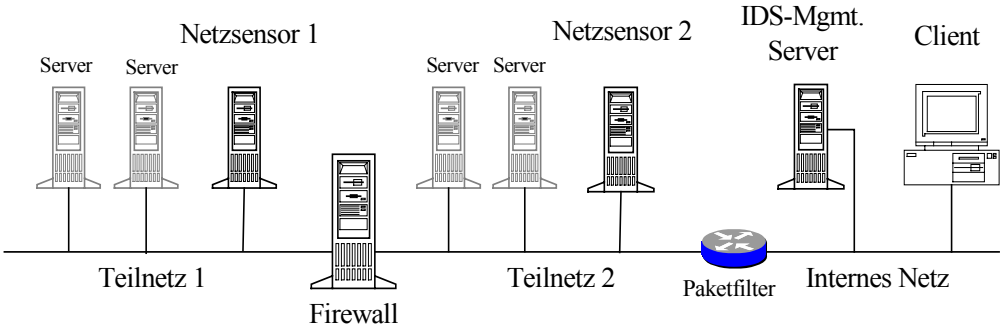

Abbildung 4-6: IDS-Kommunikation über das überwachte Netz

Vorteil des Ansatzes:

- Es sind keine Erweiterungen der Netzinfrastruktur erforderlich. Im Vergleich zu den anderen Platzierungen der Management- und Auswertungsstation ist dies der kostengünstigste Ansatz.

Nachteile des Ansatzes:

- Angriffe auf das Netz können die Funktion des IDS beeinträchtigen.
- Die Komponenten des IDS können anhand ihres Datenaustausches identifiziert und lokalisiert werden. Dies vereinfacht ein direktes Angreifen oder Umgehen der IDS-Komponenten.

4.2.3.2 Nutzung eines separaten IDS-Netzes

Die Nutzung eines separaten IDS-Netzes für die IDS-Kommunikation und der Betrieb der Management- und Auswertungsstation in diesem Netz ist beispielhaft in Abbildung 4-7 dargestellt.

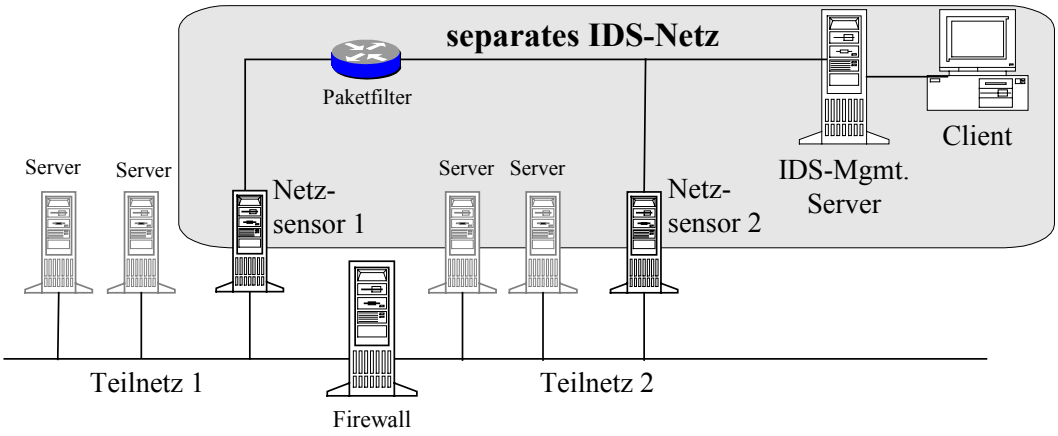

Abbildung 4-7: Nutzung eines separaten IDS-Netzes für die IDS-Kommunikation

Vorteile des Ansatzes:

- Die Netzsensoren sind von den überwachten Teilnetzen aus unsichtbar.
- Die IDS-Kommunikation ist weitmöglichst von der Kommunikation in den überwachten Teilnetzen entkoppelt.
- Die Risiken, dass Angriffe auf die überwachten Teilnetze und dort betriebener Komponenten die Funktionalität des IDS beeinträchtigen sind im Vergleich zu den beiden anderen Ansätzen minimiert.

Nachteile des Ansatzes:

- Um eine Entkopplung des IDS-Netzes zu erreichen, ist jeder Übergang zum IDS-Netz abzusichern. Dies betrifft sämtliche Kommunikationswege mit der Management- und Auswertungsstation:
  - Zugriff interner Clients auf die Management- und Auswertungsstation.
  - Intrusion-Response, z. B. über E-Mail oder SNMP-Traps.
  - Kommunikation mit Hostsensoren und Netzsensoren. Im Gegensatz zu Netzsensoren stellen Hostsensoren einen direkteren Übergang zum IDS-Netz dar, da sie auf dem überwachten System betrieben werden und ein Angreifer durch einen erfolgreichen Angriff auf das System Zugang zum IDS-Netz erhalten könnte. Konsequenterweise müsste daher die Kommunikation zwischen Hostsensor und Management- und Auswertungsstation mindestens durch einen Paketfilter kontrolliert werden.
- Wenn unterschiedliche Teilnetze oder deren Komponenten durch Netz- oder Hostsensoren überwacht werden, besteht die Gefahr, dass im Falle einer Kompromittierung oder Fehlkonfiguration eines Sensors ein Übergang zwischen den überwachten Teilnetzen über das IDS-Netz geschaffen wird. Konsequenterweise müssten daher im IDS-Netz auch die entsprechenden Sensoren durch eine Firewall-Komponente entkoppelt werden. Beim Einsatz von Netzsensoren lässt sich die Überbrückung des Sensors vom IDS-Netz zum überwachten Teilnetz durch den Abgriff des Netzverkehrs über TAPs verhindern.
- Die Einrichtung und konsequente Absicherung eines separaten IDS-Netzes ist aus den zuvor genannten Gründen sehr aufwendig.

4.2.3.3 Platzierung der Management- und Auswertungsstation in einer separaten DMZ

Die Platzierung der Management- und Auswertungsstation in einer separaten DMZ ist beispielhaft in Abbildung 4-8 dargestellt. Damit die Netzsensoren vom überwachten Netz aus unsichtbar sind, erfolgt ihre Kommunikation mit der Management- und Auswertungsstation über zusätzliche Netzinterfaces sowohl am Netzsensor als auch an der Firewall.

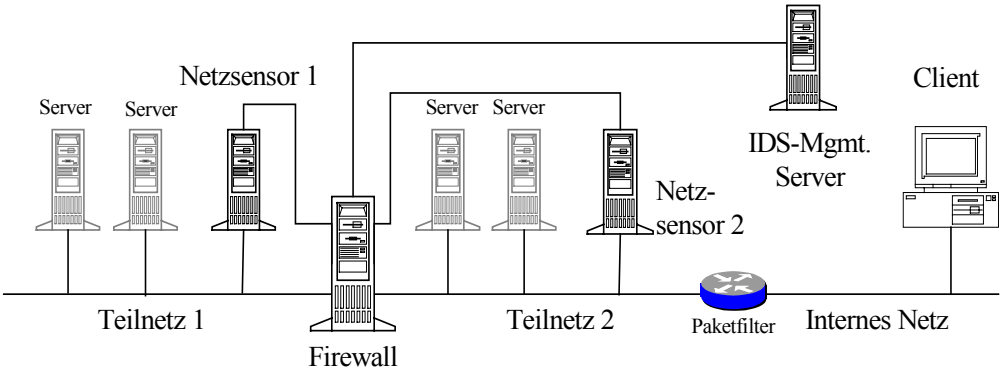

Abbildung 4-8: IDS-Kommunikation über bestehende Firewall

Vorteile des Ansatzes:

- Im Vergleich zur Einrichtung eines vollständig entkoppelten, separaten IDS-Netzes erfordert dieser Ansatz einen deutlich geringeren Aufwand, da zur Entkopplung der IDS-Teilnetze das vorhandene Firewall-System verwendet wird.
- Da die IDS-Kommunikation über die bestehende Firewall kontrolliert wird, bleibt die Firewall das zentrale System zur Steuerung des Netzverkehrs. Eine Überbrückung der Firewall ist nicht möglich.

- Die Netzsensoren sind vom überwachten Netz aus unsichtbar.

Nachteile des Ansatzes:

- Die IDS-Kommunikation hängt von der korrekten Konfiguration und Funktion der Firewall ab.
- Die IDS-Konfiguration und Überwachung muss typischerweise in räumlicher Nähe zur Firewall erfolgen, da eine separate – gesicherte – physikalische Netzverbindung zwischen Managementstation und Firewall notwendig ist.

Hinsichtlich der Kommunikation mit Hostsensoren, des Zugriffs von Remote-Clients auf die Management- und Auswertungsstation und der Kommunikation für das Intrusion-Response (E-Mail, SNMP-Trap, etc.) bietet der Ansatz unterschiedliche Erweiterungsmöglichkeiten. Diese erlauben je nach Ausprägung eine weitere Entkopplung der IDS-Kommunikation.

4.2.4 Ableitung von Anforderungen

Die folgenden Fragestellungen dienen dazu, aus der Ist-Situation und den Zielsetzungen heraus abzuleiten, welche Anforderungen an ein einzusetzendes IDS zu stellen sind.

Dabei wird davon ausgegangen, dass eine Überwachung des Netzverkehrs erfolgen soll.

Frage 1: Ist der Einsatz hostbasierter Sensoren erforderlich?

Hostbasierte Sensoren beobachten typischerweise ein oder mehrere der nachstehenden Elemente:

- Logdaten des Betriebssystems,
- Logdaten von IT-Anwendungen,
- Prozessdaten (z. B. Start und Beendigung von Prozessen),
- Integrität spezifischer Dateien und/oder
- den hostspezifischen Netzverkehr.

Frage 2: Welche Plattformen sollen durch hostbasierte Sensoren überwacht werden?

Hostbasierte Sensoren werden auf den zu überwachenden Systemen betrieben. Daher ist sicherzustellen, dass der IDS-Hersteller für jede zu überwachende Plattform geeignete Hostsensoren anbietet.

Frage 3: Welche Standardapplikationen sollen mit host- bzw. netzbasierten Sensoren überwacht werden?

Falls Standardapplikationen überwacht werden sollen, sollte das einzusetzende IDS über die entsprechenden Signaturen verfügen.

Frage 4: Sollen mit hostbasierten Sensoren proprietäre Anwendungen überwacht werden?

Falls proprietäre Anwendungen von hostbasierten Sensoren überwacht werden sollen, ist darauf zu achten, dass

- die zugehörigen Logdateien mit in die Überwachung des Sensors einbezogen werden können und

- der Hostsensor bzw. das IDS die Definition von Signaturen durch den Anwender erlaubt.

Die Definition von Signaturen durch den Anwender ist erforderlich, um proprietäre Logdaten auswerten zu können.

Frage 5: Soll mit hostbasierten Sensoren der hostspezifische Netzverkehr überwacht werden?

Die Überwachung des Netzverkehrs durch hostbasierte Sensoren kann z. B. aus folgenden Gründen sinnvoll sein:

- Es wird ein geswitchtes Netz eingesetzt, in dem aufgrund hoher Verkehrslast ein Abgriff des Netzverkehrs am Switch nicht sinnvoll realisierbar ist.
- Der Netzverkehr wird bis zum Host verschlüsselt übertragen und kann daher durch Netzsensoren nicht geeignet kontrolliert werden.

Frage: 6 Welche Typen von Netzen sollen mit dem IDS überwacht werden?

Es ist sicherzustellen, dass das IDS sowohl die zugehörigen Netzmedien (Ethernet, Tokenring, X.25, etc.) unterstützt als auch die Sensoren die entsprechenden Protokolle (IP, IPX, etc.) auswerten können.

Frage: 7 Wie hoch ist die Netzlast an den Punkten, an dem der Netzverkehr überwacht werden soll?

