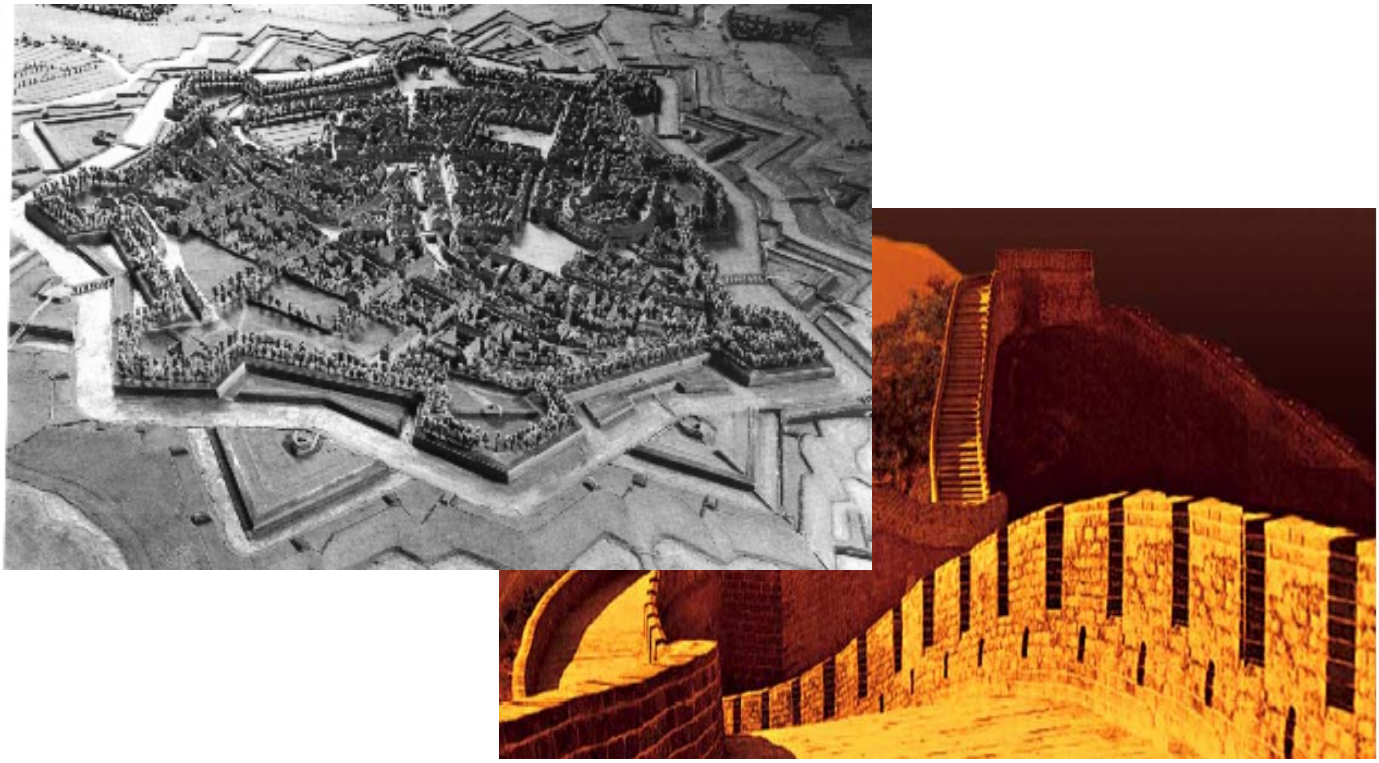
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Die Verteidigung in der Tiefe angewandt auf IT-Systeme

Memento



Version 1.1 – 19. Juli 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01 71 75 84 15 - Fax 01 71 75 84 00

Dieses Dokument wurde vom Beratungsbüro der DCSSI realisiert
(SGDN / DCSSI / SDO / BCS)

Kommentare und Vorschläge sind willkommen und können an folgende Adresse geschickt werden
(siehe Kommentarsammelformular am Ende des Leitfadens):

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

1.1 Präsentation der Studie

Nicht nur im Bereich der IT-Sicherheit besteht die größte Gefahr häufig darin, sich fälschlicherweise - bewusst oder unbewusst - in Sicherheit zu wähnen. Bei einer vernünftigen Grundhaltung sollten vielmehr die Ungewissheit im Auge behalten, eine angemessene Besorgnis bewahrt und große Wachsamkeit gepflegt werden. In diesem Rahmen hat das Beratungsbüro der DCSSI eine Studie durchgeführt, die sich der Definition und der Formalisierung des Konzepts der Verteidigung in der Tiefe, angewandt auf den Bereich der IT-Sicherheit, widmet. Die Studie soll es erlauben, praktische und operationelle Schlussfolgerungen bezüglich der IT-Architektur und des Risikomanagements zu ziehen. Um dieses Ziel erreichen zu können, wurde eine große Anzahl Experten und Vertreter französischer Industrieunternehmen zu Rate gezogen.

1.2 Aufbau des Dokuments

Dieses Dokument umfasst drei Hauptteile, die die Vorgehensweise widerspiegeln:

- Im ersten Teil wird eine umfassende Untersuchung der bibliografischen Lage über die Praktiken in der Industrie und im militärischen Bereich angestellt, um die großen Prinzipien der Verteidigung in der Tiefe bestimmen zu können;
- im zweiten Teil kommen die Konzepte und Definitionen der Verteidigung in der Tiefe angewandt auf den Bereich der IT-Sicherheit zur Sprache;
- im dritten Teil wird die Methode vorgestellt, die aus den zuvor definierten Prinzipien hervorgeht und die auf die IT-Sicherheit anzuwenden ist;
- im Anhang wird die Methode anhand eines Fallbeispiels veranschaulicht, mit dem die Bewertungsmodalitäten hervorgehoben werden konnten.

Eine Schlussfolgerung übernimmt die Überlegungen, die im Rahmen dieser Studie ausgeführt wurden, um deren Beiträge hervorzuheben und die späteren Arbeiten zu orientieren.

1.3 Bibliographie

Die folgende Tabelle gibt die wichtigsten Dokumente an, die im Rahmen dieser Studie behandelt werden. Falls ein Verweis in diesem Dokument zitiert wird, steht die entsprechende Nummer zwischen Klammern (die Nummerierung der gesamten Studiendokumentation wurde beibehalten).

Ref	*Auteur(s)*	*Datum*	*Titel*	*Editeur*
[SALI]	R. Mackey	Juni 2002	Security Architecture, Layered Insecurity	http://www.infosecuritymag.com/2002/jun/insecurity.shtml
[RATP]	J. VALANCOGNE	28.02.02	La défense en profondeur (Jacques VALANCOGNE von den Pariser Verkehrsbetrieben RATP)	http://www.institutbull.com.fr/sujets/valancogne
[SBGN]	Bob Clark	11.06.02	Small Business Guide to Network Security	http://www.giac.org/practical/Bob_Clark_GSEC.doc
[DRQR]	Tim Bass Silk Road, LLC Vienna, VA		Defense-in-depth revisited: qualitive risk analysis methodology for complex network-centric operations	http://www.silkroad.com/papers/pdf/milcom2001-430.pdf
[IATF]	IATF Release 3.1	.September 2002	Chapter 2 Defense in Depth	http://www.iatf.net
[DNCW]	CAPT Dan Galik, USN		Defense in Depth Security for Network-Centric Warfare	http://www.chips.navy.mil/archives/98_apr/Galik.htm
[DRA7]	D. HOURTOLOU	.September 2002	Analyse des risques et prévention des accidents majeurs (DRA-007)	http://www.ineris.fr/recherches/download/assurance.pdf
[DEQS]	Yves Deswarte, Mohamed Kaâniche, Rodolphe Ortalo		Évaluation quantitative de sécurité	http://www.inria.fr/rapportsactivite/RA95/saturne/node11.html

Tabelle 1: vereinfachtes bibliographisches Verzeichnis

1.4 Sigel und Abkürzungen

Die im vorliegenden Dokument benutzten Sigel und Abkürzungen werden in der folgenden Tabelle angegeben.

Begriff	***Bedeutung***
IAEA	Internationale Atomenergiebehörde
CDES	Commandement de la Doctrine et de l'Enseignement militaire Supérieur (Kommandobehörde der Doktrin und der militärischen Hochschulbildung)
DoD	Department of Defense (US-Verteidigungsministerium)
IATF	Information Assurance Technical Framework (IATF)
IDS	Intrusion Detection System (Instrusionsmeldesysteme)
IIS	Internet Information Services (Internetserver Microsoft)
INERIS	Institut National de l'Environnement Industriel et des Risques (staatliches Institut für industrielle Umwelt und Risiken)
INSAG	International Nuclear Safety Advisor Group (internationale Beratungsgruppe für nukleare Sicherheit)
IPSN	Institut de Protection et de Sûreté Nucléaire (Institut für nukleare Sicherheit)
IS	Informationssystem
SFEN	Société Française d'Energie Nucléaire (Französische Nuklearenergiegesellschaft)
SIS	IT-Sicherheit

Tabelle 2: Sigel und Abkürzungen

2 Analyse des Konzepts

2.1 Konzepte anhand der Bibliographie

2.1.1 Studie des militärischen Bereiches

Wie es scheint, hat sich das Konzept der Verteidigung in der Tiefe mit Vauban eingebürgert. Durch das Aufkommen von Metallkugeln im 15. Jahrhundert, die fähig waren, die vertikalen Befestigungswerke zu zerstören, wurden niedrigere Befestigungsanlagen gebaut, die die Tiefe des Geländes nutzen. Die tiefer liegenden Konzepte sind folgende:

- die zu schützenden Werte sind von mehreren Verteidigungslinien **umgeben**;
- jede Verteidigungslinie nimmt an der **globalen Verteidigung** teil;
- jede Verteidigungslinie spielt eine **Rolle**; den Angriff schwächen, behindern, verzögern (z.B. Tausch von Gelände gegen Zeit);
- jede Verteidigungslinie ist **autonom** (der Verlust der vorhergehenden Linie ist vorgesehen, um einen Kartenhauseffekt zu vermeiden): der Verlust einer Verteidigungslinie schwächt die nächste, diese verfügt jedoch über eigene Verteidigungsmittel gegenüber den verschiedenen Angriffen (jeder Angriffsprozess führt zu einer entsprechenden Verteidigung);
- Es werden alle Mittel eingesetzt, um die Verteidigung der verschiedenen Linien zu stärken:
  - Verwendung des Geländes (die Befestigungsanlage ist eine Geländeeinrichtung);
  - Abtrennung, um die Effekte eines Durchbruches und der Prellschüsse zu begrenzen;
  - Auskunft, um die Überraschung zu vermeiden.

Derzeit ist das Konzept der Verteidigung in der Tiefe nicht mehr an der Tagesordnung, da die Defensive nur das Ergebnis einer Unterlegenheitsposition ist, die eingesetzt wird, um wieder die Initiative zu ergreifen. Folglich haben zwei Prinzipien erheblich an Bedeutung gewonnen:

- die Auskunft, mit der die über die gegnerischen Aktionen aufgestellten Hypothesen bestätigt oder entkräftet und seine Absichten erkannt werden können, usw.;
- die Bewegung (dynamischer Aspekt der Verteidigung).

Bei den grundlegenden Prinzipien der Verteidigung in der Tiefe handelt es sich um folgende:

- die **Auskunft** ist die erste Verteidigungslinie: von der Information über die effektiven Gefahren, die Erkennung von Machenschaften, die oft Angriffen vorangehen, bis zur Erkennung nicht nur von erwiesenen und identifizierten Angriffen, sondern auch von jedwedem „unnormalen“ und somit verdächtigem Verhalten;
- Es sind mehrere **koordinierte und geordnete** Verteidigungslinien pro Verteidigungskapazität notwendig;
- der Verlust einer Verteidigungslinie muss **den Angriff schwächen** (zumindest indirekt, indem möglichst viele Informationen über seinen oder seine Ursprünge, seine Art, sowie die nächsten möglichen oder wahrscheinlichen Schritte gesammelt werden) und nicht zum Verlust der anderen Verteidigungslinien führen, sondern es ganz im Gegenteil erlauben, sie zu **stärken**;

- eine Verteidigungslinie muss die Abwehr (selbst wenn sich dies auf die Erkennung von Anomalien und die Verfolgung bei nicht identifizierbaren Angriffen begrenzt) aller möglichen Angriffe umfassen (**Vollständigkeit** einer Linie selbst);
- die Verteidigung schließt offensive Aktionen nicht aus.

2.1.2 Studie des industriellen Bereiches

2.1.2.1 Kernkraft

Das im Rahmen der nuklearen Sicherheit angewandte Konzept der Verteidigung in der Tiefe geht aus den Arbeiten hervor, die nach dem am Donnerstag, den 29.03.1979 stattgefundenen Three-Miles-Island-Unfall ausgeführt wurden, bei dem der ungenügend gekühlte Reaktorkern zum Teil schmolz. Sie wird als eine Verteidigung definiert, die drei unabhängige aufeinander folgende Barrieren aufweist, welche die Wahrscheinlichkeit, dass ein Unfall außerhalb der Zentrale Auswirkungen haben kann, möglichst gering halten. Die Idee besteht darin, dass jede Sicherheitsvorrichtung a priori als empfindlich angesehen werden muss und somit durch eine andere Vorrichtung zu schützen ist[1].Die staatliche frz. Elektrizitätsgesellschaft EDF identifiziert ebenfalls drei Verteidigungslinien verschiedener Art:

- Die Angemessenheit der Konzeption (insbesondere die Umsetzung der Redundanz und der Diversifizierung);
- Die Erkennung der latenten Fehler und der Zwischenfälle;
- Die Begrenzung der Konsequenzen („Milderung“).

Die Verteidigung in der Tiefe ist mit einem Risikomanagement verbunden, dessen 8 normalisierte Kategorien nachstehend dargelegt sind.

Abbildung 1: INES-Bewertungsskala[2]

[1] « Die Sicherheit gerade der französischen Kernkraftwerke basiert auf der Philosophie der "Verteidigung in der Tiefe", die auf mehreren Schutzniveaus mit sukzessiv aufeinander folgenden Barrieren beruht, die die Wahrscheinlichkeit, dass ein Unfall außerhalb der Zentrale Auswirkungen haben kann, äußerst gering halten. Die Idee besteht darin, dass jede Sicherheitsvorrichtung a priori als empfindlich angesehen werden muss und somit durch eine andere Vorrichtung zu schützen ist. » Fachzeitschrift Clefs CEA Nr. 45 Kasten D: Les trois barrières, illustration du concept de "défense en profondeur" (Die drei Barrieren, Illustration des Konzepts der "Verteidigung in der Tiefe" (Aktualisierung März 2002).

[2] Quelle: http://nucleaire.queret.net

Die drei Barrieren (die Brennelementhülle, der 20 cm dicke Stahlbehälter des Reaktors, die Sicherheitshülle (90 cm dick), die den Reaktor[3] umgibt) werden im folgenden Schema veranschaulicht.

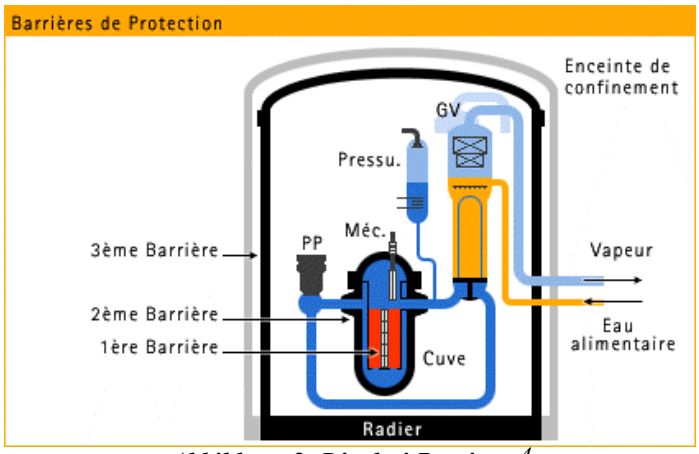


Abbildung 2: Die drei Barrieren[4]

[3] Wobei diese Hülle in den modernen Reaktoren sogar doppelt so dick ist.
[4] Quelle: http://perso.club-internet.fr/sorinj/la_surete.htm

2.1.2.2 Pariser Verkehrsbetriebe RATP

Die in der Kernenergie eingesetzten Prinzipien der Verteidigung in der Tiefe tauchen ebenfalls in zahlreichen Industriekomplexen auf, die bedeutende Risiken aufweisen. Genau wie bei der Kernenergie, kommt das Risiko meistens von Innen und die verschiedenen Barrieren haben das Ziel der Abschirmung. In [4] führt J. Valancogne eine Charakterisierung der Barrieren ein:

- die Barrieren können entweder technologisch, prozedural oder menschlich sein. Sie können ebenfalls gemischt sein, d.h. diese verschiedenen Attribute kombinieren;
- die Barrieren sind entweder statisch oder dynamisch (eine Sicherheitshülle ist eine statische Barriere, während ein Automatismus, der ein Ventil öffnen muss, eine dynamische Barriere ist). Die dynamischen Barrieren (die sich öffnen und schließen) können:
  - technologisch, menschlich oder gemischt sein,
  - die Aggression zu dem Zeitpunkt, zu dem sie auftritt, hemmen (sie schließt sich) oder sich im Gegenteil dem Strom öffnen, falls dieser nicht aggressiv ist (sie öffnet sich),
  - auf verschiedenen Zeitskalen wirken,
  - erfolgreich oder erfolglos sein,
  - verschiedene Realisationsprinzipien einsetzen (intrinsisch, probabilistisch);
- sie können entweder auf das angreifende Element, auf den Strom, oder auf das zu schützende Element wirken.

Die Wirksamkeit der Barrieren hängt nicht nur von ihrer Konzeption ab; die Aspekte der Wartung und der Entwicklung in der Zeit sind ebenfalls wichtig. Jeder Barriere kann ein Fehlerbaum zugeordnet werden. Das Beispiel der Katastrophe von Bhôpal zeigt den sukzessiven Misserfolg der drei unfallverhütenden Barrieren, hauptsächlich auf Grund von Verfahrens- und Wartungsfehlern. J. Valancogne legt auch den Akzent auf die Bedeutung der Erfahrungsrückmeldung und insbesondere auf die Analyse der Zwischenfälle (diese Elemente tauchen auch in der Kernenergie auf). Da das System darüber hinaus noch nicht verfestigt ist, muss die Wirksamkeit der Verteidigungen periodisch neu bewertet werden.

