



Ein nationales IT- Frühwarnsystem für Deutschland

Positionspapier der ITK-Wirtschaft

■ Impressum

Herausgeber:

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10

10117 Berlin-Mitte

Tel.: 030/27 576 – 0

Fax: 030/27 576 – 400

bitkom@bitkom.org

www.bitkom.org

Eine Arbeit des Fachausschusses Frühwarnsysteme

Version: 1.0, Stand 1.8.2005

Leitung:

Dr. Welsch, Günther, Deutsche Telekom AG

Frießem, Paul; Fraunhofer SIT

Greifzu, Ulf; IBM Deutschland GmbH

Dr. Lamsa, Andreas, Datev eG

Neurath, Rudolf J.; IABG mbH

Sander, Jürgen; Presecure Consulting GmbH

van Nouhuys, Jo; Condat AG

Woitke, Martin; secunet Security Networks AG

Ansprechpartnerin:

Dr. Sandra Schulz, BITKOM e.V.

Tel: +49 (0)30 / 27576 – 242

E-Mail: s.schulz@bitkom.org

Inhaltsverzeichnis

1	Einleitung	4
2	Problembeschreibung	5
2.1	Die heutige Situation	5
2.2	Konsequenzen	9
3	Referenzbereiche.....	11
3.1	Warn-Management des Deutschen Wetterdienst	11
3.2	Vorhersage von Epidemien	12
3.3	Mess- und Informationssystem zur Umweltradioaktivität	13
4	Das nationale IT-Frühwarnsystem.....	16
4.1	Einordnung des Begriffs Frühwarnsystems	16
4.2	Ziele und Aufgaben des IT-Frühwarnsystems	18
4.3	Grundsätzliche Implikationen	18
5	Elemente eines IT-FWS	19
5.1	Zielgruppen.....	19
5.2	Akteure	19
5.3	Organisationsstruktur	21
5.4	Technik und Informationsmanagement	23
5.5	Dienstleistungen	27
6	Fazit und Handlungsempfehlungen.....	30

1 Einleitung

Durch den Einsatz von leistungsfähiger Informationstechnik, die über das Internet stark vernetzt ist, erhöhen sich die Bedrohungen für die Infrastruktur in den Unternehmen. Schwachstellen werden immer intelligenter ausgenutzt, um auf fremde Infrastruktur zuzugreifen und um dort erhebliche Schäden zu erzeugen (siehe Kapitel 2). Heute werden pro Tag ca. 16 neue Schwachstellen in IT-Produkten gemeldet, während es 1998 gerade mal eine Schwachstelle pro Tag war.

Die Bundesregierung hat dies frühzeitig erkannt. Schon 2003 hat Innenminister Otto Schily den Aufbau eines nationalen IT-Frühwarnsystems für Deutschland angekündigt. Die ITK-Wirtschaft nimmt diese Aufgabe ernst und hat daher frühzeitig beim BITKOM einen Fachausschuss IT-Frühwarnsysteme (IT-FWS) eingerichtet. Das vorliegende Positionspapier ist im Rahmen einer neunmonatigen Arbeit dieses Fachausschusses entstanden.

Ausgangslage der Arbeit war ein öffentlicher Workshop des BITKOM mit dem BMWA im Mai 2004. Fachleuten und Anwendern haben in Workshops Informationen über und Erfahrungen mit Frühwarnsystemen interdisziplinär ausgetauscht. Die daraus resultierenden Anforderungen an Industrie, Wirtschaft und Politik wurden diskutiert und erste Anforderungen an ein IT-FWS erarbeitet. Im vorliegenden Positionspapier befinden sich die Ergebnisse des Workshops in Kapitel 3.

Aufgabe eines Frühwarnsystems im IT-Bereich ist die rechtzeitige Anzeige von Gefahrensituationen für gesellschaftlich relevante IT-Infrastrukturen. Dabei ist aufgrund der schnellen Verbreitung von Bedrohungen besonders wichtig, Warnungen bei minimalen Anzeichen für bevorstehende Angriffe an die primären Zielgruppen zu geben – idealerweise im Verbund mit entsprechenden Handlungsempfehlungen. Wichtig ist weiterhin, dass sich ein IT-FWS nicht nur auf einzelne konkrete Probleme fokussiert, sondern eine übergreifende Einschätzung der aktuellen Gefahren erlaubt. Besonderes Augenmerk ist auch darauf zu legen, dass für die Einschätzung von Gefahren Informationen aus technischen und gesellschaftlichen Quellen zu einem umfassenden Lagebild zu verdichten sind. Eine detaillierte Beschreibung eines nationalen IT-FWS aus Sicht der Wirtschaft ist in Kapitel 4 zu finden. Die daraus resultierenden einzelnen Elemente eines IT-FWS sind in Kapitel 5 erläutert.

Konkrete Handlungsempfehlungen für einen notwendigen Aufbau eines nationalen IT-Frühwarnsystems sind im letzten Kapitel zu finden. Nach Ansicht der Autoren und des BITKOM ergibt sich die Notwendigkeit, ein IT-Frühwarnsystem in Deutschland zu etablieren.

2 Problembeschreibung

In diesem Kapitel wird die heutige Situation des Managements von IT-Systemen sowie die daraus resultierenden Herausforderungen für das Management beschrieben. Im Mittelpunkt des Interesses steht die Abwehr von Angriffen auf IT-Systeme, die heute hoch vernetzt in allen Bereichen der Wirtschaft der Verwaltung und den Privathaushalten vorhanden sind.

Diese hochgradige Vernetzung wird immer mehr unter dem Gesichtspunkt von „kritischen Infrastrukturen“ gesehen. Durch die Abhängigkeit vieler wichtiger Infrastrukturen von funktionsfähigen IT- und TK-Systemen sind heute gesellschaftlich oder volkswirtschaftlich wichtige Prozesse berührt, deren Ausfall das öffentliche oder privatwirtschaftliche Leben beeinträchtigen würde.

2.1 Die heutige Situation

2.1.1 Schwachstellen, Verwundbarkeiten und deren Ausnutzung

Das IT-System- und Sicherheitsmanagement ist heute in einer extrem schwierigen Lage. Täglich erscheinen Informationen über potenzielle Schwachstellen in den von ihnen eingesetzten bzw. überwachten Systemen. Dabei entsteht bei jeder Schwachstelle aufs neue ein Wettlauf zwischen Personen, die solche Schwachstellen ausnutzen, um bösartige Zugriffe auf IT-Systeme zu erzielen, und dem Sicherheitsmanagement, rechtzeitig Updates und Patches zu erhalten, um die Schwachstelle zu schließen. Die größte Sorge ist heute, dass mit Erscheinen einer Schwachstelle auch unmittelbar deren Ausnutzung erfolgt (so genannter Zero-Day-Exploit).

Wo liegen die Gründe? Die besonders intensive und weiter zunehmende vernetzte Nutzung von IT offenbart wesentlich häufiger Schwachstellen und Verwundbarkeiten.

Es ist empirisch belegt, dass Software kaum fehlerfrei erstellt werden kann, und insbesondere ihre vernetzte Anwendung Seiteneffekte auslöst. Es ist daher nicht verwunderlich, dass die Zahl öffentlich bekannter Schwachstellen stetig zunimmt. Schwachstellen, die unmittelbar in einem IT-Produkt angesiedelt sind, lassen sich als primäre Schwachstellen bezeichnen, während sich Schwachstellen, die sich durch das Zusammenwirken unterschiedlicher, vernetzter IT-Produkte ergeben, als sekundäre Schwachstellen bezeichnen lassen.

Für die meisten der gemeldeten Schwachstellen erscheinen relativ schnell Patches und Updates, die dafür sorgen sollen, die erkannten Schwachstellen zu schließen. Es ist aber nicht verwunderlich, dass sich nach deren Einsatz bei der technischen Komplexität manchmal zusätzliche Verwundbarkeiten ergeben. So erscheint schon häufiger einmal ein Patch zum Patch oder ein Update zum Update, um neu entstandene Schwachstellen wieder auszumerzen.

Es lässt sich nur äußerst schwer schätzen, wie viele Schwachstellen in IT-Systemen und Anwendungen verborgen sind. Gerade im IT-Bereich führen die kurzen Innovationszyklen ggf. auch zu kürzeren Testzyklen. Verschärfend kommt hinzu, dass bei vielen Anwendern und Nutzern IT-Systeme und Anwendungen im Vergleich zu den Innovationszyklen sehr lange verwendet werden. Somit ist der Hersteller eines IT-Systems bzw. einer Anwendung gezwungen, nicht nur in der aktuellen Generation seines Produktes nachzubessern, sondern ggf. in der ganzen betroffenen Produktfamilie. Der damit verbundene Aufwand ist natürlich ungleich höher und zeitaufwändiger.

Selbst durch vollständige Tests der Produkte vor ihrer Markteinführung kann eine Fehlerfreiheit kaum garantiert werden. Aufgrund der Variantenvielfalt der möglichen Einsatzszenarien können nicht alle möglichen sekundären Schwachstellen und Seiteneffekte erkannt werden. Jeder Fehler, der bei einem individuellen Einsatzszenario auftritt, hat den Charakter eines Unikats. Aus diesem Grund lassen sich empirische Ansätze aus anderen technologischen

Disziplinen zur Fehlervermeidung und -behebung, z. B. erfahrungsbasierte Problemlösungsansätze, nur schlecht oder gar nicht auf den IT-Bereich übertragen.

Das größte Risiko für die IT-Sicherheit liegt im Gegensatz zu vielen anderen Technologiebereichen allerdings im menschlichen Faktor. Es ist beängstigend, mit welchem Aufwand Hacker, Cracker, Skriptkiddies, usw. Schwachstellen und Verwundbarkeiten in IT-Produkten suchen, um danach Angriffe auf betroffene IT-Systeme zu initiieren. Hackerszenen haben mittlerweile mächtige Werkzeugkästen für die Konstruktion von Schadsoftware und automatisierten Angriffe konstruiert, die selbst von relativ unversierten Personen leicht zu bedienen sind. Große Hacker-Gemeinden beschäftigen sich tagtäglich damit, neue und effektive Angriffsmethoden zu entwickeln und anzuwenden.

2.1.2 Komplexität

Die Komplexität der Zusammenhänge in der IT ist äußerst hoch und kaum beherrschbar. Während man etwa bei mechanischen Systemen eher eine „White-„ oder „Grey-Box“- Betrachtung durchführen kann, indem die inneren Prozessabläufe des mechanischen Systems beobachtet werden können, entzieht sich die IT in ihren inneren Vorgängen der Beobachtbarkeit. Dort gibt für einen Beobachter ein typisches „Black-Box“-Verhalten, bei dem Ein- und Ausgangsgrößen des Systems beobachtet werden können, aber nicht die im System sich vollziehenden Prozesse. Umso anspruchsvoller muss dann die Erkennung von potenziellen Fehlern, Verwundbarkeiten und Schwachstellen sein.

2.1.3 Reaktionsfähigkeit

Manche Personengruppen nutzen erkannte Schwachstellen aus, um unberechtigten Zugang zu betroffenen Systemen zu erhalten, oder die betroffenen Systeme zu missbrauchen. Die entsprechenden Angriffe in Form von Würmern, Viren oder direkten Zugriffen werden immer anspruchsvoller, gezielter und schneller. Häufig werden mehrere Verwundbarkeiten bei einem Angriff intelligent und autonom angesprochen, um so auf das IT-System zuzugreifen. Der Angreifer ist adaptiv tätig, indem er die Individualität der eingesetzten Systeme gezielt berücksichtigt.

Dies hat Bedeutung für das Sicherheitsmanagement. Denn die Zeit zum Reagieren zwischen einer erkannten Verwundbarkeit und deren Ausnutzung verringert sich rapide. Konnte man in der Vergangenheit noch einen Zeitraum von Jahren und Monaten angeben, verbleiben heute bei schwerwiegenden Lücken nur noch wenige Tage. Die immer kürzere Reaktionszeit wird in der Zukunft das Sicherheitsmanagement vor bedeutende Aufgaben stellen. Zwischen dem Sicherheitsmanagement und den Hackern entsteht so ein Wettlauf, bei dem derzeit eindeutig die Hackern in Führung liegen, während das Sicherheitsmanagement notgedrungen nur reagieren kann.

Bei der Reaktion auf IT-Sicherheitsprobleme ist der Mensch in einer klar nachteiligen Situation. Während die IT dank der hohen Verarbeitungs- und Übertragungsgeschwindigkeit mit extrem kleinen Zeitkonstanten abläuft, hinkt der Mensch mit seiner sehr langsamen Reaktionsgeschwindigkeit hinterher. Will der Mensch damit Schritt halten, kann er sich selber nur auf automatisierte oder sogar autonome IT-Systeme verlassen. Hier liegt eine Paradoxie. Wie will man sich gegen fehlerbehaftete IT-Systeme mit wiederum anderen IT-Systemen schützen, die genauso fehlerbehaftet sind? Kann man ein System konstruieren, das ein hohes Vertrauen genießt?