Die zu überwachende Netzlast bestimmt die erforderliche Performance der Netzsensoren. Diese wiederum hängt weitgehend von den genutzten Betriebssystemen und der Rechnerhardware des Sensors ab. Falls eine vollständige Überwachung des Netzverkehrs erforderlich ist, hierfür jedoch die Performance eines einzelnen Netzsensors nicht ausreicht, bieten sich folgende Lösungen an:

1. Der Netzverkehr wird auf mehrere Netzsensoren verteilt, so dass insgesamt eine vollständige Überwachung möglich ist.
2. Der Netzverkehr wird auf Basis hostbasierter Sensoren auf den Endsystemen überwacht.

Frage 8: Wird mit dem IDS-Einsatz auch die Erkennung von Fehlverhalten bei der Netznutzung angestrebt, wie z. B. die unberechtigte Nutzung spezieller Kommunikationsdienste für bestimmte Systeme oder die Umgehung vorgesehener verschlüsselter Kommunikation?

Wodurch Fehlverhalten charakterisiert ist, hängt von der speziellen Einsatzumgebung des IDS ab. Im Vergleich zur Erkennung allgemeiner Angriffe erfordert die Erkennung von Fehlverhalten daher, dass die Ereigniserkennung des IDS entsprechend anpassbar ist.

Selbst wenn ein IDS sowohl weitgehende Möglichkeiten zur Anpassung mitgelieferter Signaturen bietet als auch die Definition von Signaturen durch den Anwender erlaubt, ist nicht sichergestellt, ob die Erkennung bestimmter Fehlverhaltensmuster abbildbar ist.

Es ist daher sinnvoll, zuvor zu spezifizieren, welche typischen Verhaltensweisen erkannt werden sollen, und vom IDS-Hersteller abzufragen, ob konkret diese durch Signaturen abbildbar sind.

Beispiele für Fehlverhaltensweisen:

- Verbindungsbestätigung bei Diensten, die eigentlich gesperrt sein sollten.
- Klartext-Nachrichten bei Verbindungen, die eigentlich verschlüsselt sein sollten.
- Netbios Broadcast von fehlkonfigurierten Windows-Systemen.

Frage 9: Durch wen soll das IDS administriert werden? (Systemadministratoren, IT-Sicherheitsmanager)

Bei IDS-Produkten variiert der erforderliche Kenntnisstand der IDS-Administratoren erheblich. Einige IDS erlauben die Administration vollständig über eine grafische Oberfläche, während bei anderen wesentliche Funktionen nur über Kommandozeilen aktiviert werden können und ggf. ein zusätzlicher Einsatz von Systemkommandos erforderlich ist.

Daher sind bei der IDS-Auswahl die Systemkenntnisse des vorgesehenen Administrationspersonal zu berücksichtigen.

Frage 10: Für welche Plattformen ist Administrationspersonal im Hause verfügbar?

Es ist vorteilhaft, wenn die IDS-Komponenten auf Plattformen betrieben werden können, für die im Hause Personal zur Systemadministration verfügbar ist.

Frage 11: Über welche Kommunikationsdienste erfolgen in ihrem Hause üblicherweise Alarmierungen?

Optimalerweise sollten die Alarme des IDS über Kommunikationswege erfolgen, die im Hause bereits für Alarmierungen genutzt werden. Hieraus resultieren für das einzusetzende IDS Anforderungen an Intrusion-Response-Funktionalitäten.

Falls das IDS den Alarmierungsweg nicht vorsieht, kann eine Integration ggf. über spezifische Kommandos oder Skripte erfolgen, die im Falle eines Alarms vom IDS ausgeführt werden. Es ist darauf zu achten, dass vom IDS dabei Parameter übergeben werden können.

Frage 12: Zu welchen Zwecken sollen Reporting-Funktionen eingesetzt werden?

Reporting Funktionen können insbesondere für zwei unterschiedliche Zwecke eingesetzt werden:

1. Darstellung der Angriffslast und Angriffsverteilung gegenüber dem Management. Wichtig sind in diesem Fall Funktionen zur grafischen Aufbereitung der Daten.
2. Langfristanalyse und Auswertung zur Erkennung spezifischer Angriffsmuster. In diesem Fall sind Funktionen zur spezifischen Auswertung der Datenbasis wichtig (z. B. Verteilung bestimmter Angriffe über längere Zeiträume, Analyse spezifischer IP-Quelladressen).

4.2.5 Dokumentation der Anforderungen

Es ist zu unterscheiden zwischen Anforderungen, die sich aus der Ist-Situation und den Zielsetzungen herleiten und die von Fall zu Fall verschieden sein können, und Basisanforderungen, die ein IDS in jedem Fall erfüllen sollte.

Bei den im Folgenden angegebenen Anforderungen ist zusätzlich gekennzeichnet, ob sie aktuell von marktverfügbaren IDS typischerweise erfüllt werden (🏳) oder ob sie höchstens in Ausnahmefällen erfüllt werden (⃠).

Sensortypen: Welche Sensortypen soll das IDS unterstützen?			
	Netzbasierte Sensoren		Hostbasierte Sensoren

Konkretisierung der Anforderungen an Netzsensoren	
Welche Anforderungen an Überwachungsfunktionen bestehen für die Netzsensoren?	
	Angriffserkennung im Netzverkehr. Spezifizieren Sie die maximale Netzlast, die überwacht werden soll: _____
	Angriffe sollen von den Sensoren unmittelbar gemeldet werden (Push-Technologie) 🏳
	Erkennung von Fehlverhalten. Spezifizieren Sie die Anforderungen an die Erkennung von Fehlverhalten:
	- Spec1:
	- Spec2:
	...
Welche Anforderungen bestehen hinsichtlich der Plattformen, auf denen Netzsensoren betrieben werden sollen?	
	Netzsensoren sollen auf dem nachstehend genannten Betriebssystem oder einem der nachstehend genannten Systeme betrieben werden: _____
	Netzsensoren sollen als Appliance verfügbar sein.
Welche Netztypen sollen vom IDS überwacht werden?	
	Ethernet (10/100Mb)
	Gigabit Ethernet
	Token Ring
	...

Konkretisierung der Anforderungen an Hostsensoren					
Für welche Systeme sollen Hostsensoren eingesetzt werden und welche Überwachungsfunktionen sollen sie aufweisen?					
Überwachung des Systems (Logdaten, Prozesse, etc.)	WinNT/2000	Solaris	Linux	...	...
Überwachung der Integrität spezifischer Dateien					
Überwachung des hostspezifischen Netzverkehrs					

Überwachung von Applikationen (nachfolgend bitte die einzelnen Applikationen aufführen):						
- Appl1:						
- Appl2:						
...						
	Ein Wiederanlauf von Hostsensoren soll ohne Neustart des Systems möglich sein.					

Kalibrierung und Skalierbarkeit von Sensoren	
Welche Anforderungen bestehen an die Kalibrierung und Skalierbarkeit der Sensoren?	
	Das IDS soll die Definition von Signaturen für Hostsensoren durch den Anwender erlauben.
	Das IDS soll die Definition von Signaturen für Netzsensoren durch den Anwender erlauben.
	Das IDS soll die Anpassung bestehender Signaturen durch Kopieren dieser und Änderung von Parametern erlauben.
	Die Funktionsweise der Signaturen soll detailliert dokumentiert und für den Anwender nachvollziehbar sein.
	Die Auswertungsfunktionen des Hostsensors sollen auf proprietäre Logdateien erweiterbar sein.
	Das IDS soll die Definition unterschiedlicher Alarmklassen zulassen, denen die Ereignisse / Signaturen zugeordnet werden können und für die jeweils spezifische IDS-Reaktionen (Intrusion-Response) definierbar sind.

Intrusion-Response	
Über welche Intrusion-Response-Funktionen soll das System verfügen?	
	Alarmierung per E-Mail
	Alarmierung per SNMP
	Alarmierung per SMS
	Rohdaten-Log (Aufzeichnung der angriffsspezifischen Pakete im Netzverkehr)
	Aufzeichnung der nutzerspezifischen Aktivitäten für eine bestimmte Zeitspanne
	Unterbrechung von Verbindungen
	Logout von Nutzern
	Automatische Rekonfiguration von Komponenten. Spezifizieren Sie die Komponenten und die Zielfunktionalität: _____
	Ausführung nutzerdefinierter Kommandos/Skripte
	Parameterübergabe bei der Ausführung nutzerdefinierter Kommandos/Skripte

Managementfunktionen	
Welche Anforderungen bestehen an Managementfunktionen?	
	Das IDS soll die Definition von Regelwerken für Sensoren (Sensor-Policy) sowie deren Zuweisung an Sensoren erlauben.
	Das IDS soll die Möglichkeit bieten, Gruppen von Sensoren zu bilden, denen in einem Schritt dieselbe Policy zugewiesen werden kann.
	Nach dem Neustart von Sensoren soll das System dieses automatisch erkennen und die Sensoren automatisch den zugehörigen Policies zuordnen und aktivieren.
	Das IDS soll die Nutzung mehrerer Managementstationen erlauben, zwischen denen Sensor-Policies ausgetauscht werden können.
	Das IDS soll automatisch prüfen, ob neue Signatur-Updates verfügbar sind.
	Das IDS soll über Funktionen zur Pseudonymisierung von Ereignissen verfügen.
	Das IDS soll über Funktionen verfügen, die ein Backup der Konfiguration (Sensor-Policies, etc.) in einfacher Weise ermöglichen.

Auswertungsfunktionen	
Welche Anforderungen bestehen an Auswertungsfunktionen?	
	Das IDS soll über Funktionen zur Generierung management-orientierter, grafisch aufbereiteter Berichte enthalten.
	Das IDS soll umfangreiche Such- und Auswertungsfunktionen für die Ereignisdatenbank bieten. (z. B. Abfrage spezifischer Ereignisse und deren Verteilung über spezifische Zeiträume)
	Das IDS soll Möglichkeiten bieten, zu erkannten Ereignissen beschreibende Informationen abzurufen (Angriffsbeschreibung, Gegenmaßnahmen, etc.), entweder durch eine im IDS integrierte Datenbank oder durch Links auf entsprechende Informationen im Internet.
	Das IDS soll die CVE[20]-Nummern für die dort registrierten Ereignisse mitliefern.

Sicherheit des IDS	
Welche Anforderungen bestehen an Sicherheitsfunktionen?	
	Die Kommunikation zwischen Sensoren und Management-/Auswertungsstation soll gesichert erfolgen (verschlüsselt und authentisiert).
	Das IDS muss erkennen, wenn Sensoren ausfallen (Lebendüberwachung der Sensoren).
	Das IDS soll intern Zugriffe und Konfigurationsänderungen protokollieren.
	Das IDS soll über eine Benutzer- und Rechteverwaltung verfügen, welche die Abbildung unterschiedlicher Rollen erlaubt.

[20] CVE = Common vulnerability enumeration, siehe www.mitre.org

	Management- und Auswertungsstation des IDS sollen separat betrieben werden können, um Zugriffsrechte für Auswertungsfunktionen zur IDS-Administration trennen zu können.
	Beim Download von Signatur-Updates sollen Authentizität und Integrität durch entsprechende Mechanismen (z. B. SSL) sichergestellt sein.

Nutzungsoberfläche	
Welche Anforderungen bestehen an die Bedienoberfläche?	
	Das IDS soll eine GUI-basierte Bedienoberfläche aufweisen, über die sämtliche Funktionen verfügbar sind.

4.2.6 Dokumentenrahmen für Grobkonzept und Anforderungsanalyse

Kapitel 1: Zielsetzungen des Einsatzes eines IDS

Die mit dem Einsatz eines IDS für das Unternehmen verbundenen Zielsetzungen sind zu beschreiben.