2.1.2.3 Chemie

Das INERIS (staatliche Institut für industrielle Umwelt und Risiken) hat ein besonders interessantes Werk mit dem Titel „Analyse des risques et prévention des accidents majeurs“ (Analyse der Risiken und Verhütung der Großunfälle) (DRA-007) [43] herausgebracht. Es handelt sich um den Endbericht (September 2002) des Projekts ASSURANCE dessen Ziel darin bestand, eine Vergleichsanalyse der Methoden der Risikoanalyse und Sicherheitsansätze in Europa anhand der Studie von einer bestehenden chemischen Installation als Bezugsbeispiel zu realisieren. Die globale Vorgehensweise umfasst folgende Phasen:

- Bestimmung der Risiken;
- Hierarchisierung der Risiken;
  - Schweregradklassen in Abhängigkeit von den Effekten (letal, irreversibel);
  - Häufigkeit/Wahrscheinlichkeit in Abhängigkeit von der Anzahl der Barrieren;
  - Annehmbarkeitsmatrix der Risiken (in Abhängigkeit vom Schweregrad und von der Häufigkeit): zugelassene, annehmbare und kritische Zonen;
- qualitative Analyse, die eingesetzten Methoden unterteilen sich in drei Kategorien:

  - die Methoden der induktiven Analyse (meistens: HAZSCAN, SWIFT, HAZOP, APR) beruhen auf einer absteigenden Analyse der Unfallsequenz (von den Ursprüngen zu den Konsequenzen);
  - die Methoden der deduktiven Analyse (Fehlerbaum) stützen sich auf eine aufsteigende Analyse der Unfallsequenz (von den Konsequenzen zu den Ursprüngen);
  - die Methoden, die auf der systematischen Identifizierung der Rückweisungsursprünge beruhen und die auf der Basis der Gutachterbewertung und der Erfahrungsrückmeldung (nationaler Leitfaden oder Auditübersicht) aufgebaut sind.
- qualitative Analyse, die eingesetzten Methoden unterteilen sich in zwei Kategorien, die im nachstehenden Schema dargestellt sind:
  - probabilistischer Ansatz;
  - deterministischer Ansatz.

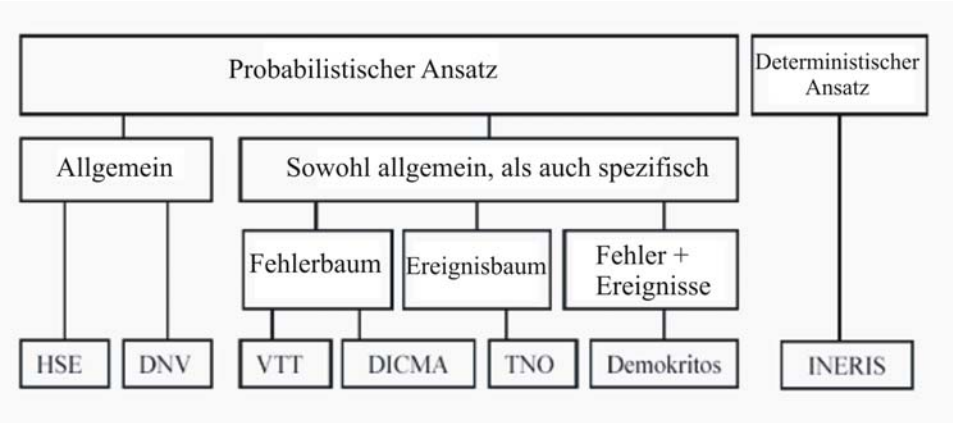


Abbildung 3: Die methodologischen Ansätze (Quelle: [DRA7])

Infolge einer Vergleichsanalyse der deterministischen und probabilistischen Ansätze des Risikos, ist keiner der beiden Ansätze wirklich für das IT-Risikomanagement geeignet. Eine vorgeschlagene Alternativlösung würde darin bestehen, sich auf das Konzept der Verteidigungsbarrieren und der Verteidigung in der Tiefe zu stützen, wobei es sich um das grundlegende Sicherheitsprinzip in den nuklearen oder industriellen Installationen von Frankreich handelt. Nach Ansicht des INERIS ermöglicht der Ansatz mit Verteidigungsbarrieren mehr Transparenz in der Präsentation des Risikomanagements, und folglich eine besser von der Öffentlichkeit und den Verbänden wahrgenommene Kommunikation.

2.1.3 Studie des IT-Bereiches

Es werden drei Dokumentarten unterschieden:

- Dokumente, in denen einfach auf den gesunden Menschenverstand Bezug genommen wird: die Verteidigung soll sich nicht auf die Peripherie begrenzen oder auf einem einzigen Mittel beruhen;
- Dokumente, hauptsächlich in den Vereinigten Staaten ab 1998, in denen insbesondere die IT-Sicherheit des Verteidigungsministeriums behandelt wird und die diesen Begriff verwenden;
- Dokumente, die methodologischer sind, wurden im Dokument der Phase 2 detailliert:
  - [13] gibt sich als eine vereinfachte Methode für kleine Einrichtungen;
  - [31] nähert sich eher einer qualitativen Risikoanalyse;
  - [3] preist die Verteidigung in der Tiefe durch ein Gegenbeispiel an;
  - [7] von der NSA, die die vom DoD umgesetzten Konzepte entwickelt hat.

2.1.4 Analyse der Kontexte

Zuerst müssen die Kontextunterschiede zwischen den drei untersuchten Bereichen berücksichtigt werden. Die folgenden Punkte erscheinen interessant:

- der Überraschungsfaktor:
  - im militärischen Bereich wird er systematisch angestrebt und ist Bestandteil des Manövers;
  - im nuklearen Bereich ist er zweifellos der Faktor, der weitmöglichst reduziert wird, selbst wenn er nicht zurückgestellt werden darf;
  - im Bereich der Datensicherheit ist er dadurch gegenwärtig, dass stets neue Angriffsformen bestehen werden (derzeit hat die Verteidigung nicht die Initiative);

- die Auskunft: sie wird es insbesondere erlauben, die Ungewissheit hinsichtlich der gegnerischen Aktionen zu verringern, indem die Hypothesen bestätigt oder entkräftet werden, und die verhängnisvollen Folgen der Überraschung zu vermeiden; die Auskunft darf nicht von der Planung getrennt werden;

- die Zusammenarbeit zwischen den verschiedenen Verteidigungslinien:
  - im militärischen Bereich wird systematisch die Synergie zwischen den verschiedenen Mitteln angestrebt; durch das Hinzufügen eines weiteren Mittels muss ein bedeutenderer Vorteil geschaffen werden, als die einfache Summe der nicht unabhängigen Verteidigungslinien;
  - im nuklearen Bereich wird der Aspekt der Unabhängigkeit gegenüber den Bedrohungen (die Fehlerursprünge) der verschiedenen Schutzlinien hervorgehoben;
  - in der Datensicherheit scheint das Hinzufügen von Schutzvorrichtungen eng mit der Anwesenheit von Bedrohungen verbunden zu sein, wobei diese auf unitäre Weise genommen werden;

- der Ursprung der Bedrohungen (intern/extern):
  - das Konzept der Nahverteidigung veranschaulicht bestens dieses Prinzip: der Gegner kann sich in der gesamten Tiefe der Vorrichtung auffinden; woher jeder Kämpfer unabhängig von seiner Rolle für seinen eigenen Nahschutz sorgen muss;
  - im industriellen Bereich werden die externen Bedrohungen (Terrorismus zum Beispiel) und auch die internen Bedrohungen (der industrielle Prozess selbst) berücksichtigt;
  - bei der Datensicherheit findet man den globalen Aspekt des Angriffs wieder, der von Innen und von Außen kommt; die Tiefe der Schutzvorrichtung muss folglich in mehreren Dimensionen definiert werden. Das bedeutet, dass die Tiefe der Verteidigung die Organisation, die Umsetzung von Maßnahmen und die Technologien einbeziehen muss, und sich nicht mit einem einfachen perimetrischen Verteidigungsschutz des Systems "nach außen" begnügen darf.

- für eine Verteidigung in der Tiefe muss mindestens folgendes gesichert sein:
  - mehrere unabhängige Verteidigungslinien in dem Sinne, wo jeder fähig ist, sich allein gegen alle Angriffe zu verteidigen (d.h., dass der Verlust der vorhergehenden Linie vorgesehen ist, es wird nicht vorausgesetzt, dass die vorhergehende Linie besteht); in aller Strenge wäre es angebracht, von Verteidigungslinien zu sprechen, die autonom oder komplett sind, d.h. fähig sind, auf alle Bedrohungen zu antworten; eines der Prinzipien von den militärischen Doktrinen sieht nämlich vor, dass die Linien zusätzlich an der globalen Verteidigung teilnehmen, die somit eine größere Verteidigungsstärke darstellt, als die Verteidigungssumme von jeder Linie (dieser Punkt wird im industriellen Bereich nicht als Prinzip übernommen, der mehr nach der Unabhängigkeit von den Barrieren strebt);
  - Zusammenarbeit zwischen den Verteidigungslinien, ansonsten wird das Konzept nur auf einfache aufeinander folgende Barrieren reduziert, deren Widerstand nicht von der vorhergehenden abhängt (sie können somit nacheinander angegriffen werden);
  - der Verlust einer Verteidigungslinie muss es erlauben, die Verteidigung zu stärken und nicht zu schwächen (obwohl dieser Punkt eine Folge des vorhergehenden ist, ist er hier vorgesehen, um den dynamischen Aspekt der Verteidigung einzubringen).

Das Konzept der Verteidigung in der Tiefe ist militärischen Ursprungs. Dieser Begriff wird anschließend im nuklearen Bereich benutzt, der daraus eine Methode entwickelt. Das Konzept wird später im allgemeineren Rahmen der Industrie (Chemie) und des Transports (Pariser Verkehrsbetriebe RATP) übernommen. Im industriellen Bereich kann mit der Verteidigung in der Tiefe, die probabilistische Analyse der Risiken durch einen deterministischen Aspekt und eine Modellbildung im Bereich der Komponenten vervollständigt werden. Das Konzept wird anschließend im Bereich der IT-Sicherheit, hauptsächlich in den Vereinigten Staaten, übernommen, ohne dass es jedoch tatsächlich entwickelt wird, da es scheinbar verschiedene Ideen miteinander vereint, die sich um den Ausdruck Tiefe im Sinne von mehreren redundanten oder zusätzlichen Mitteln drehen. Zwei Ansätze scheinen jedoch zu bestehen, der erste unterstreicht den globalen Aspekt der Verteidigung und der andere befasst sich mehr mit Komponenten. In diesem letzten Ansatz ist der Bezug auf die Risikoanalyse deutlicher.

2.2 Beitrag der Gespräche

Aus dem mit dem militärischen Personal geführten Gespräch zeigen sich folgende Bedeutungen:

- des Faktors Auskunft, der zwar bereits angegeben wurde, jedoch noch gestärkt werden muss;
- des dynamischen Aspekts und der Planung;
- der Konzepte der Verantwortung pro Ebene.

Diese drei Punkte müssen im Rahmen der Verteidigung in der Tiefe der IT-Systeme durch die Berücksichtigung der nachstehenden Prinzipien zum Ausdruck kommen:

- bei der Einrichtung einer „Barriere“ muss gleichzeitig folgendes vorgesehen werden:
  - der Punkt der Kontrolle ihrer Funktionstüchtigkeit oder ihres Zusammenbruchs (Funktion Auskunft);
  - die notwendigen Informationen, die gesammelt werden müssen, um zu wissen, dass sie ein Angreifer als Zielscheibe wählen wird;
- bei der Ausarbeitung der globalen Politik muss der Zusammenbruch einer Barriere vorgesehen werden und dementsprechend:
  - ist dynamische Abwehr vorzusehen;
  - sind die möglichen Aktionen in Abhängigkeit von den verschiedenen Fällen zu planen;
- das gesamte Personal und nicht nur die Spezialisten müssen um die IT-Sicherheit besorgt sein; auf jeder Ebene müssen Beauftragte bestimmt werden:
  - auf individueller Ebene (die sofortige Sicherung): Charta, ein Verfahrenshandbuch, usw.;
  - auf der Ebene von jeder Zelle der Organisation (die Nahsicherung): angepasstes Sicherheitsdossier mit Verfahren und mehreren Rettungsplänen eines elementaren Niveaus;
  - im Bereich der Einrichtung (die Fernsicherung) werden die Rettungspläne eine allumfassendere Reichweite mit Multiservicen, Rettungsspots, usw. aufweisen.

Das Konzept der Verteidigung in der Tiefe muss im industriellen Bereich als ein logisches Ergebnis der Risikobeherrschung angesehen werden:

- sobald das Sicherheitsziel definiert ist (eine Verbreitung außerhalb des Standortes, einen Unfall, usw. vermeiden) wird eine Risikoanalyse nach den bekannten Methoden ausgeführt, wobei die Verteidigung in der Tiefe folglich sowohl den deterministischen, als auch den probabilistischen Ansatz kombiniert; diese beiden komplementären Ansätze ermöglichen es, die Barrieren vorzusehen und einzurichten (deterministischer Ansatz zum Zeitpunkt der Entwicklung) und anschließend die Ausfallwahrscheinlichkeit der Barrieren zu bewerten (probabilistischer Ansatz);
- anschließend können die verschiedenen Zwischenfälle in einer globalen Skala eingeteilt werden, die bedeutende pädagogische und mediatische Vorteile aufweist.
  - Skala der gemeinsamen Werte,
  - ermöglicht es, die Verteidigung anhand eines allgemeinverständlichen Schemas zu präsentieren,
  - ermöglicht es, den Schweregrad eines Zwischenfalls leicht zu bestimmen, der von der überschrittenen Barriere abhängt;
- letztlich ruft jedes Barriereüberschreiten vorbeugende und korrigierende Maßnahmen hervor und dies, indem bis zur Endphase vorgesehen wird, wenn das befürchtete Ereignis eintritt.

2.3 Schlussfolgerung der ersten Phase

Gemäß den für die Verteidigung in der Tiefe definierten Kriterien, wurde keine komplette im Rahmen der Sicherheit von Informationssystemen dargelegte Lösung gefunden. Demgegenüber liefern die Prinzipien aus den militärischen und industriellen Bereichen jedoch interessante Ideen. Hinsichtlich der Aspekte Angriff/Verteidigung steht der militärische Bereich der Datensicherheit nah; der industrielle Bereich verleiht die globale, systematische und quantitative Seite und somit eine ermessene Strenge, die im DV-Bereich fehlt.
Schon jetzt zeigt sich:

- dass der Begriff der Verteidigung in der Tiefe, so wie er derzeit im Bereich der IT-Sicherheit in Erscheinung tritt, keine Revolution in Bezug auf die gegenwärtig angewendeten Prinzipien darstellt;
- dass die Bereicherung der derzeitigen Prinzipien der Datensicherheit durch Beiträge aus der Methode der Verteidigung in der Tiefe, angewandt auf den industriellen und den militärischen Bereich, es wahrscheinlich erlauben wird, eine tatsächliche Methode der Verteidigung in der Tiefe zu definieren, bei der es mehr um Verteidigung, als um Sicherheit geht.

3 Die Verteidigung in der Tiefe angewandt auf den Bereich der IT-Sicherheit

3.1 Definition des Konzepts

3.1.1 Allgemeine Beurteilungen des Konzepts

Das universellste Prinzip des Konzepts der Verteidigung in der Tiefe, das in den drei Bereichen Militär, Industrie und IT-Sicherheit erscheint, ist das mit mehreren unabhängigen Barrieren.

Die anderen Prinzipien sind anschließend je nach den Fällen mehr oder weniger gut entwickelt. Darüber hinaus muss bemerkt werden, dass, obwohl das Konzept im industriellen Bereich stets das gleiche ist, dies in der IT-Sicherheit nicht der Fall ist.

Er erscheint jedoch, dass das Konzept der Barriere i) nur mit der Schutzkomponente (Kontingentierung, Abtrennung) verbunden ist und somit weitere wesentliche Dimensionen ignoriert, ii) zu sehr von der Bedrohung abhängt und folglich schwer hinsichtlich der IT-Sicherheit zu manipulieren ist, wenn man sich an Entscheidungsträger oder Nutzer wendet, hauptsächlich aufgrund ihres technischen und multiplen Charakters.

Das Konzept der Verteidigungslinie scheint demgegenüber jedoch reicher und bedeutungsvoller zu sein, obgleich es sehr willkürlich ist.

> Im Fall z.B. einer Arbeitsstation, die durch eine FireWall und einen Antivirus gegen unerlaubte Zugriffe aus dem Internet geschützt ist, stellt der Antivirus die zweite Barriere gegen den Versuch dar, einen bösartigen Code durch Intrusion abzulegen, aber die erste, wenn der eingesetzte Träger eine elektronische Post ist, da diese von der FireWall zugelassen ist. Im Rahmen der Datensicherheit sind die Schutzmittel (im vorliegenden Beispiel die FireWall) eher ein Filter, als echte Barrieren (vgl. 3.1.2), wie bei der Kernenergie.

Aufgrund des Multiform- und Multibedrohungs-Charakters der Verteidigung ist es nämlich nicht möglich, eine direkte Verbindung zwischen Barriere, Verteidigungslinie und Schweregradstufe zu erstellen. Der Begriff der Verteidigungslinie ermöglicht es demgegenüber jedoch, Barrieren für einen „Kommunikations“-Aspekt zu vereinen und mit den Schweregradstufen[5] zu korrelieren. Eine Verteidigungslinie entspricht in diesem Fall einem Übergang zwischen zwei Schweregradstufen und schließt eine entsprechende geplante Reaktion mit ein.

Die vorgeschlagene Vorgehensweise führt somit dazu, die Barrieren[6] zu bestimmen, die je nach den Bedrohungen und den zu schützenden Werten eingerichtet werden müssen, und

[5] Die unterbreiteten Schweregradstufen werden weiter oben in diesem Kapitel angegeben.

[6] Der Begriff Barriere (siehe w.o. im Kapitel angegebene Definition) wird hier als Synonym einer Sicherheitsmaßnahme (menschlich, prozedural, technisch) verstanden, wobei die von M. Valancogne unterbreitete allgemeine Definition dieses Begriffs übernommen wird, um dem Begriff Verteidigungseinheit einen allgemeineren und „kommunizierenderen“ Sinn zu bewahren“. Folglich lassen wir auf diese Weise den von der CEA gegeben Sinn dieser beiden Begriffe fallen.

anschließend die Schweregradstufe der Sicherheitszwischenfälle zu bestimmen, die durch die Überschreitung der Barrieren hervorgerufen wurden, um sie nach Schweregradstufe zu vereinen und somit die Verteidigungslinien hervorzuheben. Diese tragen zur Kommunikationsbemühung zu den Entscheidungsträgern und Nutzern bei, ersetzen jedoch nicht die Studie der Barrieren für die Sicherheitsexperten. Diese Vorgehensweise ist auf nachstehender Abbildung dargestellt.