Wie kann ein CERT in einem Unternehmen überhaupt rechtzeitig auf bekannte und ggf. unbekannt Schwachstellen reagieren? Dazu bedarf es einer soliden Datenlage über verwendete IT-Systeme und Anwendungen sowie bekannter Schwachstellen. Diese Datenlage im Unternehmen aktuell zu halten ist schwierig. Gerade in größeren Organisationen kommt es zu kontinuierlichen Veränderungen, die heute kaum in einem Konfigurations- und Ände-

rungsmanagementprozess erfasst werden. Hier ist noch erheblicher Verbesserungsbedarf zu erkennen.

2.1.4 Asymmetrische Bedrohung

Bei IT-Angriffen unterliegt man einer klassischen asymmetrischen Bedrohungssituation. Die Angriffe erfolgen global und ortsungebunden, während die Reaktion auf einen Sicherheitsvorfall stets nur lokal erfolgt. Wobei sich der Aufwand mit der Anzahl der Opfer multipliziert, die alle für sich den gleichen Aufwand treiben müssen, den Schaden zu begrenzen und zu beheben. Schlimmer noch ist es für den Einzelnen, wenn massiv verteilte „Denial of Service“ Angriffe auf einen Punkt auftreten. Es ist die Frage zu stellen, inwiefern eine manuelle („menschliche“) Reaktion am Schadensort in solchen Fällen noch erfolgsträchtig ist. Es deutet einiges darauf hin, dass eine ernsthafte und effektive Reaktion auf solche Vorfälle nur maschinengestützt, also automatisiert, erfolgen kann. Dabei ist noch eingehender zu prüfen, ob nur die Reaktion automatisiert ablaufen soll, oder nicht sogar die Entscheidung, ob eine Reaktion erfolgen muss, automatisiert gefällt werden muss.

2.1.5 Der zwischenmenschliche Faktor

Die menschliche Dimension darf bei der Betrachtung der heutigen Lage nicht unbeachtet bleiben. Leider muss festgestellt werden, dass Empfehlungen von Sicherheitsexperten kaum Beachtung finden. Dies kann daran liegen, dass nur bei richtigen Großschadensereignissen wie dem „I-love-you-Virus“ die Nutzer persönlich betroffen sind. Viele handeln nach dem Motto: „Es hat mich noch nie erwischt“, und nehmen Hinweise nicht ernst. Andererseits begegnet man auch selbsternannten Sicherheitsexperten, die für Sicherheitshinweise grundsätzlich nicht aufgeschlossen sind oder durch ihr Handeln neue Schwachstellen erst eröffnen.

Nicht zu vergessen dabei ist auch die Vertrauenskultur. Was glaubt man einer Informationsquelle, zu der es meistens nur elektronische, aber keine sozialen Bindungen gibt? Die fehlende Kultur des Vertrauens führt ihrerseits auch dazu, dass von Angriffen Betroffene ihre Informationen nicht gerne öffentlich oder in Expertenkreisen bekannt machen. Selbst statistische Informationen, gewonnen beispielsweise aus Kommunikationsprotokollen der Gatewaysysteme, werden aufgrund gesetzlicher Bestimmungen oder auf Unternehmensebene geltenden Richtlinien kaum mit anderen geteilt, obwohl daraus möglicherweise wichtige Informationen für alle Nutzer ableitbar wären.

2.1.6 Sicherheitsbewusstsein und Patchmanagement

Ganz oben bei einer Beschreibung der Ist-Situation der Sicherheit von IT-Systemen steht das fehlende Bewusstsein von Mitarbeitern und auch teilweise von Verantwortlichen bezüglich Sicherheitsfragen. Untersuchungen sowohl der nationalen und internationalen Fachpresse als auch von Sicherheitsbehörden, Agenturen und der Wissenschaft zeigen, dass selbst nach Jahrzehnten des Einsatzes moderner IT das Bewusstsein nicht mit der technologischen Entwicklung Schritt gehalten hat. Zwar gibt es gute Ansätze, die beispielsweise auch durch öffentliche Förderung der Bundesministerien unterstützt werden, aber der rasante Fortschritt der Technologie und die damit verbundene Schaffung neuer technischer Möglichkeiten zur Vernetzung überfordern dennoch die meisten Menschen bei der Frage, welche Sicherheitsrisiken mit dem Einsatz der Techniken verbunden sind.

Standardisierte Methoden, wie man das Risiko des Einsatzrisiko von IT-Systemen darstellen und beschränken kann, sind zwar bekannt, aber Bedrohungs- und Risikoanalysen verbunden mit der Erarbeitung von Sicherheitskonzepten werden im IT-Bereich heute immer noch zu wenig eingesetzt. Damit können konkrete Risiken nicht erfasst und als Folge auch nicht mittels geeigneter Sicherheitsmaßnahmen adressiert werden. Hier ist ein starkes Gefälle zu

beobachten: Leisten sich größere Organisationen diesen Aufwand, ist es im mittelständischen Umfeld eher noch die Ausnahme. Da zahlenmäßig die IT-Systeme des Mittelstands die der Großindustrie jedoch übersteigen, ist die Lage zumindest bedenklich.

Ein ähnliches Bild zeigt das heutige Patchmanagement. In kleineren Unternehmen mit wenigen IT-Systemen wäre es ausgehend von der zu beachtenden Anzahl Systeme noch am einfachsten, zeitnah Patches einzupflegen. Jedoch existieren in den wenigsten Unternehmen, unabhängig von ihrer Größe, verbindliche Richtlinien und Regeln zum Patchmanagement. Damit bleiben auch wichtige Patches so lange unbeachtet, bis es zu konkreten Schadensereignissen kommt.

2.1.7 Umgang mit Incidents und Schwachstellen

Der Umgang mit Zwischenfällen und Schwachstellen läuft heute noch individuell ab, wobei sich die Betrachtung auf die im eigenen Verantwortungsbereich vorhandenen IT-Systeme beschränkt. Denn nur ansatzweise sorgt die CERT-Gemeinschaft dafür, dass bei einer Schwachstelle oder auch Risikobetrachtung zwischen allgemeinen und individuellen, auf bestimmte IT-Systeme bezogene Bedrohungen unterschieden wird.

Damit wird viel Mehrfachaufwand, der durch eine abgestufte Bearbeitung vermieden werden könnte, durch beliebig viele ganzheitliche Betrachtungen betrieben.

Nicht unerwähnt bleiben sollte die auch für CERTs in einem Unternehmen manchmal schwierige Lage, relevante Sicherheitsinformationen aus dem laufenden IT-Betrieb zu erhalten. Sind Protokolldateien von Firewalls, Gateways, internen Servern und Log-Dateien von IDS-Systemen für das interne Sicherheitsmanagement verfügbar, heißt dies noch lange nicht, dass auch das Unternehmens-CERT automatisch darauf Zugriff hat. Diese Informationen werden meistens vertraulich behandelt und manchmal übereilig und unnötig als geschützte personenbezogene oder personenbeziehbare Daten gewertet und der weiteren Analyse des CERTs entzogen.

Ein besonderes Phänomen in Europa ist sicherlich auch die Zurückhaltung und das ansatzweise vorhandene Misstrauen gegenüber amerikanischen Informationsquellen. Obwohl die moderne IT durchgehend von US-Unternehmen dominiert wird, genießen diejenigen amerikanischen Institutionen und Organisationen, die sich mit Schwachstellen moderner IT-Systeme und der Abwehr von Angriffen beschäftigen, eine in Europa verbesserungswürdige Reputation. Leider tragen US-Organisationen in den Augen europäischer Nutzer immer wieder zu dem Vorurteil bei, nicht alle Informationen offen und transparent zur Verfügung zu stellen. Auch fühlen sich manche Europäer von den Amerikanern nicht als gleichwertiger Partner akzeptiert.

Aber auch die Zusammenarbeit der in Europa und speziell in Deutschland tätigen CERTs ist immer noch verbesserungsfähig. Zu konstatieren ist, dass heute nur wenig sicherheitsrelevante Informationen zwischen den CERTs ausgetauscht werden. Wohlwissend, dass die von den Unternehmen gegründeten CERTs primär für die Sicherung des eigenen Unternehmens eingerichtet wurden, würde eine verstärkte Kooperation und Zusammenarbeit die Reaktion auf Incidents und Schwachstellen verbessern. Dabei müssen Tiefe und Intensität der Zusammenarbeit natürlich noch Gegenstand weitergehender Prüfungen sein.

2.1.8 Wirtschaftspolitische und -strategische Fragen

Der überwältigende Teil der heute genutzten IT-Technik stammt von wenigen sehr großen US-Anbietern. Darüber hinaus werden die Softwareprodukte der Anbieter vom Leistungsumfang immer mächtiger und beinhalten Zusatzprogramme, die früher noch separat eingekauft wurden. Leider lassen sich heute vielfach bestimmte Programmteile gar nicht mehr deaktivie-

ren, ohne die Funktionsfähigkeit des ganzen Programms aufzuheben. Die Abhängigkeit der Nutzer hat damit, nüchtern betrachtet, eine bedenkliche Dimension erreicht. Würden Monopolstellungen einiger Hersteller im IT-Umfeld ausgenutzt, wäre mit einer merklichen Einschränkung bei der Nutzung moderner IT-Systeme zu rechnen. Die Möglichkeit, zukünftig damit andere Wirtschaftsräume im IT-Umfeld zu behindern, lässt sich per se nicht von der Hand weisen – wenngleich die Umsetzung eines solchen Denial-of-Service-Angriffs sicherlich anspruchsvoll wäre.

Die IT-Sicherheitslage in Unternehmen ließe sich auch verbessern, wäre der Umgang mit Protokolldateien von IT- und Netzwerksystemen nicht durch gesetzliche Bestimmungen so stark eingeschränkt. Gerade Datenschutzbestimmungen rücken viele Verkehrsdaten von Netzwerksystemen in die Nähe von geschützten personenbeziehenden Daten und engen die Auswertung somit stark ein. So erlaubt zwar die neue Datenschutzrichtlinie der EU die Auswertung von Protokolldateien aus Netzwerksystemen durch Sicherheitsbehörden, der Zugriff auf diese Daten durch Unternehmenssicherheitsabteilungen ist aber verwehrt, obwohl dadurch relevante Informationen zur Sicherheitslage gewinnbar und ggf. Missbrauch und Angriffe früher erkennbar wären.

2.2 Konsequenzen

Die bisherigen Ausführungen haben deutlich gemacht, mit welcher Entwicklung bezüglich der Bedrohungssituation mittelfristig zu rechnen ist. Zu welchen Konsequenzen wird es aber führen, wenn dieser Entwicklung nicht durch den Aufbau eines IT-Frühwarnsystems rechtzeitig begegnet wird?

Aus **technischer Sicht** sehen wir die folgenden problematischen Entwicklungen:

- Die Anzahl sicherheitskritischer Angriffe wird weiter steigen.
- Die Reaktionszeiten für Betreiber von IT-Infrastrukturen werden immer kürzer, so dass früher oder später keine effektive Reaktion mehr möglich sein wird. Die Folge: Auch die Anzahl erfolgreicher Angriffe wird steigen.
- Der Kostendruck wird zu einer verstärkten Ausprägung von technische Monokulturen führen, die (wie in der Natur) grundsätzlich gegenüber Angriffen weniger resistent sind als Mischkulturen; d.h. die „natürliche“ Widerstandsfähigkeit der IT-Infrastrukturen wird abnehmen.
- Die Unternehmen werden ihren Perimeter-Schutz verstärken, da in der Regel dort angesiedelte Schutzmaßnahmen das günstigste Kosten/Nutzen-Verhältnis aufweisen. Die Konsequenz: Möglichkeiten zur großräumigen Kooperation, zum verteilten Arbeiten usw., die die Wettbewerbsfähigkeit der Unternehmen stärken könnten, bleiben aus Sicherheitsgründen ungenutzt.
- Jedes Unternehmen hat nur eine Teilsicht auf Sicherheitsprobleme der globalen IT-Infrastruktur und verfolgt daher (ausgehend von dem eigenen, begrenzten Know-How) primär lokale Lösungen. Dieser Ansatz ist grundsätzlich unzureichend, da die Probleme in der Regel globaler Natur sind.