Kapitel 2: Anforderungsanalyse

Die von einem einzusetzenden IDS zu erbringenden Anforderungen sind zu beschreiben, zu gewichten und zu begründen. Anhang 4.2.5 kann als Dokumentationsvorlage verwendet werden.

Kapitel 3: Grobkonzeption des IDS-Einsatzes

Technisch und organisatorisch ist die Einsatzweise eines IDS grob zu konzipieren.

Kapitel 3.1: Technik

Die Platzierungen von Sensoren und der Management-/Auswertungsstation sind darzustellen und zu begründen.

Kapitel 3.1.1: Platzierung der Sensoren

Die Platzierungen von Netz- und Hostsensoren sind im Rahmen eines Netzdiagramms zu verdeutlichen. Für jeden Sensor ist sein Einsatzzweck an der jeweiligen Position zu erläutern.

Die Platzierungen sind zu priorisieren.

Um ein späteres Nachvollziehen der Sensorplatzierung zu ermöglichen, ist es darüber hinaus sinnvoll, unterschiedliche Möglichkeiten von Sensorplatzierungen zu diskutieren.

Kapitel 3.1.2: Platzierung der Management- und Auswertungsstation

Die Platzierung von Management- und Auswertungsstation ist/sind im Netzwerkdiagramm darzustellen. Kommunikationswege zwischen Sensoren und Management- bzw. Auswertungsstation sowie ggf. für den Remote-Zugriff auf die Management- bzw. Auswertungsstation sind zu beschreiben.

Um ein späteres Nachvollziehen der Platzierung zu ermöglichen, ist es darüber hinaus sinnvoll, unterschiedliche Möglichkeiten der Platzierung zu diskutieren und die ausgewählte Platzierung zu begründen.

Kapitel 3.2: Organisation

Es ist darzustellen, welche Stellen beim IDS-Betrieb welche Aufgaben übernehmen. Die Zuständigkeiten und Verantwortlichkeiten des im Leitfaden angegebenen generischen Rollenmodells sind hierzu auf die konkrete Organisation abzubilden.

4.3 Hilfsmittel für die Entscheidungsvorlage

4.3.1 Links auf IDS-Testberichte

Zum Zeitpunkt der Erstellung des Leitfaden aktuelle Testberichte und Vergleichstests:

www.nss.co.uk

NSS IDS Group Test, Ausführlicher Vergleichstest unterschiedlicher marktverfügbarer IDS, Stand August 2002

www.nwfusion.com/reviews/2001/1008rev.html

Network Workd, “Intrusion-Detection products grow up”, Test von 5 netzbasierten IDS, Stand August 2001

www.nc-india.com/coverstories/stories/32377.html und

www.networkcomputing.com/1217/1217f2.html

Network Computing , “To catch a thief”, Network Computing, Test von 8 netzbasierten IDS, Stand August 2001

4.3.2 Kosten- und Aufwandsabschätzung

Bei den Anschaffungskosten marktverfügbarer IDS wird zwischen den Kosten für Netzsensoren, Hostsensoren und der Management-/Auswertungsstation unterschieden.

IDS-Software

Netzsensoren kosten (als Softwareausführung) 6-10 T€, einfache Hostsensoren, als Bestandteil integrierter IDS, liegen im Bereich zwischen 300 € und 1000 €. Kosten für Management-/Auswertungsstation werden von den Herstellern unterschiedlich gehandhabt. Während sie bei einigen im Preis der Sensoren inbegriffen sind, fallen bei anderen zusätzlich Kosten bis zu 10 T€ an. Neben den Kosten für reine IDS-Komponenten können abhängig vom eingesetzten Produkt Kosten für zusätzlich erforderliche Software (wie etwa Datenbanken) anfallen.

IDS-Plattformen

Netzsensoren, Management-/Auswertungsstation und ggf. zusätzliche Datenbanken sollten auf eigens hierfür vorgesehenen Rechnern betrieben werden. Für die Rechner inklusive Systemsoftware sind je nach Ausführung ca. 5-10 T€ zu veranschlagen. Auch die Zusatzkosten für IDS-Komponenten, die als Appliances ausgeführt sind, bewegen sich im gleichen Bereich. Daneben können Kosten für Komponenten anfallen, die zur technischen Integration des IDS benötigt werden (z. B. TAPs, Hubs oder Switches).

IDS-Integration

Der Aufwand für die reine technische Integration und Inbetriebnahme des IDS ist überschaubar und liegt grob bei ca. 2-3 PT pro Komponente. Nicht berücksichtigt ist dabei ggf. entstehender organisatorischer Aufwand für das Change-Management. Insbesondere der Abstimmungsaufwand zur Integration von Hostsensoren hängt stark von der Organisation und vom zu überwachenden System ab.

Der Aufwand für den Aufbau einer angemessenen Incident-Response-Organisation hängt stark von den damit verbundenen Anforderungen und der gegebenen Organisation im Unternehmen ab.

IDS-Kalibrierung

Der Kalibrierungsaufwand verteilt sich auf eine Erstkalibrierung bei Inbetriebnahme sowie die regelmäßige Verfeinerung der Kalibrierung auf Basis von Erfahrungen im Betrieb.

Für die Erstkalibrierung sind pro Netzsensor bis zu 10 PT zu veranschlagen. Der Aufwand sinkt dabei, falls mehrere Sensoren ein ähnliches Überwachungsprofil aufweisen sollen. Der Kalibrierungsaufwand von Hostsensoren hängt stark von dem mit dem Einsatz verbundene Zielsetzungen ab. Es sind grob 5 PT pro Sensor zu veranschlagen.

Bei gleicher Einsatzumgebung kann sich die Verfeinerung der Kalibrierung im Betrieb des IDS über mehrere Monate erstrecken. Neben der Verfeinerung der Kalibrierung sind Anpassungen der Kalibrierung bei Signatur-Updates und bei Änderungen der zu überwachenden IT-Infrastruktur des IDS erforderlich. In direktem Zusammenhang mit der Kalibrierung steht die regelmäßige Verfolgung vom IDS gemeldeter Ereignisse und die regelmäßige Aktualisierung von Kenntnissen über neue Angriffe und Sicherheitslücken. Beim Einsatz des IDS zur ergänzenden Absicherung am Internet-Übergang sollte der regelmäßige Aufwand hierfür nach einer „Einschwingphase“ ca. 5 PT monatlich nicht überschreiten. Die Einschwingphase kann mehrere Monate betragen. Der Zusatzaufwand in der Einschwingphase hängt stark von den Erfahrungen der IDS-Administration mit dem IDS-Einsatz, ihren Kenntnissen von Angriffen und Sicherheitslücken sowie Detailkenntnissen der überwachten Infrastruktur ab.

IDS-Betrieb

In der nachstehenden Tabelle sind Aktivitäten des IDS-Betriebs und Aufwände aufgeführt, die zusätzlich zu den bei der IDS-Kalibrierung angegebenen Aktivitäten anfallen.

Aktivität	Aufwand
Regelmäßige Aktualisierung des IDS und fortlaufende Abstimmung des IDS-Einsatzes (Meetings, IT-Planung und Entwicklung im Unternehmen, etc.)	monatlich ca. 3 PT
Betrieb einer Incident-Response-Organisation	organisationsabhängig
Betrieb der HW-/SW-Plattformen des IDS	es sind organisationsspezifische Erfahrungswerte anzusetzen
Wartung des IDS und zugrundeliegender HW-/SW-Plattformen	jährlich ca. 15-20% der jeweiligen Investitionen

4.3.3 Dokumentenrahmen für eine Entscheidungsvorlage

Kapitel 1: Zielsetzungen des Einsatzes eines IDS

Management-orientierte Beschreibung der mit dem Einsatz eines IDS für das Unternehmen verbundenen Ziele.

Kapitel 2: Lösungsansätze

In diesem Kapitel der Entscheidungsvorlage ist für jeden Lösungsansatz ein Abschnitt mit folgenden Inhalten vorzusehen:

- Skizzierung des Lösungsansatzes (insbesondere Architekturdiagramm mit Sensorplatzierungen),
- Abdeckung der Einsatzziele (Nutzenaspekte des Lösungsansatzes),
- zu erwartende Kosten und personelle Aufwände,

- ggf. zusätzlich Gegenüberstellung von Kosten und Nutzenaspekten (Kosten-Nutzen-Analyse).

Kapitel 3: Diskussion der Lösungsansätze

Benennung von Vor- und Nachteilen der einzelnen Lösungsansätze und Vergleich der Lösungsansätze untereinander.

Kapitel 4: Empfehlung

Begründete Empfehlung eines Lösungsansatzes und Darstellung der zu erwartenden Kosten und Aufwände.

4.4 Hilfsmittel für Feinkonzept und Produktauswahl

4.4.1 Abgriff des zu überwachenden Netzverkehrs

Nachstehend werden unterschiedliche Möglichkeiten des Abgriffs des zu überwachenden Netzverkehrs kurz erläutert:

- **Abgriff von einem Hub**

  Ein Hub dient zur Anbindung mehrere Komponenten an dasselbe Netzsegment. Sämtliche am Hub angeschlossene Komponenten „sehen“ den gleichen Netzverkehr. Bei der Anbindung eines Netzsensors an den Hub kann von dem Netzsensor der gesamte Netzverkehr des entsprechenden Netzsegments abgehört und überwacht werden.

- **Abgriff von einem Switch**

  Im Gegensatz zum Hub kann bei einem Switch der Verkehr zwischen den unterschiedlichen Ports des Switches über Regeln gesteuert werden. Dies ermöglicht die Bildung von VLANs. So kann z. B. eine an Port 1 angeschlossene Komponente mit einer an Port 2 angeschlossenen Komponenten kommunizieren, während gleichzeitig eine an Port 3 angeschlossene Komponente mit einer an Port 4 angeschlossenen Komponenten kommuniziert. Dabei ist der Netzverkehr der Verbindungen separiert, d. h. der Verkehr auf der Port 1/3 Verbindung ist auf der Port 3/4 Verbindung nicht sichtbar und umgekehrt.

  Die Anbindung eines Netzsensor an einen Switch hat für die Überwachung des Verkehrs den Vorteil, dass über die Programmierung des Switches eingestellt werden kann, welcher Verkehr zur Überwachung zum Sensor geleitet wird. Handelsübliche Switches bieten daneben auch sog. SPAN Ports (SPAN = Switch Port Analyser) an, über die der Netzverkehr des Switches gespiegelt werden kann. Dabei ist darauf zu achten, dass der Port über eine ausreichende Bandbreite verfügt, um auch bei hoher Last den Verkehr der Switch-Ports vollständig spiegeln zu können (vgl. auch Kapitel 4.4.2).

- **Abgriff über einen TAP**

  TAPs dienen speziell zum Abgriff von Netzverkehr zu Überwachungszwecken. Sie sind grundsätzlich mit einem Hub (mit 3 Anschlüssen) vergleichbar, weisen jedoch an einem der Anschlüsse eine „Dioden“-Funktion auf: Über den TAP wird der Verkehr auf der Kommunikationsstrecke abgegriffen, es können jedoch keine Datenpakete in die Kommunikation hineingespielt werden. Selbst falls es einem Angreifer gelingt, über den vom Sensor überwachten Datenstrom den Netzsensors zu Fehlfunktionen zu verleiten, ist somit eine aktive Rückkopplung des Sensors auf die überwachte Strecke ausgeschlossen. Diesem Vorteil steht der Nachteil gegenüber, dass aktive Reaktionen des Netzsensors, wie z. B. das Einspielen von Reset-Paketen, auch nicht über den TAP erfolgen können.