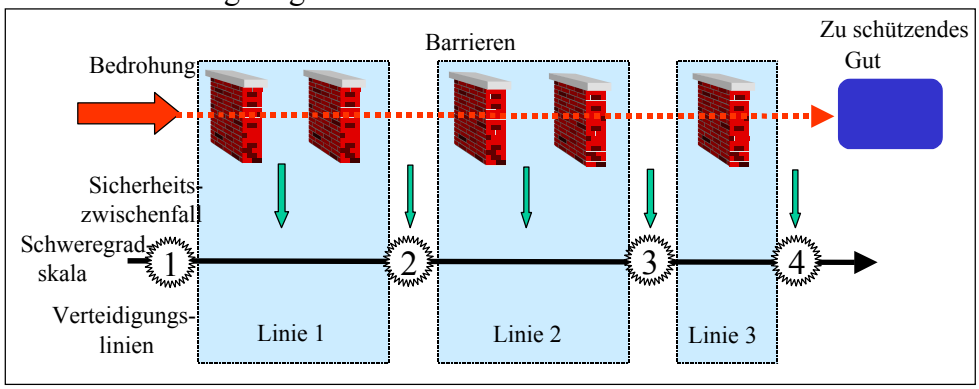


Abbildung 4: Vorgehensweise zur Hervorhebung der Verteidigungslinien

Die Vorgehensweise muss auf iterative Weise den deduktiven (über die Ressourcen) und anschließend induktiven Ansatz (über die Bedrohungen) kombinieren. Sie unterbricht die Konzeption, sobald die Architektur und die Schutzmittel validiert und die verbleibenden Risiken bestimmt werden können (Qualifizierung des untersuchten Systems).

Es muss bemerkt werden, dass die Barrieren mit Bedrohungen in Verbindung gebracht werden (was einen induktiven Ansatz voraussetzt), wobei jedoch der Schweregrad der Sicherheitszwischenfälle von den Ressourcen abhängt (was eine Risikoanalyse und einen deduktiven Ansatz voraussetzt). Die beiden Ansätze (induktiv und deduktiv) vervollständigen sich folglich miteinander und müssen wiederholt werden, bis ein ausreichendes Schutzniveau erzielt wird. Nun können die Architektur und die Schutzmittel, die im Hinblick auf die Risiken eingesetzt werden, validiert und die verbleibenden Risiken hervorgehoben werden (Qualifizierung des Systems).

Darüber hinaus kann eine Barriere (und demzufolge eine Verteidigungslinie) mehrere Bedrohungen decken und ihre Überschreitung ruft einen Zwischenfall hervor, dessen Schweregrad von der Anzahl der Verteidigungslinien abhängt, die noch zu überschreiten sind, sowie vom Wert der zu schützenden Werte. Somit existiert eine doppelte Darstellung:

- eine für die Entscheidungsträger und Nutzer, die gewollt global und einfach ist (der im vorstehenden Schema dargestellte Aspekt Verteidigungslinie und Schweregradskala);

  Diese Darstellung ist wichtig für den Aspekt **Kommunikation** von der Methode.

- die andere feinere stützt sich auf besondere Modellbildungen der kritischen Prozesse über Hauptbedrohungen und ist für die Spezialisten bestimmt; in diesem Fall ist es zweifellos interessant, die verschiedenen Niveaus zu unterteilen, wobei die Unterteilungen den Varianten in der Planung entsprechen würden (wobei beim Aspekt Szenario Barrieren und Zwischenfälle des Schweregrads vom vorstehenden Schema aufeinander folgen).

Diese Darstellung ist wichtig für den Aspekt **Qualifizierung der Methode** (schematische Darstellung der verschiedenen Sicherheitsmaßnahmen in Verbindung mit einer Bedrohung und ein Wert schützend), die während der Gestaltung der Szenarien ausgearbeitet wird, und die es erlaubt: i) die umzusetzenden Barrieren anhand einer induktiven und anschließend iterativen deduktiven Analyse zu bestimmen, bis das notwendige Schutzniveau erzielt wird, ii) den Schweregrad eines Sicherheitsereignisses in Abhängigkeit von der Kritizität des Wertes und der Anzahl der verbleibenden Linien zu bewerten.

Die besondere Modellbildung, die für die kritischen Werte und die Hauptbedrohungen ausgeführt wird, ermöglicht es, die direkte Verbindung zu erstellen und folglich die „Sicherheitslöcher“ leichter zu erkennen und demzufolge eine Bewertung zu erlauben.

3.1.2 Definitionen

Mit der Analyse der verschiedenen Prinzipien und des Konzepts der Verteidigung in der Tiefe können die nachstehenden Definitionen unterbreitet werden:

*Der **Schweregrad eines** Sicherheitsereignisses bemesst die tatsächliche Auswirkung des Ereignisses in Abhängigkeit von der Kritizität des Wertes (Fall, in dem sich ein Ereignis direkt auf ein Wert auswirkt) oder der potentiellen Auswirkung von diesem Ereignis auf das bedrohte Wert in Abhängigkeit von der Anzahl der verbleibenden Verteidigungslinien und der Kritizität dieses Wertes (Fall, in dem sich das Ereignis nicht auf das Wert, sondern auf die Verteidigungsmittel auswirkt).*

*Die Methode schlägt eine Skala vor, in der die **Schweregradstufen** festgelegt sind, um verschiedene Sicherheitszwischenfälle miteinander vergleichen zu können. Für einen bestimmten Sicherheitszwischenfall unterliegt es den verantwortlichen Nutzern, die entsprechende Schweregradstufe zu bestimmen, die in Abhängigkeit von der Auswirkung dieses Zwischenfalls auf das zu schützende Wert ermessen wird.*
*Eine **Barriere** ist ein Sicherheitsmittel, das fähig ist, einen Teil des Informationssystems gegen mindestens eine Bedrohung zu schützen. Eine Barriere kann menschlich, prozedural oder technisch, statisch oder dynamisch, manuell oder automatisch sein. Sie muss über ein Mittel zur Kontrolle ihres Zustands verfügen.*

*Eine **Verteidigungslinie** ist eine Entität von Barrieren, nach Szenario oder Szenarienfamilie, deren Überschreitung einen Zwischenfall hervorruft, dessen Schweregrad von der Anzahl der verbleibenden Barrieren abhängt, die von der oder den Bedrohungen überschritten werden müssen, um das oder die zu schützenden Werte zu erreichen und vom Wert dieser Werte (d.h. dass einem bestimmten Sicherheitszwischenfall eine Schweregradstufe zugeordnet ist, die die abstrakte überschrittene Verteidigungslinie angibt). Um eine Linie und nicht nur eine Entität aus Schutzmitteln zu sein, muss jede Verteidigungslinie mit den Vorrichtungen und Mitteln zur Erkennung/Überwachung und Meldung ausgestattet sein.*

Die Verteidigung in der Tiefe des Informationssystems ist eine globale und dynamische Verteidigung, bei der mehrere Verteidigungslinien koordiniert und die gesamte Tiefe des Systems abgedeckt werden. Der Begriff Tiefe ist dabei im weitesten Sinne zu verstehen, er umfasst die Organisation des Informationssystems, seine Umsetzung und schließlich die zum Einsatz kommenden Technologien. Es geht darum, zu geringen Kosten Neutralisierungsaktionen der Verletzungen gegen die Sicherheit an Hand eines Risikomanagements, eines Auskunftssystems, einer Planung der Reaktionen und die permanente Bereicherung durch Erfahrungsrückmeldung zuzulassen. Diese Verteidigung in

der Tiefe hat ein doppeltes Ziel: i) den Schutz des Informationssystems durch einen qualitativen Ansatz, mit dem die Vollständigkeit und die Qualität der Vorrichtung geprüften werden können, zu stärken, ii) ein starkes Kommunikationsmittel zu verschaffen, mit dem die Entscheidungsträger und die Nutzer der Schweregrad der Sicherheitszwischenfälle bewusst wird.

In der Sicherheit der Informationssysteme wird eine Barriere, ein Mittel oder eine Vorrichtung mindestens einer besonderen Bedrohung zugeordnet und an einem festgelegten Ort platziert (zwischen dem Ursprung der Aggression und dem zu schützenden Wert). Sie kann mehrere Werte schützen, jedoch nicht unbedingt auf die gleiche Weise. Folglich muss die Analyse der Verteidigungslinien für jedes Wert (oder jede Werteentität) und für jede Bedrohung ausgeführt werden, d.h. für jede Art an Sicherheitszwischenfällen.
Diese Analyse wird mit einer Granularität realisiert, die von der Bedeutung des entsprechenden Risikos abhängt (Funktion der Kritizität des Wertes und/oder der Erscheinungswahrscheinlichkeit von der Bedrohung), wobei der induktive (durch die Bedrohungen) und anschließend der deduktive Ansatz (durch die zu schützenden Ressourcen) kombiniert werden.

3.1.3 Allgemeine Prinzipien

Das Konzept der Verteidigung in der Tiefe gehorcht also folgenden allgemeinen Prinzipien. Dabei kann jedes dieser Prinzipien einzeln bestehen, aber die Tiefe der Verteidigung wird erst durch ihr Zusammenspiel erreicht.

Titel	***Beschaffenheit***
Globalität	**Die Verteidigung muss global sein, d. h. sie muss alle Dimensionen des Informationssystems umfassen:** a) Organisatorische Aspekte; b) Technische Aspekte; c) Aspekte der Umsetzung.
Koordination	**Die Verteidigung muss koordiniert sein, d. h. die zum Einsatz kommenden Mittel wirken:** a) dank einer Warnungs- und Weitergabekapazität; b) infolge einer Korrelation der Zwischenfälle.
Dynamik	**Die Verteidigung muss dynamisch sein, d. h. das Informationssystem muss über eine IT-Sicherheits-Policy verfügen, die folgende Elemente zulässt:** a) Reaktionskapazität; b) Vorausplanung der Aktionen; c) Schweregradskala.
Hinlänglichkeit	**Die Verteidigung muss hinlänglich sein, d. h. jedes (organisatorische oder technische) Schutzmittel muss über:** a) einen eigenen Schutz; b) Mittel zur Erkennung; c) Reaktionsverfahren verfügen.
Vollständigkeit	**Die Verteidigung muss vollständig sein, d. h.:** a) die zu schützenden Werte werden in Abhängigkeit von ihrer Kritizität geschützt; b) jedes Wert wird durch mindestens drei Verteidigungslinien geschützt, c) die Erfahrungsrückmeldung ist formalisiert.
Nachweis	**Die Verteidigung muss nachweisbar sein, d. h.:**

	a) die Verteidigung ist qualifiziert; b) es besteht eine Strategie zur Abnahme; c) die Abnahme muss dem Lebenszyklus des Informationssystems angepasst sein.

Tabelle 3: die Schritte der Methode

Das Prinzip der Vollständigkeit stammt in ihrer Komponente « Mindestanzahl an Barrieren » von einem pragmatischen Ansatz aus der Kerntechnik: Man geht davon aus, dass die eine der drei Barrieren vom Zwischenfall oder von der zwischenfallbewirkenden Aggression betroffen ist, dass die eine der beiden anderen aus einem unerwarteten Grund gestört ist und dass die Auswirkungen „unweigerlich“ von der dritten begrenzt werden.

3.2 Umsetzung des Konzepts

Die Verteidigung in der Tiefe zielt somit darauf ab, die Information und das sie unterstützende System durch das Gleichgewicht und die Koordinierung der dynamischen oder statischen Verteidigungslinien über die ganze Tiefe des Informationssystems unter Kontrolle zu halten. Darin inbegriffen sind die Dimensionen Organisation, Umsetzung und Technologien. Es geht hier nicht darum, einen Baukasten der Verteidigung in der Tiefe oder eine der "Best Practices" anzubieten, sondern an Hand von Beispielen zu illustrieren, wie eine Verteidigung in der Tiefe konkret aussehen kann. Für eine kohärente und strukturierte Vorgehensweise muss die im folgenden Kapitel vorgestellte Methodik befolgt werden.

3.2.1 Tiefe der Organisation

Tiefe in eine Organisation im Sinne der Verteidigung in der Tiefe zu bekommen, könnte zunächst bedeuten, eine Kette von Verantwortungen von Anfang bis Ende, also vom Nutzer bis hin zum Sicherheitsbeauftragten, zu definieren. Diese Kontinuität innerhalb der Organisation setzt regelmäßige und überprüfte Aktionen der Sensibilisierung und Schulung voraus.

Diese Kette der Verantwortungen muss allgemein bekannt sein, und innerhalb dieser Kette müssen Verfahren zur Weiterleitung von Zwischenfällen und zur Meldung bzw. Alarmierung der Sicherheitsdienste definiert worden sein. Wie alle Verteidigungslinien müssen die Linien, die aus organisatorischer Sicht eingerichtet wurden, überwacht werden; zudem sind Ersatzverfahren vorzusehen.

Die Organisation in der Tiefe besteht auch darin, Erfahrungsrückmeldungen vorzusehen, damit alle von den Erfahrungen aller profitieren können. Diese Erfahrungsrückmeldung trägt auch dazu bei, dass das Sicherheits-Bezugssystem während des gesamten Lebenszyklus des Informationssystems mitwachsen kann. Dabei hängt das System nicht nur von den zum Einsatz kommenden Technologien ab, sondern auch vom Faktor Mensch und dem zur Verfügung stehenden Know-how. Die Erfahrungsrückmeldung ist danach zu unterscheiden, ob man sich an Nutzer oder an Betreiber des Systems wendet. Es kann sinnvoll sein, dieses Feedback so zu organisieren, dass es anonym oder zumindest außerhalb jedweder funktionellen Hierarchie erfolgt.

Das Sicherheits-Bezugssystem des Informationssystems muss auf höchster Ebene validiert werden und allgemein bekannt sein. Das bedeutet also, dass das Sicherheits-Bezugssystem

nur insofern seine Rolle ausspielen kann, als es die ganze Tiefe der Organisation berührt. Sicherheit muss die Angelegenheit aller und nicht nur einer Handvoll Experten sein.

Die Organisation muss dauerhaft und dynamisch darauf abzielen, das Schutzniveau im Hinblick auf die Sicherheitsziele, die aus einer Risikoanalyse hervorgegangen sind, zu bewerten. Die Organisation muss entweder in der Lage sein, sich selbst zu kontrollieren oder einen Dritten mit der Bewertung des Schutzniveaus zu beauftragen.

Das Informationssystem befindet sich in einer physiskalischen Umgebung und ist dadurch permanenten Interaktionen ausgesetzt. Diese Aktionen müssen überwacht werden, und es sind Notmaßnahmen vorzusehen.

Das Konzept der Einbindung der Sicherheit in die Projekte beweist auch eine gewisse Reife. Die Abnahme der Sicherheit und die Fähigkeit der Organisation, sich in Abhängigkeit von der Umgebung, vom Lebenszyklus der Systeme und von Sicherheitszwischenfällen anzupassen, sind die Kernpunkte bei der Verteidigung in der Tiefe.

3.2.2 Tiefe bei der Umsetzung

Die Umsetzung der Sicherheitsmaßnahmen muss sich auf validierte und bewährte Strategien stützen können. Das setzt auch voraus, dass die Nutzer aktiv bei der Weiterleitung von Zwischenfällen mitwirken und über Anweisungen zur Meldung von Sicherheitsstörfällen verfügen.

Um in der Tiefe verteidigt werden zu können, muss das Informationssystem eine dynamische Strategie zur Aktualisierung der Tools und der Bezugsdokumente besitzen. Ohne diese Aktualisierungen und Infragestellung der Sicherheitsverfahren besteht die Gefahr einer illusorischen Verteidigung.

Beim Einsatz von Tools sind Administration, Folgeüberwachung und Kontrolle erforderlich. Dies geschieht insbesondere durch eine Trace-Analyse zur Erkennung von Zwischenfällen. Eine Verteidigungslinie, egal welcher Art, muss überwacht werden.

Auch die Wartungspolitik muss in die Tiefe gehen, indem Lieferanten gestreut und Verträge geprüft und auf ihre Konformität mit den Sicherheitszielen hin untersucht werden.

3.2.3 Tiefe bei den Technologien

Die Verteidigung in der Tiefe besteht also darin, den Bedrohungen koordinierte und unabhängige Verteidigungslinien entgegen zu stellen. Im Bereich der Technologien kann das beispielsweise. bedeuten, dass der Ausfall eines Netzwerkdienstes keinesfalls bewirken darf, dass höhere Rechte auf das gesamte System erworben werden. In diesem Kontext ist anzumerken, dass die Vergabe von Administrationsrechten an alle Nutzer eines Systems im Widerspruch zur Verteidigung in der Tiefe steht. Auf dem Gebiet des Datenschutzes kann das auch bedeuten, dass die Chiffrierung auf der Anwendungsebene an sich nicht ausreicht und dass es notwendig werden könnte, zusätzlich auch die IP-Schicht zu schützen.

Die Verteidigung in der Tiefe hat zur Folge, dass die Sicherheit nicht auf einem Element, sondern auf einem kohärenten Ganzen beruht. Das bedeutet, dass es theoretisch keinen Punkt geben darf, auf dem das ganze Konstrukt ruht. So darf die Verteidigung nicht nur auf einer Technologie oder einem Sicherheitsprodukt beruhen, auch wenn dessen Qualität noch so gut ist. Als Barriere muss das Sicherheitsprodukt kontrolliert und geschützt werden, und es muss im Falle eines Zwischenfalls über einen Reaktionsplan verfügen.

Es ist anzustreben, das System so wenig wie möglich den verschiedenen Bedrohungen auszusetzen. Das bedeutet z. B., mit Hilfe von FireWalls und Intrusionsmeldesystemen Enklaven zu schaffen. In diesem Rahmen geringerer Aussetzung ist es systematisch erforderlich, die angebotenen Dienstleistungen auf das strikte Minimum zu reduzieren.

Tiefe in die Technologien zu bringen bedeutet auch, bis hin zum individuellen Arbeitsplatz die Arbeitsstationen mit FireWalls und einer regelmäßig aktualisierten Antivirensoftware auszurüsten, wobei diese mit dem Antivirenprogramm der Mailbox-Gateway nicht identisch sein darf. Der Einsatz solcher Tools erfordert eine diesbezügliche Schulung der Nutzer, damit ihnen bewusst wird, dass Technologie alleine nicht ausreicht, und dass Wachsamkeit unersetzlich ist, egal welche Unterstützungstools auch immer vorhanden sind.