Mit diesen technischen Aspekten eng verknüpft sind aus unserer Sicht die folgenden **organisatorischen** Entwicklungen:

- Der Bedarf für Informationsaustausch über bekannte oder vermutete Sicherheitslücken wird überproportional wachsen, da sich höchsten bilaterale Zweckgemeinschaften einzelner Unternehmen und Organisationen bilden und somit jede Information zu einem IT-Sicherheitsproblem viele Informationskanäle durchlaufen muss, bis die gesamte Community informiert ist.
- Die Arbeitsbelastung des CERT-Personals für die Abwehr realer Angriffe wird ebenfalls überproportional wachsen und in absehbarer Zeit die Überlast-Grenze erreichen. Damit werden die CERTs nur noch in der Lage sein, auf aktuelle Probleme zu reagieren; für eigene Analysen und eigene Recherchen, um sich abzeichnenden Problemen zuvorzu-

kommen, bleibt praktisch keine Zeit mehr. Damit wird eine wirkungsvolle koordinierte Abwehr von Angriffen nicht mehr möglich sein.

Aus **wirtschaftspolitischer Sicht** ist mit folgenden nachteiligen Effekten zu rechnen:

- Die Wirtschaft wird unmittelbare bzw. mittelbare wirtschaftliche Einbußen erleiden:
 - Der lokale Ansatz bei der Bekämpfung von IT-Sicherheitsproblemen führt in hohem Masse zu Parallelarbeit bzw. zu teuren Einzellösungen, statt die Synergieeffekte eines gemeinschaftlichen Ansatzes zu nutzen.
 - Sicherheitsbedenken zwingen zum Verzicht auf innovative Lösungen und damit zum Verzicht auf die damit verbundenen wirtschaftlichen Vorteile.
 - Die Kostenbelastung durch Versicherungsprämien für IT-Infrastrukturen steigt.
 - Die Unternehmen werden zunehmend erpressbar, in dem die Ausnutzung bestehender oder vorgeblicher IT-Sicherheitsmängel angedroht wird.

Aus **gesamtgesellschaftlicher Sicht** besonders bedenklich ist die zu befürchtende Abkoppelung ganzer Wirtschaftszweige und gesellschaftlicher Gruppen – die sich den Aufwand für eine sichere Gestaltung nicht leisten können – vom Zugang zu innovativen IT-Infrastrukturen zu sehen,.

Schließlich ist mit verstärkten regulierenden Eingriffen der Exekutivorgane des **Staates** zu rechnen, der so aus seiner Sicht (und auf Kosten der Betreiber) die Funktionsfähigkeit der sog. „kritischen Infrastrukturen“ zu gewährleisten versucht.

3 Referenzbereiche

In einer Reihe von Anwendungsgebieten sind Warn- und Frühwarnsysteme seit Jahren im Einsatz bzw. befinden sich in der Konzeptionsphase. Wesentliche Triebfeder für solche Früherkennungs- bzw. -warnsysteme ist, wirtschaftlichen Schaden oder Gefahren für Leib- und Leben rechtzeitig vor zu beugen oder im Eintrittsfall in ihrer Auswirkung zu begrenzen.

Als Beispiele seien genannt

- Vorhersage von Vulkanausbrüchen und Erdbeben
- Warnsysteme vor Hochwasser, Flut und Überschwemmungen
- Unwetter- und Sturmwarnung
- Früherkennung von Epidemien
- Früherkennung von strategischen Raketenangriffen oder Angriffsvorbereitungen
- Indikatorsystem für Insolvenzgefahr
- Warnung vor radioaktiver Verseuchung

All diese Frühwarnsysteme haben

- klare Aufgabenstellungen
- ihre spezifische Sensorik
- Indikatoren und Messwerte, bei deren Schwellwertüberschreitungen Meldungen oder Reaktionen ausgelöst werden
- Methoden und Algorithmen zur Lagefeststellung bzw. –beurteilung
- vereinbarte, teilweise standardisierte Meldeformate
- vorab festgelegte Zielgruppen und Akteure
- definierte und erprobte Strukturen und Prozesse

Um die Möglichkeiten des Methodentransfers auf IT-Frühwarnsysteme zu bewerten, seien im Folgenden einige Beispiele kurz beschrieben.

3.1 Warn-Management des Deutschen Wetterdienst

3.1.1 Gefährdung

Unsere Kultur ist vom Wetter abhängig. Durch unvorhersehbare Wetteränderungen können Ereignisse eintreten, die für ganze Regionen, Landstriche oder auch Individuen lebens- und umweltbedrohend sind. Von daher ist es für unser Überleben notwendig, möglichst frühzeitig negative Wetterveränderungen für die Bevölkerung zu erkennen, darüber zu informieren und Schutzmaßnahmen einzuleiten.

3.1.2 Zielgruppe

- Katastrophenschutzbehörden der Länder, Feuerwehr, Polizei
- THW, Verkehrswarndienst usw.
- Medien / Öffentlichkeit (Rundfunk/Fernsehen, Internet, SMS), Bürger

3.1.3 Akteure

Akteur ist der Deutsche-Wetterdienst,

3.1.4 Sensorik

Der DWD hat einen Radarverbund in Deutschland aufgebaut. Dieser besteht aus 16 miteinander vernetzten Standorten, die die Wetterdaten innerhalb Deutschlands und teilweise über die Grenzen von Deutschland hinaus erfassen.

3.1.5 Prozesse

Die Standorte melden regelmäßig ihre aktuellen Wetterdaten. Diese werden zusammengefasst und ausgewertet.

3.1.6 Meldewesen, -wege und -inhalte

Der Wetter-Warndienst des DWD ist in drei Bereiche eingeteilt:

- Warnmanagement (Radardaten)
- Informationsplattform (FeWIS (Feuerwehr-Wetter-Informationssystem))
- Lokale Prognosen (KONRAD (KONvektionsentwicklung in RADarprodukten))

Es gibt drei verschiedene Stufen der Warnmeldung je nach Zielgruppe sowie eine ständige Telefonhotline für jeden Bürger.

- Frühwarnung (48 – 120 h)
Signale in den numerischen Prognosen im Mittelfristbereich mit Schwerpunkt auf probabilistischen Aussagen.
- Vorwarnung (48 - 6 h)
Erkenntnisse aus numerischen Analysen und Prognosen, statistische Anschlußrechnungen und Beobachtungen
- Kurzzeitfrist (2 - 0 h)
Erkenntnisse aus Fernerkundungssystemen (Blitz-, Satelliten- und Radardaten)

Des Weiteren gibt es noch regionale Warnmeldungen (0 – 48 h). Sie sind übers Internet abrufbar. Anhand der jeweiligen Farbe in der Region ist ein Unwetter, eine Vorwarnung, eine definierte Wetterwarnungen oder keine Warnungen erkennbar.

3.1.7 Anwendbarkeit auf IT-Frühwarnsysteme

- Globale Bereitstellung lokaler Messdaten
- Akzeptanz, dass die Warnmeldung falsch sein könnte
- Art der Informationsverteilung

3.2 Vorhersage von Epidemien

3.2.1 Gefährdung

Dieses System ist ein bundesweites, umfassendes Überwachungssystem, welches das Auftreten sowohl meldepflichtiger Krankheiten als auch meldepflichtiger Erreger ständig im gesamten Bundesgebiet überwacht. Die niedergelassenen Ärzte und Krankenhäuser, die Gebietskörperschaften (Städte, Landkreise), Länder und der Bund teilen sich diese Aufgabe.

- Ärzte/Krankenhäuser: Identifizieren Krankheiten und beauftragen Labore zur Identifikation von Erregern
- Gesundheitsämter: Bewerten eingehende Meldungen und setzen ggf. Maßnahmen um
- Labore: Testen u. a. auf diejenigen Erreger, welche der Arzt angibt
- Referenzlabore: Testen u. a. nicht oft vorkommende eventuell sehr gefährliche Erreger
- Robert-Koch-Institut: Ermittelt ein möglichst stimmiges Gesamtbild aus den dezentralen Meldungen, indem es Ausbrüche von Krankheiten bzw. das Auftreten von Erregern nach Raum und Zeit in so genannte „Herde“ einteilt

Das Meldesystem ist durch Gesetz und Verordnungen geregelt.

3.2.2 Zielgruppe

Zielgruppe von Warnungen sind die Exekutivorgane auf Bundes- bzw. Landesebene. Dort wird dezentral über einzuleitende Maßnahmen entschieden.

3.2.3 Akteure

Die zuständigen Akteure sind Kommunal- (Gesundheitsämter), Landes- und Bundesbehörden (Ministerien), niedergelassene Ärzte und Krankenhäuser sowie Labore

3.2.4 Sensorik

- Liste meldepflichtiger Krankheiten jeweils mit ca. 650 Einzelmerkmalen und ca. 7000 Ausprägungen
- Liste meldepflichtiger Erreger
- Diagnosen der Ärzte/Krankenhäuser
- Laborbefunde

3.2.5 Prozesse

- Das Meldesystem der Ärzte ist i. a. wenig verlässlich, denn es kann nur „Erkanntes“ gemeldet werden (ärztliche Falldiagnosen, nicht getestete Erreger)
- Klassifizierung von Krankheitsfällen nach: „wichtig“, „eher nicht vorkommend“, „Einzelfälle“, „kurz-, langfristig“ und „chronisch“
- Datenspeicherung: Verteilte Datenbank im Robert-Koch-Institut und den Gesundheitsämtern mit Replikation
- Die Herausforderung besteht in der Erkennung von Ausbrüchen und deren zeitlicher und räumlicher Korrelation (Fallzahlenvergleiche, Gruppenbildung). Die Erreger sind immer existent (aber normalerweise vom Immunsystem unterdrückt), es müssen Krankheitsausbrüche und –Herde erkannt werden.
- Das Gesamtsystem ist dezentral-föderal aufgebaut: die Erkennung erfolgt i. a. zentral, die Umsetzung von Maßnahmen ausschließlich dezentral
- Durch das mehrstufige Meldeverfahren entsteht ein erheblicher Zeitverzug, der letztlich seine Ursache im Gesetz hat

3.2.6 Meldewesen, -wege und -inhalte

- Inhalte und Form der Meldungen sind definiert; die Meldungen sind bezüglich des Krankheits- bzw. Erreger-„Trägers“ anonym
- Üblicher Meldeweg: Arzt ---> Labor ---> Arzt ---> Gesundheitsamt ---> RKI ---> (Behörden)

3.2.7 Anwendbarkeit auf IT-Frühwarnsysteme

- Primäre Zielgruppe sind Experten und Entscheidungsträger
- Geregeltes Verfahren für Diagnose und Prognose
- Methodik zur Erkennung von „Herden“ und „Ausbrüchen“

3.3 Mess- und Informationssystem zur Umweltradioaktivität

3.3.1 Gefährdung

IMIS steht für "Integriertes Mess- und Informationssystem zur Überwachung der Umweltradioaktivität". IMIS ist ein bundesweites, umfassendes Messsystem, das die Radioaktivität in allen wichtigen Umweltmedien ständig im gesamten Bundesgebiet überwacht. Bund und Länder teilen sich diese Aufgabe:

- Bundesbehörden überwachen den großräumigen Transport radioaktiver Stoffe und deren Verteilung in Luft und im Wasser
- Länderbehörden überwachen die Radioaktivität dort, wo sich radioaktive Stoffe ablagern und ggf. in die Nahrungskette des Menschen gelangen können

IMIS umfasst über 2000 ortsfeste Messstationen zur Überwachung der Gamma-Ortsdosisleistung sowie der Aktivitätskonzentration in Luft, Niederschlag und Gewässern. Darüber hinaus wird die Radioaktivität in Lebensmitteln, Futtermitteln, Trinkwasser aber auch in Reststoffen und Abwässern ständig ermittelt. Alle Messeinrichtungen bei Bund und Ländern sind durch ein rechnergestütztes Datenüberwachungssystem mit der Zentralstelle des Bundes beim Bundesamt für Strahlenschutz verbunden.

Gesetzliche Grundlage ist das Strahlenschutzvorsorgegesetz.

In IMIS werden zwei Betriebsarten unterschieden: **Normalbetrieb** und **Intensivbetrieb**. IMIS befindet sich grundsätzlich im Normalbetrieb. Aus den Messnetzen des Bundes erfolgt bei Überschreitung voreingestellter Schwellenwerte eine **Frühwarnung**. Im Falle von „Ereignissen mit möglichen nicht unerheblichen radiologischen Auswirkungen“ wird vom Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit der Intensivbetrieb angeordnet (**Alarmierung**). Der Intensivbetrieb unterscheidet sich vom Normalbetrieb u.a. in einer höheren zeitlichen Frequenz der Überwachungsaktivitäten und je nach Gefährdungslage einer Konzentration auf bestimmte Beobachtungsparameter oder Regionen.

Ziel von IMIS ist es, in einem radioaktiven Störfall die Strahlenexposition des Menschen und die Kontamination der Umwelt durch angemessene Maßnahmen, wie z.B. Verbleiben im Haus, Einnahme von Jodtabletten, Evakuierung, so gering wie möglich zu halten.

3.3.2 Zielgruppe

Zielgruppen sind die Exekutivorgane auf Bundes- und Landesebene sowie die Bevölkerung.

