CERT-Dienstleistungen für kleine und mittlere Unternehmen (KMU)

Erstellt im Auftrag des Bundesministeriums für Wirtschaft und Technologie

Dr. Marcus Pattloch
Dr. Klaus-P. Kossakowski

Inhaltsverzeichnis

1 Ausgangssituation

Im Rahmen der im Mai 2000 von BM Dr. Müller gegründeten "Partnerschaft sichere Internet-Wirtschaft" ist auch die Verbesserung der Alarmierung über sicherheitsrelevante Vorfälle erörtert worden.

Die Vorstellung, öffentliche Netze würden allen Anwendern und Benutzern ermöglichen, in einem "globalen Dorf" miteinander ohne Sicherheitsprobleme zu kooperieren, ist irreführend. Mag dieses Bild bis Mitte der neunziger Jahre für das Internet als "Netz der Netze" noch gepasst haben, sind mittlerweile viele Faktoren dafür verantwortlich, dass die heutige Situation eher mit einer "globalen Megacity" vergleichbar ist.

Als Heranwachsende haben viele Menschen in "ihrem Dorf" erleben können, dass die Türen tagsüber nicht abgeschlossen wurden. Doch hat auch dort die Entwicklung nicht halt gemacht. Selbst wenn es immer noch ein Dorf ist, prägen die äußeren Einflüsse und verändern das Verhalten aller Dorfbewohner. Genauso mussten viele Enthusiasten und Pioniere einsehen, dass die Stimmung im Netz nicht mehr dieselbe ist und der Gedanke, wieder zu einer kleinen, geschlossenen Gemeinde zurückzufinden, ist illusorisch. Ohne eine Vernetzung gibt es keine globale und offene Kommunikation. Niemand würde z. B. ernsthaft vorschlagen, zum Schutz vor Kriminellen die realen Straßen zwischen realen Häusern abzuschaffen - der Schutz konzentriert sich "im Endsystem", d. h. im Haus, und in einer Infrastruktur, die Täter abschreckt und sanktioniert.

1.1 Computer-Notfallteams als neues Element

Das Auftreten von Sicherheitsproblemen und konkreten Vorfälle hat eine lange Tradition. Betrachtet man neben der Existenz von Sicherheitslücken auch die Motivation von Personen, diese zu suchen und sofern vorhanden auszunutzen, findet sich ein Spiegelbild der Gesellschaft mit all ihren Problemen im Netz. Dies sollte nicht verwundern - eher erstaunt das "Zwiedenken" vieler Menschen, die einerseits im sozialen Umfeld jede Minute mit der Unsicherheit einer Risikogesellschaft leben und andererseits für das Netz nach absoluter und nicht zu erreichender Sicherheit streben. Daraus sollte nicht abgeleitet werden, dass Sicherheit kein erstrebenswertes Ziel sei. Dennoch ist es nicht entscheidend, das ideelle Ziel zu erreichen, sondern sich ihm möglichst weit anzunähern. Akzeptiert man diese Auffassung, muss zwangsläufig das Auftreten von Angriffen und Vorfällen zugestanden und dementsprechend behandelt werden.

In der Praxis haben sich seit dem ersten großen Internet-Vorfall, dem sogenannten Internet-Wurm, im November 1988 Computer-Notfallteams (engl.: CERT, Computer Emergency Response Team - heute wird auch über IRTs, Incident Response Teams, gesprochen) als eine wichtige Komponente bei der Bewältigung von Internet-Vorfällen herausgebildet. Die steigende Bedeutung solcher Teams zeigt sich z. B. an der Entwicklung der Vorfallszahlen im internationalen Umfeld (Tabelle 1-1). Durch diesen grundlegenden Paradigmenwechsel - weg von der Vorstellung, es sei überflüssig, sich mit Angriffen und Vorfällen zu beschäftigen, weil ein ausreichendes

Maß an Sicherheit erreicht wurde, hin zu der Erkenntnis, dass auf jeden Fall mit Vorfällen umzugehen ist - eröffnen sich neue Möglichkeiten.

Jahr	AUSCERT (.au)	CERT/CC ("Internet")
1988	-	6
1989	-	132
1990	-	252
1991	-	406
1992	-	773
1993	110	1.334
1994	171	2.340
1995	191	2.412
1996	309	2.573
1997	572	2.134
1998	1.342	3.734
1999	1.816	9.859
2000	8.197	21.756

Tabelle 1-1: Vorfallszahlen verschiedener Computer-Notfallteams

Anders als bei den traditionellen Maßnahmen der Rechner- und Netzwerksicherheit werden Angriffe und Vorfälle nicht ignoriert. Stattdessen wird das Wissen über Vorfälle genutzt, um Schäden zu begrenzen oder ganz abzuwehren. Angepasste Verfahren machen Vorfälle erkennbar, verringern mögliche Schäden, erlauben erst effiziente Gegenmaßnahmen und tragen so ebenfalls wirksam zu dem globalen Ziel bei, die Zahl von Angriffen und Vorfällen - und damit Schäden - zu minimieren. Viele Incident Response Teams bieten folgerichtig vorbeugende Informationen über neue Sicherheitslücken oder Angriffsverfahren an. Dazu kommen häufig auch konkrete Hinweise zur Konfiguration von Rechnern und Netzwerken zum Schutz vor Angriffen. Nur dadurch können Vorfälle verhindert werden, bevor sie auftreten können.

Viele Unternehmen schätzen die Bedeutung dieser Art der Vorsorge eher gering ein, treten Vorfälle scheinbar doch nicht sehr häufig auf und stellen meist kein großes Problem dar. Aus dieser Perspektive sind Kosten für die Bereitstellung entsprechender Dienstleistungen vergeudet oder könnten besser in "absichernde" Maßnahmen investiert werden. Nur eine Erfassung und Analyse tatsächlicher Angriffe und Vorfälle kann hier Antworten geben und ein entsprechendes Bewusstsein schaffen.

Alle bisherigen Computer-Notfallteams zeichnen sich dadurch aus, dass sie für einen mehr oder weniger festgelegten Anwenderkreis - ihre Zielgruppe[1] - tätig sind. Ihre Dienste sind nur ein Teil aller Maßnahmen zur Rechner- und Netzwerksicherheit dieses betreuten Anwenderkreises. Durch ihre Arbeit soll die Fähigkeit gefördert werden, auf "Security Incidents" - Sicherheitsvorfälle - effizient, angemessen und schnell reagieren zu können. Was ein Vorfall ist, wird dabei durch die lokalen Policies und Einschätzungen festgelegt.

1.2 Situation in Deutschland

International gibt es Mitte des Jahres 2001 ca. 90 CERTs, die in dem Dachverband FIRST, Forum of Incident Response and Security Teams, organisiert sind. In Deutschland gibt es sieben Mitglieder, die folgende Zielgruppen betreuen:

- Das DFN-CERT als Einrichtung des DFN-Vereins[2] betreut den Wissenschaftsbereich, hat aber als "ältestes" Team auch noch eine gewisse Koordinierungsfunktion inne.
- Das BSI ist mit dem Aufbau eines CERTs für die Bundesverwaltung beauftragt.
- Das S-CERT etabliert eine verteilte Struktur von CERTs und Sicherheitsteams innerhalb der Sparkassen-Finanzgruppe.
- Das SIEMENS-CERT ist international und national für die Unternehmen der SIEMENS Gruppe zuständig.
- Die drei weiteren Teams sind interne Teams der Universität Karlsruhe und der secunet Security Networks AG sowie das FSC-CERT für den Hersteller Fujitsu-Siemens.

Darüber hinaus gibt es weitere Teams, z. B. das dCERT (ein Dienstleistungsangebot der debis IT Security Services GmbH), das RUS-CERT an der Universität Stuttgart und das im Aufbau befindliche Team der Deutschen Telekom AG.