4.4.2 Abgriff des Netzverkehrs bei Lastverteilung

Für die Überwachung von Netzverkehr, der auf mehrere physikalische Verbindungen verteilt ist, bieten sich folgende Lösungsmöglichkeiten an:

1. **Einsatz mehrerer Netzsensoren**: Für jede physikalische Verbindung wird ein separater Netzsensor vorgesehen. Dieser Ansatz hat den Vorteil, dass auch die Überwachung lastverteilt erfolgt. Da der Netzverkehr auf mehrere Sensoren verteilt wird, kann eine höhere Verkehrslast überwacht werden als beim Einsatz von nur einem Sensor. Nachteilig ist der hohe technische Aufwand, der sich aus dem Betrieb mehrerer Netzsensoren ergibt. Des Weiteren ist für die Angriffserkennung zu beachten, dass Zusammenhänge zwischen einzelnen Ereignissen, die von verschiedenen Sensoren erkannt wurden, erst nach deren zentraler Zusammenführung korreliert werden können. Um dieselbe Erkennungsqualität wie bei Einsatz eines einzelnen Sensors zu gewährleisten, muss die Analyse später, nach der Zusammenführung der Ereignisse erfolgen. Dies ist als Anforderung für ein auszuwählendes IDS zu berücksichtigen.

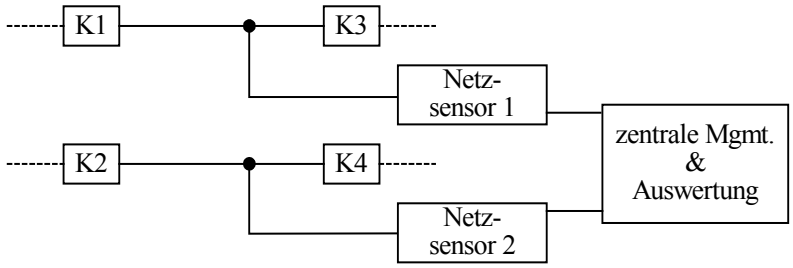

Abbildung 4-9: Einsatz mehrerer Netzsensoren

2. **Einsatz eines Netzsensors mit mehreren Netzinterfaces**: Der von den Verbindungen abgegriffene Netzverkehr wird zu separaten Netzinterfaces desselben Sensors geleitet und durch diesen ausgewertet. Dieses Vorgehen hat den Vorteil, dass ein Sensor den Netzverkehr insgesamt sieht und auswerten kann. Bei der Auswahl des Sensors ist jedoch darauf zu achten, dass dieser die Überwachung des Verkehrs mehrerer Netzinterfaces unterstützt und die Sensor-Performance die Überwachung des gebündelt vorliegenden Verkehrs erlaubt.

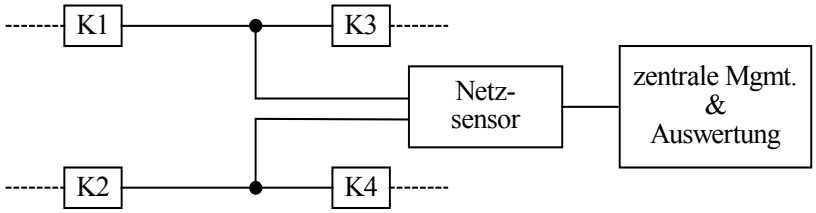

Abbildung 4-10: Einsatz eines Netzsensors mit mehreren Netzinterfaces

3. **Zusammenführung des Netzverkehrs über einen Switch**: Der von den Verbindungen abgegriffene Netzverkehr wird über einen Switch zusammengeführt und zu einem Netzsensors geleitet. Wie zuvor ist der Vorteil gegeben, dass ein Sensor den Netzverkehr insgesamt sieht und auswerten kann. Bei der Auswahl des Sensors ist darauf zu achten, dass die Sensor-Performance die Überwachung des gebündelt vorliegenden Verkehrs erlaubt.

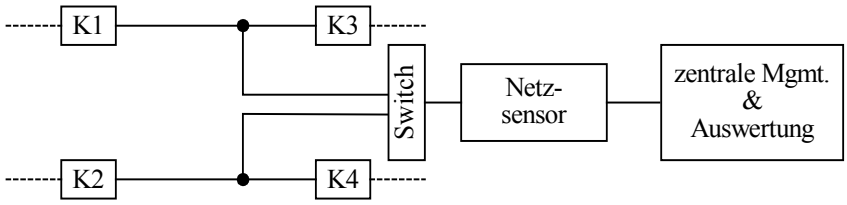

Abbildung 4-11: Zusammenführung des Netzverkehrs über einen Switch

4. **Anpassung der Konfiguration von Switches**: Falls der zu überwachende Netzverkehr über Switches auf die Zielsysteme verteilt wird, besteht ggf. die Möglichkeit, den gesamten Netzverkehr durch die Anpassung der Konfiguration der Switches zentral auf einen zusätzlichen Port eines Switches zu spiegeln. Dies hat den Vorteil, dass vorhandene Komponenten für die Zusammenführung des Verkehrs genutzt werden können.

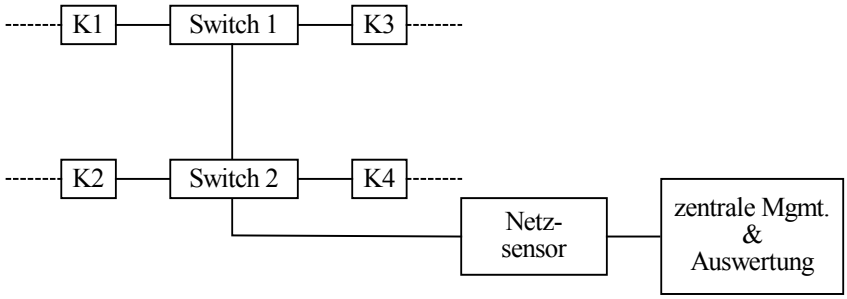

Abbildung 4-12: Abgriff des Netzverkehrs von einem Switch

4.4.3 Abgriff des Netzverkehrs in Multicast-Szenarien

Beim Multicast werden mehrere Systeme mit derselben Adresse (IP-/MAC-Adresse) konfiguriert. Eingehender Netzverkehr erreicht sämtliche dieser Systeme parallel und wird von diesen verteilt bearbeitet. Auf der Ebene des Netzverkehrs hat dies zur Folge, dass am Netzinterface eines Systems zwar der eingehende Verkehr vollständig anliegt, der ausgehende Verkehr jedoch nur für den von diesem System bearbeiteten Teil des Verkehrs. Diese Situation ist in Abbildung 4-13 skizziert. Der eingehende Netzverkehr (A, B, C, D) wird über Switches (K1, K2) zu den Komponenten K3 und K4 gesendet. K3 und K4 teilen sich die Bearbeitung des Verkehrs (K3 bearbeitet A und B, K4 bearbeitet C und D). Die Überwachung des Verkehrs an dieser Stelle durch einen Netzsensor ist problematisch, da der Netzsensor nicht weiß, welcher Teil des eingehenden Verkehrs durch das System weiterbearbeitet wird und welcher nicht. Dies betrifft den oben diskutierten Ansatz 1 (Einsatz mehrerer Sensoren). Ein Netzsensor vor K3 würde z. B. C und D als suspekt erkennen, da auf diese (policy-konformen) Pakete von K3 keine Reaktion erfolgt.

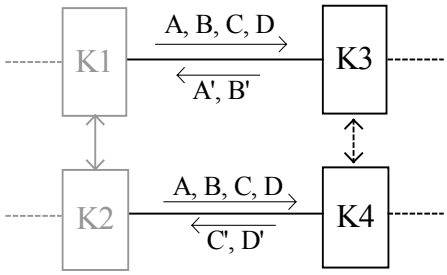

Abbildung 4-13: Skizze der Multicast-Problematik

Auch die direkte Zusammenführung des Verkehrs (oben beschriebene Ansätze 2 und 3) stellt keine Lösung dar, da im zusammengeführten Verkehr sämtliche eingehenden Pakete doppelt auftreten. Ein Filterung der doppelt auftretenden Pakete aus dem eingehenden Verkehr wäre erforderlich.

Die Problematik und eine Lösungsmöglichkeit soll am Beispiel eines hochverfügbar ausgelegten Internet-Übergang dargestellt werden, bei dem interne Router, Firewalls und externe Router doppelt ausgelegt sind (siehe Abbildung 4-14). Die Verfügbarkeit ist sichergestellt, solange nicht beide internen Router, beide Firewalls oder beide externen Router gleichzeitig ausfallen.

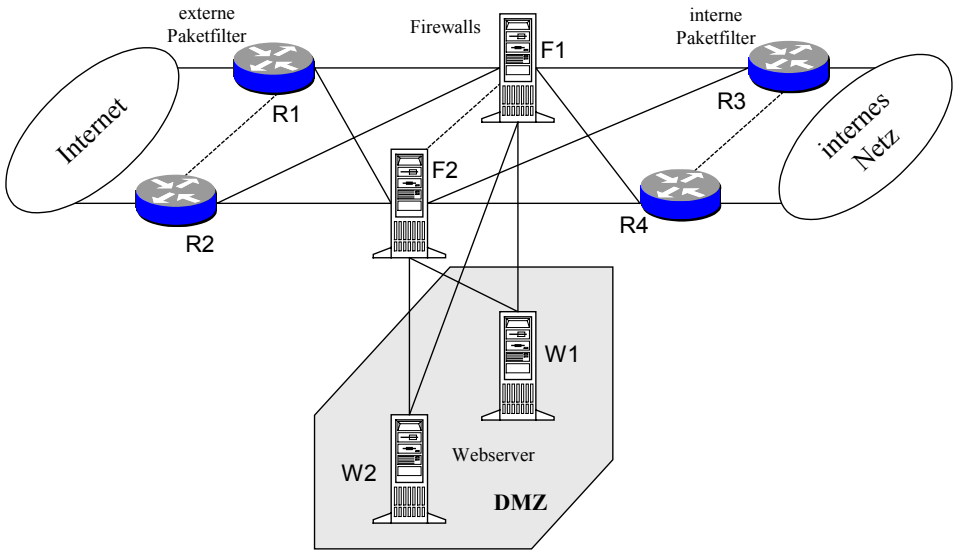

Abbildung 4-14: Beispiel eines hochverfügbaren Internet-Übergangs

Realisiert wird dies typischerweise durch den Einsatz von Switches, die den Netzverkehr zwischen den Komponenten verteilen (siehe Abbildung 4-15). Z. B. wird der von R3 kommende Verkehr über S3 an F1 und gleichzeitig (über S4) an F2 gesendet.

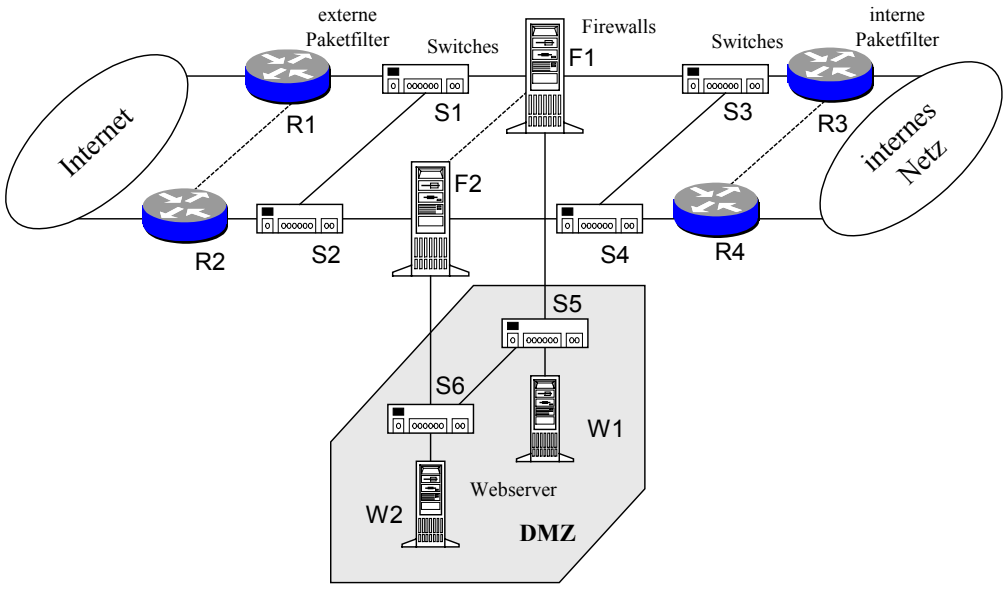

Abbildung 4-15: Realisierung eines hochverfügbaren Internet-Übergangs

Falls die beiden Firewalls im Multicast betrieben werden, tritt die oben dargestellte Situation an jedem der drei Netzinterfaces der Firewalls auf. Ein Abgriff des vollständigen Netzverkehrs auf den Strecken F2-S4-R4 und F1-S3-R3 ist damit nicht direkt möglich. Dies gilt in gleicher Weise für die anderen Schnittstellen der Firewalls.