3.3.3 Akteure

Akteure sind die zuständigen Landes- und Bundesbehörden.

3.3.4 Sensorik

- Kontinuierliche Messungen an festgelegten Messstellen bzw. in Messnetzen
- Probenahmen auf der Basis von Probenahmeplänen
- Messungen aus der Luft für schnelle flächendeckende und punktuelle Kontaminationen.
- Auf der Basis der geprüften Messwerte werden Diagnosen und Prognosen in Form von Lagedarstellungen als Karten oder Tabellen erstellt.

3.3.5 Prozesse

- Akteure und Datenübermittlung
Die Ergebnisse der Messungen der Bundesmessnetze werden an die Zentralstelle des Bundes (ZdB) mit Hilfe des IT-Systems IMIS übermittelt. Die Ergebnisse der Messungen der Landesmessstellen werden mit Hilfe des IT-Systems IMIS über die Landesdatenzentralen an die ZdB übermittelt.
- Plausibilitätsprüfung
Die Messstellen der Länder und die Messstationen des Bundes überprüfen die Plausibilität der Messwerte bezüglich der Funktion der Messgeräte, auf äußere lokale Einflüsse und auf Vollständigkeit. Die Landesdatenzentralen können die Plausibilität der Messwerte auf zeitliche und räumliche Konsistenz prüfen. Die Leitstellen des Bundes prüfen zu-

sätzlich bezüglich die synoptische Plausibilität (mit Daten aus anderen Umweltbereichen, die in einem radioökologischen Zusammenhang stehen).

- Diagnosen, Prognosen, Lagedarstellung
Auf der Basis der geprüften Messwerte werden Diagnosen und Prognosen in Form von Lagedarstellungen als Karten oder Tabellen erstellt.
- Frühwarnung
Aus den Messnetzen des Bundes erfolgt bei Überschreitung voreingestellter Schwellenwerte eine Frühwarnung.
- Alarmierung
Im Falle einer Frühwarnung entscheidet das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) über eine Alarmierung (Intensivbetrieb).
- Empfehlung von Verhaltensmaßnahmen an die Bevölkerung
In einem Ereignisfall erfolgen die Information der Öffentlichkeit und die Empfehlung geeigneter Verhaltensmaßnahmen durch das BMU.

3.3.6 Meldewesen, -wege und -inhalte

(entspricht im wesentlichen Punkt 3.3.5)

3.3.7 Anwendbarkeit auf IT-Frühwarnsystem

Folgende Elemente sind anwendbar (bei gegebener Festlegung der „Beobachtungsobjekte“ eines IT-Frühwarnsystems):

- Der zweistufige Betrieb: Routine- und Intensivbetrieb
- Die Beobachtung in drei Ebenen: Kontinuierliche (automatische) Messungen, regelmäßige Messungen nach einem Beobachtungsplan, anlassbezogene Messungen im Falle eines Ereignisses
- Frühwarnung bei Überschreitung von Schwellwerten in automatischen Messnetzen
- Alarmierung auf Grund einer Lageentscheidung
- Geregelte Verfahren für Diagnose und Prognose
- Plausibilitätsprüfungen in mehreren Schritten unter Berücksichtigung unterschiedlicher Gesichtspunkte
- Rufbereitschaft

4 Das nationale IT-Frühwarnsystem

In diesem Kapitel wird ein IT-FWS für Deutschland aus Sicht der Wirtschaft definiert sowie seine Aufgaben und Ziele näher erläutert. Anschließend werden die sich daraus ergebenden Implikationen dargestellt.

4.1 Einordnung des Begriffs Frühwarnsystems

Mittlerweile sind durch aktuelle Ereignisse Frühwarnsysteme aus anderen Kontexten in den Mittelpunkt der öffentlichen und fachlichen Diskussion gerückt, so zum Beispiel Frühwarnungen vor Tsunamis (Flutwellen) oder Erdbeben.

Eine Übertragung auf den Bereich Informationstechnik ist erheblich komplexer, da nicht vor Erscheinungen und empirisch bekannten Verläufen von Naturkräften gewarnt wird, sondern vor möglichen Schädigungen der IT- und TK-Infrastruktur aufgrund bösartiger menschlicher Handlungen. Diese Handlungen können eine mannigfaltige Ausprägung hinsichtlich der Ziele und Methoden beinhalten und sind dadurch schwer bis kaum vorhersagbar.

Das IT-Frühwarnsystem hat daher das langfristige Ziel, bei minimalen Anzeichen für bevorstehende Angriffe bereits „Vorhersagungen“ über Ziele und Ausbreitungsvektoren festzustellen. Als kurzfristiges Ziel soll es möglich sein, bei bereits erkennbaren Angriffen noch nicht Betroffene zu warnen, so dass noch Maßnahmen zur Verhinderung oder Abmilderung von Schäden ergriffen werden können.

Zur Verdeutlichung des Ablaufs von Frühwarnungen und deren Einbettung in einen Gesamtkontext dient die folgende Abbildung 1. Diese zeigt den zeitlichen Verlauf des Betriebs eines beliebigen IT-Systems, der durch einen Zwischenfall oder Angriff beeinflusst wird. Im Normalbetrieb können auswertbare Anzeichen auftreten, die auf einen bevorstehenden gezielten Angriff oder Zwischenfall hindeuten können. Dabei sei explizit darauf hingewiesen, dass noch nichts über die Beobachtbarkeit und Interpretationsfähigkeit solcher Anzeichen ausgesagt werden kann! Unter der Prämisse, dass die Anzeichen korrekt interpretiert würden, könnte zu einem von mehreren Parametern abhängigen Zeitpunkt¹ vor dem bevorstehenden Angriff eine Früh- oder Vorwarnung publiziert werden, um noch **wirksame Gegenmaßnahmen** einleiten zu können. Verstreicht dieser Zeitpunkt können immer noch bis zum konkreten Schadenseintritt Warnungen publiziert werden. Die Wirksamkeit der empfohlenen Gegenmaßnahmen würde aber grundsätzlich immer weiter abnehmen und schließlich ganz entfallen, wenn die Warnung schließlich mit Erkennung des Schadensereignis zusammenfällt. In diesem Fall könnten aber dennoch diejenigen, die noch nicht betroffen sind, gewarnt werden².

Angenommen, der Angriff käme ohne Vorwarnung, so würde zu einem Zeitpunkt nach dem Angriff dieser bemerkt werden, da erkennbare Schäden entstünden. Zum Zweck der Schadensbegrenzung würde das Sicherheitsmanagement erste Gegenmaßnahmen ergreifen. Nach dem Verstreichen weiterer Zeit würden weitere erprobte und wirksame Gegenmaßnahmen ergriffen und Schäden beseitigt bzw. die Wiederherstellung des Systems bewerkstelligt. Anschließend würde das System wieder im Normalzustand betrieben.

¹ Der Zeitpunkt vor dem tatsächlichen Schadensereignis ist nur modellhaft oder virtuell zu sehen. Ob dieser in der Realität überhaupt definierbar ist, bleibt dahingestellt. Eine quantitative mathematische Beziehung lässt sich sicherlich nicht angeben. Qualitativ hängen die Parameter zur Angabe eines solchen Zeitpunkts von dem konkreten bevorstehenden Schadensereignis und den individuell betroffenen IT-Systemen ab.

² So zum Beispiel, wenn vor dem Auftreten einer neuen Schadsoftware (Virus, Wurm, Trojaner) gewarnt wird, bei der eine große Zahl von potentiell Betroffenen existiert.

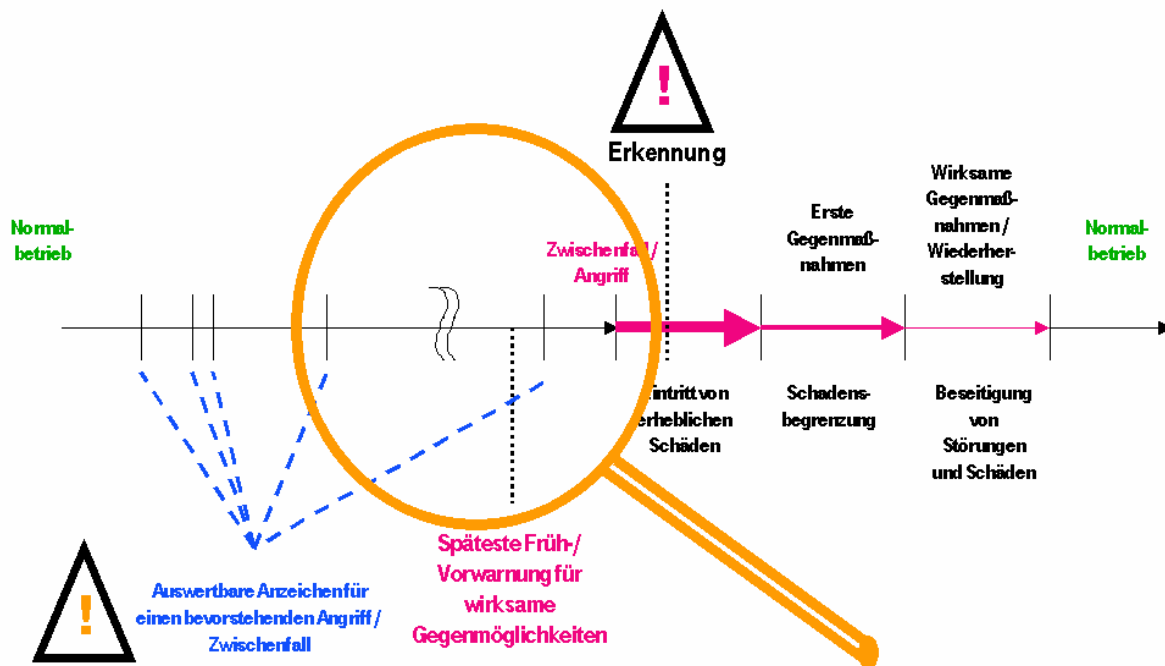


Abbildung 1: Zeitlicher Verlauf eines Angriffes ohne ein IT-FWS

In der Abbildung 2 wird angenommen, die Anzeichen für einen bevorstehenden Angriff würden korrekt interpretiert. In einer wohl definierten Zeit würden die vermuteten Erkenntnisse verifiziert. Sofern eine genügend große Wahrscheinlichkeit für einen konkreten Angriff/Zwischenfall festgestellt wird, würde das Frühwarnsystem vor dem Angriff eine Frühwarnung an potentiell Betroffene aussprechen. Sogleich beginnt auch der Prozess zur Erarbeitung geeigneter Gegenmaßnahmen. Ziel sollte stets sein, möglichst frühzeitig erste präventive oder mildernde Gegenmaßnahmen zu kommunizieren. Zu einem späteren Zeitpunkt können dann wirksame Gegenmaßnahmen veröffentlicht werden, die unverzüglich von potentiell Betroffenen umgesetzt werden sollten. Ist dieses geschehen, verbleibt das IT-System im Normalbetrieb und kann vom Angriff nicht mehr betroffen werden.

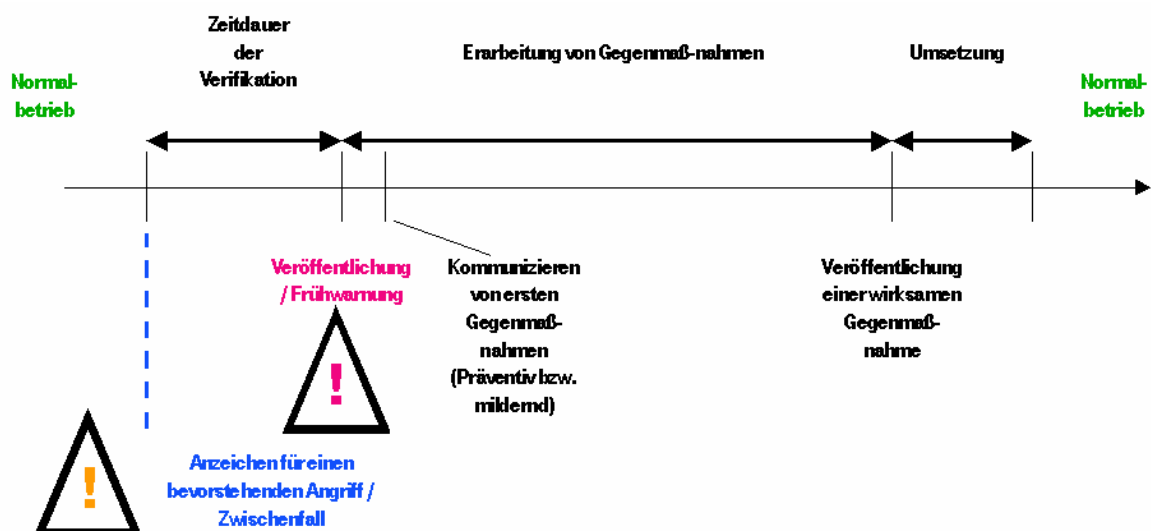


Abbildung 2: Zeitlicher Verlauf eines Angriffes mit einem IT-FWS

4.2 Ziele und Aufgaben des IT-Frühwarnsystems

Das vom BITKOM vorgeschlagene IT-Frühwarnsystem soll mehrere Ziele und Aufgaben verfolgen:

- Analyse und Ermittlung eines stimmigen übergeordneten Lagebildes über Bedrohungen, Ereignisse, Tätergruppen und deren Ziele, die auf elektronischem Wege die IuK-Infrastruktur von Unternehmen und Behörden massiv beeinträchtigen.
- Vor einem Angriff potentiell Betroffene durch frühe Warnungen zu sensibilisieren, so dass genügend Reaktionszeit zur Verfügung steht, um den Eintritt eines konkreten Ereignisses zu verhindern oder die Folgen zu mindern.
- Wenn bereits ein konkretes Schadensereignis eingetreten ist, noch nicht Betroffene rechtzeitig zu warnen, sofern sie als potentielle Opfer in Betracht kommen.
- Tendenzielle Aussagen über die Veränderungen in der Bedrohungs- und Risikosituation für die Nutzer von IuK-Infrastruktur abzuleiten sowie Strategien zur Verhinderung oder Abwehr neuer Bedrohungen zu entwickeln.