Insgesamt ist die Bedeutung der "Incident Response" als Teil eines zeitgemäßen adaptiven Sicherheitsmanagements von vielen Verantwortlichen noch nicht erkannt worden. Daher fehlen für die deutsche Wirtschaft, insbesondere für die kleinen und mittleren Unternehmen (KMU), eigene Sicherheits- und Notfallteams, die diese Aufgabe wahrnehmen können. Es fehlt zudem an einer Unterstützung der deutschen Wirtschaft und insbesondere der KMUs bei dem Aufbau solcher Teams, so dass sich diese Lücke ohne Intervention nur sehr langsam schließen wird.

Ohne eine übergreifende CERT-Infrastruktur gibt es keine Koordinierung bei Vorfällen, die viele einzelne Unternehmen gemeinsam betreffen, so wie dies bei Melissa, I-LOVE-YOU, aber auch bei dem aktuellen BIND-Angriff, der Fall war und ist. Durch die fehlende Repräsentanz der deutschen Wirtschaft im internationalen CERT-Verbund sind deren Unternehmen von dem Informationsfluss zwischen den existierenden CERTs abgeschnitten und können notwendige Maßnahmen oft nur

---

1 Der Fachbegriff hierfür ist im Englischen "Constituency". Im Deutschen findet sich oft dafür der Begriff "Klientel", hier erscheint "Zielgruppe" geeigneter zu sein.

2 DFN bezeichnet das Deutsche Forschungsnetz, getragen durch den DFN-Verein, Berlin.

verspätet umsetzen - zu einem Zeitpunkt also, zu dem häufig bereits Schäden eingetreten sind.

1.3 Untersuchte Fragestellungen

Im folgenden soll eine umfassende, aber vor allem pragmatische Grundlage für die Entscheidung über eine CERT-Infrastruktur für die KMUs - im weiteren als KMU-CERT-Infrastruktur bezeichnet - in der gewerblichen Wirtschaft geschaffen werden. Um diese Anforderungen zu erfüllen, werden folgende Fragestellungen in diesem Gutachten adressiert:

1. Welche relevanten (Infra)Strukturen gibt es im nationalen und internationalen Bereich? Welche Erkenntnisse können auf die KMU-CERT-Infrastruktur übertragen werden?

2. Welche Dienstleistungen sollen im Rahmen einer KMU-CERT-Infrastruktur durch welche Komponenten erbracht werden? Worin bestehen die Abweichungen von anderen CERTs und wodurch sind solche Abweichungen begründet? Gibt es Migrationspfade von einem minimalen hin zu einem erweiterten Dienstleistungsangebot?

3. Welche Interaktionen sind zwischen den Komponenten einer KMU-CERT-Infrastruktur zu etablieren? Wie werden die Interaktionen mit anderen nationalen und internationalen CERTs bzw. (Infra-)strukturen gestaltet?

4. Welche Aufwände müssen für eine erfolgreiche Implementierung der in Punkt 2 und 3 empfohlenen Infrastruktur kalkuliert werden?

5. Welche Vor- bzw. Nachteile haben verschiedene Betreibermodelle, durch die die Dienstleistungen der KMU-CERT-Infrastruktur erbracht werden können?

2 CERT-Infrastrukturen im nationalen und internationalen Bereich

Über die Jahre hat sich ein für Außenstehende nicht immer transparentes Netzwerk gebildet, das viele existierende CERTs einbindet und informell einen Teil der Aktivitäten koordiniert. Neue CERT-Infrastrukturen müssen in dieses Umgebung eingebettet werden, um ein effektives und effizientes Arbeiten zu ermöglichen. Gegenstand dieses Kapitels ist neben der Darstellung der entstandenen Strukturen auch die Bewertung, welche Ansätze für die weitere Entwicklung in Deutschland und somit auch für die KMU-CERT-Infrastruktur erfolgreich und richtungsweisend sein können. Zunächst wird als Einstieg jedoch die "Geschichte" der CERTs bis hin zur ersten Kooperation mehrerer Teams dargestellt.

2.1 Die Ursprünge der CERTs

Bereits 1973, als das Internet erst aus 31 Rechnern bestand, existierten drei weithin bekannte Sicherheitsprobleme, die noch heute relevant sind: Passworte, "offene" Adressen und der Anreiz, in Systeme einzubrechen [Salus 1995]. Trotzdem gab es im Internet vor 1987 nur wenige, isolierte Angriffe auf die angeschlossenen Rechner.

Mit der Zahl der angeschlossenen Nutzer und Netze stieg die Zahl der Angriffe und Sicherheitsprobleme. Anfang 1987 schließlich war eine als dramatisch zu bezeichnende Steigerung Anlass, durch organisatorische Ansätze gegen diese Angriffe vorzugehen [Schultz Jr. et al. 1990a].

Bereits damals gab es Diskussionen über den Aufbau von "Incident Response Teams" bei einzelnen Einrichtungen, z. B. für das amerikanische Department of Energy (US DoE). Rick Carr (der später zur NASA wechselte und sich dort ebenfalls auf diesem Gebiet engagierte) schlug ein solches Team vor. Die Idee wurde schnell von anderen staatlichen Einrichtungen aufgegriffen. Zunächst verfolgte man den Gedanken, ein einzelnes Team solle für alle Einrichtungen zuständig sein. Dies wurde später zugunsten mehrerer eigenständiger Teams aufgegeben, um Interessenkonflikte zu vermeiden. Diese Erkenntnis gilt auch heute noch, verspricht doch die Individualisierung eine bessere Ausrichtung auf die betreute Zielgruppe.

Aufgrund von Verzögerungen bei der Aufstellung der Charter sowie anderen Problemen wurde das Team für das DoE, das den Namen "Computer Incident Advisory Capability (CIAC)" erhielt, erst im Frühjahr 1989 gegründet [Schultz Jr. 1990] - nach Gründung des ersten CERTs im Dezember 1988.

Dass sich alle heutigen Computer-Notfallteams als CERT und nicht etwa als CIAC bezeichnen, liegt an der Tatsache, dass im November 1988 Robert T. Morris Jr. von Cornell aus den Internet-Wurm startete [Kossakowski 1992]. Dieser Vorfall machte allen Verantwortlichen unmissverständlich klar, wie empfindlich das Netzwerk als Infrastruktur gegenüber ausgedehnten Angriffen war. Der Internet-Wurm brachte die gesamte netzbasierte Kommunikation für drei Tage zum Erliegen. Dabei wurde deutlich, dass die technischen Probleme (also die Analyse des Angriffs, die Behebung der Schäden sowie die Schließung der Sicherheitslücken) relativ schnell beherrscht werden konnten. Schwierigkeiten ergaben sich aus dem Ausfall des

primären Kommunikationsmediums. Die wenigen Kompetenzzentren (MIT, Berkeley, etc.), die in der Lage waren, Teile der Fehleranalysen und -korrekturen zügig durchzuführen, waren nicht erreichbar und konnten ihre Lösungen nicht verteilen. Gleiche Schwierigkeiten traten bei der Kommunikation und Koordination zwischen den betroffenen Anwendern auf. Außerdem war es aufgrund der fehlenden Koordination unmöglich, die Arbeiten zu verteilen, bzw. die Ergebnisse der Untersuchungen miteinander zu vergleichen. Letzteres wäre insbesondere deswegen wünschenswert gewesen, da einige Gruppen nur Teilaspekte analysiert hatten oder lediglich über eingeschränkte Gegenmaßnahmen verfügten [Scherlis et al. 1990].