Da die Switches den Netzverkehr gleichzeitig an beide Firewalls senden, liegt jedoch auf der Übertragungsstrecke zwischen S3 und S4 der vollständige Netzverkehr zwischen internem Netz und Firewall genau einmal an. Er kann hier entweder direkt über einen TAP abgegriffen werden oder auf einen zusätzlichen Port an einem der Switches gespiegelt werden. Gleiches gilt wiederum für die Schnittstellen der Firewall ins Internet und die DMZ.

Bei komplexeren, geswitchten Netztopologien ist häufig eine Konfigurationsänderung eingesetzter Switches erforderlich, um den Netzverkehr vollständig abgreifen zu können und dabei sicherzustellen, dass jedes Paket genau einmal vorkommt (vgl. auch Anhang 4.4.2, Punkt 4.).

4.4.4 Beispiel für Festlegungen zur IDS-Eskalation

IDS-Monitoring

Dem IDS-Monitoring obliegt die Beobachtung der IDS-Meldungen und eskaliert gemäß IDS-Eskalationsplan. Da das IDS-Monitoring keine Analyse der IDS-Alarme durchführt, kann auch keine qualitative Bewertung der Alarme vorgenommen werden. Die vom IDS gemeldeten Alarmlevel dienen als Grundlage für die Eskalation.

- Bei Ereignissen der Alarmstufe 1 erfolgt eine Benachrichtigung des IDS-Incident-Response per E-Mail, so dass das IDS-Incident-Response spätestens am nächsten Arbeitstag auf den Alarm reagiert.
- Bei Ereignissen der Alarmstufe 2 erfolgt eine sofortige Benachrichtigung des IDS-Incident-Response über eine telefonische Rufbereitschaft.

IDS-Incident-Response

Das IDS-Incident-Response bewertet das Ereignis und dessen Auswirkungen qualitativ und entscheidet,

- ob das Ereignis nicht weiter zu berücksichtigen ist, da es unwichtig erscheint (z. B. Fehlalarm),
- ob das Ereignis mit geringerer Priorität zu behandeln ist, da ggf. wichtigere Ereignisse vorliegen,
- ob das verursachte Problem innerhalb der IT-Abteilung gelöst werden kann,
- ob eine weitergehende Eskalation erforderlich ist, z. B. an den Abteilungsleiter.

Gemäß IDS-Eskalationsplan ist dabei vorgeschrieben, dass eine Benachrichtigung des Abteilungsleiter zu erfolgen hat, falls ein Problem nicht innerhalb von 4 Std. nach Kenntnisnahme behebbar ist.

Eskalationsebenen

Die oben genannten Eskalationsebenen IDS-Monitoring und IDS-Incident-Response werden je nach Organisation durch weitere Eskalationsebenen ergänzt, die über den Bereich des IDS hinausgehen.

Sobald das Problem auf Ebene der IT-Abteilung eskaliert wurde, muss ein hier definiertes (oder zu definierendes) IT-Krisenmanagement eingreifen. Ab dieser Ebene werden Angriffe, die durch das IDS erkannt werden, wie andere schwere IT-Störungen behandelt. Folgende Tabelle zeigt beispielhaft die Einbindung des IDS in eine Eskalationshierarchie.

Eskalationsstufe	Abteilung	Involvierte Rolle	Ereignisabhängige Aktion	Mitteilung an
Stufe 1	Unternehmensleitung	Vorstand		
Stufe 2	Organisationsbereiche	Bereichsleiter	- Eskalation zu Stufe 1	
Stufe 3	IT-Gesamt	Abteilungsleiter IT	- Einberufung eines IT-Krisenstabs - Eskalation zu Stufe 2	IT-Abteilungen
Stufe 4	IT-Abteilungen (IT-Systeme, IT-Netzbetrieb)	IDS-Incident-Response	- Rückstufung des Ereignisses (Downgrade) - Abteilungsinterne Lösung des Problems - Eskalation zu Stufe 3	IDS-Administration ggf. IDS-Manager
Stufe 5	IDS-Betrieb	IDS-Monitoring	- Alarmlevel 1: Eskalation per E-Mail zu Stufe 4 - Alarmlevel 2: Eskalation per Rufbereitschaft zu Stufe 4	
		IDS-Administration	- Nachverfolgung von Ereignissen - Ggf. Eskalation zu Stufe 4	

4.5 Hilfsmittel für die Integration

4.5.1 Verantwortlichkeiten und Zuständigkeiten IDS-spezifischer Rollen

Am Beispiel der Rollen des generischen Rollenmodells aus Kapitel 3.2.6 werden nachstehend Zuständigkeiten und Verantwortlichkeiten benannt, die für einen ordnungsgemäßen Betrieb des IDS notwendig sind.

4.5.1.1 IDS-Manager

Der IDS-Manager hat folgende Zuständigkeiten und Verantwortlichkeiten.

Vertretung der IDS-Ziele bei der IT-Planung und Entwicklung

Der IDS-Verantwortliche ist in die IT-Planung und -Entwicklung des Unternehmens einzubinden. Bei Änderungen der IT-Infrastruktur, wie z. B.

- Erweiterungen oder Änderungen der Netzinfrastruktur oder
- die Einführung von neuen Applikationen und/oder Systemen

hat er die Auswirkungen auf die Überwachungsfunktionalität des IDS hinsichtlich folgender Punkte zu prüfen.

- Gibt es Änderungen hinsichtlich der Zielsetzungen des IDS-Einsatzes?
- Ist das eingesetzte IDS geeignet, um die Zielsetzungen in der veränderten IT-Infrastruktur zu erreichen?
- Welche Anpassungen des IDS sind ggf. notwendig, um die Zielsetzungen zu erreichen, bzw. welche Einschränkungen ergeben sich hinsichtlich des Erreichens der Überwachungsziele?

Technische Einzelheiten zur Beantwortung der Fragestellungen werden in Abstimmung mit der IDS-Administration geklärt.

Umsetzung organisatorischer Maßnahmen

Der IDS-Manager ist für die Umsetzung sämtlicher organisatorischer Maßnahmen für den Betrieb des IDS verantwortlich.

Festlegung des IDS-Eskalationsplans

In Abstimmung mit den Mitarbeitern des IDS-Incident-Response und der IDS-Administration wird der IDS-Eskalationsplan erstellt.

Aufnahme der IDS-Überwachungsziele in den Sicherheitsstandard

Der IDS-Manager ist für die Aufnahme der Überwachungsziele des IDS in den Sicherheitsstandard (im Sinne einer Policy) des Unternehmens zuständig (vgl. Kapitel 3.6.4).

Sicherstellung der Berücksichtigung rechtlicher Vorgaben

Es liegt im Verantwortungsbereich des IDS-Managers sicherzustellen, dass die rechtliche Vorgaben - insbesondere zum Datenschutz - beim Betrieb des IDS eingehalten werden. Er sollte hierzu Anforderungen und Maßnahmen mit dem Datenschutzbeauftragten und der Arbeitnehmervertretung abstimmen und die zugehörigen Maßnahmen umsetzen (siehe auch Kapitel 3.6.8).

4.5.1.2 IDS-Administration

Der IDS-Administration obliegen sämtliche Aufgaben, die mit der technischen Verwaltung, Aktualisierung und Aufrechterhaltung des Betriebs des IDS verbunden sind. Nachfolgend sind zugehörige Zuständigkeiten und Verantwortlichkeiten angegeben:

Anpassung und Kalibrierung des IDS

Insbesondere nach Änderungen der zu schützenden Infrastruktur sind Anpassungen erforderlich. Anpassungen an der Einsatzweise des IDS ergeben sich, falls neue Teilnetze oder neue IT-Systeme integriert werden, die z. B. durch Einsatz weiterer Sensoren, in die Überwachung einbezogen werden sollen. Änderungen an der Kalibrierung sind erforderlich, wenn sich etwa sicherheitsrelevante Konfigurationseinstellungen bestehender Systeme ändern oder Applikationen auf eine andere Systemplattform migriert werden. Die IDS-Administration sollte daher in ein bestehendes IT-Konfigurationsmanagement eingebunden werden.

Regelmäßige Aktualisierung der IDS-Signaturen

Nach der Bereitstellung neuer Signaturen durch den IDS-Hersteller sind diese in das IDS zu importieren. Hinzugekommene Signaturen sind zu kalibrieren.

Regelmäßige Aktualisierung der IDS-Software

Es ist regelmäßig zu prüfen, ob für das IDS Patches oder neue Produktversionen vorliegen. Das IDS ist auf Basis dieser Informationen zu aktualisieren.

Regelmäßige Auswertung von IDS-Meldungen und Kalibrierung

Im Rahmen der Erstkalibrierung als „zur Nachverfolgung“ gekennzeichnete Ereignisse und Ereignisse, für die die zugehörigen Signaturen bislang nicht konfiguriert wurden, sind hinsichtlich ihrer Auswirkungen auf die zu schützende IT-Infrastruktur zu bewerten. Die Kalibrierung des IDS ist auf Basis der Bewertung anzupassen. Bei der Definition von IDS-Alarmen für neue Ereignisse ist ein Alarmlevel festzulegen.

Dokumentation und Datensicherung des aktuellen Stands des IDS

Nach jeder Aktualisierung des IDS ist der aktuelle Stand des IDS zu sichern. Der aktuelle Stand der Softwarekomponenten (Patchlevel, Version) und die letzte Aktualisierung der IDS-Signaturen sind zusammen mit ihren Zeitpunkten zu dokumentieren[21]. Die Kalibrierung des IDS ist implizit durch den aktuellen Stand des IDS dokumentiert. Eine explizite Dokumentation der Kalibrierung ist aufgrund ihres Umfangs nicht sinnvoll. Auch bieten marktverfügbare IDS hierzu typischerweise keine Funktionen an.

Regelmäßiges Reporting an den IDS-Manager

Es ist festzulegen, wie oft und in welcher Form der IDS-Manager regelmäßig von der IDS-Administration über vom IDS erkannte Ereignisse informiert wird. Einzelheiten zur Benachrichtigung des IDS-Managers bei sicherheitskritischen Ereignissen sind im Rahmen des IDS-Eskalationsplans festzulegen.

Unterstützung bei der Klärung von Angriffen

Im Bedarfsfall unterstützt die IDS-Administration Mitarbeiter des IDS-Incident-Response bei der Klärung von Angriffen.

Regelmäßige Aktualisierung der Kenntnisse über neue Angriffe und Sicherheitslücken

Die IDS-Administration hat hinsichtlich der Kenntnisse über Angriffe und Sicherheitslücken ständig auf einem aktuellen Stand zu sein, um die Bedrohungslage und die Aktualität der Angriffserkennung durch das IDS beurteilen zu können.