Wenn die aufgeführten Ziele erreicht werden, wird es möglich sein, zielgruppenspezifisch genauer zu warnen, als es heute auf Basis der CERT Zusammenarbeit erfolgt. Außerdem werden die heute vielfach doppelt oder mehrfach ausgeführten Arbeiten im CERT Umfeld gebündelt und zur Verfügung stehende Ressourcen an Fachexpertise erheblich besser und gezielter eingesetzt.

4.3 Grundsätzliche Implikationen

Damit die skizzierten Ziele erreichbar sind, müssen in einem Frühwarnsystem deutlich mehr Daten verarbeitet und analysiert werden, als es heute üblich ist. Bislang gehen hauptsächlich klassische Daten aus dem unmittelbaren IT-Umfeld in die Analyse und Bewertung ein (Monitoring des Netzwerkverkehrs, das Auftreten neuer Viren und Würmer usw.). Das IT-Frühwarnsystem muss jedoch auf einer stark erweiterten interdisziplinären Daten- und Informationsbasis arbeiten, bei der Erkenntnisse aus gesellschaftlich-sozialen Kontexten mit einfließen, zum Beispiel aus dem Bereich der Sicherheits- und Nachrichtendienste. Ebenso sind die Ziele nur dann erreichbar, wenn das gesamte IT-Frühwarnsystem weitestgehend automatisierte Prozesse nutzt, um zeitintensive Medienbrüche beim Übergang von IT-Systemen auf menschliche Instanzen und umgekehrt zu vermeiden.

Diese Aufgaben umfassen in vielen Aspekten wesentliche Elemente der Daseinsvorsorge. Hierbei wird der Begriff der Daseinsvorsorge ausgedehnt, von den rein physischen und physikalischen Bedrohungen der Infrastrukturen und der Bürger der Bundesrepublik Deutschland auf nunmehr logische Bedrohungen, die durch die Nutzung elektronischer Netze und Datenverarbeitung im globalen Kontext entstehen. Diese Ausdehnung einer staatlichen Schutzfunktion ist deshalb unumgänglich, da sich zukünftige Bedrohungen der Bundesrepublik Deutschland wahrscheinlich wesentlich weniger auf militärische Kontexte im Sinne einer physischen Auseinandersetzung beziehen werden. Vielmehr dürfte es zu einer Verlagerung auf elektronische Mittel kommen. Die Erkennung und Abwehr solcher (konzertierter) Angriffe („Cyber-War“) kann aber nicht auf die Nutzer der IuK-Infrastruktur abgewälzt werden, sondern verbleibt als staatliche Aufgabe.

Das IT-Frühwarnsystem ist damit ein präventiv orientiertes Element im Rahmen eines Gesamtsystems, um zukünftige Angriffe rechtzeitig zu erkennen. Ein weiteres, mehr reaktiv orientiertes Element³ im Gesamtsystem koordiniert die Reaktion auf Vorfälle und Angriffe.

Um die Funktionsfähigkeit sicherzustellen, ist eine Einbettung in eine geeignete Organisations- und Kommunikationsstruktur unverzichtbar. Wobei das Zusammenwirken von Staat und Wirtschaft unabdingbar ist.

³ Dieses Element liegt aber außerhalb des hier vorliegenden Positionspapieres.

5 Elemente eines IT-FWS

Im folgendem Kapitel werden die einzelnen Elemente eines IT-FWS, ähnlich den Erläuterungen zu schon vorhandenen FWS in Kapitel 3, dargestellt.

5.1 Zielgruppen

Das IT-Frühwarnsystem ist ein präventiv orientiertes Element im Rahmen eines Gesamtsystems. Es soll zukünftige Angriffe auf die nationale IuK-Infrastruktur rechtzeitig erkennen und die Betroffenen warnen. Es liegt in der Natur der Sache, dass ein durch ein solches System gewonnenes Lagebild nicht exakte Vorhersagen liefern kann. Eine Verteilung von ggf. unscharfen Informationen an eine breite Nutzergruppe oder gar der Öffentlichkeit ist somit ausgeschlossen. Es werden daher zunächst zwei primäre Zielgruppen identifiziert:

- Operative Stellen der Exekutivorgane auf nationaler Ebene und Betreiber kritischer/wesentlicher Infrastrukturen:
Diese Stellen sind in die Lage zu versetzen, geeignete vorbeugende Maßnahmen zum Schutz der IuK-Infrastruktur zu ergreifen, sobald sich akute Gefahren abzeichnen. Dieser Zielgruppe obliegt ebenfalls die Entscheidungsgewalt in einem Notfall durch Wahrnehmung des Krisenmanagements. Das Krisenmanagement ist ein reaktiv orientiertes Element im Gesamtsystem und koordiniert die Reaktion auf Vorfälle und Angriffe. Dieses Element liegt aber außerhalb des hier vorliegenden Positionspapieres.
- CERTs und IT-Sicherheitsorganisationen von Behörden und Wirtschaft:
Deren Hauptaufgabe liegt in der Betreuung der jeweils eigenen Zielgruppe. Sie übernehmen sowohl präventive wie auch reaktive Aufgaben. Die Informationen aus einem IT-Frühwarnsystem werden dabei helfen, die Arbeit dieser Teams nachhaltig zu verbessern sowie die Reaktionsfähigkeit zu beschleunigen. Sie liefern dadurch einen wichtigen Beitrag zur Schadensminimierung innerhalb ihrer Zielgruppe, da Warnungen und Alarmierungen nicht direkt durch ein IT-Frühwarnsystem der jeweiligen Zielgruppe übermittelt werden.

Darüber hinaus steht allen beteiligten Akteuren, die sich an einem nationalen IT-Frühwarnsystem z. B. durch die Bereitstellung von Informationen oder Sammlung von Daten über Sensoren beteiligen, ein Zugriff auf Informationen in Form von Statistiken und Berichten zu. Ein IT-Frühwarnsystem kann nicht die Aufgaben eines CERTs oder einer IT-Sicherheitsorganisation substituieren, sondern trägt zur Verbesserung der Qualität der jeweiligen Dienstleistungen bei. Hier liegt der eigentliche Gewinn für alle Akteure bzw. letztendlich für alle Nutzer von IuK-Infrastrukturen.

5.2 Akteure

Ein nationales IT-Frühwarnsystem kann nur in einer starken interdisziplinären Zusammenarbeit vieler Akteure erfolgreich sein. Die bloße Erfassung und Verarbeitung von rein technischen Daten ist nicht ausreichend, um ein umfassendes Lagebild zu konstruieren, welches darüber Aufschluss geben soll, welche unmittelbaren Gefährdungen bestimmter Infrastrukturen zu befürchten sind. Daher sind unbedingt Informationen aus sowohl technischen als auch gesellschaftlichen Quellen zu nutzen.

Häufiger Diskussionspunkt bei IT-Frühwarnsystemen ist die Ausprägung der Rolle der Strafverfolgungsbehörden. Aufgrund der Intention des Frühwarnsystems, deliktisches Handeln im ITK-Umfeld bereits im Ansatz zu erkennen und den Eintritt von Schäden entweder ganz zu verhindern oder zu mindestens zu mildern, steht ein stark präventiver Charakter im Vordergrund. Hier geht es nicht primär um die Strafverfolgung, sondern um die Kriminalprävention. Die Strafverfolgungsbehörden haben bereits heute Befugnisse und Mandate, um Informatio-

nen und Daten im Rahmen der individuellen Strafverfolgung einzufordern, also auch bei einem IT-Frühwarnsystem. Ebenso würde ein IT-Frühwarnsystem eigeninitiativ aufgrund der Rechtsstaatlichkeit gesicherte Erkenntnisse oder starke Hinweise auf deliktisches Handeln den Strafverfolgungsbehörden zugänglich machen. Eine darüber hinausgehende, aktivere Rolle der Strafverfolgung, z. B. ein Weisungs- und Direktionsrecht gegenüber dem kooperativ betriebenen IT-Frühwarnsystem, wäre aus Sicht der ITK-Industrie nicht wünschenswert und rechtsstaatlich problematisch. Nicht zuletzt wäre es äußerst fraglich, ob sich unter solchen Rahmenbedingungen eine starke Beteiligung einzelner Unternehmen abzeichnen würde.

In folgender Abbildung 3 wird verdeutlicht, wie ein Frühwarnsystem mit den unterschiedlichsten Akteuren verzahnt werden muss:

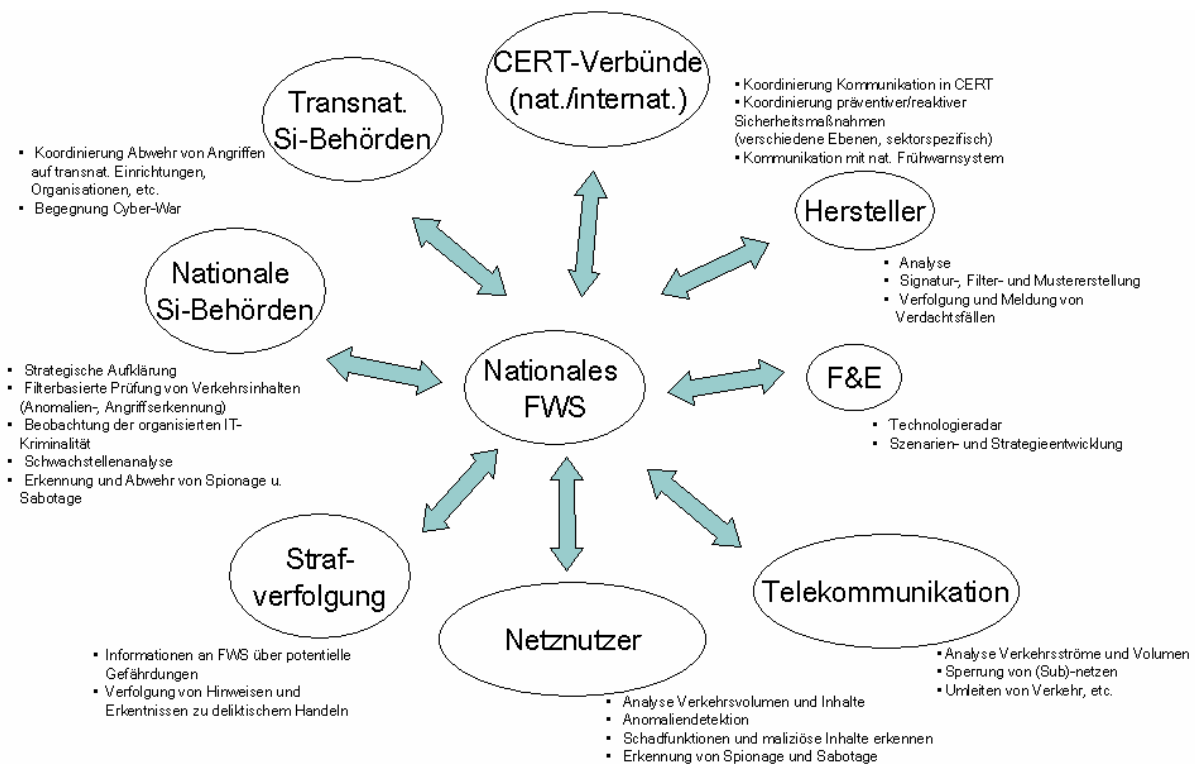


Abbildung 3: Akteure eines IT-FWS

Die unterschiedlichen primären Rollen der Beteiligten sind in der Abbildung 4 aufgeführt. Sie ist als Diskussionsgrundlage anzusehen, sowohl hinsichtlich der Zuordnung der Rollen als auch der Benennung der Rollen als solche.