4 Die Methode der Verteidigung in der Tiefe

Mit Hilfe dieser Methode kann der Auftraggeber die Grundsätze der Verteidigung in der Tiefe entsprechend den obigen Definitionen (vgl. § 3.1.3) in die Praxis umsetzen. Sie bietet v. a. die Möglichkeit, ein System zu qualifizieren und in gewisser Weise sein Verteidigungsniveau zu ermessen. Zum Erreichen dieses Ziels wird bei der Methode davon ausgegangen, dass zuvor ein Risikomanagement durchgeführt wurde. Schließlich trägt diese Methode auch zur Integrierung der IT-Sicherheit in die Projekte bei.

Die Methode, die die Anwendung des Konzepts der Verteidigung in der Tiefe auf dem Gebiet der Sicherheit von Informationssystemen zulässt, umfasst folgende Schritte:

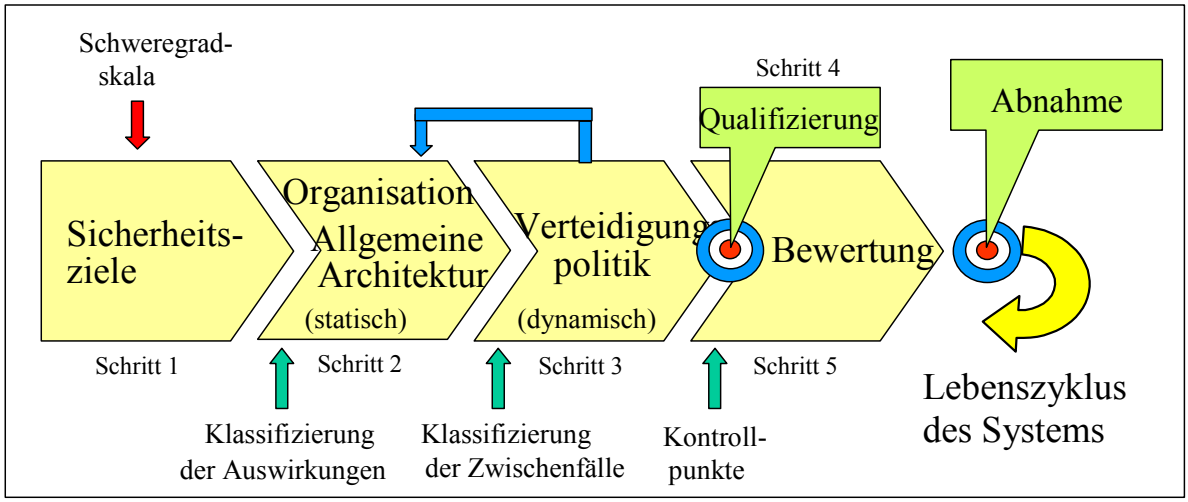


Abbildung 5: die Schritte der Methode

1. Bestimmung der Werte der Sicherheitsziele. Der Aufbau der Verteidigung in der Tiefe ist von den Ergebnissen dieses Schritts abhängig. Die Sicherheitsziele ermöglichen es, die Auswirkungen auf der Schweregradskala zu klassifizieren, wodurch anschließend die Sicherheitszwischenfälle auf dieser Skala festgelegt werden können. Die Zwischenfalltabelle in Verbindung mit einer schematischen Darstellung des Informationssystems und der Verteidigungslinien stellen somit eine einheitliche Kommunikationsbasis dar.

2. Ausarbeitung der Organisation und der allgemeinen Architektur des Systems (die Tiefe der Vorrichtung). In diesem Schritt müssen die Kontroll- und Bewertungspunkte definiert werden. Diese Definition muss so weit wie möglich im Vorfeld der Projekte durchgeführt werden; dadurch können die Barrieren, der Schweregrad der Sicherheitszwischenfälle (in Abhängigkeit von der Anzahl der verbleibenden Barrieren) und die Verteidigungslinien hervorgehoben werden.

3. Ausarbeitung der Verteidigungspolitik, die zwei Teile umfasst: Der erste organisiert die Auskunft und der zweite die entsprechende reaktive Verteidigung (*Interreaktion, Planung)*. Dieser Schritt definiert die operationelle Verteidigungspolitik und hebt die Kontrollpunkte hervor. Diese Verteidigungspolitik muss die Systemüberwachung, den Aufstieg der Sicherheitsereignisse, um das Kontrollschema zu versorgen und die Beschlussfassung hinsichtlich der umzusetzenden Reaktionsmittel erlauben. Dieser Schritt weist einen operationellen und dynamischen Aspekt auf, während der vorhergehende statischer ist.

4. Die globale Kohärenz des Systems, sowie die im folgenden Schritt getroffenen Maßnahmen müssen es erlauben, ein hohes Schutzniveau zu erreichen. Dieses Niveau muss dann **nachweisbar sein**. Das Ziel dieses Schrittes ist es somit, das Informationssystem hinsichtlich der Kriterien der Verteidigung in der Tiefe zu qualifizieren.

5. Bewertung der permanenten und periodischen Verteidigung an Hand der Angriffsmethoden und der Erfahrungsrückmeldung. Dieser Schritt entspricht dem Kontroll- und Audit-Teil. Aktualisierung der Verteidigung anhand der Bewertungsergebnisse und um die Entwicklungen zu berücksichtigen. Dieser Schritt entspricht den Operationen der Zustandserhaltung der Sicherheit. Er sollte eine Abnahmeentscheidung herbeiführen, die mit den Weiterentwicklungen des Systems über den gesamten Lebenszyklus hinweg kohärent bleiben muss.

4.1.1 Erster Schritt: Bestimmung der Werte und der Sicherheitsziele

Dieser erste Schritt setzt sich demgemäß aus den folgenden Aktionen zusammen, die letztlich klassisch sind. Bestimmung der zu verteidigenden Werte und ihrer Kritizität (die Risikoanalyse, die es anschließend erlauben wird, den Wert der Verteidigung zu quantifizieren: die Zuverlässigkeit einer Ausrüstung muss mit dem Wert der Auswirkung ihres Verlustes gewichtet werden, um die Warnstufe einzuteilen).

Nach diesem ersten Schritt sind die Akteure des Modells identifiziert und die Sicherheitsbedarfe definiert.

Eine Methode des Typs EBIOS erscheint zur Durchführung dieses Schritts besonders geeignet. **In der Tat hilft die EBIOS-Methode bei der Definition von Aufgaben, die der Auftraggeber wahrzunehmen hat**. Die Methode ermöglicht nämlich, den Umkreis der Studie unter Bewahrung einer Globalsicht des in seinem Kontext studierten Systems zu bestimmen, die Bedürfnisse zu äußern (gebunden an die zu schützenden Werte), die Bedrohungen zu identifizieren und einen Projektplan sowie die Verantwortlichkeiten zu definieren[7].

Die vorgeführte Schweregradskala zur Klassifizierung der Sicherheitsereignisse in Abhängigkeit von ihrer Auswirkung auf das Informationssystem ist in der nachstehenden Tabelle angegeben. Sie lehnt sich an die INES-Bewertungsskala an.
Die INES-Bewertungsskala unterscheidet jedoch die Zwischenfälle von den Unfällen in Abhängigkeit von der bestehenden oder nicht bestehenden Off-Site-Auswirkung des Ereignisses. Im Rahmen der Sicherheit der Informationssysteme ist diese Unterscheidung überflüssig. Die vorgeschlagene Skala beruht folglich nur auf der Auswirkung des Ereignisses.

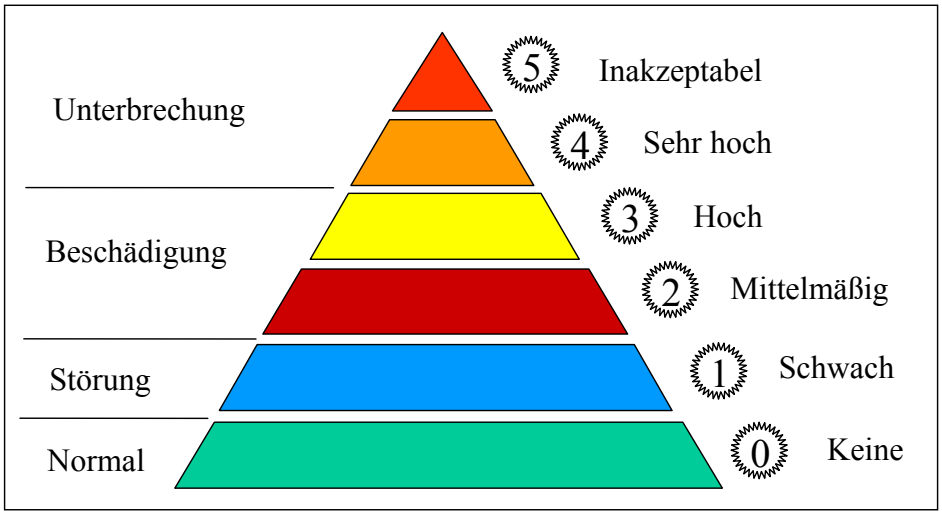


Abbildung 6: IT-Sicherheitsschweregradskala

Dieser Schweregrad kann auf ganz verschiedene Art gemessen werden: In bestimmten Fällen kann es darum gehen, den wirtschaftlichen Verlust zu messen, in anderen Fällen kann es um eine gerichtliche Vorladung gehen. Daher ist es so wichtig zu verstehen, dass diese Messung des Schweregrades eines Zwischenfalls im Anschluss an ein Risikomanagement und nicht nur infolge einer einfachen Einschätzung der Situation zu erfolgen hat.

[7] Äußerung der Bedürfnisse und Identifizierung der Sicherheitsziele – Memento – Version vom 4. Februar 2004

Kategorie	Ebene	Schweregrad	Kriterium
Unterbrechung	5	Inakzeptabel	Das Ereignis gefährdet das Überleben des Unternehmens (das befürchtete Ereignis ist eingetreten).
	4	Sehr hoch	Das Ereignis stellt ein sehr bedeutendes Risiko dar, wodurch unverzüglich Notmaßnahmen eingeleitet werden müssen.
Beschädigung	3	Hoch	Das Ereignis bewirkt kein bedeutendes Risiko, aber ein signifikanter Teil des Systems ist betroffen.
	2	Mittelmäßig	Das Ereignis wirkt sich auf den normalen Betrieb aus und muss zu einer unverzüglichen Reaktion führen.
Störung	1	Gering	Das Ereignis weist keine nennenswerte Auswirkung auf, muss jedoch behandelt werden, um wieder einen normalen Betrieb herzustellen.
Normaler Betrieb	0	Sicherheitstechnisch ohne Bedeutung	Normaler Betrieb.

Tabelle 4: IT-Sicherheitsschweregradskala.

In diesem Schritt geht es folglich darum, die Schweregradstufe der grundlegenden befürchteten Ereignisse (es können die Risikofaktoren genommen werden, die beispielsweise in der Risikoanalyse untersucht wurden) für die verschiedenen zu schützenden Werte anzugeben.
Es ist wichtig, dass sich die in diesem Schritt ausgeführte Analyse aus der Kombination und der gegenseitigen Validierung eines deduktiven (durch die Ressourcen) und anschließend induktiven Ansatzes (durch die Bedrohungen) ergibt und dass der menschliche Faktor berücksichtigt wird. Die in diesem Schritt ausgearbeiteten Szenarien werden im folgenden Schritt modelliert.

4.1.2 Zweiter Schritt: Allgemeine Architektur des Systems

In diesem Schritt werden die Tiefe der Vorrichtung bestimmt und die Organisationen, Technologien und Sicherheitsverfahren ausgewählt. Um diese Auswahl treffen und die empfindlichsten Punkte bezüglich der verschiedenen Bedrohungen identifizieren zu können, wird in der Methode empfohlen, zunächst induktiv vorzugehen (die natürlichste und am weitesten verbreitete Vorgehensweise), indem von der Bedrohung ausgehend Verteidigungslinien bis hin zum zu schützenden Wert vorzusehen sind. Anschließend folgt der IT-Experte einem deduktiven Ansatz ausgehend vom zu schützenden Wert bis hin zur Bedrohung, um eventuell weitere Linien aufzubauen, v. a. aber um die anfälligsten Punkte im System zu identifizieren.

In diesem Teil werden folgende Punkte identifiziert:
- Aufteilung der Zonen in Abhängigkeit von den Risiken, den Aktionen, den großen Funktionen des Unternehmens (Urbanisierung des Sicherheitssystems). Diese Aufteilung erfolgt gemäß den Prinzipien der Unabhängigkeit der Entitäten und der Abtrennung;
- Bestimmung der Barrieren (technisches, prozedurales und menschliches Mittel);
- Klassifizierung der Zonen in Abhängigkeit von ihrer Sensibilität und Bestimmung der Übergangsregeln von der einen zur anderen (in diesem Schritt ist es angebracht, den Fall der Klassifizierung der Informationen und der zu treffenden Maßnahmen für die Zusammenschaltung von zwei Domänen mit verschiedenen Sicherheitsniveaus zu behandeln);
- Unterteilung der Zonen in Vertrauensbereiche: Einführung der organisatorischen Abtrennungen im Allgemeinen (die Tiefe der Organisation);
- Aufteilung privat/gemeinschaftlich in jedem Bereich und zwischen Bereichen.

In diesem Schritt scheint folgendes unerlässlich:

- Ausarbeiten einer „Tabelle der Maßnahmen“, die getroffen werden, um die Verteidigungsmittel in der gesamten Tiefe zu zeigen;
- Modellbildung der kritischen Systeme, um sie zu bewerten;
- Festlegen der Zwischenfälle (Überschreiten einer Barriere) auf der globalen Schweregradskala in Abhängigkeit von der vorher definierten Klassifizierung der Auswirkungen, da sie es im Bereich der operationalen Politik erlauben wird, die Graduierung der Aktionen zu verschaffen und die Verteidigungslinien zu definieren (in diesem Schritt erfolgt die Umsetzung der Barrieren in Verteidigungslinien).

Dieser Schritt muss normalerweise im Vorfeld der Projekte ausgeführt werden, d. h. eine Sicherheitsstudie muss in die Projektverwaltung **integriert** sein. Sofern das System bereits besteht, ist die Methode wie folgt[8] :

- die Topologie des Informationssystems analysieren, sowohl technisch, als auch funktionell;
- die bestehenden Barrieren identifizieren;
- die wichtigsten Prozesse modellieren (Modellbildung der kritischen Daten und der Hauptbedrohungen, um die Barrieren hervorzuheben);
- die bereits eingerichtete Architektur bewerten, um die auszuführenden Änderungen zu bestimmen, damit sie den Kriterien entspricht (z.B. Hinzufügen neuer Barrieren).

4.1.3 Dritter Schritt: Ausarbeitung der Verteidigungspolitik

Dieser Schritt umfasst zwei Teilschritte:

- Bestimmung der globalen und koordinierten Verteidigung[9] :
  - Erkennung (Bestimmung der Kontroll- und Erkennungspunkte der Angriffe);
  - Informationsaufstieg;
  - Korrelation der Ereignisse;
  - Warnung;

- Planung:
  - Bestimmung der möglichen Rekonfigurationen mit einem normalen (Pannentoleranzvorrichtung mit identischen Leistungen) und einem gestörten Betrieb (zum Beispiel: nur lokaler Betrieb, geringere Leistungen, usw.);
  - Reaktionspläne (Planung der in Abhängigkeit von den befürchteten Ereignissen möglichen Aktionen, z.B. Kontinuitätsplan, aber auch Netzrekonfiguration, Umsetzung von Notmitteln, usw.).

[8] In diesem Zusammenhang sollte der Leser die von der DCSSI herausgegebenen Best Practices zu Rate ziehen:
- **BEST PRACTICES BEIM IT-RISIKOMANAGEMENT –** Auswertung der Ergebnisse der EBIOS®-Methode für ein bestehendes System – Version vom 2. Februar 2004 ;
- **BEST PRACTICES BEIM IT-RISIKOMANAGEMENT –** Auswertung der Ergebnisse der EBIOS®-Methode für ein zu konzipierendes System – Version vom 13. Januar 2004.
- [9] In diesem Zusammenhang sollte der Leser die von der DCSSI herausgegebenen Best Practices zu Rate ziehen: **BEST PRACTICES BEIM IT-RISIKOMANAGEMENT –** Auswertung der Ergebnisse der EBIOS®-Methode zur Ausarbeitung einer PSSI – Version vom 21.März 2003.

Die globale Verteidigung dekliniert sich nach drei Achsen (organisatorisch, umsetzungsspezifisch, technologisch), die die Verteidigungslinien integrieren, die in den im vorhergehenden Schritt definierten Zonen eingerichtet sind. Jede Line verfügt im Idealfall über drei Sicherheitsfunktionen: Schutz, Erkennung und Reaktion. Die Verteidigungspolitik muss ihren Schweregrad für die verschiedenen Sicherheitszwischenfälle bestimmen, um Nutzen aus dem „pädagogischen" Methodenbeitrag zu ziehen, was eine bessere Sensibilisierung des Personals erlaubt. Die Schweregradstufen der Zwischenfälle werden anschließend von der Anzahl der verbleibenden Verteidigungslinien abgeleitet.

Der Schweregrad eines Zwischenfalls hängt mehr von den verbleibenden, als von den überschrittenen Verteidigungsmitteln ab. So kann es zum Beispiel ein interner Angriff ermöglichen, mehrere Barrieren zu überspringen, die im Fall eines externen Angriffs überschritten werden müssten. Nach den zuvor definierten Prinzipien der Verteidigung in der Tiefe:

- müssen mindestens 3 Verteidigungslinien vorhanden sein;
- muss die Anzahl der Verteidigungslinien dem Risiko angepasst sein (Eintrittswahrscheinlichkeit und Kritizität des Wertes).

Die Verteidigung muss sowohl global (alle Mittel beteiligen sich am selben Sicherheitsziel), als auch koordiniert sein. Diese Koordinierung betrifft hauptsächlich die Mittel der Auskunft (wodurch die tatsächliche Bedrohung anhand der Analyse von mehreren Informationen über einen laufenden Angriff genau angegeben werden kann) und der Reaktion (Rekonfiguration von Verteidigungsmitteln durch die Erkennung eines anderen Verteidigungsmittels, inklusive der Filtermittel). Es muss bedacht werden, dass diese Koordinierung eher die Barrieren als die Verteidigungslinien betrifft.