Bei einem post mortem Meeting kurz nach dem Vorfall im November 1988 wurde Richard D. Pethia mit dem Aufbau einer Expertengruppe am Software Engineering Institute der Carnegie Mellon University in Pittsburgh, PA, von ARPA[3] als verantwortlicher Stelle für das Internet, beauftragt. Aus dieser kleinen Gruppe entwickelte sich das heutige CERT Coordination Center, das die Keimzelle für weitere Gruppen am Software Engineering Institute bildete und noch heute fast unverändert seiner damaligen Charter folgend agiert:

> The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

War der Internet-Wurm das Ende einer Ära allgemeinen Vertrauens innerhalb des Internets, so war er gleichzeitig der Auslöser für eine wichtige Erkenntnis: Die Sicherheit eines Netzwerkes geht alle angeschlossenen Anwender an. Probleme orientieren sich weder an den althergebrachten Schranken (z. B. den nationalen Grenzen oder der Zuständigkeit einer Einrichtung) noch an den Grenzen zwischen Systemplattformen. Die Gemeinschaft der Anwender ist nur ungenügend auf viele Angriffe oder Probleme vorbereitet. Gerade für das Gebiet der Rechner- und Netzwerksicherheit ist heute ein Spezialwissen notwendig, das nur bei wenigen Experten vorhanden ist. Die Bildung kleiner Gruppen, sogenannter CERTs oder Computer-Notfallteams, die ein solches Spezialwissen aufbauen und dieses ihrer Zielgruppe zur Verfügung stellen, ist darum attraktiv.

Im Laufe der Entwicklung gab es weiterführende Ansätze, um die Arbeit solcher Gruppen international zu koordinieren und zusammenzuführen. Erst diese Zusammenarbeit ermöglicht es, eine Lösung auf die Frage zu finden, wie im internationalen Rahmen angemessen auf die heutige Bedrohung der Systeme und Netzwerke zu reagieren ist [Pethia, van Wyk]. Aus dieser Erkenntnis heraus wurde die Idee des "CERT Systems" entwickelt. Ein erster Schritt hin zu mehr Zusammenarbeit war die Einladung zu einem Workshop über Incident Response und über die Erfahrungen verschiedener Anwender bezüglich der Angriffe und Sicherheitsprobleme im August 1989 [CSIHW 1/1989].

---

[3] Advanced Research Project Agency, mit dessen Fördergeldern das Internet entwickelt wurde.

Nach der erfolgreichen Zusammenarbeit von CERT Coordination Center, CIAC und NASA während des WANK/OILZ-Wurm-Vorfalls im Herbst 1989 kamen die drei Teams in dem folgenden Ziel überein [Schultz Jr. 1991]:

> to form a cooperative effort to freely share information among these response teams, and, if needed, to mutually aid one another during incidents

Dies war der Beginn der bis heute weitgehend informellen Infrastrukturen, auf die im folgenden eingegangen wird.

2.2 Internationale Entwicklung

2.2.1 FIRST

Seit 1992 gibt es FIRST, das internationale Forum von Sicherheits- und Computer-Notfallteams. FIRST fasst mit seinen derzeit 91 Mitgliedern die wichtigsten, international agierenden Teams zusammen, wobei die Mitglieder vor allem aus den USA und Europa stammen. Einige wenige Teams kommen aus Kanada, Australien und dem asiatischen Raum.

Die Aufnahmeprozedur stellt sicher, dass ein existierendes Mitglied als Sponsor für ein neu aufzunehmendes Mitglied eintritt. Dies soll gewährleisten, dass es sich tatsächlich um ein reales Team handelt, dem durch den Sponsor wesentliche Konzepte von FIRST vermittelt werden:

- Vertraulichkeit der in FIRST ausgetauschten Informationen.
- Freigabe der Informationen für die Weitergabe bzw. Veröffentlichung durch den Urheber.
- Kooperation bei Anfragen von anderen Mitgliedern, um Angriffen oder Vorfällen nachzugehen.
- Kooperation bei der technischen Analyse neuer Angriffswerkzeuge.

Bei der Aufnahme spielen die Möglichkeiten der einzelnen Teams keine große Rolle, so dass durchaus relativ kleine Teams (z. B. 2 Personen für eine Universität) mit großen Teams (z. B. 50 Personen beim CERT Coordination Center) gleichberechtigt nebeneinander stehen. Zentrale Bedeutung hat die Verantwortung für eine Zielgruppe, die quasi durch das Team vertreten wird. Gleichermaßen sind auch Hersteller als Mitglieder zu finden, die damit als Ansprechpartner für die jeweiligen Produkte zur Verfügung stehen.

Für jeden Interessierten zugänglich sind die jährlichen Konferenzen, die sich speziell dem Thema "Incident Response" annehmen und viele Mitglieder zum Erfahrungsaustausch zusammenführen. Sensitive technische Entwicklungen, die vielleicht noch nicht allgemein bekannt sind, sowie Fallstudien werden allerdings nicht im Programm dieser Konferenzen diskutiert. Hierfür werden technische Workshops (Technical Colloquium genannt) veranstaltet, an denen nur Mitglieder teilnehmen können.

Es findet keine zentrale Koordinierung von Aktionen der Mitglieder bei Vorfällen oder neuen Angriffswerkzeugen statt. Dies bleibt der Initiative von ad hoc Arbeitsgruppen überlassen, die sich aus einem gemeinsamen Interesse heraus zusammenfinden. Für die Organisation von Workshops und Konferenzen sowie die Pflege der internen Mailinglisten und die Betreuung der Mitglieder gibt es eine Sekretariatsfunktion, die von einem Dienstleister bereitgestellt wird.

Bisher gab es keine Bemühungen, eine Standardisierung der CERT-Tätigkeiten oder der Koordinierung voranzutreiben. Dies mag sich in Zukunft ändern, da vor allem neue Mitglieder Unterstützung bei dem Aufbau geeigneter Strukturen und Prozesse benötigen.

Der Mitgliedsbeitrag für FIRST ist für das Jahr 2001 auf USD 550,00 festgesetzt.

Bewertung: Grundsätzlich ist jedem Computer-Notfallteam oder größerem Sicherheitsteam zu empfehlen, eine FIRST-Mitgliedschaft zu prüfen und anzustreben. Aus der Mitgliedschaft ergeben sich vielfältige Möglichkeiten, die für eine Verbesserung der Dienstleistung und der Betreuung genutzt werden können. Zu betonen sind hier vor allem die Kontakte zu anderen Teams, durch die die Reaktion auf Angriffe und die Aufklärung von Vorfällen erheblich verbessert werden können.

2.2.2 Internet Engineering Task Force (IETF)

Seit 1995 gibt es innerhalb der Internet Engineering Task Force - quasi dem Standardisierungsgremium des "Internets" - eine Arbeitsgruppe, die sich mit der Dienstleistung von Computer-Notfallteams beschäftigt. Ziel war es, für die Anwender das Angebot eines bestimmten Teams transparenter zu gestalten. Ergebnis war mit dem RFC 2350 ein als "Best Current Practice" eingestuftes Dokument, das ein Format für eine angemessene Beschreibung vorgibt.

Inzwischen haben verschiedene - vor allem kommerziell agierende - Teams diese Art der Beschreibung aufgegriffen. Hier sind z. B. das deutsche dCERT (ein Service der debis IT Security Services GmbH) und das dänische CSIRT.DK (ein Service der TeleDanmark) zu nennen.

Mehrere Initiativen (siehe dazu z. B. Abschnitt 2.3.3) bauen ebenfalls auf diesem RFC auf, um möglichst aussagekräftige Informationen über Computer-Notfallteams zu sammeln.

Bewertung: Grundsätzlich ist jedem Computer-Notfallteam oder größerem Sicherheitsteam zu empfehlen, seine Dienstleistung angemessen zu dokumentieren und der betreuten Zielgruppe darzulegen. Insbesondere wenn es sich um extern angebotene Dienstleistungen handelt, bietet sich ein Format nach dem RFC 2350 als state-of-the-art an.