Schulung und Einweisung der Mitarbeiter des IDS-Incident-Response und des IDS-Monitoring

Die IDS-Administration schult Mitarbeiter des IDS-Monitoring in der Anwendung der IDS-Eskalationsplans und weist Mitarbeiter des IDS-Incident-Response in die erforderlichen IDS-Kenntnisse ein.

Nachbearbeitung aufgetretener IDS-Alarme

Die IDS-Administration trägt die Verantwortung für die Nachbereitung aufgetretener IDS-Alarme. Eine Nachbearbeitung erfolgt, nachdem das IDS-Incident-Response auf den IDS-Alarm reagiert hat und die IDS-Administration über den Alarm informiert wurde. Die Nachbearbeitung umfasst die Klärung folgender Fragestellungen und/oder die Durchführung bzw. Veranlassung der zugehörigen Aktivitäten:

- Soll eine Rückverfolgung des Angriffs bzw. Angreifers oder eine gezielte Überwachung der IP-Adresse erfolgen, von der aus der Angriff initiiert wurde?
- Gibt es sinnvolle Gegenmaßnahmen, um zukünftige Angriffsversuche gleicher Art begegnen oder vermeiden zu können? Es ist zu prüfen, ob ein automatisches Auslösen von Gegenmaßnahmen durch das IDS (wie z. B. die Unterbrechung der Kommunikationsbeziehung) sinnvoll ist oder der Angriff durch eine Konfigurationsänderung des Firewall-Systems abgewehrt werden kann.

[21] Falls das IDS diese Daten nicht selbst protokolliert, ist ein schriftliches Protokoll vorzuhalten.

- Ist das Einschalten oder Verständigen weiterer, bislang nicht im IDS-Eskalationsplan festgelegter Stellen (z. B. Revision) erforderlich?
- Ist der Alarm einem anderen Alarmlevel zuzuweisen? (Änderung des IDS-Eskalationsplans)
- Ist auf Basis der vorliegenden Erfahrungen eine Anpassung der Kalibrierung erforderlich? Falls der Alarm sich bereits mehrfach als Fehlalarm erwiesen hat, sollte die Kalibrierung ggf. dahingehend verändert werden, dass bei Erkennung des Ereignisses keine Alarmierung erfolgt.

4.5.1.3 IDS-Monitoring

Die Zuständigkeiten des IDS-Monitoring umfassen die folgenden zwei Aktivitäten:

- Annahme von Alarmen des IDS
- Anstoßen der definierten Eskalation

4.5.1.4 IDS-Incident-Response

Das IDS-Incident-Response ist im Wesentlichen für eine zeitgerechte und angemessene Reaktion auf IDS-Alarme zuständig. „Zeitgerecht“ bedeutet dabei die Einhaltung der ggf. im IDS-Eskalationsplan angegebenen Fristen für die Problembehebung und die ggf. weitere Eskalation. Eine angemessene Reaktion umfasst folgende Aktivitäten:

Identifizierung des Angriffs und seiner Randbedingungen

- Um welche Art Angriff handelt es sich genau (Angriffsart, Parameter)?
- Gegen welche Systeme richtete sich der Angriff?
- Welche möglichen Auswirkungen hat der Angriff auf die betroffenen Systeme?
- Von wo aus wurde der Angriff initiiert? (Internet, internes Netz, ggf. System)

Klärung der Auswirkungen des Angriffs

- Welche Auswirkungen hat bzw. hatte der Angriff?
- Benachrichtigung zuständiger Stellen über eventuelle Schäden.

Ggf. Einleitung von Maßnahmen zur Schadensbehebung bzw. -begrenzung.

Zur Schadensbehebung oder -begrenzung bedarf es ggf. der Mitarbeit weiterer Stellen (wie z. B. der Firewall-Administration, falls eine Konfigurationsänderung an der Firewall erforderlich ist). Es ist abzustimmen, ob dem IDS-Incident-Response gegenüber den erforderlichen Stellen für diese Fälle ein direktes Weisungsrecht eingeräumt wird. Alternativ hierzu kann die Weisung durch übergeordnete Stellen (z. B. Abteilungsleiter) erfolgen, der im Rahmen der Eskalation verständigt wird.

Informieren der IDS-Administration

Die IDS-Administration ist über den Alarm, dessen Auswirkungen und eingeleitete Maßnahmen zu informieren. Auf dieser Basis erfolgt die Nachbearbeitung des IDS-Alarms (siehe Abschnitt 4.5.1.2).

4.5.2 Einzelaktivitäten zur Kalibrierung

Im Rahmen der Kalibrierung sind grundsätzlich für jede Signatur[22] folgende Aktivitäten durchzuführen:

- Klärung der Funktionsweise und des Zwecks der Signatur:
  - Welcher Angriff, welche Sicherheitsverletzung wird durch die Signatur erkannt?
  - Gegen welche Art von Zielsystem richtet er sich?
  - Welche Auswirkungen hat ein erfolgreicher Angriff auf das Zielsystem?
  - Wie groß ist die Wahrscheinlichkeit von Fehlalarmen, d. h. wie wahrscheinlich ist es, dass die Signatur triggert, obwohl kein Angriff vorliegt oder der Angriff keine Auswirkungen hat?[23]
- Klärung potenzieller Auswirkungen auf die zu schützende Infrastruktur:
  - Welche Relevanz hat der Angriff bzw. die Sicherheitsverletzung für die zu schützende Infrastruktur? Gibt es in der Infrastruktur Komponenten, gegen die sich der Angriff richtet?
  - Sind die Komponenten, gegen die sich der Angriff richtet, gegen die Sicherheitsverletzung bzw. den Angriff anfällig oder sind sie bereits resistent (etwa durch eine geeignete Konfiguration oder dem Einspielen aktueller Security-Patches)?
- Festlegung einer sinnvollen technischen und organisatorischen Reaktion auf das Ereignis, in Abhängigkeit der potenziellen Auswirkungen des Ereignisses:
  - Wie soll das IDS auf die Erkennung des Ereignisses reagieren? (Deaktivierung der Signatur, Protokollierung zu Auswertungszwecken oder zur Nachverfolgung, Alarmierung)
  - Für Ereignisse, bei denen alarmiert wird, sind des Weiteren folgende Aktivitäten durchzuführen:
    - Im Rahmen der Kalibrierung ist dem Alarm ein IDS-Alarmlevel zuzuordnen.
    - Die im IDS-Eskalationsplan für den Alarmlevel vorgesehene Eskalation ist auf Eignung zu prüfen. Ggf. ist eine ereignisspezifische Eskalation festzulegen und der IDS-Eskalationsplan zu aktualisieren.

4.5.3 Beispielvereinbarungen zur Arbeitnehmer-Mitbestimmung und zum Datenschutz

Um datenschutzrechtliche Anforderungen zu erfüllen und sicherzustellen, dass das IDS über den festgelegten Einsatzzweck hinaus nicht zur Verhaltenskontrolle von Mitarbeitern eingesetzt wird, sind die nachstehend genannten Maßnahmen umzusetzten[24]. Unternehmensspezifisch festzulegende Parameter sind dabei als <*Parameter*> gekennzeichnet.

1. Alle Mitarbeiter werden über den Einsatz des IDS und die Einsatzzwecke informiert[25].

---

[22] Unter Signatur wird hier allgemein - unabhängig von der Verfahrensweise - ein Mechanismus zur Erkennung eines bestimmten Ereignisses verstanden.

[23] Diese Fragestellung kann typischerweise nicht ohne Erfahrungen im IDS-Einsatz beantwortet werden. Eine geringe Wahrscheinlichkeit von Fehlalarmen ist jedoch eine grundlegende Voraussetzung dafür, dass eine Alarmierung als Reaktion des IDS auf das Triggern der Signatur vorgesehen werden kann.

[24] Die Maßnahmen sind als Beispiel gedacht. Sie erheben keinen Anspruch auf Vollständigkeit und sind im Einzelfall mit dem Datenschutzbeauftragten und der Rechtsabeitlung abzustimmen.

[25] Abhängig von der Einsatzweise des IDS bleibt zu prüfen, ob es erforderlich ist, dass jeder Mitarbeiter sein Einverständnis zum IDS-Einsatz erklärt.

2. Sämtliche Mitarbeiter, die das IDS administrieren oder Zugriff auf Daten des IDS-Ereignisprotokolls haben, sind auf das Datenschutzgesetz zu verpflichten.
3. Im Rahmen des IDS-Einsatzes erfolgt die Aufzeichnung personenbezogener Daten ausschließlich, um den ordnungsgemäßen Betrieb von Datenverarbeitungsanlagen sicherzustellen. Eine Aufzeichnung von Daten erfolgt in dem Umfang, wie es für die Erkennung von Angriffen, Angriffsversuchen und Sicherheitsverletzungen und ggf. deren Rückverfolgung erforderlich ist. Personenbezogene Daten werden zu keinem anderen Zweck aufgezeichnet.
4. Vom IDS aufgezeichnete Daten, die zur Zuordnung erkannter Ereignisse (etwa Angriffe oder Sicherheitsverletzungen) zu deren Verursachern dienen, dürfen von IDS-Mitarbeitern nur dann an <*befugte Dritte*> weitergegeben werden, wenn aufgrund des Ereignisses, dessen Auswirkungen oder sich ergebenden Gefährdungen vom <*Vorgesetzten*> entschieden wurde, den Verursacher des Ereignisses zu ermitteln, oder die Weitergabe der Daten gemäß <*Richtlinie*> vorgesehen ist[26].
5. Die aufgezeichneten Daten werden spätestens nach einem Zeitraum von <*2 Monaten*> gelöscht. Ausgenommen hiervon sind Daten, deren weitere Speicherung aufgrund von Beweis- oder Nachweiszwecken erforderlich ist.
6. Änderungen der Einsatzweise des IDS oder der IDS-Einsatzzwecke erfordern die Zustimmung des Betriebsrats bzw. Personalrats.

4.6 Hilfsmittel für den Betrieb

4.6.1 Dokumentenrahmen für ein IDS-Betriebshandbuch

Die im Betriebshandbuch aufgeführten Punkte können im Fall der Auslagerung des IDS an externe Betreiber durch Dienstgüte-Vereinbarungen (Service-Level-Agreements) referenziert werden.

Kapitel 1: Motivierende Einleitung

Die Zielsetzungen des IDS-Einsatzes sind managementorientiert und technikorientiert zu beschreiben. Die Verankerung des IDS-Einsatzes in den Sicherheitsstandards[27] des Unternehmens ist an dieser Stelle zu referenzieren bzw. zu zitieren.

Kapitel 2: Allgemeines

In diesem Abschnitt werden alle zum Dokument gehörenden „Metadaten“ aufgeführt:

- die Einordnung des Dokuments in Bezug auf weitere Dokumente zum organisationsweiten IT-Sicherheitsmanagement,
- Stand und Versionsnummer des Dokuments, Bearbeiter, Versionshistorie,
- Verantwortlichkeiten für die Fortschreibung des Dokuments,
- Adressaten des Handbuchs: Sämtliche direkt oder indirekt am IDS-Einsatz und Betrieb beteiligte Organisationseinheiten, Institutionen oder Partner.

Kapitel 3: Beschreibung der Infrastruktur

Kapitel 3.1: Architektur des IDS

---

[26] Im Rahmen einer Richtlinie kann festgelegt werden, ab welchem Gefährdungs- bzw. Schadensausmaß in jedem Fall versucht werden soll, den Verursacher zu ermitteln.

[27] Sicherheitsstandards im Sinne einer „Policy“.

Der konkrete Aufbau des eingesetzten IDS, die Komponenten des IDS und ihr Einsatzzweck im IDS-Umfeld sind zu beschreiben:

- IDS-Management- und Auswertungsstation,
- IDS-Ereignisdatenbank,
- eingesetzte IDS-Sensoren und ihre Platzierungen,
- IDS-relevante Netzwerkkomponenten (Hubs, TAPs, Switches, Teilnetze),
- IDS-relevante sonstige Systeme.