Die Dynamik der Verteidigung wird durch die Planung der Reaktionen im Fall einer Sicherheitsverletzung geschaffen. Die Zwischenfälle und Unfälle müssen nach der Schweregradskala klassifiziert werden und obligatorisch eine Reaktion auslösen, die technisch (automatische Antwort), prozedural (Anwendung des Verfahrens oder des entsprechenden Plans) oder menschlich (Entscheidung, Initiative, usw.) ist. Die Reaktionspläne müssen genauso graduiert sein wie die Sicherheitsverletzungen, um die Maßnahmen in Abhängigkeit von der Schweregradstufe zu stärken. Im Rahmen der Verteidigung in der Tiefe muss nämlich die gleichzeitige Berücksichtigung von mehreren Zwischenfällen vorgesehen sein.

Unter den zu treffenden nicht-technischen Maßnahmen, müssen diejenigen, die Klagen gegen externe Dritte bewirken genauso vorgesehen werden, wie diejenigen, die in der Betriebsordnung gegen das Unternehmenspersonal vorgesehen sind (die Technik muss das Beweismaterial liefern, das diese Maßnahmen untermauert).

4.1.4 Vierter Schritt: Die Qualifizierung der Verteidigung in der Tiefe

In diesem Schritt geht es um die Führung der Qualifizierung (Validierung der Organisation und der Architektur) des Systems, die sich aus zwei Ansätzen ergibt: Der erste Ansatz ist qualitativ, während der zweite als demonstrativ durch die Studie der anwendbaren Szenarien zu bezeichnen wäre.

4.1.4.1 Der qualitative Ansatz

Dieser formelle Ansatz zielt darauf ab, die Einhaltung der zuvor definierten Prinzipien der Verteidigung in der Tiefe (§ 3.1.3) zu überprüfen. Er überprüft auch die Einhaltung der Methode, so wie sie auf Institutionsebene formalisiert werden kann.

Dieser Teil ähnelt folglich einer Qualitätssicherung. Sie erinnert an das Kapitel 7 (« rational ») der Norm ISO 15408 (Common Criteria), mit dem die Vollständigkeit der Sicherheitsziele bezüglich der relevanten Bedrohungen nachgewiesen werden kann.

4.1.4.2 Der demonstrative Ansatz

Die Qualifizierungsmethode muss mit der globalen Methode der Verteidigung in der Tiefe, so wie diese ausgearbeitet wurde, kohärent sein und sich insbesondere auf die Ergebnisse stützen, die während der verschiedenen Schritte erzielt wurden.

Diese Methode wird in der nachstehenden Abbildung schematisiert und w.u. erläutert.

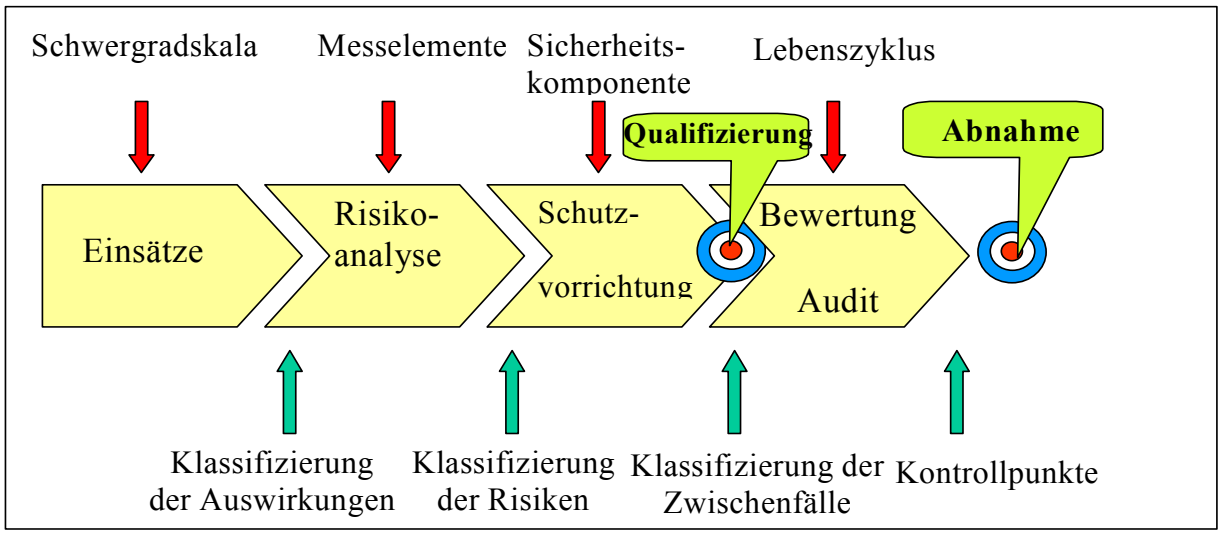


Abbildung 7: Prinzipien einer Bewertung

Der erste Schritt, d.h. die Bestimmung der Sicherheitsziele, erlaubt es einerseits die potentiellen Auswirkungen auf die Schweregradskala in Abhängigkeit von den Einsätzen zu klassifizieren und andererseits die Messelemente für die Klassifizierung der Risiken zu bestimmen.

Der zweite Schritt, d.h. die Architektur des Systems, ergibt die Klassifizierung der Sicherheitszwischenfälle in Abhängigkeit von den fehlerhaften Komponenten.

Der dritte Schritt, d. h. die Ausarbeitung der Verteidigungspolitik, hat die Kontrollpunkte hervorgehoben, die der permanenten Bewertung der Vorrichtung im Laufe dieses Qualifizierungsschritts dienen werden.

Die Methode stützt sich folglich auf:

- eine Methode der Risikoanalyse von der Sicherheit der Informationssysteme, vervollständigt durch die Hierarchisierung der Risiken nach Hauptkomponenten und Sicherheitsfunktionen auf der vorher definierten Schweregradskala mit der die Sicherheitszwischenfälle klassifiziert werden können;
- eine Modellbildung der Verteidigung in der Tiefe, angewandt auf die Hauptrisiken und die Analyse der wichtigsten (insbesondere der "Kumulszenarien") oder der wahrscheinlichsten Szenarien. Diese Szenarien sind iterativ, sie erlauben es, die Barrieren zu bestimmen und die Verteidigung zu bewerten, indem die Methode der fehlerhaften Komponente praktiziert wird, bis die Robustheit der Verteidigung "demonstriert" wird;
- eine Klassifizierung der Sicherheitszwischenfälle auf der vorhergehenden Schweregradskala, die in Abhängigkeit von den definierten Risiken ausgeführt wird. Die Kontrollpunkte der Funktionstüchtigkeit, sowie diejenigen, mit denen die möglichen Angriffe erkannt werden können, werden hervorgehoben; sie erlauben es, die permanente und periodische Bewertung durchzuführen;
- die Bewertungen, die einerseits durch die üblichen Auditmethoden und andererseits durch die Bewertung der Verteidigungen über die Szenarien und Sicherheitszwischenfälle (Suche der potentiellen Auswirkungen) ausgeführt werden;
- die verschiedenen Studien, die es erlauben, das erreichte Sicherheitsniveau nachzuweisen und über das Thema zu kommunizieren, um die Verteidigung in der Tiefe einzurichten und das Personal hinsichtlich der Sicherheitszwischenfälle zu sensibilisieren (durch die Anwesenheit eines Sicherheits-Kontrollschemas, das die Zwischenfälle auf der Schweregradskala hervorhebt, verstärkter Kommunikationsaspekt).

Die Qualifizierungsmethode der Verteidigung in der Tiefe wendet folglich die beiden nachstehenden demonstrativen Analysemethoden an:

- Die Analyse mit „Kumulszenario“: diese Analyse besteht darin, ein Szenario zu erstellen, dass das Maximalrisiko deckt (die Zerstörung des Hauptstandortes) und zu zeigen, dass die anderen Szenarien (z.B. die Unmöglichkeit, in den Hauptstandort einzudringen) im „Kumulfall“ inbegriffen sind und demgemäß, dass die zurückbehaltene Lösung sie deckt. Dieser Ansatz ermöglicht es, die Kohärenz zwischen der Anzahl Barrieren und dem Schweregrad des befürchteten Ereignisses zu überprüfen;

- die Analyse mit "fehlerhafter Komponente". Es geht darum, einen Sicherheitszwischenfall und einen zufälligen Fehler von einer anderen Komponente, die sich zwischen dem Zwischenfall und dem befürchteten Ereignis befindet, zu postulieren, um den verbleibenden Schutz zu analysieren und um zu prüfen, ob er ausreicht.

4.1.4.3 Schlussfolgerung

Folglich vervollständigt die Methode die klassische globale qualitative Analyse durch eine deterministische quantitative Analyse in den Sonderfällen der Szenarien von bedeutenden Risiken, indem der Begriff Kumulszenario und fehlerhafte Komponente eingesetzt wird. Diese Methode ist bestens dem Prinzip der „Demonstration“ von der Sicherheit angepasst, die die Regel im Fall der nuklearen Sicherheit ist und die gefördert werden muss.

Die Qualifizierung, die dem Konzept der Verteidigung in der Tiefe eigen ist, muss es ermöglichen, die Kohärenz zwischen der Anzahl an Verteidigungslinien und des am Ende des ersten Schritts bestimmten Schweregrads der befürchteten Ereignisse, sowie die Akzeptierung der verbleibenden Risiken im Fall von Mangel zu überprüfen.

Die drei ersten Schritte sind nicht sequentiell, sondern iterativ, bis das Schutzniveau erreicht wird, das von der Kritizität der zu schützenden Ressourcen, der potentiellen Bedrohungen und der verbleibenden Risiken gefordert wird. Dieser Schritt erlaubt es, die verbleibenden Risiken hervorzuheben, die bekannt und akzeptiert sein müssen.

4.1.5 Fünfter Schritt: permanente und periodische Bewertung

Weiterhin muss die Bewertung sowohl periodisch (Anfangseinrichtung und eigentliche periodische Revision), als auch permanent (Auswertung der Erfahrungsrückmeldung und der technologischen Überwachung) sein.

Dieser Schritt hat das Ziel, die Verteidigung systematisch zu bewerten:

- statische Studie der Komponenten;
- Dynamik auf Zwischenfall (Erfahrungsrückmeldung);
- Kontrollschema;
- periodisches Audit;
- Rückwirkung (siehe w.u.).

Dieser Schritt ist eng mit dem nächsten verbunden, da er demselben Ziel beisteuert, d.h. die Verteidigung aktualisieren und stärken, indem für die in Bezug auf Kosten/Gewinn unqualifizierbaren Fälle zwei wesentliche Kriterien aus dem Beispiel der Pariser Verkehrsbetriebe RATP genommen werden:

- sich nicht rückläufig entwickeln;
- verbessern, wenn die Kosten der Mühe wert sind.

Die Ergebnisse dieses Schritt müssen es erlauben, den Entscheidungsträgern die Maßnahmen zu präsentieren, die getroffen wurden, um den im Schritt 1 definierten Sicherheitsbedarfen zu entsprechen und somit nachzuweisen, dass die Ziele tatsächlich erreicht sind.

In diesem Schritt muss eine Kommunikationsbemühung ausgeführt werden, um die Szenarien nach Familie zu vereinen und die wichtigsten Verteidigungslinien, sowie die geplanten Reaktionsmaßnahmen hervorzuheben.

Dieser Schritt ist an den Lebenszyklus des Systems gebunden, und als solcher muss er die Operationen der operationellen Zustandserhaltungen berücksichtigen, die im Zusammenhang mit den organisatorischen, technologischen und verfahrensbedingten Weiterentwicklungen stehen.

Er muss eine sicherheitsspezifische Abnahmeentscheidung herbeiführen, die es ermöglicht zu erklären, dass das Informationssystem zur Verarbeitung von Informationen eines gegebenen Sensitivitätsniveaus in der Lage ist. Die Abnahme ist eng an den Lebenszyklus des Systems gebunden und niemals eine Entscheidung von Dauer.

5 Schlussfolgerungen

Die Studie der Verteidigung in der Tiefe im Rahmen der Sicherheit der Informationssysteme zeigt:

- dass das Konzept häufig als Konzept des gesunden Menschenverstandes bezüglich der Redundanz der verwendeten Technologien oder der Vereinigung verschiedener, weit gestreuter Prinzipien angeführt wird, dass aber derzeit noch keine grundsätzlichen Überlegungen auf dem Gebiet der IT-Sicherheit entwickelt wurden;
- dass das im industriellen Bereich eingesetzte Konzept zwar reicher ist, als die herkömmlich eingesetzten Methoden der Risikoanalyse, jedoch pragmatisch und dadurch leicht umsetzbar bleibt;
- dass das Konzept mit seiner Dynamik und seiner Kommunikationsfähigkeit eine bemerkenswerte Bereicherung der üblichen Methoden ist, mit denen es kompatibel ist;
- das das Konzept konkret zur Qualifizierung der Systeme insbesondere in der Kerntechnik angewendet wird.

Gegenüber den herkömmlich für die Sicherheit von Informationen eingesetzten oder in der Bibliographie präsentierten Methoden, die als aus der Methode der Verteidigung in der Tiefe hervorgehend dargelegt werden, scheint die in diesem Dokument vorgeschlagene Methode die nachstehenden Verbesserungen zu liefern:

- Bedeutung der **quantitativen Analyse,** mit der das System in der Zukunft bewertet werden kann;
- Qualifizierung anhand der besonderen **Modellbildungen,** die eine Anfangsbewertung liefern; Kumulszenarien scheinen nämlichen besser geeignet und realisierbarer zu sein, als probabilistische Analysen;
- **Tiefe der Organisation**, die sich auf eine Demonstration der Sicherheit der Vorrichtung anhand der Risiko-Szenarien und der Verteidigungslinien stützt;
- Bewertung nach einer **Schweregradskala**, z.B. die INES-Bewertungsskala, die einen besonders starken **Kommunikationsaspekt** verschafft;
- **globaler** Aspekt der Verteidigung;
- Bedeutung der **Auskunft und der** Überwachung (Kontrollpunkte), die die Aktionsfreiheit schützt;
- **dynamischer** Aspekt der Verteidigung, der den Prozess Überwachung, Warnung, Antwort und Planung integriert;
- **Evolutivität** der Verteidigung durch die Organisation von Erfahrungsrückmeldungen (Suche nach den potentiellen Auswirkungen und nicht nur nach den Ursprüngen), wobei es diese erlaubt die Szenarien zu validieren, zu aktualisieren usw.;
- **Nachweis der Verteidigung zur Qualifizierung eines Informationssystems.**

Es muss bedacht werden, dass der Begriff **Verteidigung** (anstelle von Sicherheit) starke Ideen mit sich führt, da er die Nebensinne der Dynamik, Initiative und Aktionsfreiheit, des gestörten Betriebs usw. mit sich bringt und sich nicht darauf beschränkt, passive Schutzmittel einzurichten.

Das Konzept der Verteidigung in der Tiefe angewandt auf Informationssysteme bietet auch einen interessanten Ansatz in Bezug auf die Problematik der Qualifizierung von Systemen. Die Bereiche des Transports oder der Kerntechnik haben dieses Konzept zur Qualifizierung ihrer Anlagen zu Grunde gelegt, die IT-Sicherheit muss sich daran anlehnen können. Die im Rahmen der IT-Sicherheit anwendbaren Prinzipien, die im vorliegenden Dokument identifiziert wurden, sowie die zu ihrer Umsetzung vorgeschlagene Methode könnten sinnvoll dazu beitragen, die Qualifizierung eines Informationssystems zu definieren.

Es muss hervorgehoben werden, dass das Konzept der Verteidigung in der Tiefe in allen Schichten eines Informationssystems Anwendung finden kann, sowohl auf makroskopischer Ebene, wie in diesem Dokument gezeigt wurde, als auch unter eher mikroskopischen Aspekten, wie z. B. bei der Bewertung eines einzelnen Produktes oder der Implementierung eines Algorithmus.

Achsen von Zusatzstudien erscheinen interessant:

- die Entwicklung eines Werkzeuges der Methode, um die Szenarien zu modellieren und die Verteidigungslinien in Abhängigkeit von den Auswirkungen der Sicherheitszwischenfälle hervorzuheben;
- die Formalisierung der Methode und eine Erfassung der Komponenten, Kontrollmittel, Angriffserkennungsmittel, usw.;
- die Realisierung von Komponenteneinheiten mit Standardarchitekturen, deren Widerstand nachgewiesen ist, was es erlaubt, hinsichtlich der verschiedenen Studien zu kapitalisieren (zum Beispiel für die Kernkraftwerke mit derselben Technologie); diese Entitäten müssten modular sein, damit sie wieder verwendbar sind;
- die Realisierung von eher theoretischen Studien über die Bestimmung einer Widerstandswahrscheinlichkeit der Komponenten, die mit einer Idee der Zertifizierung oder einer quantitativen Bewertung der Sicherheit verbunden sein müsste .

6 Anhang: Anwendung der vorgeschlagenen Methode

In diesem Dokument werden nur die signifikantesten Besonderheiten der Methode vorgestellt.

6.1 Präsentation des konkreten Falls

Der hier untersuchte konkrete Fall ist der Fall eines Teleservices, über den via Internet Anträge zur Ausstellung von Ausweisen gestellt werden können. Über diesen Teleservice verfügt jeder Nutzer über eine Funktion, die es ihm ermöglicht, zu einem beliebigen Zeitpunkt zu erfahren, in welchem Stadium sich sein Antrag befindet.

Die Nutzer werden beim Einloggen identifiziert (Identitätskontrolle, Feststellung der Antragsbedingungen usw.). Nach der Erstellung werden die angefertigten Dokumente über diesen Teleservice so nah wie möglich am Wohnort des Antragstellers abgelegt (Rathaus und Präfektur), um diesem unnötig weite Wege zu ersparen.

Der Teleservice ist in mehrere Abteilungen aufgegliedert, wobei jede Abteilung einer bestimmten Funktion entspricht:

- Zentralisierung der über das Internet gestellten Anträge;
- Anweisung der verschiedenen Verwaltungsbehörden zur Bearbeitung des Antrags;
- Weitergabe der Informationen an eine Archivabteilung.