2.2.3 International Standardization Organization (ISO)

In der Vergangenheit gab es verschiedene Vorstöße, um Arbeitsgruppen für das Thema CERT zu etablieren. In der Regel gab es sehr unterschiedliche Auffassungen, ob und wie ein solches Thema behandelt werden sollte, u. a. auch deswegen, weil dieses Thema sehr stark durch die Arbeit der CERTs definiert ist

und bisher keine Zusammenarbeit mit CERTs zustande kam. Zur Zeit gibt es daher keine relevanten Dokumente.

Bewertung: Für eine umfassende und an der Praxis orientierten Behandlung des Themas wäre eine Zusammenarbeit der ISO mit bestehenden CERTs wünschenswert.

2.3 Europäische Entwicklung

2.3.1 Informelle Arbeitsgruppen

Informelle Arbeitsgruppen europäischer Teams haben seit 1993 eine lange Tradition. Zunächst wurden diese Treffen von europäischen Forschungsnetzen getragen, später kamen vor allem FIRST-Mitglieder aus dem kommerziellen Bereich hinzu.

Immer noch haben die Forschungsnetze einen großen Einfluss. Durch die TERENA[4] Task Force CSIRT werden zweimal pro Jahr jeweils zweitägige Treffen organisiert, die grundsätzlich allen interessierten Teams offen stehen.

In der Folge hat die Task Force auch die Definition der "Trusted Introducer" Dienstleistung initiiert (siehe dazu 2.3.3). Des weiteren wird versucht, innerhalb der Task Force gemeinsame Probleme zu diskutieren und anzugehen, oder aber Entwicklungen von gemeinsamen Interesse voranzutreiben. Einen großen Raum nimmt der Erfahrungsaustausch ein, wobei einzelne Teams über ihre Erfahrungen mit Dienstleistungen, Angriffen, Hilfsmitteln, etc. berichten.

Bewertung: Für Teams, die als internationaler Ansprechpartner für ihre Zielgruppe auftreten, empfiehlt sich die Teilnahme an den Sitzungen der Task Force CSIRT.

2.3.2 EuroCERT

Nach langen Diskussionen, die 1995 begannen, wurde 1997 das EuroCERT als europäisches Koordinierungszentrum ins Leben gerufen. Die Finanzierung wurde durch mehrere Forschungsnetze sichergestellt. Bereits beim Start der Dienstleistung gab es verschiedene Probleme:

- Die bestehenden Teams empfanden die Einbeziehung einer weiteren Instanz als lästig und überflüssig. Da bereits etablierte Kontakte untereinander bestanden, war jede zentrale Koordinierung unnötig.
- Durch das EuroCERT wurden Dienstleistungen existierender Teams kopiert. Verschiedene Teams befürchteten daher, dass das zentrale EuroCERT[5] ihre eigenen Dienstleistungen überflüssig machen würde oder zumindest ihre Finanzierung gefährden könnte.
- Es gab kein Konzept für die Darstellung des Mehrwerts, den die einzelnen Teams durch die Arbeit des EuroCERTs hätten gewinnen können.

---

4 Trans-European Research and Education Networking Association, http://www.terena.nl.

5 Bereits diese Namenswahl war unglücklich, EuroCERT Coordination Center wäre angemessener gewesen.

- Da neue Teams beim Aufbau nicht begleitet wurden und deren Aufbau nicht gefördert wurde, blieb die Anzahl der Teams, die für die Dienstleistung zu zahlen bereit war, gering.

Da diese Probleme auch in der Folge nicht gelöst werden konnten, wurde das Projekt schließlich 1999 eingestellt.

Bewertung: Eine zentrale Koordinierung von Computer-Notfallteams ist nur notwendig, wenn diese Koordinierung nicht - wie z. B. in Deutschland - auf informeller Ebene geleistet werden kann. Da es bei der Koordinierung nicht um ein Kopieren einer bestimmten Dienstleistung auf "höherem" Niveau geht, muss hierfür zudem zunächst ein sehr fein abgestimmtes Konzept entwickelt werden.[6] Aufgrund der bereits erfolgten Positionierung vorhandener Teams müssen weiterhin Veränderungen für diese Teams in eine Betrachtung miteinbezogen werden.

2.3.3 Trusted Introducer

Nach der Einstellung des EuroCERTs gab es seitens der europäischen Teams eine Skepsis bezüglich großer Projekte, die gleichzeitig alle offenen Probleme lösen sollten. Statt dessen wurden verschiedene Dienstleistungen und Anforderungen identifiziert, die einerseits eine Verbesserung der Gesamtsituation bedingen würden und andererseits mit begrenzten Mitteln erfüllt werden können. In der Folge wurde die informelle Zusammenarbeit wieder gestärkt. Eine Dienstleistung jedoch wurde als wichtig erkannt, die eine ständige Präsenz bedingt: Das europäische Verzeichnis bekannter Computer-Notfallteams.

Das Verzeichnis wird von dem sogenannten "Trusted Introducer" im Auftrag von TERENA gepflegt. Das Konzept beruht auf einem Prozess, der die Informationen über alle bekannten (als "Level 0" oder auch "known" bezeichneten) Teams zusammenführt. Diese sind über die Web-Site http://www.ti.terena.nl öffentlich zugänglich und werden ständig aktualisiert.

Durch eine Akkreditierung kann ein Team erreichen, dass es als "Level 2" eingestuft wird. Hierzu muss das Team eine definierte Menge von Informationen liefern und zusichern, diese aktuell zu halten, d. h. Änderungen zu melden. Des weiteren muss sich das Team verpflichten, die vertrauliche Kommunikation mit anderen Teams zu gewährleisten. Level 2 Teams sind aufgefordert, ihre Dienstleistungen auf Basis des RFC 2350 zu beschreiben.

Ein Review Board bestehend aus Repräsentanten der Level 2 Teams überwacht die Arbeit des Trusted Introducers. Die Bearbeitungsgebühr für den Schritt zum Level 2 Team wurde auf EURO 450,00 festgelegt, der jährliche Beitrag für Level 2 Teams auf EURO 600,00.

Bewertung: Grundsätzlich ist jedem europäischem Computer-Notfallteam oder größerem Sicherheitsteam zu empfehlen, sich in das Verzeichnis aufnehmen zu lassen. Insbesondere wenn es sich um extern angebotene Dienstleistungen handelt,

[6] Es gibt zur Zeit weder ein Beispiel für eine solche Dienstleistung, noch liegt eine Spezifikation einer solchen Dienstleistung vor, die als Grundlage herangezogen werden könnte. Hier gibt es noch einen erheblichen Bedarf für weitere Arbeiten, bevor ein konsensfähiges Konzept vorgelegt werden kann.

deren Qualität demonstriert werden soll und bei denen viele Kontakte mit anderen Teams zu erwarten sind, empfiehlt sich eine Einstufung als Level 2.

2.3.4 Entwicklungstendenzen in verschiedenen europäischen Ländern

Die ursprüngliche Idee, die 1995 durch eine Arbeitsgruppe zur Frage einer europäischen CERT-Koordinierung dokumentiert wurde, beruhte auf dem Konzept einer horizontalen Struktur: nationale Teams sollten dabei auf europäischer Ebene koordiniert werden. Begründung für diese Betonung der nationalen Teams war vor allem:

- Da eine Betreuung und Unterstützung auch rechtliche Gesichtspunkte adressieren muss, ist dies am ehesten auf nationaler Ebene zu gewährleisten.
- Die nationalen Besonderheiten - Kultur und Sprache - müssen berücksichtigt werden, damit eine Akzeptanz gewährleistet und eine angemessene Betreuung möglich wird.