(Die Beschreibung kann aus dem Feinkonzept übernommen werden).

Kapitel 3.2: Funktionsweise des IDS

Beschreibung der Gesamtfunktion des IDS sowie der Teilfunktionen der einzelnen IDS-Komponenten.

Kapitel 3.3: Ausstattungsmerkmale der IDS-Komponenten

Detailbeschreibung der einzelnen IDS-Komponenten (Namensgebung, IP-Adressen, Konfigurationsmerkmale).

Kapitel 4: Regelungen zur Inbetriebnahme der einzelnen IDS-Komponenten

Kapitel 4.1: Inbetriebnahme der Management- und Auswertungsstation(en)

Die Inbetriebnahme der eingesetzten Management- und Auswertungsstation(en) ist zu beschreiben. Dies umfasst

- Installationshinweise,
- Zuständigkeit für die Installation der Komponente und
- Zuständigkeit für die Abnahme der Komponente.

Kapitel 4.2: Inbetriebnahme der IDS-Ereignisdatenbank

Die Inbetriebnahme der eingesetzten Ereignisdatenbank ist zu beschreiben. Dies umfasst

- Installationshinweise,
- Zuständigkeiten für die Installation der Komponente und
- Zuständigkeiten für die Abnahme der Komponente.

Kapitel 4.3: Inbetriebnahme der Netzsensoren

Für sämtliche Netzsensoren ist in separaten Abschnitten das Vorgehen ihrer Inbetriebnahme zu beschreiben. Dies umfasst

- Installationshinweise,
- Zuständigkeiten für die Installation des Netzsensors und
- Zuständigkeit für die Abnahme der Komponente.

Kapitel 4.4: Inbetriebnahme der Hostsensoren

Für sämtliche Hostsensoren ist in separaten Abschnitten das Vorgehen ihrer Inbetriebnahme zu beschreiben. Dies umfasst

- Installationshinweise,
- Zuständigkeiten für die Installation des Hostsensors,
- Zuständigkeit für die Abnahme des Hostsensors.

Kapitel 4.5: Anbindung sonstiger mit dem IDS in Zusammenhang stehender Systeme

Die Inbetriebnahme sonstiger, mit dem IDS in Zusammenhang stehender Systeme, wie z. B. Mailserver oder SMS-Gateway, ist zu beschreiben. Dies umfasst

- Installations- und Konfigurationshinweise,
- Zuständigkeiten für die Installation der Komponenten und
- Zuständigkeiten für die Abnahme der Komponenten.

Kapitel 5: Regelungen für den Betrieb der IDS-Komponenten

Kapitel 5.1: Hardwareservice und Systemwartung

- Wer (welche Organisationseinheit/Rolle) ist für den Hardwareservice und die Systemwartung verantwortlich?
- Durch wen werden die Arbeiten durchgeführt?
- In welchem zeitlichen Abstand sind die Arbeiten auszuführen?
- Welche Berechtigungen (Zutritt, Zugang, Administrationsrechte) gelten für die Ausführung der Arbeiten?

Kapitel 5.2: Monitoring

- Wer (welche Organisationseinheit/Rolle) ist für das IDS-Monitoring verantwortlich?
- Durch wen werden die Arbeiten durchgeführt?
- Zu welchen Zeiten soll das IDS-Monitoring durchgeführt werden? (7 x 24 Stunden?)
- Welche Berechtigungen (Zutritt, Zugang, Administrationsrechte) gelten für die Ausführung der Arbeiten?

Kapitel 5.3: Backup

- Wer (welche Organisationseinheit/Rolle) ist für das Backup des IDS verantwortlich?
- Durch wen werden die Arbeiten durchgeführt?
- In welchem zeitlichen Abstand sind die Arbeiten auszuführen?
- Welche Berechtigungen (Zutritt, Zugang, Administrationsrechte) gelten für die Ausführung der Arbeiten?

Kapitel 5.4: Präventive Dienste

- Welche Arbeiten sind präventiv durchzuführen?
  - Kalibrierung der IDS-Sensoren
  - Beobachtung von Veränderungen an überwachten IT-Systemen und Netzen
  - Regelmäßige Durchführung von Alarm- und Eskalationsübungen
- Wer (welche Organisationseinheit/Rolle) führt die jeweiligen Arbeiten durch?
- Wer ist für die Durchführung verantwortlich?
- In welchem zeitlichen Abstand sind die Arbeiten auszuführen?

Kapitel 5.5: Dokumentation

- Wer (welche Organisationseinheit/Rolle) ist für die Dokumentation des IDS verantwortlich?
- Durch wen werden die Arbeiten durchgeführt?

- In welchem zeitlichen Abstand ist die Dokumentation zu überprüfen und ggf. zu ergänzen?

Kapitel 5.6: Change Management

- Was unterliegt dem Change Management des IDS?
  - Berücksichtigung von Änderungen an überwachten IT-Systemen und Netzen,
  - IDS-Signatur-Updates,
  - IDS-Versions-Upgrades.
- Wer (welche Organisationseinheit/Rolle) ist für die Fortentwicklung des IDS verantwortlich?
- In welchem zeitlichen Abstand ist die Notwendigkeit von Änderungen zu prüfen?
  - IDS-Signatur-Updates,
  - IDS-Versions-Upgrades.
- Durch wen werden die Arbeiten durchgeführt?

Kapitel 5.7: Administration des IDS

- Wer (welche Organisationseinheit/Rolle) ist für die Administration des IDS verantwortlich?
- Durch wen werden die Arbeiten durchgeführt?
- Zu welchen Zeiten soll die Administration des IDS erfolgen?
- Welche Berechtigungen (Zutritt, Zugang, Administrationsrechte) gelten für die Ausführung der Arbeiten?

Kapitel 6: Regelungen zur Behebung von Betriebsunterbrechungen

Kapitel 6.1: Störungsmanagement

In diesem Abschnitt werden Regelungen für den Fall einer Betriebsstörung des IDS (nicht Störungen der überwachten Systeme) dokumentiert:

- Verantwortlichkeit für das Management bei Störungen des IDS
- Regelung zur Meldung (Eskalation) bei Störungen des IDS
- Grobkriterien zur Ersteinschätzung der Schwere der Störung des IDS

Kapitel 6.2: Behebung von Funktionsstörungen (Recovery-Maßnahmen)

- Hinweise zur Störungsbeseitigung für die betreffende Komponente
- Hinweise zu Störungen, die in der Vergangenheit auftraten (Störfallszenarien) und Erfahrungsberichte

Kapitel 7: Richtlinien zur Nutzung des IDS

Kapitel 7.1: Benutzer-Rollen, Zugangs- und Zugriffsrechte

Kapitel 7.2: Verantwortung für Vergabe und Entzug von IDS-spezifischen Zugangs- und Zugriffsrechten

Anlage

In der Anlage sollten Detailinformationen, die sich in kurzen Zeitabständen ändern können (Telefonnummern, Rolleninhaber) aufgeführt werden. Hinzu kommen Informationen zu Organisationseinheiten und Systemstandorten sowie ein Literatur- und Abkürzungsverzeichnis.

4.6.2 Übersicht über betriebsrelevante Prozesse und Aktivitäten

Die nachfolgende Tabelle gibt eine Übersicht über die wesentlichen betriebsrelevanten Prozesse und Aktivitäten. Die einzelnen Ablaufschritte wurden im Rahmen der Beschreibung der Zuständigkeiten und Verantwortlichkeiten der Rollen in Anhang 4.5.1 erläutert.

Prozess/Aktivität	Ablaufschritte	Rolle	Ausführungszeitpunkt
Verfeinerung der IDS-Kalibrierung	- Prüfung der möglichen Auswirkungen des Ereignisses - Festlegung einer Intrusion-Response auf das Ereignis - Falls Alarmierung vorgesehen wird: Festlegung eines Alarmlevels und Prüfung bzw. Anpassung des IDS- Eskalationsplans	IDS-Administration	Regelmäßig beim Auftreten von Ereignissen, die bislang nicht bewertet wurden[28]
Nachverfolgung von Ereignissen	- Prüfung der Auswirkungen des Ereignisses und angemessene Reaktion - Prüfung, ob Einstufung als „Protokollierung zur Nachverfolgung“ weiterhin sinnvoll und korrekt ist - Ggf. Anpassung der Kalibrierung	IDS-Administration, ggf. unterstützt durch IDS-Incident-Response	Regelmäßig beim Auftreten von Ereignissen, für die eine „Protokollierung zur Nachverfolgung“ erfolgt
Reaktion auf IDS-Alarme	- Annahme des Alarms und Eskalation gemäß IDS-Eskalationsplan	IDS-Monitoring	Bei IDS-Alarmierungen
	- Prüfung der Auswirkungen des Ereignisses und angemessene Reaktion (vgl. Anhang 4.5.1) - Informieren der IDS-Administration	IDS-Incident-Response	
	- Nachbearbeitung des IDS-Alarms (vgl. Anhang 4.5.1)	IDS-Administration	
Aktualisierung der Signaturen	- Einspielen der Signaturen - Kalibrierung der neuen Signaturen - Dokumentation der Aktualisierung	IDS-Administration	Regelmäßig sobald neue Signaturen verfügbar sind
Aktualisierung der IDS-Software	- Aktualisierung der IDS-Software - Funktionsprüfung der aktualisierten Komponenten - Dokumentation der Aktualisierung	IDS-Administration, Systemadministration	Falls Software-Patches oder neue IDS-Versionen verfügbar

[28] Es wird von den in Kapitel 3.6.3 beschriebenen generischen Reaktionen ausgegangen: „Alarmierung“, „Protokollierung zur Nachverfolgung“, „Protokollierung zu Auswertungszwecken“, „Unterdrückung“ und „Nicht bearbeitet“.

Prozess/Aktivität	Ablaufschritte	Rolle	Ausführungszeitpunkt
Begleitung der IT-Planung und IT-Entwicklung	IDS-Manager ist in IT-Planungs- und Entwicklungsprozesse einzubinden - Stellungnahme zu Auswirkungen der Planung/Entwicklung auf die Überwachungsfunktionen des IDS	IDS-Manager	Regelmäßig, sobald konkrete Planungen vorliegen
Anpassung des IDS	- Abstimmung der Einsatzziele und der Einsatzweise des IDS in der veränderten IT-Infrastruktur - Ggf. Aktualisierung der Sicherheitsstandards im Hinblick auf veränderte IDS-Einsatzziele	IDS-Manager	Änderungen der zu überwachenden IT-Infrastruktur
	- Durchführung der notwendigen Anpassungen, z. B. • Integration zusätzlicher Sensoren • Aktualisierung der Kalibrierung - Aktualisierung der Dokumentation	IDS-Administration, Systemadministration	
Datensicherung des IDS	- Datensicherung veränderter bzw. aktualisierter Komponenten - Dokumentation der Datensicherung	IDS-Administration, Systemadministration	Regelmäßig, nach jeder wesentlichen Änderung bzw. Aktualisierung des IDS

4.7 Hilfsmittel für die Revision

4.7.1 Fragen und Prüfmethoden zur Prüfung der Dokumentation

Frage: **Gibt es einen IDS-Eskalationsplan? Erfüllt der Eskalationsplan folgende Anforderungen?**

- Für jeden Alarm bzw. Alarmlevel ist angegeben, welche Eskalation bei dessen Auftreten zu erfolgen hat, d. h. wer mit welcher Dringlichkeit zu benachrichtigen ist und über welche Kommunikationsmedien mit welchen Adressen die Benachrichtigung erfolgt.
- Für Alarme des IDS, kann in einfacher Weise ohne spezielles IDS-Know-How ermittelt werden, welche Eskalationsschritte durchzuführen sind.