Die Sicherheitsstudie gemäß der im vorliegenden Dokument vorgeschlagenen Methode betrifft demnach nur die folgenden Informationssysteme:

- die Schnittstelle mit den Nutzern, mit der die Anträge per Internet-E-Mail empfangen werden können (Kommunikationssystem mit einer Zugangsvorrichtung zum Internet und einem Nachrichtenaustauschsystem);
- die Schnittstelle mit den anderen Verwaltungen (Kommunikationssystem, Typ erweitertes Intranet);
- die Schnittstelle mit der Behörde (System der Zusammenschaltung von zwei Intranets);

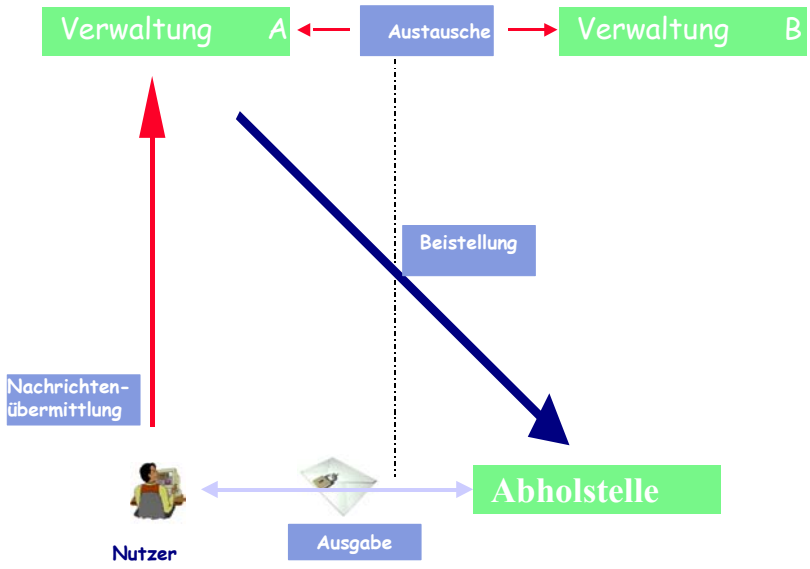


Abbildung 8: Beschreibung des Teleservices

Aus der Sicht der Sicherheit enthält der Teleservice Elemente mit folgenden Merkmalen:

- Das eigentliche System (Hardware, Software und Intranet-Netz):
  - Die Server und Arbeitsstationen, die ein dediziertes Netz bilden;
  - dieses System ist in jeder Verwaltung vorhanden und untersteht deren Verantwortung;
  - die Nutzer sind Angestellte der Verwaltung;
  - die technische Unterstützung wird durch identifizierte, externe Arbeitskräfte sichergestellt;

- die Schnittstelle mit den Nutzern per Internet-E-Mail (Kommunikationssystem mit einer Zugangsvorrichtung zum Internet und einem Nachrichtenaustauschsystem):
  - Die E-Mails mit Anhang kommen an einer dedizierten Arbeitsstation mit Internet-Anschluss an; die Anhänge werden automatisch über ein entsprechendes Tool ausgespeichert, das die Gültigkeit der Anfrage überprüft (Übereinstimmung zwischen E-Mail-Adresse und der Nummer zur Identifizierung des Nutzers bei der Antragstellung);
  - Nutzung eines kaum gesicherten Kommunikationssystems (Internet);

- die Schnittstelle mit den anderen Verwaltungen (Kommunikationssystem, Typ erweitertes Intranet):
  - Verbindung zwischen den beiden Netzen über VPN Internet ;
  - Nutzung eines mäßig gesicherten Kommunikationssystems (VPN Internet);

- die Schnittstelle mit der Abholstelle (System der Zusammenschaltung von zwei Intranets);
  - Verbindung zwischen den beiden Netzen (Teleservice und Archive) über eine Gateway;

- Verwaltungspersonal.

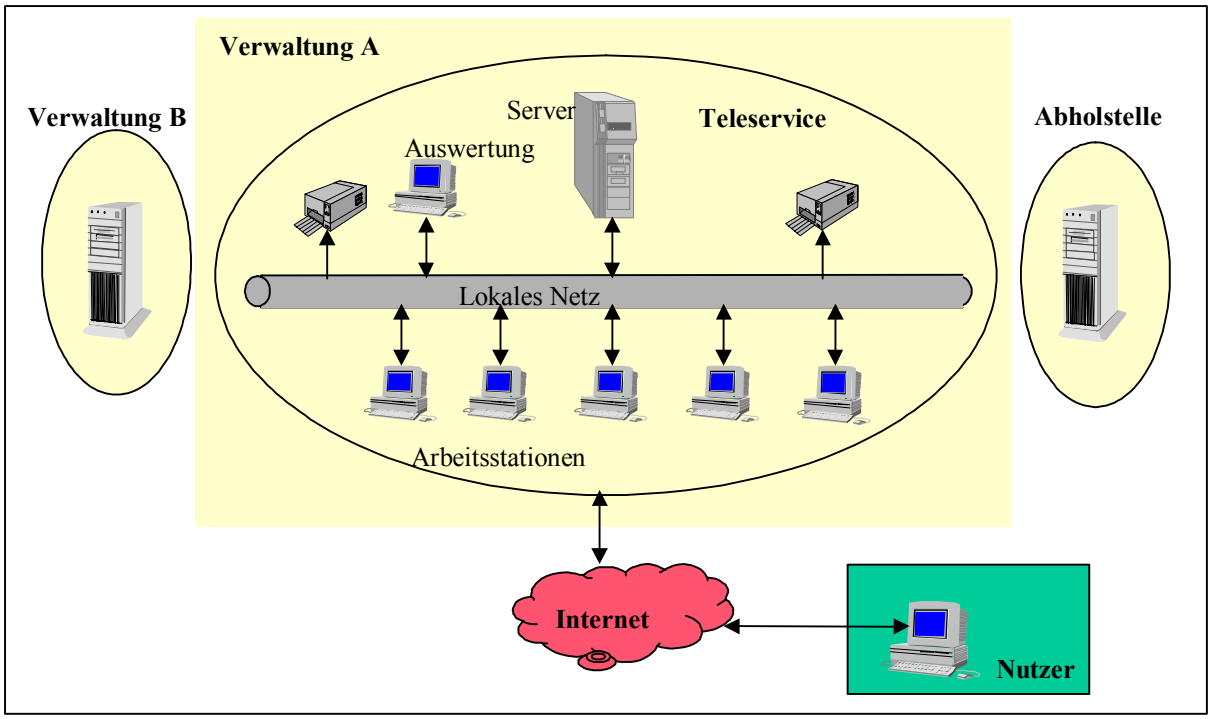
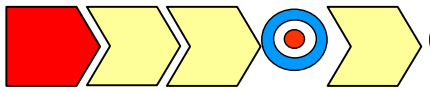


Abbildung 9: Beschreibung des Teleservices

6.2 Ablauf der Methode

In diesem konkreten Fall werden nur die sicherheitsspezifischen Bedürfnisse des Teleservices untersucht, es wird davon ausgegangen, dass die "allgemeinen" Bedürfnisse (physischer Schutz, Personenschutz u. ä.) anderweitig abgedeckt sind. Genauso sollten auch die Systemmerkmale (z. B. Leistungen) im Rahmen des eigentlichen globalen Projekts untersucht werden. Wie bei der Beschreibung der Methode bereits erwähnt, ist die Durchführung einer Risikoanalyse zwingende Voraussetzung für die Nutzung dieser Methode. Es wäre in der Tat unsinnig, sich um eine Verteidigung in der Tiefe von Werten zu bemühen, die man noch nicht identifiziert hat, gegenüber von Bedrohungen, die lediglich auf einer einfachen Einschätzung der Lage beruhen.

6.2.1 Erster Schritt: Bestimmung der Sicherheitsziele



In diesem konkreten Fall werden nur die sicherheitsspezifischen Bedürfnisse des Teleservices untersucht, es wird davon ausgegangen, dass die "allgemeinen" Bedürfnisse (physischer Schutz, Personenschutz u. ä.) anderweitig abgedeckt sind. Genauso sollten auch die Systemmerkmale (z. B. Leistungen) im Rahmen des eigentlichen globalen Projekts untersucht werden.

Der erste Schritt ermöglicht es, die Sicherheitsbedarfe des globalen Systems und seiner Komponenten nach Sicherheitsgrundwerten zu definieren.

Der gesamte Teleservice hat einen großen Bedarf an Verfügbarkeit, die durch Redundanz der IT-Mittel und Vorhandensein systematischer Ersatzmittel sichergestellt werden muss. Während der gesamten Betriebsdauer ist es sehr wahrscheinlich, dass eine oder mehrere Komponenten irgendwann vom Ausfall eines Betriebsmittels, eines Programms o. ä. betroffen werden. Die Verfügbarkeit des Systems an sich ist der wesentliche Punkt. Dieser große Bedarf an Verfügbarkeit hängt mit der Auswirkung eines Ausfalls auf die Funktionstüchtigkeit des Systems zusammen. Die intrinsische Schwere eines Zwischenfalls, der dauerhaft die Verfügbarkeit des Systems in Frage stellen würde, ist folglich als "inakzeptabel" zu bewerten.

Das Ergreifen besonderer Maßnahmen beim Umgang mit Daten und Kommunikationen muss es ermöglichen, dem besonderen Bedarf an Integrität und Vertraulichkeit gerecht zu werden. In Anbetracht der Tatsache, dass das Internet zum Einsatz kommt, hat es die Risikoanalyse bereits ermöglicht, eine bestimmte Anzahl Risiken zu identifizieren. Die intrinsische Schwere eines Zwischenfalls ist somit "Stark", was die Integrität anbelangt und "Sehr stark", was die Vertraulichkeit angeht; verstärkt durch die Anwesenheit externer Arbeitskräfte, die möglicherweise das Risiko von Indiskretionen erhöhen.

Es bleibt festzuhalten, dass der gesamte Teleservice in Anbetracht des Datentransports ein hohes Schutzniveau im Hinblick auf die Vertraulichkeit aufweisen muss. Beim Austausch von Arbeitsstationen durch den Wartungsbetrieb ist Vorsicht angebracht, da es sich um externes Personal handeln kann. Gegebenenfalls ist eine Verschlüsselung der gespeicherten Dateien ins Auge zu fassen.

Beim Betrieb des Systems in seiner Gesamtheit ist der Bedarf an Nachweisbarkeit und an Überprüfbarkeit zu beachten, da dieser Punkt für die gesamte Sicherheit von Bedeutung ist. Die Rückverfolgbarkeit sämtlicher Aktionen und ein systematisches Streben nach "stabilen" Systemzuständen muss es ermöglichen, die Gültigkeit der Informationen kontinuierlich zu überprüfen und gleichzeitig Gewissheit über die Authentizität des Informationsflusses zu haben. Die intrinsische Schwere eines Zwischenfalls ist somit « Stark ».

Die einzusetzenden Mittel zur Erzielung eines ausreichenden Schutzniveaus im Hinblick auf die Nutzer können auch von deren zum Einsatz kommenden Einrichtungen und Systemen abhängen, wobei die einzelnen Maßnahmen erheblich voneinander abweichen können. *A priori* kann jedoch davon ausgegangen werden, dass herkömmliche Rechner mit Internetzugang zu privaten Zwecken benutzt werden. In diesem Fall ist es angebracht, marktübliche Lösungen zu bevorzugen.

Dennoch erfordert dieser Punkt eine zusätzliche Studie, in der die Typologie der Nutzer und die von ihnen voraussichtlich eingesetzten Mittel zu bestimmen sind.

- Dedizierte Arbeitsstation oder herkömmlicher Rechner: A priori dediziert; (??)
- Verbindung zu einem IT-System oder nicht: A priori keine Verbindung;
- usw.

Die Zusammenfassung der Bedürfnisse ist in nachfolgender Tabelle aufgeführt:

Teilsystem	Verfügbarkeit	Integrität	Vertraulichkeit	Nachweis und Kontrolle
Teleservice an sich	Unterbrechung < 1 Std.	Keine Veränderung der Daten	Informationen mit personenbezogenen Daten, also vertrauliche Informationen	Überprüfung der Gültigkeit der Informationen
Annahme und Bearbeitung der Anträge	Unterbrechung < 2 Std.	Keine Veränderung der Daten	Vertraulichkeit durch Verschlüsselung (Gebrauch des Internets)	Authentifizierung des Absenders und Empfangsnachweis
Kommunikation mit den anderen Verwaltungen	Unterbrechung < 1 Std.	Keine Veränderung der Daten	Vertraulichkeit durch Verschlüsselung (Gebrauch des Internets)	Authentifizierung des Absenders und Empfangsnachweis
Kommunikation mit den Abholstellen	Unterbrechung < 4 Std.	Keine Veränderung der Daten	Vertrauliche Informationen	Protokollierung

Tabelle 5: Sicherheitsbedarfe nach Kriterien

Da die Methode die Bewertungsmittel verschaffen soll, erscheint es wichtig, die Sicherheitsziele in diesem Studienschritt zu hierarchisieren. Anschließend erlaubt es diese Hierarchisierung, die Zwischenfälle nach der von der Methode unterbreiteten Schweregradskala einzuteilen. Für diese Hierarchisierung ist es angebracht, die potentiellen Auswirkungen der Sicherheitszwischenfälle zu berücksichtigen.

Die Analyse der vorstehenden Tabelle zeigt, dass eine implizite Hierarchisierung der zu schützenden Werte besteht, die absteigend angegeben sind: Der Teleservice an sich, das Antragsannahmesystem, das Kommunikationssystem mit den Verwaltungen, das Kommunikationssystem mit den Abholstellen.

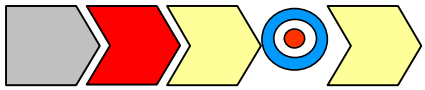
Es besteht ebenfalls eine Hierarchisierung der Sicherheitsziele: die Verfügbarkeit ist ausschlaggebend, die Integrität ist der Vertraulichkeit untergeordnet. Die nachstehende Tabelle zeigt folglich ein Beispiel der Hierarchie der potentiellen Zwischenfälle, wie sie durch die Verwendung der von der Methode unterbreiteten Schweregradskala entstehen kann.

Schweregrad des befürchteten Ereignisses	Schwere Verletzung der für dieses Kriterium ausgedrückten Sicherheitsbedarfe			
	Verfügbarkeit	Integrität	Vertraulichkeit	Nachweis und Kontrolle
5 - Inakzeptabel	Teleservice			
5 – Sehr hoch	Antragsannahme		Teleservice	
3 – Hoch	Kommunikation Verwaltung	Teleservice	Antragsannahme	Antragsannahme
2 - Mittelmäßig	Kommunikation Abholstelle	Antragsannahme	Kommunikation Verwaltung	Teleservice
1 - Schwach		Kommunikation Verwaltung und Abholstelle	Kommunikation Abholstelle	Kommunikation Verwaltung und Abholstelle

Tabelle 6: Hierarchisierung der befürchteten Ereignisse

Da es sich in diesem Dokument um ein Beispiel handelt, betrifft die Modellbildung der Verbindungsketten nur die Risiken, die mit der Anwesenheit von Kommunikationen mit den Verwaltungen, die Internet benutzen, verbunden ist, wobei bedacht wird, dass ein Chiffriermittel, mit dem der Kommunikationspartner authentifiziert, die Integrität der Daten garantiert und deren Vertraulichkeit bewahrt werden können, sowie ein Anwendungssystem zur Kontrolle der Anträge vorgesehen sind.

6.2.2 Zweiter Schritt: Allgemeine Architektur des Systems



6.2.2.1 Präsentation der globalen Lösung

Im nachfolgenden Schema wird die allgemeine Systemarchitektur dargestellt, so wie sie nach Berücksichtigung der Sicherheitsbedarfe in Erscheinung tritt.

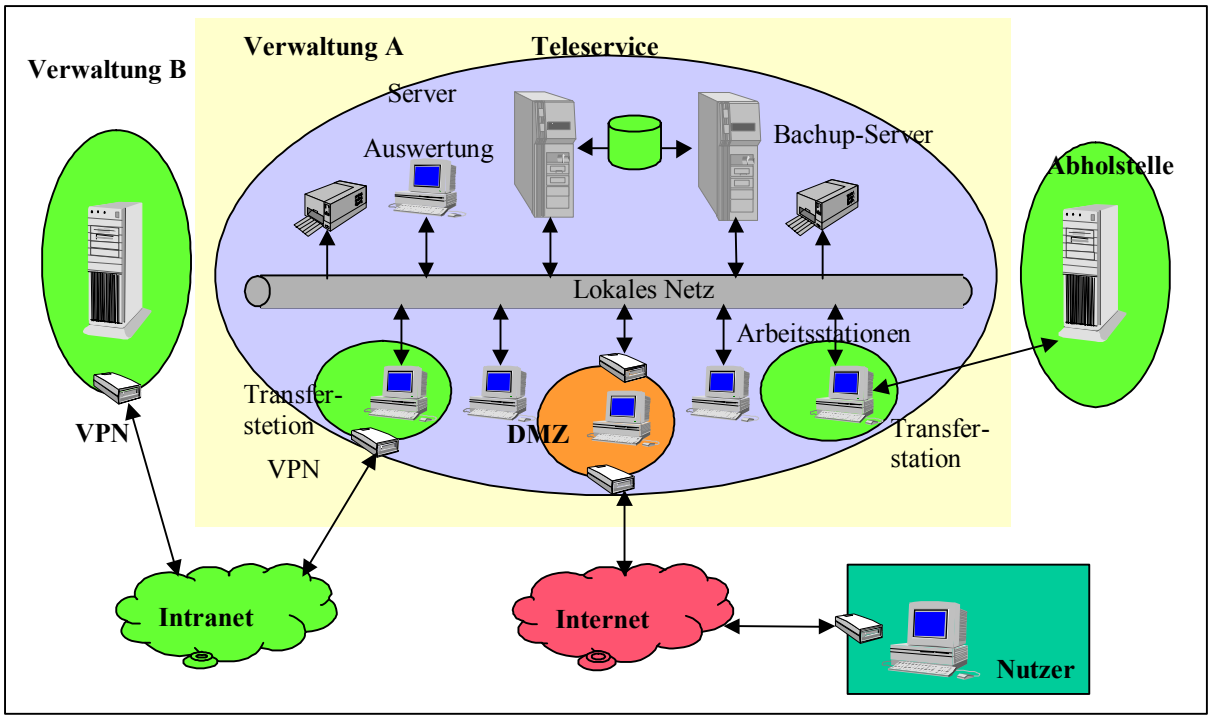


Abbildung 10: Allgemeine Architektur nach Berücksichtigung der Sicherheitsbedarfe

Beim Entwurf des Systems werden folgende Prinzipien berücksichtigt:

- Zwei Server sind mit RAID-Platten ausgerüstet, die von einem Server zum anderen wechseln können, die Ersatzzentrale wird über ein DAT gespeist und ein CD-Brenner dient der Archivierung;
- Was die Vertraulichkeit betrifft, ist der Datenaustausch nach Außen geschützt, dieser Schutz besteht jedoch nicht für den Austausch mit der Abholstelle. Der Austausch erfolgt ausschließlich über dedizierte Arbeitsstationen und es bestehen Ersatzmöglichkeiten. Die Stationen mit Datenaustausch verfügen über eigene FireWalls;
- Aufgrund der Benutzung des Internets und des Vorhandenseins von Diskettenkaufwerken werden Antivirenprogramme (Server und Arbeitsstationen) allgemein eingesetzt;
- Zum Einsatz kommen organisatorische (z. B. Kontrollen) und softwarespezifische Maßnahmen (bezüglich des Datenmanagements, der Archivierung, der Protokollierung usw.).