Traditionell wurden die ersten Teams von nationalen Forschungsnetzen aufgebaut, wobei es eher zufällig zu zwei durch den Namen geprägten Ansätzen kam: Die Konzentration der Dienstleistung auf ein konkretes Forschungsnetz (wie beim DFN-CERT) oder die Betonung einer nationalen Zuständigkeit (wie beim CERT-IT). Während die erste Variante, die vor allem in Ländern mit sehr großen Nutzerzahlen auftritt, Raum für die Gründung weiterer überregionaler Teams ließ, besetzte der zweite Ansatz diesen Raum. Die Erfahrung zeigt, dass eine einmal eingenommene Position bisher nicht aufgegeben oder verändert wurde.

In dem Moment, wo ein weiteres überregionales Team gegründet wurde, z. B. das BSI-CERT für die deutsche Bundesverwaltung, stellte sich zwangsläufig die Frage, wie die Arbeit zwischen den beiden Teams koordiniert werden kann. Hier kam es dann in der Regel zu einvernehmlichen Absprachen und informellen Vorgehensweisen.

Inzwischen setzt sich die Erkenntnis durch, dass in der Regel ein nationales Team nicht ausreicht. Vielmehr sind Teams auf verschiedenen Ebenen mit speziellen Zielrichtungen notwendig:

1. Institutionen und Unternehmen müssen die Fähigkeit zur Bewältigung von Angriffen und Vorfällen in ihr Sicherheitsmanagement integrieren.
2. Größere Institutionen und Unternehmen sollten zur Unterstützung diese Funktionen in einem eigenen Team institutionalisieren.
3. Institutionen und Unternehmen, die gleiche Interessen und Sicherheitsanforderungen haben, sind eher bereit, eine übergreifende Koordinierung mit dem notwendigen Informationsaustausch zu akzeptieren, die den gemeinsamen Interessen Rechnung trägt.

   Bereiche, die traditionell unterschieden werden können, sind: Militär, Verwaltung, Banken, Industrie sowie Forschung und Ausbildung. Hier ist die Erstehung übergreifender Teams folgerichtig bereits erfolgt oder zu erwarten.
4. Eine wirklich nationale Koordinierung ist nur dann notwendig, wenn bereits viele Teams national agieren und zusammen mit den führenden Teams diese Rolle

definiert wird. Hier stellen sich übrigens die gleichen Probleme, wie die auf europäischer Ebene (s. Abschnitt 2.3.2).

Inzwischen existieren z. B. in Großbritannien und Frankreich jeweils mehrere Teams auf nationaler Ebene sowie für verschiedene Unternehmen. Eine nationale Koordinierung ist bisher jedoch nicht etabliert.

Die zu beobachtende vertikale Strukturierung anhand der Zielgruppen hat zusätzlich Auswirkungen auf die internationale Zusammenarbeit. Parallel zu der nationalen Koordinierung verschiedener Zielgruppen gewinnt die internationale Koordinierung einer Zielgruppe an Bedeutung. Es liegt nahe, dass es eine große inhaltliche Nähe z. B. aller Banken in Europa gibt, die den Grund für die Zusammenarbeit darstellt.

Bewertung: Aufgrund der erfolgreichen Etablierung von CERTs in Deutschland für die Bundesverwaltung sowie für das nationale Forschungsnetz wird es nicht ein einziges CERT geben, das seine Dienstleistung allgemein anbietet und alle möglichen Zielgruppen abdeckt. Dies ist zudem durch die Zahl der miteinander vernetzten Rechner und Netze unwahrscheinlich, da sich quasi in allen größeren Nationen (z. B. USA, Kanada, Deutschland, Großbritannien, Frankreich) verschiedene CERTs für verschiedene Zielgruppen - Wirtschaft, Forschung, Verwaltung und Militär - herausbilden.

2.3.5 Vorschläge der europäischen Gemeinschaft

In einem Perspektivpapier [KOM(2001)298] in Vorbereitung des weiteren Vorgehens auf europäischer Ebene zur Verbesserung der Sicherheit von Netzwerken und Informationen wurden bereits Maßnahmen vorgeschlagen, die für das CERT-Umfeld relevant sind, insbesondere der Aufbau eines europäischen Warn- und Informationssystems. Dieses beruht auf dem Informationsaustausch zwischen den einzelnen Teams und ermöglicht vor allem eine Sammlung relevanter Informationen, deren Analyse und daraus wiederum die Ableitung adäquater Aktionen.

Bewertung: Für jedes auf nationaler Ebene agierende Team stellt die Mitarbeit an der Realisierung dieser Perspektive eine Herausforderung dar. Zugleich werden durch die Umsetzung der vorgeschlagenen Maßnahmen eventuell auch Anforderungen an die Gestaltung einzelner Dienstleistungen gestellt.

2.4 Entwicklungstendenzen auf nationaler Ebene

In Deutschland zeigen verschiedene Entwicklungen seit Herbst 2000 das weiter steigende Interesse an der Thematik:

- Im Rahmen der Initiative D21 hat sich eine Arbeitsgruppe zum Thema "CERT.DE" zusammengefunden.
- Das BSI ist mit den Planungen für die Erweiterung des BSI-CERTs zu einem CERT-BUND befasst.
- Der BITKOM hat in einem "Fachausschuss CERT" Vorarbeiten des Jahres 2000 fortgesetzt.
- Mit der Deutschen Telekom AG hat ein weiterer großer Konzern begonnen, ein internes CERT aufzusetzen.

Durch diese Aktivitäten wird auch allgemein das Bewusstsein für CERT-Dienstleistungen verstärkt und Interesse daran geweckt.

Seit etwa 1996 wurden informell Treffen deutscher CERTs durch verschiedene Teams organisiert. Diese dienten vor allem der Verbesserung des Kontakts zu neu etablierten Teams und der Diskussion verschiedener Aspekte, die für Deutschland spezifisch sind. Es ist zu erwarten, dass auch in Zukunft diese Treffen von Freiwilligen organisiert werden.

3 Dienstleistungen im Rahmen einer KMU-CERT-Infrastruktur

Die Definition der im Rahmen einer KMU-CERT-Infrastruktur zur erbringenden Dienstleistungen wirft zwei Fragen auf: welche Dienstleistungen sollen erbracht werden und für wen sollen diese erbracht werden?

Nur durch die Verknüpfung der speziellen Eigenschaften und Anforderungen der Zielgruppe mit der Gesamtmenge an möglichen CERT-Dienstleistungen lässt sich ein spezielles Dienstleistungsangebot definieren, das auf die Zielgruppe zugeschnitten ist.

3.1 KMUs in Deutschland

Zielgruppe für die Dienstleistungen im Rahmen einer KMU-CERT-Infrastruktur sind die KMUs in Deutschland.[7] Um diese Gruppe näher zu definieren, dient z. B. ein Bericht des "Instituts für Mittelstandforschung (IfM) Bonn". Dort werden KMUs u. a. definiert durch:

- Zahl der Beschäftigten: klein (bis 9), mittel (10-499).
- Umsatz in DM/Jahr: klein (unter 1 Million), mittel (1-100 Millionen).

Der Mittestand, der als Summe der kleinen und mittleren Unternehmen definiert ist, bestand in Deutschland im Jahr 1999 aus rund 3,2 Millionen Unternehmen mit gut 20 Millionen Beschäftigten.

Die IT-Ausstattung des Mittelstands ist aufgrund der großen Spannweite an Unternehmen sehr heterogen. Sie reicht von Unternehmen mit nicht vorhandener bzw. minimaler IT-Ausstattung (Einzel-PC) bis zu Unternehmen mit Hunderten von Endgeräten.[8] Das gleiche spiegelt sich auch im Vernetzungsbereich wider. In vielen Unternehmen gibt es nur "stand-alone" Systeme, während in anderen eine umfassende interne (Intranet) und externe (Internet) Vernetzung besteht.