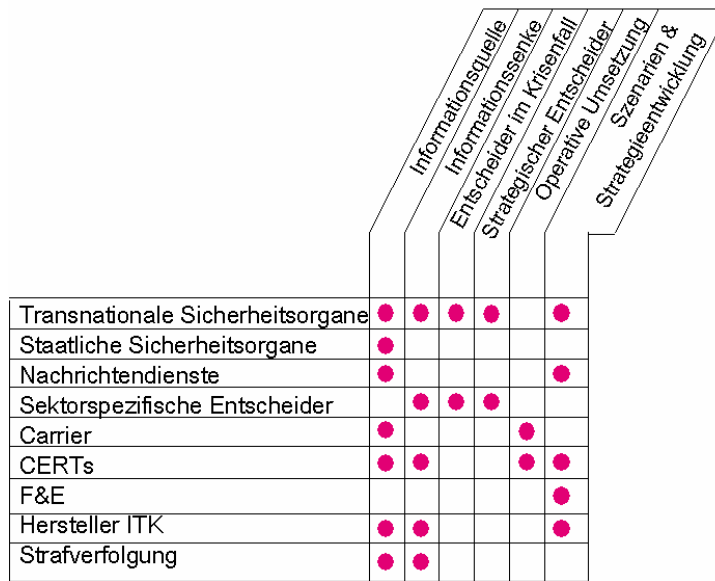


Abbildung 4: Akteure und ihr Rollen (Diskussionsgrundlage)

5.3 Organisationsstruktur

Die Annahme, ein Frühwarnsystem könnte rein virtuell mit unterschiedlichen Akteuren aufgesetzt werden, greift zu kurz. Vielmehr bedarf es einer zentralen Instanz, welche die Daten und Informationen aus unterschiedlichen Quellen zusammenträgt, analysiert, bewertet und Schlussfolgerungen zieht. Selbstverständlich kann und muss die zentrale Organisation durch dezentrale Strukturen unterstützt werden. Die Zusammenarbeit zwischen zentralen und dezentralen Anteilen ist zu regeln. Insbesondere sind Spielregeln und Prozesse zu verabreden, wenn sich Partner auf rein freiwilliger Basis an dem Frühwarnsystem durch Stellung von Ressourcen und/oder Informationen beteiligen.

Es deutet einiges darauf hin, dass die optimale Struktur eine partnerschaftliche, nicht auf finanziellen Gewinn zielende Organisation sein sollte. Insbesondere spricht dafür, dass sowohl die staatliche als auch die private Seite nicht über ein vollständiges Lagebild verfügen kann, wenn nicht Informationen und Daten von der jeweils anderen Seite beigetragen werden. Aufgrund gesetzlicher Restriktionen ist es den einzelnen Akteuren von staatlicher oder privater Seite gar nicht möglich, umfassende Informationen und Daten für sich allein zusammen zu tragen. Eine dartige Änderung der gesetzlichen Rahmenbedingungen stellt sich eher als nicht wünschenswert dar, würden doch damit einschneidende Befugnisse für die Akteure einhergehen, die schnell als Instrumente eines Überwachungsstaates angesehen werden könnten bzw. nicht kompatibel sind mit dem geltenden Telekommunikationsgeheimnis nach dem Grundgesetz.

In der Abbildung 5 ist ein Vorschlag für eine Grobstruktur einer solchen partnerschaftlichen Organisation dargestellt:

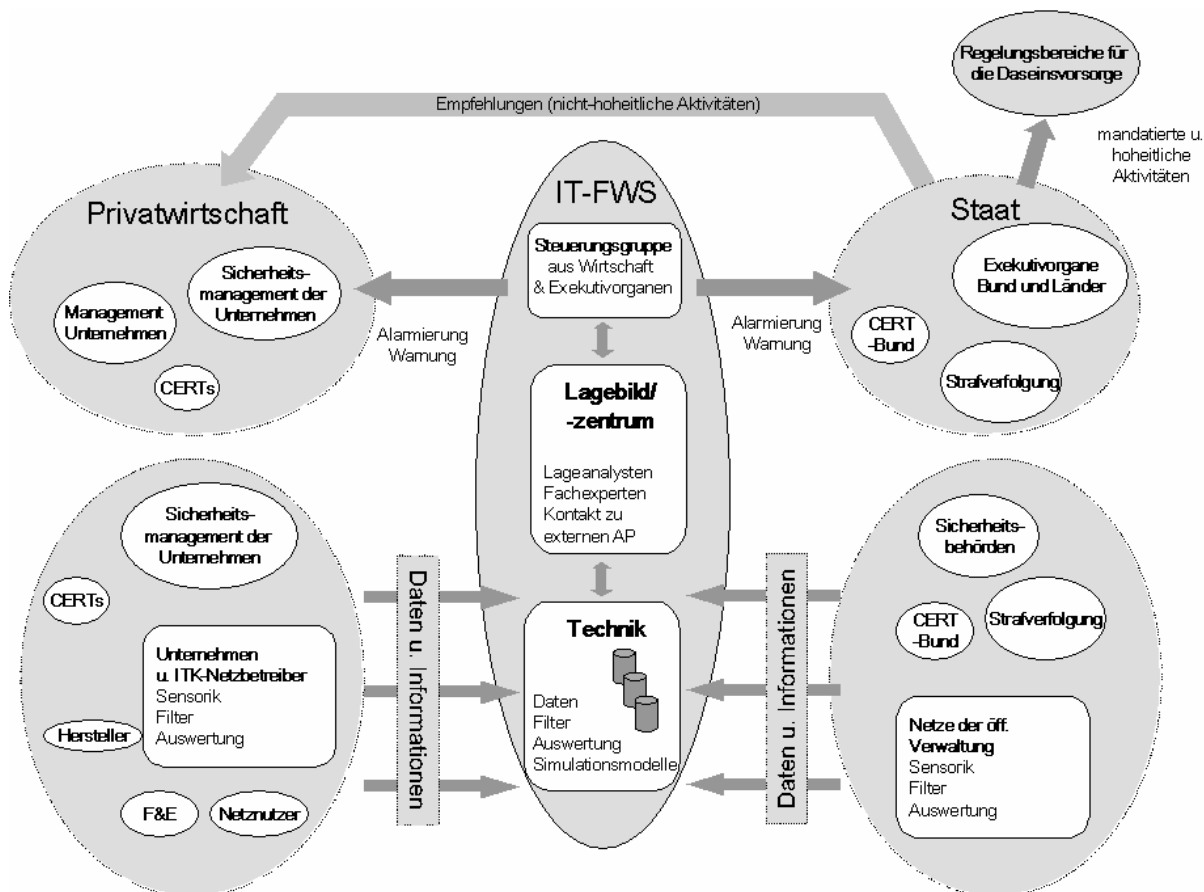


Abbildung 5: Grobaufbau eines nationalen IT-FWS (Vorschlag)

In diesem Vorschlag besteht das nationale Frühwarnsystem aus einer zentralen Instanz (IT-FWS), die Kernkompetenzen im Bereich Technik, Lagebild und Kommunikation vorhält. Die Instanz wird gemanagt durch eine Steuerungsgruppe, die sich zusammensetzt aus den Vertretern der Wirtschaft, der öffentlichen Verwaltung und den Exekutivorganen, die sich an dem IT-Frühwarnsystem beteiligen. Zu den wichtigen Aufgaben der Steuerungsgruppe gehören: Spielregeln für die gemeinsame Arbeit zu definieren und Richtlinien für die Warnung und Alarmierung zu erarbeiten.

Hervorzuheben ist, dass das IT-Frühwarnsystem als „Mediator“ oder „Schnittstelle“ definiert ist. Informationen und Daten aus den Bereichen der Wirtschaft, Industrie und der staatlichen Organe gehen zwar ein und werden verarbeitet, eine Weitergabe der Ursprungsinformationen an andere Beteiligte im IT-Frühwarnsystem ist jedoch ausgeschlossen. Die vom IT-Frühwarnsystem herauszugebenden Warnungen und Alarmierungen enthalten keine Ursprungs- bzw. Originalinformationen oder aber solche, die soweit sanitarisiert sind, dass kein Rückschluss auf die jeweilige Quelle möglich ist.

Bei den staatlichen Akteuren (Exekutivorgane) sind die besonderen hoheitlichen und mandatierten Leistungen zu berücksichtigen. Selbstverständlich werden diese Leistungen nicht durch Leistungen des kooperativen IT-FWS ersetzt. Das IT-FWS fungiert als Informationslieferant sowohl für die Bereiche der Wirtschaft als auch der staatlichen Organe. Es bleibt diesen Organen unbenommen, bspw. auf die Akteure in Industrie und Wirtschaft im Rahmen von Empfehlungen aber auch – sofern ein konkreter gesetzlicher Auftrag dies legitimiert⁴ – im Rahmen von Anordnungen und Weisungen zuzugehen. Diese Entscheidungen treffen die staatlichen Organe eigenbestimmt.

⁴ Dies trifft auf die Bereiche der staatlichen Daseinsvorsorge zu.

Mit einem solchen vom IT-FWS praktizierten Verfahren zur Informationsverarbeitung und -weitergabe kann auf eine Vielzahl bilateraler Geheimnis- bzw. Vertraulichkeitsvereinbarungen (insbesondere zwischen staatlichen und nicht-staatlichen Organisationen) verzichtet werden, da sichergestellt ist, dass alle Informationen ihrem Schutzbedarf entsprechend in der Organisation IT-FWS behandelt werden. Dies schließt aber natürlich weitergehende Vereinbarungen zwischen Einzelpartnern genauso wenig aus, wie die Möglichkeit in Einzelfällen abweichend zu agieren, wenn die Lage dies erfordert und das Einverständnis aller Beteiligten vorliegt.

5.4 Technik und Informationsmanagement

Frühwarnung ist eine komplexe Aufgabenstellung, bei der eine Vielzahl von Akteuren in unterschiedlichen Rollen miteinander kooperieren. Voraussetzung für eine erfolgreiche Zusammenarbeit ist eine effiziente Kommunikation und die Bereitstellung von Daten und Informationen in einem zentralen Informationssystem. In einer ersten Annäherung lassen sich die folgenden Funktionsblöcke identifizieren:

- Informationsgewinnung
- Datenerfassung
- Technische Analyse
- Dienste (Lagebild, Alarmierung)
- Informationsmanagement

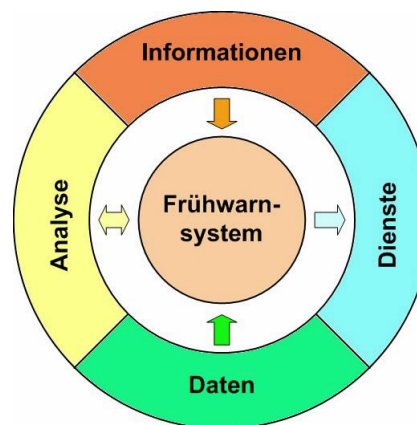


Abbildung 6: „Building blocks“ eines IT-FWS

Die zentralen Komponenten eines IT-Frühwarnsystems dienen zur Aufbereitung und Speicherung von Daten und Informationen, die zur Erbringung der Aufgabenstellung benötigt werden. In der ersten Näherung entspricht die Systemarchitektur dem klassischen Client-Server-Modell. Sensoren zur Datenerfassung wie auch Analysten kommunizieren über ein Netzwerk mit einem zentralen IT-System. Die Anforderungen an ein IT-FWS gehen aber über klassische Aufgaben wie Speicherung, Verarbeitung und Präsentation hinaus, denn gleichzeitig muss eine kooperative Arbeitsumgebung bereitgestellt werden, durch die eine interdisziplinäre Zusammenarbeit aller beteiligten Akteure ermöglicht wird.

Die Architektur eines IT-Frühwarnsystems sieht daher eine Aufteilung in zumindest drei Schichten vor. Die Basis der Gesamtarchitektur bildet ein Datenbankmanagementsystem als zentrales Repository für die Speicherung der sicherheitsrelevanten Ereignisse der beteiligten Domänen und der Analyseergebnisse. Auf dieser Schicht ist eine komplexe Mittelschicht aufgebaut, durch die eine Anzahl von Basisdienstleistungen und Anwendungen realisiert wird. Die oberste Schicht interagiert entweder durch ein Frontend (z.B. Web-Browser) mit den Anwendungen der mittleren Schicht oder nimmt direkt Basisdienstleistungen in Anspruch bzw. speist Daten und Informationen in das System ein. Folgende Basisdienste sind zentral zu realisieren:

- Erfassung von Informationen und Daten
- Kooperative Arbeitsumgebung für die Analyse
- Statistik

- Alarmierung der beteiligten Akteure
- Konfigurationsmanagement
- Sicherheitsdienste

Die technische Infrastruktur des IT-Frühwarnsystems muss entsprechende Schnittstellen für die Analyse, das Konfigurationsmanagement für die Sensoren sowie die kooperative Arbeitsumgebung bereitstellen, so dass Experten aus CERTs, Sicherheitsorganisationen, Sicherheitmanagement-Teams der Forschung und der zentralen Organisation gemeinsam Problemlösungen erarbeiten können.