6.2.2.2 Induktiver und deduktiver Ansatz

Es geht nun darum, die verschiedenen Barrieren nach dem induktiven und dem deduktiven Ansatz zu definieren. Dabei begegnen wir erneut dem Formalismus der EBIOS-Methode und der Common Criteria (ISO 15408) hinsichtlich der Beschreibung der Bedrohung, die durch ein bedrohendes Element, das zum Treffen eines Wertes eine Angriffsmethode einsetzt, charakterisierbar ist. Diese Modellbildung wird hier nur für eine Bedrohung ausgeführt, die nach Abschluss der Risikoanalyse als wesentlich bewertet wurde. In diesem konkreten Fall sind die Informationen auf dem Server des Teleservices das kritische Wert. Die Bedrohung wird somit folgendermaßen definiert:

- Die **Gefahrenquelle** ist ein Hacker, der versucht, den Teleservice zu beeinträchtigen und dem Image der Verwaltung zu schaden;
- die **Angriffsmethode** ist die Einschleusung einer Schadsoftware durch Ausnutzung von an die Nachrichtenübermittlung gebundenen Schwachstellen;
- das **befürchtete Ereignis** ist eine Verletzung der Sicherheit des Informationssystems:
  - Gegen die Integrität der Daten: Annahme eines falschen Antrags;
  - gegen die Verfügbarkeit des Informationssystems durch Nicht-Verfügbarkeit des Servers;
  - gegen die Vertraulichkeit der Daten durch Verbreitung von Informationen.

Da es sich in diesem Dokument nur um ein Beispiel handelt, betrifft die Modellbildung der Ansätze lediglich die Risiken, die an den Gebrauch des Internets zwischen Nutzern und Teleservice gebunden sind. Unter diesem Aspekt werden folgende Hauptrisiken berücksichtigt:

- Alle größeren Risiken, die eine längere Nicht-Verfügbarkeit des Systems bewirken; diese Risiken werden durch das Vorhandensein einer Ersatz-Website abgedeckt, die einen Neustart in weniger als 24 Stunden mit allen Funktionalitäten ermöglichen, auch wenn einige davon etwas eingeschränkt sind;
- Nicht-Verfügbarkeit des Teleservices infolge eines Hardwareausfalls oder menschlichen Versagens. Diese Risiken werden durch Redundanz der Betriebsmittel und manuelle Kontrollprozesse abgedeckt;
- Verlust der Integrität oder der Vertraulichkeit der Daten beim Austausch zwischen den einzelnen Systemen: Dieses Risiko wird teilweise durch die Verwendung eines Chiffriermittels abgedeckt, das es ermöglicht, den Korrespondenten zu authentifizieren, die Integrität der Daten zu garantieren und die Vertraulichkeit zu wahren;
- eine ungültige Information, die über den Kommunikationskanal zur Sammlung der von den Nutzern gestellten Anträge eingedrungen ist.

Induktiver Ansatz

Das erste Szenario untersucht den Fall der Annahme eines via Teleservice gestellten Antrags, der für eine echte Nachricht gehalten wird und folglich die Integrität des Informationssystems verletzen kann. Diese Nachricht entkommt der Zugangskontrolle zur Station, da dieser die eingehenden Nachrichten akzeptiert. Folgende Barrieren kommen zum Einsatz:

- **Barriere Nr. 11**: Die Anwendung, die die Nachrichten der Arbeitsstation ausspeichert, überprüft, ob die Nachricht gültig und korrekt ausgeführt ist;

- **Barriere Nr. 12**: Die Anwendung führt eine Überprüfung der Signatur durch, um den Absender zu authentifizieren und die Integrität des Antrags zu überprüfen;
- **Barriere Nr. 13**: Die Anwendung überprüft die Legitimität des Antrags (Rechte, erste Antragstellung, wiederholte Antragstellung usw.);
- **Barriere Nr. 14**: Die Anwendung speichert den Antrag, ebenso wie Fehler oder Ablehnungen, und startet ggf. die Bearbeitung.

Das zweite Szenario untersucht den Fall eines nicht autorisierten Zugangs, der einen bösartigen Code einführt. In diesem Szenario handelt es sich um einen zerstörenden Virus, der die Verfügbarkeit des Informationssystems verletzen kann.

- **Barriere Nr. 21**: Die Arbeitsstation ist mit einer eigenen FireWall ausgestattet, die so parametriert ist, dass nur der Ein- und Ausgang von Informationsströmen des Typs Nachrichten akzeptiert werden. Es ist anzumerken, dass diese Barriere gegenüber bösartigen Codes via E-Mail wirkungslos ist;
- **Barriere Nr. 22**: Die Arbeitsstation ist mit einer Antivirensoftware ausgerüstet;
- **Barriere Nr. 23**: Die IT-Sicherheits-Policy ist die einzige Barriere auf der Arbeitsstation, die in der Lage ist, einen Angriff per Virus einzugrenzen (z. B durch den Least-Privileg-Grundsatz oder über eine Strategie regelmäßiger Updates);
- **Barriere Nr. 24**: Der Server ist mit einer Antivirensoftware ausgerüstet;

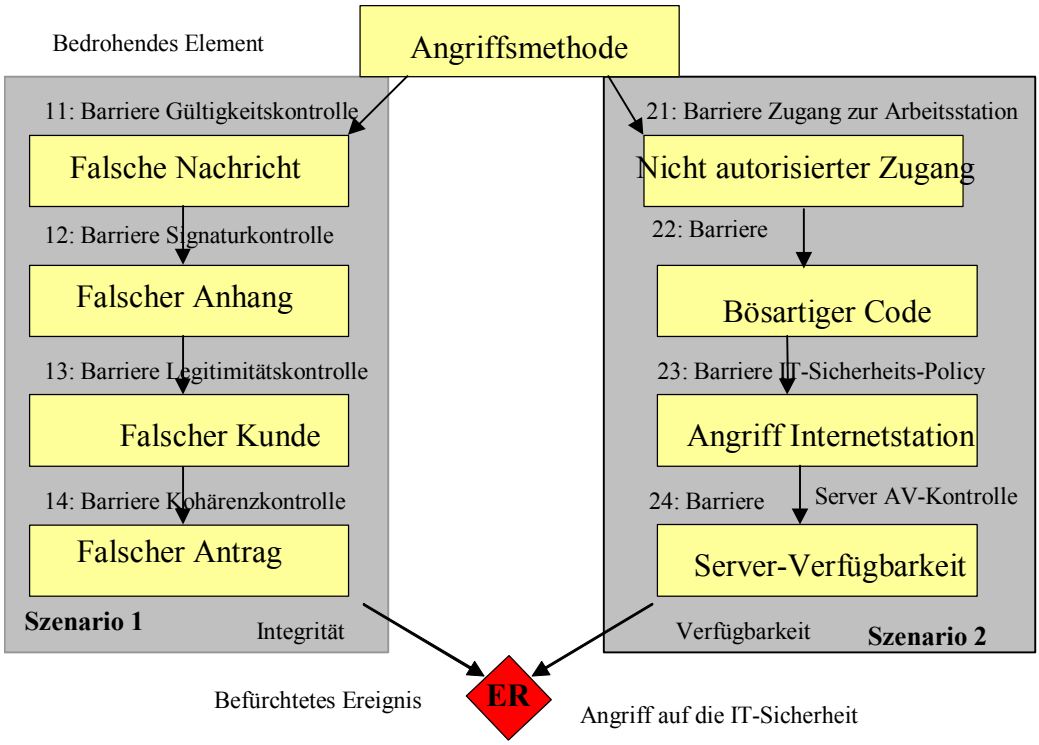


Abbildung 11: Induktiver Ansatz

Deduktiver Ansatz

Bei diesem Ansatz gilt das Interesse, ausgehend vom zu schützenden Wert, den vertraulichen Informationen wie z. B. den personenbezogenen Nutzerdaten, die im Rahmen des Teleservices bearbeitet werden.

- **Barriere Nr. 31**: Die Kontrolle der Zugangsrechte muss einen nicht autorisierten Zugang zum Datenserver unterbinden;
- **Barriere Nr. 32**: Die Arbeitsstation ist mit einer eigenen FireWall ausgestattet, die so parametriert ist, dass nur der Ein- und Ausgang von Informationsströmen des Typs Nachrichten akzeptiert werden.
- **Barriere Nr. 33**: Die Arbeitsstation ist mit einer Antivirensoftware ausgerüstet, die auch die Nachrichten in den Anhängen detektiert.
- **Barriere Nr. 34**: Die individuelle FireWall ist so parametriert, dass nur ein autorisierter Strom ausgehen kann.

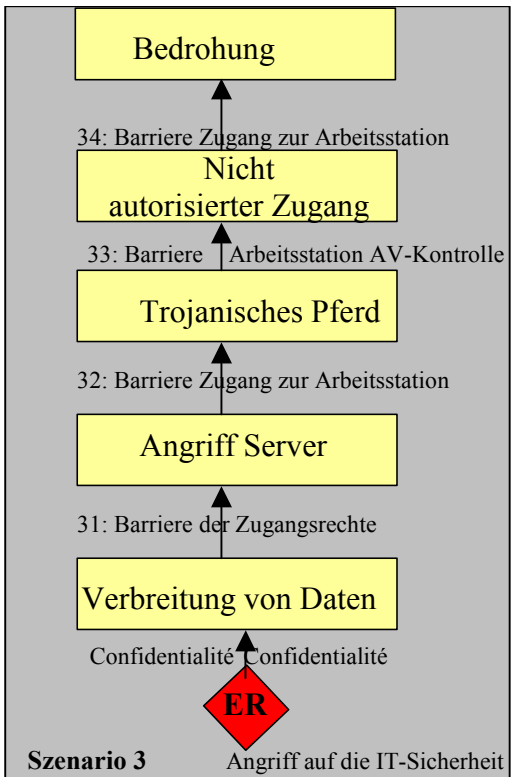


Abbildung 12: Deduktiver Ansatz

Bei Gegenüberstellung der beiden Ansätze lässt sich feststellen, dass manche Barrieren ganz besonders bestimmten Bedrohungen ausgesetzt sind, indem sie sich in mehreren Szenarien und nach beiden Ansätzen wieder finden. Diese Feststellung widerspricht dem Grundsatz der Unabhängigkeit: Die Zerstörung einer solchen Barriere würde gleichzeitig die erste und letzte Verteidigungslinie zunichte machen; also muss eine Verstärkung dieser Kernpunkte bewirkt werden.

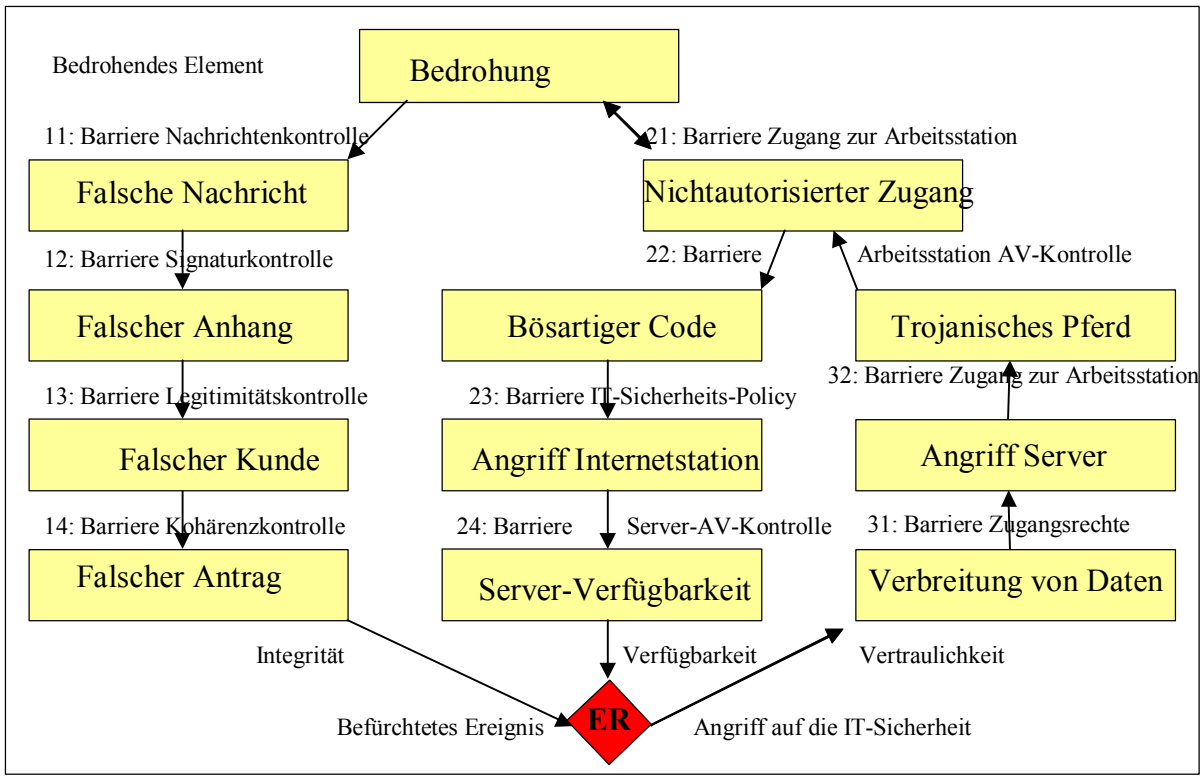


Abbildung 13: Kombination der Ansätze

Schlussfolgerung

Man sieht also, dass der Schutz in Bezug auf über E-Mails eingeschleuste zerstörende Viren äußerst fraglich ist: Die wirksamen Barrieren sind die Antivirenprogramme der Arbeitsstation und des Servers sowie die IT-Sicherheits-Policy der beiden Betriebsmittel. Es ist daher ungeheuer wichtig, den Virus auf der Arbeitsstation zu stoppen und seine Verbreitung auf den Server zu unterbinden.

Die Studie hat die Notwendigkeit offensichtlich gemacht, folgende Punkte im Hinblick auf die Arbeitsstation zu verschärfen:

- Anwendung einer strikten Strategie zur Kontrolle der Privilegien;
- Hinzufügung eines zweiten Antivirus zum Schutze des ersten, wobei dieser anders angelegt sein muss;
- Förderung einer Signatur der ausgehenden Nachrichten;
- Sensibilisierung des Personals.

Für die Schnittstelle mit den Nutzern oder im weiteren Sinne mit dem Internet kann die in Abbildung 14 (??) dargestellte Lösung ins Auge gefasst werden.

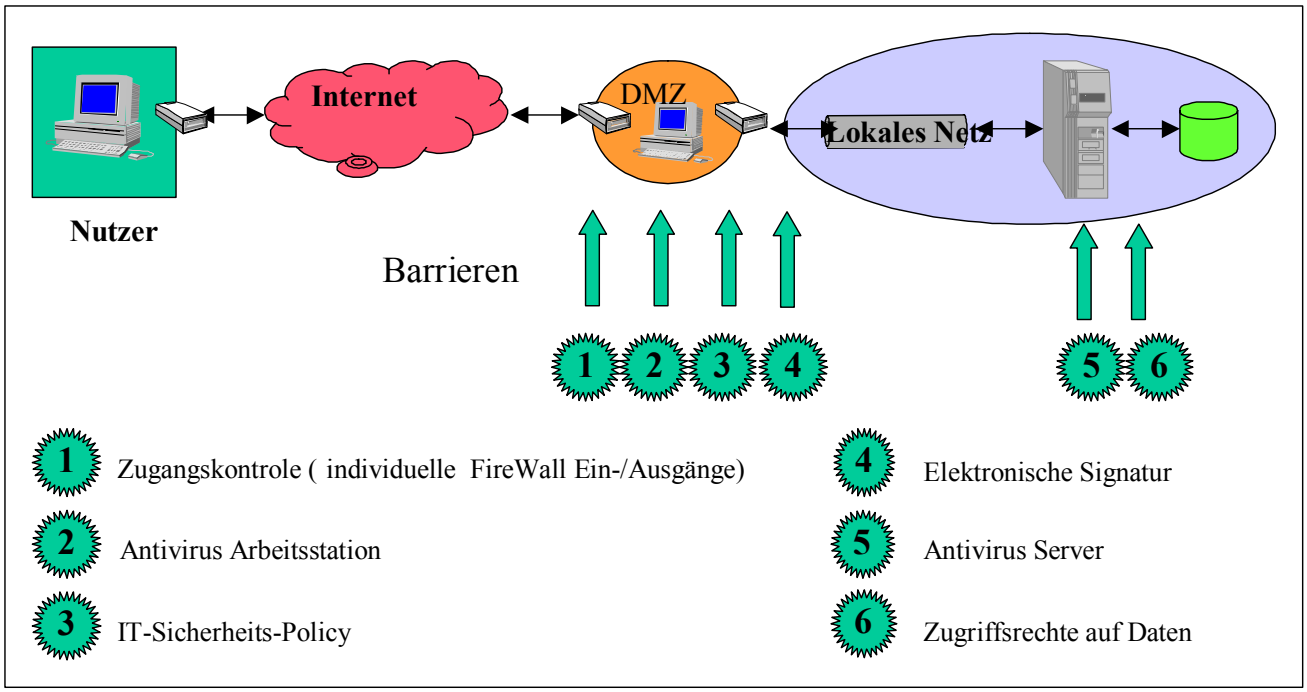


Abbildung 14: Modellbildung der Schnittstelle « Nutzer/Verwaltung »

6.2.2.3 Hierarchisierung der Sicherheitszwischenfälle

An Hand der Analyse der drei Risiko-*Szenarien* und insbesondere ihrer Auswirkung auf den Teleservice und unter Einbeziehung der Hierarchie der befürchteten Ereignisse (Tabelle 6) ist es möglich, diese Szenarien auf der Schweregradskala zu positionieren (siehe Tabelle 7).