Aus dieser Situation leitet sich auch direkt ab, dass das Bewusstsein für Maßnahmen der IT-Sicherheit im allgemeinen und für CERT-Dienstleistungen im speziellen sehr unterschiedlich ausgeprägt ist. Viele Unternehmen führen in dieser Richtung keine Vorkehrungen durch, während andere zumindest grundlegende Maßnahmen (Backup, Virenschutz, etc.) ergreifen. Dritte wiederum haben ganze Abteilungen, die sich mit Fragestellungen der IT-Sicherheit befassen.[9] Insgesamt kaum ausgeprägt ist jedoch die sich aus dem CERT-Konzept ergebende Erkenntnis, dass trotz aller Schutzmaßnahmen Vorfälle auftreten werden. Folglich gibt es in der

---

7 Bzgl. der Rolle und Bedeutung der KMUs vergleiche z. B. http://www.ifm-bonn.de sowie die Informationen des BMWi unter http://www.bmwi.de.

8 Nach Einschätzung des BITKOM setzen kleine und mittlere Unternehmen fast ausschließlich PCs und Software ein, die auf Windows und Linux basieren.

9 Es gibt auch Unternehmen, deren Unternehmenszweck ausschließlich die IT-Sicherheit darstellt oder die zumindest Dienstleistungen in diesem Bereich anbieten. Allerdings gelten auch für diese Unternehmen die hier gemachten Aussagen, wenn auch das Vorhandensein eines angemessenen Problembewusstseins bei diesen nicht in Frage gestellt werden muss.

Praxis auch kaum Prozesse, die beschreiben, wie mit solchen Ereignissen umgegangen werden sollte.

Die im Rahmen einer KMU-CERT-Infrastruktur zu erbringenden Dienstleistungen sind nur für die Unternehmen relevant, die über eine IT-Ausstattung verfügen. Je umfangreicher diese Ausstattung ist, desto nachhaltiger kann die Unterstützung durch die KMU-CERT-Infrastruktur genutzt werden. Für die Nutzung ist darüber hinaus die Identifikation verantwortlichen Personals notwendig, das z. B. sicherheitskritische Informationen und konkrete Maßnahmenvorschläge erhalten soll, die dann vor Ort im Unternehmen umgesetzt werden können.

3.2 Überblick generischer CERT-Dienstleistungen

Als in den 90er Jahren verstärkt CERTs gegründet wurden, entwickelten sich auch die von Ihnen angebotenen Dienstleistungen. Aufgrund der starken Dynamik in diesem Bereich ist eine vollständige, abschließende Darstellung aller Dienstleistungen nicht möglich. Trotzdem liegen mittlerweile Klassifikationsschemata vor, z. B. in [Kossakowski 2000]. Dort werden insgesamt 22 generische Dienstleistungen definiert, die für CERTs konkret relevant sind und die für die Zusammenstellung eines spezifischen Angebots genutzt werden können.

Grundsätzlich können CERT-Dienstleistungen in folgende drei Bereiche unterteilt werden:

- Reaktive Dienstleistungen.
- Präventive (proaktive) Dienstleistungen.
- Dienstleistungen für das Security Quality Management.

In der Realität ist jeder Dienstleistung ein dazugehöriger Dienstprozess zugeordnet, durch den die jeweilige Aufgabe realisiert wird. Die Definition eines Dienstprozesses besitzt dabei ein hohes Abstraktionsniveau, d. h. erst durch die Gestaltung in Subprozesse und die Zuordnung realen Personals und konkreter Verfahren wird eine angepasste Implementierung möglich. Je nach den zur Verfügung stehenden Möglichkeiten, Ressourcen und Rahmenbedingungen gilt es, effiziente und den Parametern der Anwendungsumgebung möglichst weitgehend angepasste Implementierungen zu identifizieren.

3.3 CERT-Dienstleistungen für KMUs in Deutschland

Die Spezifikation eines KMU-CERT Dienstangebotes darf nicht "wissenschaftlich" erfolgen, sondern muss pragmatisch an den tatsächlichen Bedürfnissen ausgerichtet sein.

Um sich darüber hinaus flexibel auf verschiedene Finanzierungskonzepte einstellen zu können, ist es sinnvoll, die Gesamtmenge aller Dienstleistungen in zentrale Basisdienstleistungen, erweiterte Basisdienstleistungen und Zusatzdienstleistungen zu unterteilen. Das Zusammenspiel dieser drei Komponenten zeigt Abbildung 3-1.

Unter **zentralen Basisdienstleistungen** werden alle CERT-Dienstleistungen zusammengefasst, die die notwendige Basis für eine erfolgreiche Etablierung der KMU-CERT-Infrastruktur darstellen. Ihre Realisierung ermöglicht es der Zielgruppe, die Sicherheit im Unternehmen zu verbessern. Durch die zentralen

Basisdienstleistungen alleine wird jedoch noch keine vollständige CERT-Dienstleistung angeboten.

Dies geschieht erst durch die zusätzliche Realisierung der **erweiterten Basisdienstleistungen**. Diese umfassen insbesondere die Unterstützung und Koordinierung bei der Reaktion auf Angriffe und bei der Bewältigung von Vorfällen. Die Gesamtmenge der Basisdienstleistungen (zentrale und erweiterte) stellt somit das (minimale) Angebot eines echten CERTs dar.

Wie in Abschnitt 3.2 angesprochen, gibt es darüber hinaus eine Reihe von **Zusatzdienstleistungen**, die in einer KMU-CERT-Infrastruktur erbracht werden können. Welche dieser Zusatzdienstleistungen letztendlich realisiert werden, hängt u. a. von den Anforderungen der Zielgruppe ab.

Die Zusatzdienstleistungen stellen wünschenswerte Ergänzungen des Basisdienstleistungskatalogs dar. Sie erhöhen den Gesamtnutzen bei den KMUs sukzessiv: je mehr Zusatzdienstleistungen etabliert werden, desto größer ist der Nutzen für die Zielgruppe.