Ebenso ist eine sichere Kommunikationsinfrastruktur von großer Bedeutung. Es dürfte kein Zweifel darüber bestehen, dass ein IT-Frühwarnsystem ein besonders gefährdetes Ziel darstellt, da die Kernaufgabe doch darin besteht, das Schadenspotenzial möglicher Angriffe im nationalen Rahmen zu minimieren. Auch ohne eine umfassende Risikoanalyse lassen sich folgende Bedrohungen allein aus der Existenz eines Frühwarnsystems ableiten:

- Verlust der Verfügbarkeit durch DoS oder DDoS Angriffe
- Verlust der Integrität durch das Einspielen falscher Daten und Informationen

Aufgrund der Vielzahl von Klienten (Sensoren und Analyseexperten) und der damit verbundenen Kommunikation, muss eine skalierbare Sicherheitsinfrastruktur implementiert werden.

5.4.1 Informationsgewinnung

Die Informationsgewinnung beinhaltet die Beschaffung von Informationen u.a. über Schwachstellen, Sicherheitslücken, Vorfälle und Metainformationen. Sicherheitsmeldungen von CERTs und Information der Hersteller über verfügbare Sicherheitsupdates können automatisiert erfasst werden, sofern diese in Formaten vorliegen, die eine maschinelle Verarbeitung erlauben. Damit ein Frühwarnsystem die geforderten Dienstleistungen erbringen kann, ist es nicht ausreichend nur technische Informationen zu erfassen, es müssen daher auch nicht-technische Informationen oder Metainformationen von den wirtschaftlichen und gesellschaftlichen Akteuren einfließen. Die Nutzung solcher Informationsquellen setzt aber das Vorhandensein von Richtlinien zum Informationsaustausch (Information-Sharing-Policies) voraus. Hierfür müssen entsprechende Schnittstellen und Datenrepräsentationen spezifiziert werden, um eine nachfolgende Informationsverarbeitung zu ermöglichen.

5.4.2 Datenerfassung

Um die aktuellen Bedrohungspotentiale in den Informationsnetzwerken erfassen zu können, müssen diese mittels Sensoren überwacht und Anomalien ausgewertet werden. Damit gesicherte Daten über Angriffe erfasst werden können, ist eine Auswertung des Netzverkehrs auf der Inhaltsebene erforderlich. Grundlagen dafür sind in erster Linie Firewall-, Router- und IDS-Logs operativer Netzwerke. In aktuellen Ansätzen werden auch Netzwerksegmente ohne operative Systeme (sog. Darknets) beobachtet und Sondersysteme (Honey Pots) eingesetzt, die auf eindeutige Anzeichen neuer Viren oder Würmer reagieren. Eine Auswertung auf der Inhaltsebene kann und darf aufgrund rechtlicher Rahmenbedingungen nur in den Netzwerken der Unternehmen, Organisationen und Privatanwender erfolgen (siehe Abbildung 8).

Um im nationalen Rahmen Aussagen über die Gefährdungslage tätigen zu können und um koordinierte Angriffe erkennen zu können, müssen diese Sensoren flächendeckend ausgerollt werden. Flächendeckend ist hier jedoch nicht geographisch zu interpretieren, sondern dahingehend, dass alle relevante Sektoren, die ITK-Infrastrukturen einsetzen, an der Datenerfassung beteiligt sind. Die Daten der einzelnen Sensoren können jedoch nicht direkt einer zentralen Datenbank zugeführt werden, folgende Gründe machen eine mehrstufige Verarbeitung erforderlich:

- **Komplexität**
Die Anforderungen hinsichtlich Speicherkapazität und Rechenleistung zentraler IT-Systeme sind bei der zu erwartenden Datenmenge sehr hoch und nur mit einem enormen finanziellen Aufwand realisierbar. Es muss daher eine Informationsverdichtung bei den Organisationen stattfinden, die Daten für das Frühwarnsystem bereitstellen.
- **Sensibilität**
Je nach Art und Einsatzort eines Sensors werden auch unternehmensspezifische Daten erfasst. Diese Daten müssen zuerst geeignet anonymisiert werden, bevor sie einer zentralen Auswertung zugeführt werden.
- **Heterogenität**
Auf dem Gebiet der Netzwerksicherheit gibt es eine Vielzahl von Produkten unterschiedlicher Hersteller. Für die Ereignismeldungen kommerzieller Produkte werden jedoch häufig herstellerspezifische Datenformate verwendet, so dass eine Konvertierung in ein Standardformat erforderlich ist.

In der Abbildung 7 ist der schematische Aufbau eines verteilten Sensornetzwerkes skizziert. In den Kommunikationsnetzen einzelner Organisationen (Domänen) sind verschiedene Sensoren implementiert, die sicherheitsrelevante Ereignisse an einen Kollektor innerhalb der Domäne melden. Hier erfolgt dann eine Verdichtung und Anonymisierung der Daten, bevor diese in einem standardisierten Datenformat an eine zentrale Instanz des IT-Frühwarnsystems übermittelt werden.

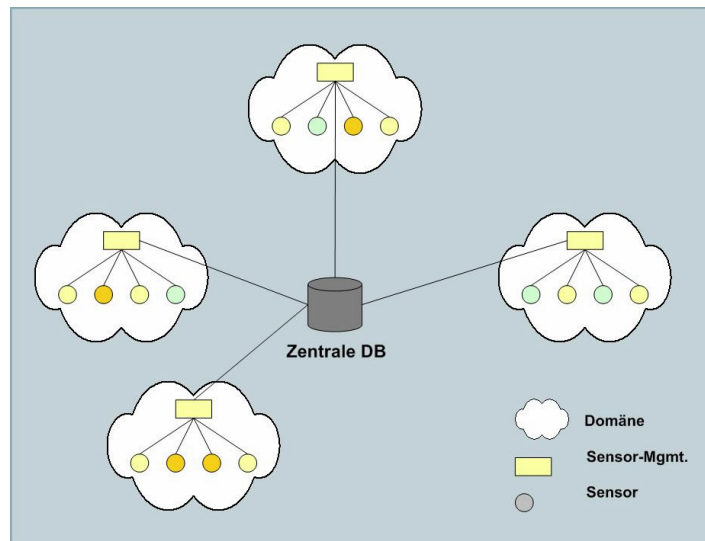


Abbildung 7: Schematischer Aufbau eines verteilten Sensornetzwerkes

Den TK-Unternehmen kommt im Rahmen des Frühwarnsystems eine wichtige Rolle zu. Sie sind es, deren Infrastrukturen für den Transport von Daten unverzichtbar sind. Betrachtet man ihre Netze in einem hierarchischen Aufbau (Abbildung 8), so können grob drei Netzebenen unterteilt werden: Die unterste Ebene stellt das Zugangnetz für Endkunden/-nutzer dar (Anschlussnetz). Die zweite Ebene sind die IT-Netz (Backbones) der Unternehmen. Die oberste Ebene stellt die Zusammenschaltung der Netze verschiedener Unternehmen (Peering-Points) dar.

Auf jeder Ebene lassen sich Informationen über die Signalisierung und die Verkehrsströme ableiten. Im Rahmen der Frühwarnung können durch geeignet platzierte Sensoren Verkehrsströme auf Ausbreitungsvektoren bestimmter Angriffsmuster untersucht werden. Nochmals sei darauf hingewiesen, dass gesetzliche Rahmenbedingungen (Fernmeldegeheimnis) es den TK-Unternehmen verwehren, Netzverkehr ihrer Kunden auch bis zu einer Inhaltsebene auf Unregelmäßigkeiten oder Anomalien hin zu kontrollieren. Denkt man über ein IT-Frühwarnsystem hinaus, könnte in einer Krisenreaktion bestimmter Netzverkehr gesperrt oder anders gelenkt werden.

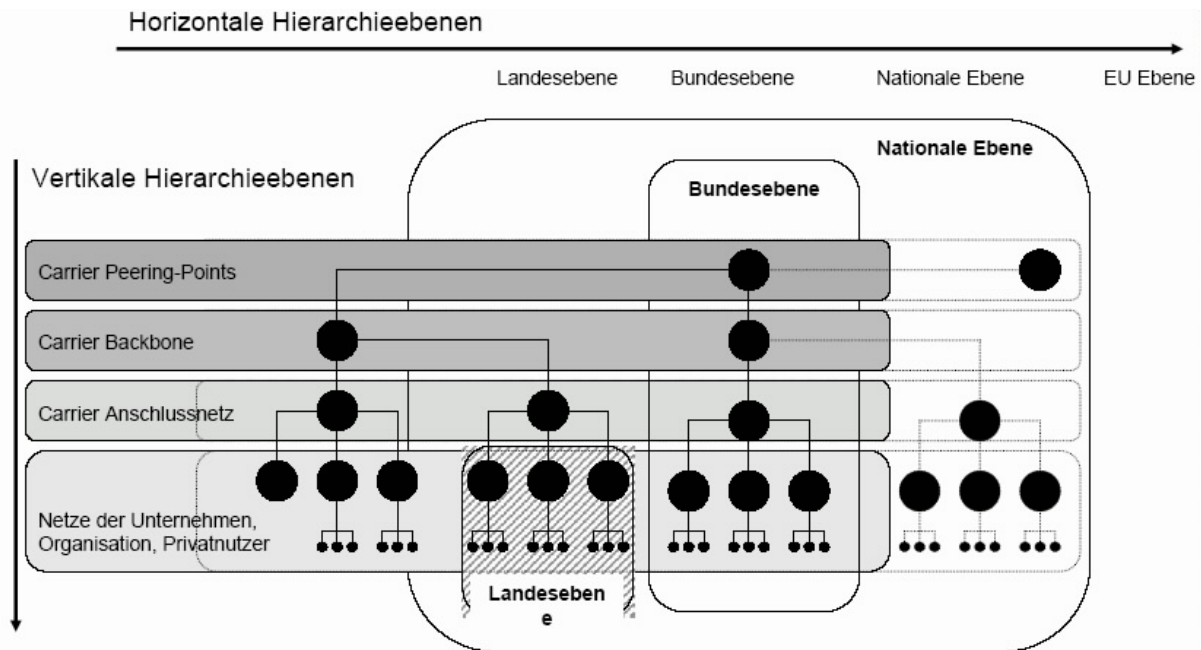


Abbildung 8: Existierende Hierarchien

Neben der Hierarchie der technischen Netzebenen ist zusätzlich eine politische Hierarchie zu berücksichtigen. Diese Hierarchie besteht aus den unterschiedlichen Jurisdiktionen. In Deutschland sind die föderalen Strukturen besonders zu betrachten, so dass hier die unterste Ebene die Landesebene ist, gefolgt von einer Bundesebene (Staatenebene), der Ebene der Europäischen Union (Transnationale Ebene) sowie einer internationalen Ebene (Drittstaaten). Die unterschiedlichen Jurisdiktionen ergeben einen legislativen Flickenteppich bezüglich der Möglichkeiten und Befugnisse der einzelnen Akteure eines IT-Frühwarnsystems. Da nämlich die technischen Netzebenen nicht notwendigerweise (bzw. in der Regel gar nicht) innerhalb einer politischen Ebene verlaufen, ergeben sich für die TK-Unternehmen sehr spezielle Randbedingungen hinsichtlich ihrer Möglichkeiten, sich an einem IT-Frühwarnsystem zu beteiligen.

5.4.3 Technische Analyse

Die technische Kernkompetenz wird neben dem Vorhalten der notwendigen technischen Infrastruktur durch eine ausreichend großen Zahl an technischen Experten dargestellt. Bei einer Realisierung eines IT-Frühwarnsystems ist anzustreben, dass durch eine automatisierte Informationsverarbeitung eine möglichst präzise Diagnose der aktuellen Situation erfolgt und sofern gesetzte Schwellwerte überschritten werden, entsprechende Warn- bzw. Alarmmeldungen versendet werden.

Wie einleitend schon gesagt wurde, können fundierte Prognosen nicht allein durch den Einsatz von Technik erbracht werden. Derzeit verfügbare Expertensysteme können den Menschen zwar unterstützen, jedoch nicht ersetzen. In diesem Baustein ist daher die vom Menschen gesteuerte Informationsverarbeitung konzentriert.