Schweregrad	Bösartiger Code (Verfügbarkeit)	Falsche Nachricht (Integrität)	Trojanisches Pferd (Vertraulichkeit)
5 - Inakzeptabel	Server unverfügbar		
5 – Sehr hoch	Internetstation unverfügbar		Verbreitung von Daten
3 – Hoch	Bösartiger Code auf der Internetstation	Falscher Antrag	Erkennung eines Zugangsversuchs zum Server
2 - Mittelmäßig	Vom Antivirus der Internetstation erkannter bösartiger Code	Erkennung falscher Antrag auf Signatur-Ebene	Vom Antivirus der Internetstation erkanntes Trojanisches Pferd
1 - Schwach	Von der FireWall blockierter Intrusionsversuch	Erkennung falscher Anhang oder unbekannter Absender	Von der FireWall blockierter Intrusionsversuch

Tabelle 7: Hierarchisierung der vorgesehenen Zwischenfälle

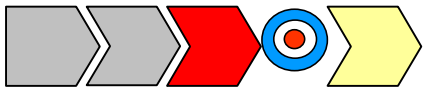
Folgende Verteidigungslinien können nun also in Bezug auf das kritische Wert, d. h. den Datenserver, der den Teleservice unterstützt, hinsichtlich der untersuchten Bedrohung hervorgehoben werden:

- Die FireWall der Arbeitsstation;
- die Arbeitsstation selbst (elektronische Signatur, Antivirus und Verteidigungspolitik);
- der Schutz des Servers an sich (Management der Sicherheitsattribute, Antivirus und Verteidigungspolitik).

Linie	Bösartiger Code (Verfügbarkeit)	Falsche Nachricht (Integrität)	Trojanisches Pferd (Vertraulichkeit)
1	Eigene FireWall	Kontrolle der Nachrichten	Eigene FireWall
2	Antivirus der Station	Kontrolle der elektronischen Signatur	Antivirus der Station
3	Sicherheits-Policy der Station		Elektronische Signatur
4	Antivirus des Servers		Kontrolle der Zugriffsrechte auf den Server
5			

Tabelle 8: Tabelle der Verteidigungslinien

6.2.3 Dritter Schritt: Ausarbeitung der Verteidigungspolitik



Ziel dieses Schritts ist die Ausarbeitung der globalen Verteidigungspolitik. Nun muss die eben durchgeführte Studie, die es ermöglicht hat, die allgemeine Architektur des Systems durch die Definition einer globalen IT-Sicherheits-Policy zu konstruieren, durch die anzuwendenden Verfahren ergänzt und die vorauszusehenden Reaktionen geplant werden. Es geht also um die Umsetzung der Sicherheitsmaßnahmen als zentrales Thema dieses Abschnitts.

Für das in diesem Dokument aufgezeigte Beispiel ist die Definition der IT-Sicherheits-Policy in ihrer Gesamtheit uninteressant. Daher kommen im Folgenden nur die Besonderheiten zur Sprache, die aus der Verteidigung in der Tiefe hervorgehen:

- Koordinierung der Verteidigungslinien, v. a.. im Hinblick auf die Erkennung der Sicherheitszwischenfälle;

Vorausplanung der Reaktionen auf die verschiedenen Zwischenfälle.

6.2.3.1 Bestimmung der globalen und koordinierten Politik

Nachdem die verschiedenen Barrieren bestimmt sind, ist es angebracht, die Kontrollpunkte (um zu wissen, ob die Barriere funktioniert oder nicht) und die Punkte zur Erkennung eventueller Angriffe zu definieren. Diese Analyse dient auch der Auswahl "tauglicher Indikatoren" im fünften Schritt der Methode.
Der Faktor Mensch darf nicht unterschätzt werden. Die Schnellerkennung von Sicherheitszwischenfällen erfolgt in der Tat häufig durch die Nutzer, da nicht immer die Möglichkeit besteht, automatisch und in Echtzeit alle von den Erkennungsmitteln registrierten Informationen auszuwerten.

Die IT-Sicherheits-Policy muss folgende Punkte berücksichtigen:
- Ein Parametrieren der Software, so dass den Nutzern Anomalien angezeigt werden können (ggf. Freigabe ?? des Stroms, während das Antivirenprogramm aktualisiert wird);
- eine spezielle Schulung der Nutzer, um sie für die Risiken im Zusammenhang mit Internet-Anschlüssen und speziell für Viren in Anhängen von E-Mails zu sensibilisieren, die das größte Risiko dieses Anschlusses darstellen, da der Nachrichtenfluss obligatorisch ist;
- Kontrollen zur Überprüfung der Funktionstüchtigkeit des ganzen Systems (Traces, Ereignisprotokolle, Plattenkapazität usw.);
- eine Abtrennung der einzelnen Systeme, so dass jedes System über seine eigenen Schutzmittel verfügt. Einsatz spezieller Eindringerkennungssysteme vom Typ IDS;
- ein System zur Weiterleitung von Sicherheitszwischenfällen, damit reagiert werden kann (siehe folgender Abschnitt über die Vorausplanung) und Warnung der Nutzer z. B. bei Erkennung eines neuen Virus.

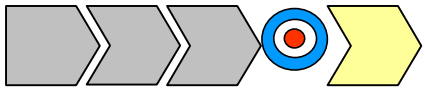
6.2.3.2 Vorausplanung

Gegenüber den voraussichtlichen Sicherheitszwischenfällen muss auch die Reaktion vorausgesehen werden.
In dem in diesem Dokument untersuchten Beispiel wurde als wesentlichstes Risiko die Nicht-Verfügbarkeit des Teleservices erkannt, die auf zwei Hauptursachen zurückgeführt werden kann:
- Auf eine Hardware- oder Softwarepanne (z. B. auf Grund eines Bedienungsfehlers), die den Server selbst, das lokale Netz oder, in geringerem Umfang, eine Kommunikationskette in Mitleidenschaft zieht;
- auf eine von Außen kommende böswillige Verletzung der Sicherheit des Systems (der Fall einer von Innen kommenden böswilligen Absicht wird an dieser Stelle nicht behandelt und der Fall eines irrtümlichen Fehlers wurde bereits besprochen).

Für den Fall eines Ausfalls des Servers auf Grund eines Hardwarefehlers sieht die Vorausplanung verschiedene Behebungsmöglichkeiten vor:
- Neustart auf dem zweiten Server über die RAID-Platten des ersten Servers ohne Datenverlust nach etwa dreißig Minuten;
- Neustart auf dem zweiten Server über "Disk-to-Disk"-Sicherung mit Wiederherstellung der aus den Kommunikationen stammenden Daten und Neueingabe der übrigen Daten innerhalb eines halben Tages;
- Neustart auf der ausgelagerten Ersatzzentrale über die Kassettenspeicherung mit Wiederherstellung der E-Mail-Daten (systematische Umleitung von einer Mailbox auf eine zweite Ersatzbox) und Neueingabe der übrigen Daten innerhalb eines Tages.

Die Möglichkeit eines Ersatznetzes ist durch Redundanz der Mittel gegeben (zwei Server und Netz-Ersatzmittel).

6.2.4 Vierter Schritt: Qualifizierung



Diese Qualifizierung erfolgt durch einen qualitativen Ansatz (Einhaltung der Prinzipien der Verteidigung in der Tiefe) und durch einen demonstrativen Ansatz (Reaktion auf *Kumulszenarien* pro fehlerhaftes Element).

6.2.4.1 Qualitativer Ansatz

Im Rahmen des konkreten Falls haftet diesem demonstrativen Aspekt sicherlich etwas Künstliches an. Deshalb sollen hier nur noch einmal die Prinzipien, die eine Verteidigung in der Tiefe bei einem Informationssystem charakterisieren, in Erinnerung gerufen werden, ohne dass ein Nachweis durchgeführt wird.

.

Titel	***Beschaffenheit***
Globalität	**Die Verteidigung muss global sein, d. h. sie muss alle Dimensionen des Informationssystems umfassen:** d) Organisatorische Aspekte; e) Technische Aspekte; f) Aspekte der Umsetzung.
Koordination	**Die Verteidigung muss koordiniert sein, d. h. die zum Einsatz kommenden Mittel wirken:** c) dank einer Warnungs- und Weitergabekapazität; d) infolge einer Korrelation der Zwischenfälle.
Dynamik	**Die Verteidigung muss dynamisch sein, d. h. das Informationssystem muss über eine IT-Sicherheits-Policy verfügen, die folgende Elemente zulässt:** d) Reaktionskapazität; e) Vorausplanung der Aktionen; f) Schweregradskala.
Hinlänglichkeit	**Die Verteidigung muss hinlänglich sein, d. h. jedes (organisatorische oder technische) Schutzmittel muss über:** d) einen eigenen Schutz; e) Mittel zur Erkennung; f) Reaktionsverfahren verfügen.
Vollständigkeit	**Die Verteidigung muss vollständig sein, d. h.:** d) die zu schützenden Werte werden in Abhängigkeit von ihrer Kritizität geschützt; e) jedes Wert wird durch mindestens drei Verteidigungslinien geschützt, f) die Erfahrungsrückmeldung ist formalisiert.
Nachweis	**Die Verteidigung muss nachweisbar sein, d. h.:** d) die Verteidigung ist qualifiziert; e) es besteht eine Strategie zur Abnahme; f) die Abnahme muss dem Lebenszyklus des Informationssystems angepasst sein.

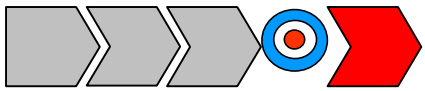
6.2.4.2 Demonstrativer Ansatz

Der demonstrative Ansatz besteht in einer Analyse eines jeden Kumulszenarios, etwa so wie sie in Schritt 2 durchgeführt wurde, pro fehlerhaftes Element. Im Rahmen unseren konkreten Falls beschränken wir uns auf den Nachweis pro fehlerhaftes Element für ein Szenario.

Untersucht werden soll das weiter oben beschriebene Szenario Nr.2:
- Über die Nachrichtenübermittlung hat sich ein bösartiger Code eingeschlichen, der – aus welchem Grund auch immer - nicht vom Antivirenprogramm entdeckt wurde;
- als Barriere bleibt die IT-Sicherheits-Policy der Arbeitsstation bestehen;
- ebenso wie die Antivirensoftware auf dem Server, die anders angelegt ist als das Antivirenprogramm der Arbeitsstation.

Falls die IT-Sicherheits-Policy versagt, besteht also noch eine weitere Barriere vor dem befürchteten Ereignis, und das ist ausreichend.

6.2.5 Fünfter Schritt: Bewertung und Audit



Im Rahmen dieses Dokuments erscheint es interessant, signifikante Sicherheitszwischenfälle zu untersuchen, um die dynamische Phase der Erfahrungsrückmeldung und Rückwirkung zur Sprache bringen zu können.
Folgende Sicherheitszwischenfälle sollen untersucht werden:
- Ein Ausfall der Servernetzkarte;
- ein Ausfall des DAT-Lesers.

Ein Ausfall der Netzkarte des Servers ist ein **inakzeptables Ereignis,** sofern er nicht im vorgeschriebenen Zeitraum behoben wird, da er die Verfügbarkeit des Teleservices in Frage stellt. Bis zur Behebung der Panne wird der Zwischenfall umgangen, indem das vorgesehene Verfahren zum Umschalten vom Hauptservernetz auf den Ersatzserver eingeleitet wird. Dieses Verfahren bewirkt einen etwa dreißigminütigen Stillstand zum Rollentausch der beiden Server.

Ein Ausfall des DAT-Lesers ist ein Sicherheitsereignis, das auf der Schweregradskala nicht vorgesehen ist. Er stellt die Verfügbarkeit der ausgelagerten Ersatzzentrale in Frage. Die Sicherheit des Hauptstandorts wird davon nicht berührt, da die Informationen zwischen den beiden Servern des Hauptstandorts dupliziert werden. Es ist also angebracht, die Mittel zur Umgehung des Ereignisses zu analysieren und die potentiellen Risiken einzuschätzen:

- Als Ersatzmittel ist eine Zip-Platte mit ausreichender Speicherkapazität vorgesehen (das Extrahieren von Daten erfolgt durch Speicherauszug der Tabellen und evtl. Komprimierung zur Reduzierung des Platzbedarfs, anstatt einer physischen Sicherung der Datenbank wie bei DAT). Es besteht also mindestens noch eine Barriere, bevor die Disponibilität der Ersatzzentrale eingeschränkt werden würde;
- das potentielle Risiko einer Verletzung der Verfügbarkeit des Hauptstandorts wird durch die Verteidigungslinien in Form einer Redundanz der Server und einer Ersatzzentrale abgedeckt. In Bezug auf das befürchtete Ereignis existieren also drei Verteidigungslinien (die Redundanz der Server, die Ersatzzentrale und der Umgehungsmechanismus).

Ein Virus im Anhang einer E-Mail stellt das Antragsannahmesystem in Frage, das zuvor modellisiert wurde und für das die Modellbildung gerade eben eine Schwachstelle im Szenario aufgedeckt hatte. Im folgenden Abschnitt soll nun untersucht werden, wie durch Erfahrungsrückmeldung die Modellbildung und die Szenarien bereichert werden können. Zwei Aspekte sind hierbei zu berücksichtigen:

- Die Klassifizierung des Ereignisses auf der Schweregradskala und die aus der Vorausplanung direkt hervorgehenden korrektiven Maßnahmen;
- die Untersuchung der potentiellen Risiken und Bereicherung der Szenarien.

Die Klassifizierung des Ereignisses hängt zunächst vom eingesetzten Mittel zur Erkennung des Zwischenfalls ab, der an den folgenden Kontrollpunkten hätte erkannt werden können, wobei die Reihenfolge nach Wichtigkeit erfolgt:

- Erkennung über die Antivirensoftware der Arbeitsstation: Dabei handelt es sich nicht um einen Zwischenfall, sondern um einen **Normalbetrieb** des Antivirusprogramms;
- Erkennung durch den Nutzer der Arbeitsstation, bevor der Virus Schaden anrichten konnte: Dies ist ein **Ereignis mittlerer Schwere** in Abhängigkeit von der Modellbildung für bösartige Codes (es besteht weiterhin der Kommunikationsschutz zwischen der Arbeitsstation und dem Server, die Antivirensoftware auf dem Server und schließlich die IT-Sicherheits-Policy des Servers (Redundanz) sowie die Existenz einer Ersatzzentrale);
- Erkennung über die Antivirensoftware des Servers: Dies ist ein **Ereignis sehr großer Schwere,** da das Antragsannahmesystem nicht mehr operationell ist und außer der IT-Sicherheits-Policy keine weitere Barriere mehr den Server schützt (wenn man die Ersatzzentrale einbezieht, nimmt der Schweregrad etwas ab, doch handelt es sich hierbei um eine mindere Verfügbarkeits-Anforderung auf Grund der sehr geringen Eintrittswahrscheinlichkeit: Die Existenz dieser Ersatzzentrale ist vielmehr darauf zurückzuführen, dass als inakzeptabel bewertete Restrisiken nicht unberücksichtigt bleiben dürfen).

Dieser Zwischenfall macht deutlich, wie wichtig es ist, die Nutzer entsprechend zu schulen und die Anwendungen regelmäßig zu aktualisieren. In diesem Zusammenhang ist die Erfahrungsrückmeldung zu fördern, ebenso wie der Einsatz von Indikatoren, über die schwache Signale erkannt werden können, und die, wenn sie zueinander in Relation gesetzt werden, dazu beitragen können, schwere Zwischenfälle zu verhindern. So muss beispielsweise die über einen längeren Zeitraum wiederholte Erkennung von Viren auf bestimmten Arbeitsstationen eine Warnung für das Verteidigungssystem darstellen.

Für jede neu erkannte Schwäche ist es angebracht, bei deren Behebung zwei Prinzipien im Auge zu behalten:
- sich nicht rückläufig entwickeln;
- verbessern, wenn die Kosten der Mühe wert sind.

Die übrigen im Rahmen dieses Schrittes vorgesehenen Aufgaben sind für die Verteidigung in der Tiefe nicht spezifisch, mit Ausnahme der Ausführungen über das Kontrollschema, das in die Schweregradskala der Zwischenfälle zu integrieren ist.

Kommentarsammelformular

Dieses Formular kann an folgende Adresse geschickt werden:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identifizierung des Beitrags
Name und Einrichtung (fakultativ): .....
E-Mail-Adresse: .....
Datum: .....

Allgemeine Bemerkungen über das Dokument
Wird dieses Dokument Ihren Bedürfnissen gerecht? Ja □ Nein □

Falls ja:

Meinen Sie, dass es von Grund auf verbessert werden kann? Ja □ Nein □

Falls ja:

Was hätten Sie noch gerne in ihm gefunden?
.....
.....

Welche Teile des Dokuments erscheinen Ihnen überflüssig oder ungeeignet?
.....
.....

Meinen Sie, dass es in seiner Form verbessert werden kann? Ja □ Nein □

Falls ja:

In welchem Bereich kann es verbessert werden?
- Lesbarkeit, Verständnis □
- Präsentation □
- sonstiges □

Geben Sie Ihre Wünsche hinsichtlich der Form an:
.....
.....

Falls nein:

Geben Sie den Bereich an, der Ihnen nicht zusagt und definieren Sie, was Ihnen gefallen würde:
.....
.....

Welche anderen Themen würden Sie gerne behandelt sehen?

.....
.....

Besondere Bemerkungen über das Dokument

Mit der folgenden Tabelle können detaillierte Kommentare abgeben werden.

"Nr." gibt die Ordnungsnummer an.

"Typ" setzt sich aus zwei Buchstaben zusammen:

Der erste gibt die Kategorie der Bemerkung an:

- O Rechtschreibe- oder Grammatikfehler
- E Fehlende Erklärungen oder ungenügende Klarheit über einen bestehenden Punkt
- I Unvollständiger oder fehlender Text
- R Fehler

Der zweite gibt seinen Charakter an:

- m unwesentlich
- m Wesentlich

"Referenz" gibt die genaue Stelle im Text an (Nummer des Paragrafen, der Zeile, usw.).

In "Darlegung der Bemerkung" kann der Kommentar erläutert werden.

In "Vorgeschlagene Lösung" kann das Mittel zur Lösung des genannten Problems unterbreitet werden.

Nr.	Typ	Referenz	Darlegung der Bemerkung	Vorgeschlagene Lösung
1				
2				
3				
4				
5				

Vielen Dank für Ihre Mithilfe