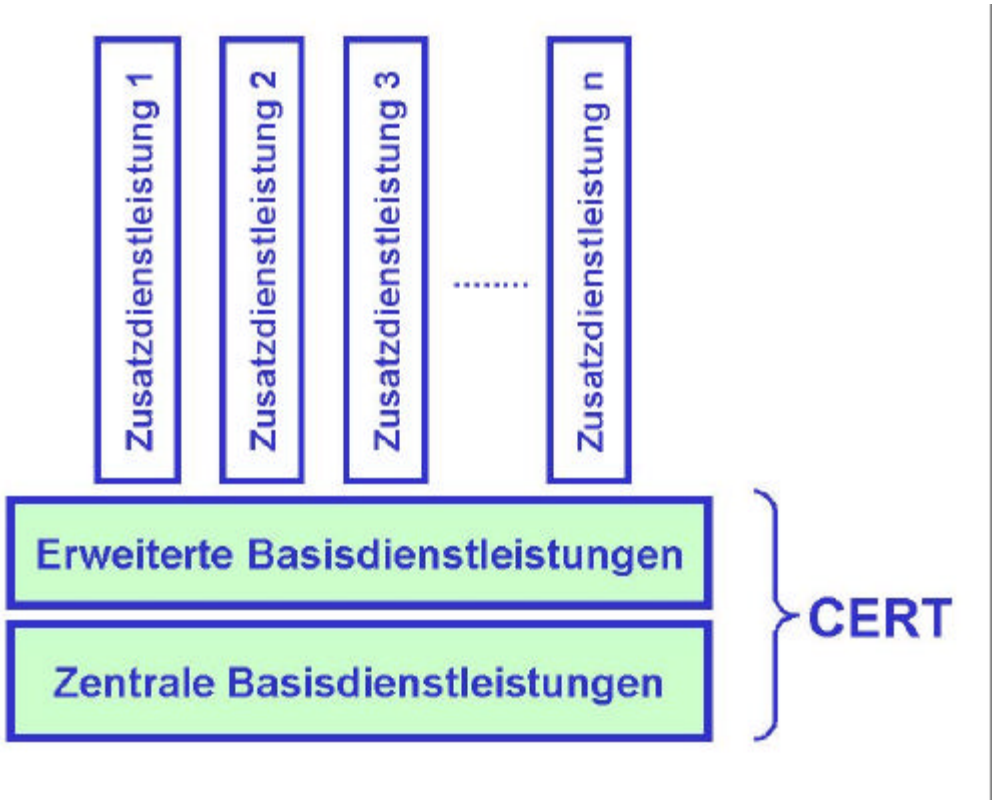

Abbildung 3-1: Struktur der verschiedenen Dienstleistungen

Der Vorteil dieses mehrstufigen Realisierungskonzeptes ist insbesondere aus finanzieller Sicht offensichtlich. Zum einen stellt der benötigte Aufwand zur Realisierung der Basisdienstleistungen eine untere Schranke bezüglich der Kosten zum Aufbau einer KMU-CERT-Infrastruktur dar: Stehen nur geringere Mittel zur Verfügung, z. B. nur für die zentralen Basisdienstleistungen, so kann der Zielgruppe zwar immer noch eine sinnvolle Hilfestellung zur Verbesserung der Unternehmenssicherheit angeboten werden, es wird jedoch keine CERT-

Dienstleistung im eigentlichen Sinne erbracht. Zum anderen können die nach Finanzierung der Basisdienstleistungen freien Mittel für die Realisierung von Zusatzdienstleistungen verwendet werden. Die Entscheidung, welche Zusatzdienstleistungen realisiert werden sollen, beruht nicht zuletzt auf der Einschätzung der Zielgruppe selbst und sollte daher in enger Abstimmung mit ihr erfolgen. Diese Abstimmung wird wiederum durch die zentralen Basisdienstleistungen, innerhalb derer die Kommunikation zu der Zielgruppe aufgebaut und gefördert wird, ermöglicht.

Durch diese stufenweise Vorgehensweise gibt es einen Migrationspfad von einem minimalen hin zu einem modular erweiterbaren Dienstleistungsangebot.

Eine Darstellung der für die KMU-CERT-Infrastruktur zu erbringenden Basis- und Zusatzdienstleistungen wird in den folgenden Abschnitten beschrieben.

Dabei stellen alle Basis- und Zusatzdienstleistungen Querschnittsdienstleistungen dar, die potentiell der gesamten Zielgruppe (1:n) zu Gute kommen. Das Angebot von unternehmensspezifischen Dienstleistungen (1:1), z. B. Vor-Ort-Betreuung, Security Audit, Intrusion Detection, Security Consulting, ist nicht enthalten. Somit stellt das dargestellte Dienstleistungsangebot keine Konkurrenz für am Markt vertretene Anbieter dar, die im 1:1 Geschäft tätig sind.

3.3.1 Zentrale Basisdienstleistungen

Die zentralen Basisdienstleistungen umfassen insbesondere Aktivitäten, die für die Erschließung der Zielgruppe sowie die Schaffung organisatorischer Strukturen erforderlich sind. Darüber hinaus wird hierdurch die Bereitstellung eines umfassenden Informationsangebotes sichergestellt und die Basis für ein vollständiges CERT-Angebot gelegt. Für die KMU-CERT-Infrastruktur lassen sich folgende zentrale Basisdienstleistungen (B1-B4) erkennen.

- **B1: Integration der KMU-CERT-Infrastruktur in das nationale und internationale Umfeld**
  - B1.1: Aufbau und Pflege der Mitgliedschaft in internationalen CERT-Strukturen. Dies beinhaltet neben dem Erwerb der FIRST-Mitgliedschaft (siehe Abschnitt 2.2.1) auch die Registrierung beim europäischen CERT-Verzeichnis (siehe Abschnitt 2.3.3).
  - B1.2: Integration in die nationale CERT-Infrastruktur. Neben der fachlichen und organisatorischen Koordinierung mit nationalen CERTs, beinhaltet dies auch einen "Roundtable" speziell mit CERTs aus dem Industrie- und Wirtschaftsbereich.

- **B2: Maßnahmen zur Erschließung der Zielgruppe**
  - B2.1: Zunächst muss das Konzept der KMU-CERT-Infrastruktur der Zielgruppe erläutert und bekannt gemacht werden. Dies kann z. B. durch Vorträge oder Rundschreiben erfolgen. Ein Ziel ist es, (insbesondere elektronische) Kommunikationswege zu den Unternehmen und verantwortlichen Personen zu etablieren.

- B2.2: Unter dem Stichwort "Awareness Building" sind Tätigkeiten zu verstehen, die bei der Zielgruppe die (Weiter)Entwicklung des Bewusstseins für Sicherheitsprobleme allgemein und im Vorfallsbereich im speziellen befördern. Darüber hinaus wird das Verständnis für Arbeiten im Rahmen der KMU-CERT-Infrastruktur entwickelt. Zu diesem Zweck ist die Durchführung von Vorträgen und Informationsveranstaltungen erforderlich.
- B2.3: Um in direkten Kontakt mit der Zielgruppe zu treten und um die Anforderungen detailliert erarbeiten zu können, sollte einmal pro Jahr ein Workshop durchgeführt werden. Dieser ermöglicht es, alle Beteiligten zusammenzubringen und wichtige Fragestellungen ausführlich zu diskutieren.

- **B3: Aufbau und Betrieb einer internen und externen Kommunikations- und Informationsinfrastruktur**
  - B3.1: Aufbau und Betrieb einer gesicherten technischen Infrastruktur. Als Plattform für die gesamte Kommunikation im Rahmen der KMU-CERT-Infrastruktur muss eine technische Basisstruktur geschaffen werden. Dies beinhaltet z. B. den Betrieb von Servern sowie eine Anbindung dieser Systeme an das Internet. Gleichzeitig muss diese Infrastruktur so gesichert werden, dass sie möglichen Angriffen Stand halten kann.
  - B3.2: Aufbau und Pflege eines WWW-Angebotes. Ein aktuelles, auf die Anforderungen der Zielgruppe zugeschnittenes WWW-Angebot ist ein wichtiger Faktor bei der Realisierung der KMU-CERT-Infrastruktur. Dieses Angebot muss neben allgemeinen Informationen auch pressespezifische Darstellungen enthalten ("Pressroom"). Als Inhalte sind weiterhin Ankündigungen von Veranstaltungen oder Hersteller- und Anbieteradressen sinnvoll. Durch Entwurf eines Logos und einer Tagline können Sichtbarkeit und Einprägsamkeit der KMU-CERT-Infrastruktur in der Zielgruppe und in der Öffentlichkeit erhöht werden.
  - B3.3: Betrieb einer Kommunikationsinfrastruktur für allgemeine Anfragen. Sobald die KMU-CERT-Infrastruktur einen gewissen Bekanntheitsgrad erreicht hat, wird eine Reihe von Anfragen auf diese zukommen. Um damit umzugehen, ist der Aufbau von Telefon-, Fax- und Email-Kontaktmöglichkeiten zu realisieren. Außerdem müssen eingehende Anfragen zeitnah beantwortet werden.
  - B3.4: Aufbau und aktive Moderation einer Mailingliste für Sicherheitsfragen. Zusätzlich zur Beantwortung allgemeiner Anfragen muss ein Forum zur Durchführung sicherheitsrelevanter Diskussionen geschaffen werden. Dies erfolgt sinnvollerweise durch eine moderierte Mailingliste, um potentiellen Missbrauch auszuschließen. Offene Fragestellungen müssen dabei beantwortet werden.
  - B3.5: Statistiken und Reporting. Die Angabe von Kennzahlen über die erbrachten Leistungen stellt eine wichtige Information über die Entwicklung der Akzeptanz der KMU-CERT-Infrastruktur dar. Darüber

hinaus ist dies auch eine Möglichkeit zur Darlegung der Aufgabenerfüllung. Dabei kann es sich z. B. um Informationen über die Anzahl der registrierten Unternehmen, der Web-Hits oder der ausgetauschten Mails handeln.[10]