Kernaufgabe der Analyse ist die Bereitstellung von Informationen, die für operative Aufgaben genutzt werden können. Aus dem stetigen Strom neuer Informationen müssen im Wesentlichen nicht-technische Indikatoren herausgefiltert werden, um gezielt bestimmte Ereignisse zu analysieren und auszuwerten. Weitere Aspekte der Analyse sind:

- Zusammenführung verschiedener Informationsquellen und Korrelation von Ereignissen
- Simulation und Modellbildung
- Trendanalysen und vergleichende statistische Auswertungen
- Analyse von Schwachstellen

Ein weiteres Ziel der Analyse ist die Weiterentwicklung von Methoden und Verfahren für eine automatische Informationsverarbeitung und deren Integration. Zum Beispiel kann durch die Analyse einer Sicherheitslücke eine Hypothese über die zu erwartenden Angriffsverfahren aufgestellt und entsprechende Filter bzw. Signaturen für die Sensoren erzeugt werden. Dies ermöglicht dann gezielt die Suche nach neuen Angriffsmustern.

5.5 Dienstleistungen

Die Bereitstellung eines kontinuierlichen Lagebilds über die Bedrohungslage aus dem Internet und eine Warnung bzw. Alarmierung der primären Zielgruppen sind die wesentlichen Aufgaben eines nationalen IT-Frühwarnsystems.

5.5.1 Lagebild

Aufgabe eines nationalen IT-Frühwarnsystems ist es, ein kontinuierliches Lagebild über Bedrohungen, Ereignisse, Tätergruppen und deren Ziele zu erstellen. Das Lagebild muss gesicherte und messbare Informationen verwenden, um einen Überblick über die aktuelle Bedrohungs- und Angriffssituation nach Regionen, Branchen, Netzen oder einzelnen Anwenderbereichen zu liefern. Während Presse, Hersteller und CERTs über aktuelle Systemschwachstellen und verfügbare Security Patches informieren, leistet ein IT-Frühwarnsystem mehr. Es sollen darüber hinaus Aussagen zu u.a. folgende Informationen geliefert werden:

- zum Verbreitungsgrad von Schadsoftware
- zu Ausgangspunkten von Angriffen
- zu Zielen von Angriffen sowie
- zu Tendenzen bei verwendeten Angriffstechniken

Für die kontinuierliche Erstellung des Lagebilds werden nicht nur Daten über Sensoren erfasst und ausgewertet. Aber auch andere Informationen dienen als Indikatoren für das Lagebild. Dies betrifft Informationen:

- zu neu verwendeten Angriffstechniken
- zu Tätern und Tätermotiven
- zur Gefährlichkeit von Angriffstechniken und
- zur voraussichtlichen Anwendbarkeit wirksamer Gegenmaßnahmen

Alle Daten und Informationen werden möglichst ohne Verzögerung analysiert und für die Erstellung des Lagebilds herangezogen. Dabei werden Verfahren verwendet, die in der Lage sind, große Mengen von Daten mehrstufig und analytisch auszuwerten, um Abhängigkeiten und Auffälligkeiten zu ermitteln und darzustellen. Das Lagebild beantwortet Fragen wie:

- Wann werden Angriffe erwartet?
- Wo werden Angriffe erwartet?
- Von welcher Seite werden Angriffe erwartet?
- Welche Intensität werden Angriffe haben?
- Welche Techniken werden verwendet?
- Wie gefährlich werden Angriffe sein?

Die Erstellung eines Lagebilds erfolgt jedoch nicht mittelbar durch ein IT-System, sondern durch Lageanalysten, welche die aggregierten Informationen und Daten analysieren und mit Informationen aus anderen (nicht-technischen) Quellen verdichten. Diese Erkenntnisse können dazu führen, dass gezielte technische Analysen von Schwachstellen erfolgen.

5.5.2 Warnung und Alarmierung

Das Lagebild eines IT-Frühwarnsystems liefert eine Voraussetzung, um die zwei primären Zielgruppen frühzeitig vor anstehenden Angriffen zu warnen und koordinierte Gegenmaßnahmen rechtzeitig einzuleiten. Ob konkreter Handlungsbedarf hinsichtlich einer Warnung

oder Alarmierung besteht, muss dabei in enger Kommunikation mit den Entscheidern der Exekutivorgane des Staates und der Wirtschaft erfolgen.

In Analogie zu Warnsystemen aus anderen Bereichen hat ein IT-Frühwarnsystem die Aufgabe, potentielle Opfer aktiv zu alarmieren, die sich im Augenblick einer großen Gefahr aussetzen. Im Gegensatz zu herkömmlichen Warnsystemen im Bereich der IT („Der Serverraum brennt“ oder das „Netzwerk ist nicht mehr verfügbar“.) liefern IT-Frühwarnsysteme nur Hinweise zur Wahrscheinlichkeit, mit der ein schädigendes Ereignis eintreten wird („Viele Angreifer versuchen derzeit den Angriff X mit der Schadsoftware Y auf die Objekte Z“). Eine Frühwarnung kann dazu dienen, dass betroffene Organisationen sich auf einen aktuell bevorstehenden Angriff besser vorbereiten, wenn bekannt ist, dass sie bereits direkt im Visier von Angreifern stehen.

In diesem Zusammenhang ist es von besonderer Bedeutung, dass Informationen zu spezifische Bedrohungszuständen, die aus der Analyse des Lageberichts resultieren, aktiv an Betroffene kommuniziert werden. Empfänger von Frühwarnungen sind CERTs und IT-Sicherheitsorganisationen der öffentlichen Verwaltung und der Wirtschaft, die sich mit der Abwehr von aktuellen Bedrohungen und Angriffen auf Computersystemen beschäftigen. Diese Organisationen übernehmen stellvertretend für ein bestimmtes Klientel oder einen Bereich von IuK-Infrastrukturen in Deutschland die Auswertung von Frühwarnungen und die Steuerung der Reaktion. Die Organe sind für den gewissenhaften Umgang mit Frühwarnungen verantwortlich und koordinieren die weitere Alarmierung. Dabei bleibt es dem IT-Sicherheitsmanagement der Organisationen selbst überlassen, eine angemessene Reaktion umzusetzen.

5.5.3 Reaktion

Die Reaktion auf eine Warnung kann vom nationalen IT-Frühwarnsystem nicht geleistet werden. Hier sind die CERT-Gemeinschaft, der IT-Stab sowie das IT-Sicherheitsmanagement von Unternehmen und Behörden gefordert – und das in Zukunft weit mehr als bisher.

Zur Reaktion auf Frühwarnungen müssen neue Mittel und Wege gefunden werden. Was nützen aktuellste Informationen zu gezielt anrollenden Angriffswellen aus dem Internet, wenn die Mittel zum Schutz vor solchen Angriffen nicht oder noch nicht vorhanden sind? Selbst wenn die Mittel bekannt oder Security Patches verfügbar sind, ist eine rechtzeitige Reaktion in großen IuK-Infrastrukturen kaum noch möglich.

Die Komplexität der eingesetzten IT-Systeme sowie die Abhängigkeit der Geschäftsprozesse von der IT bedingt es zunehmend, dass reaktive Prozesse frühzeitig angegangen werden müssen. Besonders gefordert sind große Anwenderunternehmen, Rechenzentren oder Telekommunikationsunternehmen, die für sehr viele Anwender Systeme, Netze oder gar kritische IuK-Infrastrukturen betreiben.

Warnungen eines IT-Frühwarnsystems liefern hier eine Voraussetzung, um in Zukunft Reaktionen besser und frühzeitiger planen zu können. Dies betrifft u.a.

- die Alarm- und Notfallplanung
- das Change Management
- das Sicherheitsmanagement und
- das Kunden- und Partnermanagement

für ein bestimmtes in Kürze erwartetes Ereignis, das mit einer nicht zu vernachlässigenden Wahrscheinlichkeit eintritt. Dabei bleibt eine Reaktion nicht darauf beschränkt, eine bestimmte IT-Schwachstelle zu beheben; häufig sind auch koordinierte Reaktionen unter Einbeziehung von IT-Dienstleistern und Kunden notwendig, um eine befriedigende Lösung zu schaffen. Je früher entsprechende Warnungen vorliegen, umso besser können IuK-Infrastrukturen

und sogar Geschäftsprozesse dahingehend verändert werden, dass Angriffe deutlich weniger Angriffspunkte finden.

Hiermit eng verknüpft sind Trouble Ticket Systeme, Notfallplanungssysteme im Bereich Business Continuity oder Systeme zur Bearbeitung von Sicherheitsvorfällen in Unternehmen, die helfen den Reaktionsvorgang zu beschleunigen, zu steuern und zu überwachen. Wichtig ist hier die Integration dieser Systeme mit der Kommunikationsinfrastruktur des nationalen IT-Frühwarnsystems. Der Erfüllungsstand der Reaktion kann somit in das Lagebild einfließen, d.h. es können im Lagebild Aussagen darüber getroffen werden, wie viele Unternehmen, wann welche Reaktionen geplant und umgesetzt haben, um einer Gefahr zu begegnen.

6 Fazit und Handlungsempfehlungen

Die in BITKOM vertretene Wirtschaft schlägt die Einrichtung eines nationalen IT-FWS vor. Seine Aufgabe ist die Analyse und Ermittlung eines stimmigen und übergeordneten Lagebildes über Bedrohungen und Tätergruppen, die auf elektronischem Wege die IuK-Infrastruktur von Unternehmen und Behörden in Deutschland massiv beeinträchtigen, sowie deren Ziele,

Folgende Handlungsempfehlungen werden seitens der Wirtschaft ausgesprochen:

- Das IT-FWS ist ein wesentliches Element der Daseinsvorsorge, das als eine gemeinsame Aufgabe von Wirtschaft und Staat anzusehen ist. Das IT-FWS sollte daher von einer partnerschaftlichen, nicht auf finanziellen Gewinn zielenden Organisation getragen werden.
- Das IT-FWS soll potenziell Betroffene eines Angriffs durch frühe Warnungen sensibilisieren, so dass genügend Reaktionszeit zur Verfügung steht, um den Eintritt eines konkreten Ereignisses zu verhindern oder die Folgen zu mindern. Zielgruppen der Warnungen sind CERTs und das IT-Sicherheitsmanagement von Unternehmen und Behörden.
- Für das IT-FWS ist ein der Aufgabe angemessenes Informationsmanagement aufzubauen, welches den Grundsätzen der Informations- und Datensparsamkeit sowie dem Datenschutz genügt. Die Wirtschaft bietet sich hierbei als Partner an.
- Für alle teilnehmenden Akteure ist Rechtssicherheit bei der Lieferung, Bereitstellung und Verarbeitung von Informationen und Daten herzustellen.
- Die Rollen und Aufgaben aller Akteure sind verbindlich gemeinsam von Staat und Wirtschaft festzulegen.
- Auf Seiten der staatlichen Organe ist eine klare Kompetenzabgrenzung notwendig. Die Zuständigkeit und die Verantwortung sollten dabei in einer Hand liegen. Ein föderaler Ansatz erscheint nicht Erfolg versprechend.
- Neben der Informationsgewinnung aus der Sensorik sind auch Informationen der Sicherheitsbehörden und Nachrichtendienste zu nutzen.
- Das IT-FWS versteht sich nicht als unmittelbares Instrument der Strafverfolgung.
- Die Methoden zur Gewinnung, Aufbereitung und Auswertung der gewonnenen Informationen bedürfen einer intensiven Weiterentwicklung. Dies ist ein Erfolg versprechendes Gebiet für den Forschungs- und Wirtschaftsstandort Deutschland. Hieraus ergeben sich bedeutende Kompetenzvorteile im internationalen Umfeld.
- Das IT-FWS ist ein modellhafter Ansatz für den vorbeugenden Schutz der Informationsinfrastrukturen in Deutschland.

Der BITKOM bietet dem Bundesministerium des Inneren an, dieses für den Standort Deutschland von besonderer Wichtigkeit geprägte Thema gemeinsam weiterzuentwickeln. Dazu wäre der BITKOM bereit, ein mit Vertretern der ITK-Industrie und des BMI besetztes Gremium zu installieren, in dem folgende Aktivitäten aufgenommen werden sollten:

1. Definition einer politischen Vision sowie lang- und kurzfristiger Ziele eines kooperativ getragenen nationalen IT-FWS.
2. Entwicklung von passenden Strategien, Handlungsansätzen, Regel, Prozeduren und Maßnahmenpaketen für ein nationales IT-FWS sowie die Identifikation der dafür zu beteiligenden Akteure in Industrie, Wirtschaft und staatlichen Organen.
3. Start des nationalen IT-FWS sowie Begleitung und Weiterentwicklung durch das etablierte Gremium.



Danksagung

Die vorliegende Broschüre entstand im BITKOM Fachausschuss „IT-Frühwarnsysteme“ unter der Leitung von Dr. Günther Welsch (Deutsche Telekom AG) und Paul Frießem (Fraunhofer-Institut für Sichere Informationstechnologie).

Wir danken allen Mitgliedern des Fachausschusses für das außerordentliche Engagement und die Textbeiträge.





Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org