Prüfmethode: Sichtung des IDS-Eskalationsplans beim IDS-Monitoring. Test der Anwendung des Plans auf ausgewählte IDS-Alarme.

Frage: **Liegt ein aktuelles Betriebshandbuch für das IDS vor? Enthält das Betriebshandbuch die notwendigen Informationen?**

Welche Inhalte das Betriebshandbuchs aufweisen sollte, ist im zugehörigen Dokumentenrahmen in Anhang 4.6.1 angegeben.

- Beschreibung der Infrastruktur,
- Regelungen zur Inbetriebnahme der einzelnen IDS-Komponenten,
- Regelungen für den Betrieb der IDS-Komponenten,
- Regelungen zur Behebung von Betriebsunterbrechungen,
- Richtlinien zur Nutzung des IDS.

Prüfmethode: Sichtung des IDS-Betriebshandbuchs.

Frage: **Ist der aktuelle Stand des IDS dokumentiert? Enthält die Dokumentation folgende Angaben?**

- Aktuelle Softwareversionen der einzelnen IDS-Komponenten.
- Zeitpunkt der letzten Aktualisierungen (Software, Patches, Signaturen).
- Aktuelle Änderungen des Einsatzszenarios (z. B. Einsatz zusätzlicher Sensoren), die aufgrund ihrer Aktualität noch nicht im Betriebshandbuch berücksichtigt sind.

Die Dokumentation kann teilweise auch implizit im System vorliegen und ist z. B. aus dem IDS-Systemprotokoll ersichtlich. Es ist zu prüfen, ob die IDS-Administration über die entsprechenden Daten verfügt bzw. diese schnell ermitteln kann.

Prüfmethode: Befragung der IDS-Administration.

4.7.2 Fragen und Prüfmethoden zur Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs

Die Prüfung des ordnungsgemäßen IDS-Einsatzes und Betriebs umfasst folgende Kontrollen:

- Verfügen die Mitarbeiter, die in den definierten IDS-Rollen tätig werden, über die erforderlichen Kenntnisse und sind sie mit ihren Aufgaben vertraut?
- Wird das IDS gemäß dem dokumentierten Einsatzszenario eingesetzt?

Frage: **Sind die Mitarbeiter der IDS-Administration mit ihren Aufgaben vertraut und verfügen sie über die erforderlichen Kenntnisse?**

Prüfmethode: Ausgewählte Mitarbeiter der IDS-Administration werden nach ihren Aufgaben hinsichtlich des IDS befragt. Die Antworten werden anhand der im Betriebshandbuch dokumentierten Zuständigkeiten und Verantwortlichkeiten kontrolliert.

Der Revisor lässt sich von den Mitarbeitern das IDS-Ereignisprotokoll anzeigen. Für stichprobenhaft ausgewählte Ereignisse lässt sich der Revisor

- erläutern, welche Bedeutung das Ereignis hat und welche Auswirkungen es auf die zu schützende Infrastruktur hat, sowie
- zeigen, welche Intrusion-Response für das Ereignis konfiguriert ist.

Der Revisor ermittelt kürzlich bekannt gewordene Angriffe und Sicherheitslücken, z. B. durch Anfrage bei einem CERT oder öffentlicher Quellen. Er prüft, ob der IDS-Administrator über diese Angriffe bzw. Sicherheitslücken informiert ist, ob ihre Erkennung für die zu schützende Infrastruktur relevant ist und ob das IDS sie erkennt.

Frage: **Sind die Mitarbeiter des IDS-Monitoring mit ihren Aufgaben vertraut und verfügen sie über die erforderlichen Kenntnisse?**

Prüfmethode: Ausgewählte Mitarbeiter des IDS-Monitoring werden nach ihren Aufgaben in Bezug zum Intrusion-Detection befragt. Anhand ausgewählter Beispiele möglicher IDS-Alarmierungen wird geprüft, ob die einzelnen Mitarbeiter den Alarm in korrekter Weise einer Eskalationsstufe zuordnen und die durchzuführenden Eskalationsschritte ermitteln können.

Frage: **Sind die Mitarbeiter des IDS-Incident-Response mit ihren Aufgaben vertraut und verfügen sie über die erforderlichen Kenntnisse?**

Prüfmethode: Welche Mitarbeiter im Falle welcher IDS-Alarme zu verständigen sind, ist im IDS-Eskalationsplan aufgeführt. Für ausgewählte Alarme werden die gemäß IDS-Eskalationsplan für das Incident-Response zuständigen Mitarbeiter über ihre Aufgaben im Bezug auf Intrusion-Detection befragt.

Zunächst wird dabei geprüft, ob jeder Mitarbeiter darüber informiert ist, dass er im Fall des ausgewählten IDS-Alarms für das entsprechende Incident-Response zuständig ist.

Darauf aufbauend wird vom Mitarbeiter abgefragt, wie er sich im Falle einer Alarmierung verhält. Beispielsweise kann sich hierzu der Revisor vom Mitarbeiter anhand eines Beispiels aus der Vergangenheit den Incident-Response konkret erläutern lassen.

Frage: **Sind für hostbasierte Sensoren die entsprechenden System- bzw. Anwendungsverantwortlichen mit ihren Aufgaben vertraut?**

Prüfmethode: Für Systeme bzw. Anwendungen, die durch hostbasierte Sensoren überwacht werden, werden stichprobenhaft die zuständigen System- bzw. Anwendungsverantwortlichen nach ihren Aufgaben in Bezug zum Intrusion-Detection befragt. Die Antworten werden anhand der entsprechenden Regelungen im IDS-Betriebshandbuch kontrolliert.

Frage: **Wird das IDS gemäß dem dokumentierten Einsatzszenario eingesetzt?**

Prüfmethode: Der Revisor prüft das Einsatzszenario durch einen Vergleich des im IDS-Betriebshandbuch dokumentierten Einsatzszenarios mit dem realen Einsatzszenario. Er lässt sich hierzu durch einen Mitarbeiter der IDS-Administration erläutern, welche Sensoren verwaltet werden und auf welchen Systemen die Sensoren installiert sind. Bei hostbasierten Sensoren wird der Name des System- bzw. Anwendungsverantwortlichen des überwachten Systems abgefragt und stichprobenhaft kontrolliert, ob der System- bzw. Anwendungsverantwortliche den Betrieb des hostbasierten Sensors bestätigt.

4.7.3 Fragen und Prüfmethoden zur Prüfung der Wirksamkeit des IDS und der Incident-Response-Organisation

Zur Prüfung der Wirksamkeit des IDS und des Incident-Handlings erfolgen folgende Kontrollen:

- Erkennt und meldet das IDS Angriffe und Sicherheitsverletzungen?
- Ist das IDS sinnvoll und angemessen konfiguriert und kalibriert?
- Ist das Incident-Handling funktionstüchtig ist?
  - Reagiert das IDS-Monitoring in definierter Weise auf Alarme?
  - Ist das IDS-Incident-Response permanent besetzt?

Zur Kontrolle, ob das IDS Angriffe und Sicherheitsverletzungen erkennt und meldet, ist ein Penetrationstest auf den vom IDS überwachten Netzen und ausgewählten Systemen bzw. Anwendungen durchzuführen.

Frage: **Werden Angriffe und Sicherheitsverletzungen durch das IDS erkannt?**

Prüfmethode: Es werden Penetrationstests gegen die vom IDS überwachten (Teil-)Netze und ausgewählten Systeme bzw. Anwendungen durchgeführt. Im Rahmen der Befragung der IDS-Administration wird kontrolliert, ob die Penetrationstests vom IDS korrekt gemeldet wurden.

Voraussetzung für die folgenden Fragen ist, dass der Revisor über eine Liste ausgewählter, sicherheitskritischer Ereignisse verfügt. Diese Liste kann der Revisor z. B. mit Unterstützung durch interne oder externe Sicherheitsexperten anfertigen.

Frage: **Ist das IDS sinnvoll und angemessen kalibriert?**

Prüfmethode: Zusammen mit einem Mitarbeiter der IDS-Administration wird kontrolliert, ob das IDS so konfiguriert ist, dass bei der Erkennung von Ereignissen der o. g. Liste eine Alarmierung des IDS erfolgt.

Des Weiteren wird von der IDS-Administration für ausgewählte Alarme abgefragt, in welcher Weise diese dem IDS-Monitoring angezeigt werden. Der Revisor dokumentiert die Form der Anzeige des Alarms.

Frage: **Reagiert das IDS-Monitoring gemäß der Vorgaben auf Alarme?**

Prüfmethode: Zur Prüfung, ob das IDS-Monitoring gemäß dem IDS-Eskalationsplan auf Alarme reagiert, ist es sinnvoll, einen IDS-Alarm vorzutäuschen und die Reaktion des IDS-Monitoring zu kontrollieren.

Falls dies aus technischen Gründen nicht möglich ist, können lediglich die Rahmenbedingungen geprüft werden (vgl. Abschnitt 4.7.2): Für die zuvor ausgewählten Alarme wird geprüft, ob das IDS-Monitoring den Alarm in korrekter Weise einer Eskalationsstufe zuordnen und die durchzuführenden Eskalationsschritte ermitteln kann.

Frage: **Sind die für das IDS-Incident-Response vorgesehenen Mitarbeiter erreichbar?**

Prüfmethode: Sinnvoll wäre auch hier die Vortäuschung einer IDS-Alarmierung und die Kontrolle der Reaktion der gemäß IDS-Eskalationsplan für das IDS-Incident-Response verantwortlichen Mitarbeiter.

Falls dies aus technischen Gründen nicht möglich ist, wird für die ausgewählten Alarme geprüft, ob die gemäß IDS-Eskalationsplan zu verständigenden Mitarbeiter erreichbar sind.

4.7.4 Dokumentenrahmen für eine Revisionsrichtlinie

Kapitel 1: Zuständigkeiten und Vorgaben für die Revision des IDS

Hier ist anzugeben, wer für die Revision des IDS verantwortlich ist und wie oft bzw. zu welchen Zeitpunkten eine Revision durchgeführt werden soll.

Kapitel 2: Vorgehen zur Revision

In diesem Kapitel ist das Vorgehen bzw. unterschiedliche Vorgehensweisen zur Revision des IDS zu beschreiben.

Anhang: Fragestellungen und Prüfmethoden

Zu den zuvor beschriebenen Vorgehensweisen sind Fragestellungen und Prüfmethoden vorzugeben. Die Fragestellungen und Prüfmethoden sollten dabei so allgemein gehalten werden, dass keine Verfälschung der Revisionsergebnisse durch eine gezielte Vorbereitung von Unterlagen möglich ist.

4.8 Glossar und Abkürzungen

DMZ	Demilitarisierte Zone
DoS	Denial of Service
hostbasierter Sensor (Hostsensor)	Sensor eines IDS, der auf dem zu überwachenden Host betrieben wird und dort das Betriebssystem, betriebene Anwendungen, die Integrität spezifischer Dateien und/oder den hostspezifischen Netzverkehr überwacht.
Hybridsensor	Hostbasierter Sensor, der neben dem System auch den serverspezifischen Netzverkehr überwacht.
IDS	Intrusion-Detection-System
IETF	Internet Engineering Task Force
Incident-Handling	Maßnahmen zur Verfolgung von Sicherheitsvorfällen
IT	Informationstechnik
netzbasierter Sensor (Netzsensor)	Sensor eines IDS, der auf einem separaten Rechner betrieben wird und den Netzverkehr an einer bestimmten Stelle im Netz überwacht.

4.9 Referenzen

[BSI 1-02] „Sicherheit im Internet“, BSI Kurzinformationen zu aktuellen Themen der IT-Sicherheit, Stand Januar 2002, abrufbar unter www.bsi.de

[CVE] CVE Nummerierung von Angriffen und Schwachstellen, Common vulnerability enumeration, cve.mitre.org