- B3.6: Erstellung eines monatlichen Newsletters. Um die Zielgruppe über aktuelle Entwicklungen im CERT-Umfeld zu informieren, ist die Erstellung und Verteilung eines monatlichen Newsletters sinnvoll. Dieser stellt außerdem die wichtigsten Sicherheitsupdates vor, so dass auch nicht technisch orientierte Leser elementare Schutzmaßnahmen treffen können.
- B3.7: Einführung einer Austauschstelle für Vorfallsinformationen. Auf Basis der Informationen über die Zielgruppe wird eine Datenbank der Ansprechpartner aufgebaut und kontinuierlich gepflegt. Diese kann genutzt werden, um unternehmensspezifische Informationen direkt an die Betroffenen weiterzuleiten und erlaubt auch die Etablierung von Zugangsbeschränkungen zu den Dienstleistungen, die verhindern, dass nicht als KMU einzustufende Entitäten den Service nutzen können.

- **B4: Interaktion mit den erweiterten Basisdienstleistungen**
  - B4.1: Definition der erweiterten Basisdienstleistungen. Auf Basis der Anforderungen, die sich aus der Diskussion mit der Zielgruppe ergeben, müssen die erweiterten Basisdienstleistungen so definiert werden, dass auf dieser Basis deren konkrete Implementierung erfolgen kann.
  - B4.2: Laufende Kontrolle der erweiterten Basisdienstleistungen. Nachdem mit der Implementierung der erweiterten Basisdienstleistungen begonnen wurde, muss deren Qualität regelmäßig überwacht werden.

3.3.2 Erweiterte Basisdienstleistungen

Durch die Realisierung der erweiterten Basisdienstleistungen erfolgt eine Erweiterung der zentralen Basisdienstleistungen hin zu einem vollständigen CERT-Dienstleistungspaket. Die beiden folgenden erweiterten Dienstleistungen (EB1-EB2) sind daher für die KMU-CERT-Infrastruktur mittelfristig unbedingt erforderlich. Da sie jedoch auch von den aufgebauten zentralen Basisdienstleistungen abhängen, ist eine spätere Aufnahme der Dienstleistungen akzeptabel.

[10] An dieser Stelle sei gleich vor einer Konzentration auf die Zahl der bearbeiteten Vorfälle gewarnt. Weder können solche Zahlen ohne weitere Abschätzungen Aufschluss über die Bedrohung an sich liefern, noch sagt die Zahl der bearbeiteten Vorfälle etwas über die Qualität oder Angemessenheit der Betreuung aus.

- **EB1: Sicherheitsbulletins über neue Schwachstellen und Patches**

  Durch die Sammlung und Aufbereitung von Informationen über neue Schwachstellen sowie durch Auswertung wichtiger Informationsquellen werden Sicherheitsbulletins erstellt. Die Zielgruppe sollte dabei die Möglichkeit haben, sich einen z.B. über eine Web-Schnittstelle individuell konfigurierbaren Ausschnitt dieser Informationsmenge regelmäßig und zeitnah zustellen zu lassen.

- **EB2: Unterstützung und Koordinierung bei der Reaktion auf Angriffe und bei der Bewältigung von Vorfällen**

  Die Unterstützung von Unternehmen beim Umgang mit Angriffen und Vorfällen stellt eine wichtige Dienstleistung dar. Die Erfahrung zeigt, dass viele Angriffe und Vorfälle durch andere Parteien zuerst beobachtet und gemeldet werden. Solche Informationen werden dann an entsprechende Kontakte in den Unternehmen weitergeleitet. Ergänzt werden muss diese Dienstleistung durch die Koordinierung verschiedener Parteien, die von einem Vorfall direkt oder indirekt betroffen sind sowie durch den Informationsaustausch mit anderen CERTs.

3.3.3 Zusatzdienstleistungen

Die Menge der möglichen Zusatzdienstleistungen ist umfangreich. Welche davon letztendlich realisiert werden, hängt im wesentlichen von den konkreten Anforderungen der Zielgruppe sowie den zur Verfügung stehenden finanziellen Ressourcen ab.

Aus Sicht einer KMU-CERT-Infrastruktur bieten sich die folgenden Zusatzdienstleistungen als besonders wirkungsvoll an:

- **Z1: Training und Schulung**

  Zum Verständnis der immer komplexer werdenden Sicherheitslösungen ist eine theoretische Wissensbasis erforderlich. Die Erfahrungen aus der Praxis eines CERTs können zur Verbesserung der fachlichen Kenntnisse genutzt werden, indem genau diese Orientierung vorgenommen wird. Die praktische Auseinandersetzung mit Angriffswerkzeugen, realen Angriffen und nachgestellten Situationen kann die zu fordernde Realitätsnähe herstellen.

- **Z2: Aufbau einer Vorfalls-Datenbank**

  Durch die Bereitstellung von (anonymisierten) Vorfallsinformationen in einer Datenbank können Unternehmen sich Informationen beschaffen, die beim Eintreten eines eigenen, ähnlich gelagerten Vorfalls direkt nutzbar sind. Zugleich können vorbeugende Maßnahmen anhand realer Szenarien überprüft und eventuell angepasst werden.

- **Z3: Bearbeitung von sicherheitsrelevanten Anfragen**

  Die Bearbeitung von sicherheitsrelevanten Anfragen ist eine wichtige Aufgabe. Hierdurch wird zum einen die Verbreitung von Informationen sichergestellt. Zum anderen ergibt sich aus dem Eingang der Fragen eine Art Vorwarnfunktion. Diese erstreckt sich nicht nur auf mögliche Hinweise, die auf Vorfälle hindeuten, sondern auch auf die Interessenslage bei denjenigen, die die Dienstleistung nutzen. Ziel der Beantwortung der Anfragen muss es sein, ein gesteigertes Bewusstsein zu schaffen und Informationen zu verteilen, die sich positiv auf die Sicherheit auswirken, d. h. präventive Maßnahmen fördern und empfehlen.

Diese Liste lässt sich - insbesondere nach besserer Kenntnis der Anforderungen der Zielgruppe - erweitern. Es gibt jedoch auch einige mögliche Zusatzdienstleistungen, von denen aus heutiger Sicht abzuraten ist, da Aufwand und Nutzen in einem erheblichen Missverhältnis stehen. Dies betrifft z. B. das Angebot eines 24/7-Services, da die Zielgruppe in der Mehrzahl der Fälle nicht selbst über entsprechende Voraussetzungen für dessen Nutzung verfügen wird. Nichts desto trotz kann sich im Verlauf des Vorhabens zeigen, dass durch zur Zeit nicht abschätzbare Entwicklungen auch ein solcher Dienst in die Menge der Zusatzdienstleistungen aufgenommen werden sollte.

Bei den meisten Dienstleistungen ist eine Definition eines Service-Level nur schwer möglich. Klar ist jedoch, dass die Qualität der Dienstleistungen angepasst werden muss, wenn die Menge der Anfragen zunimmt und die Ressourcen fix sind. Wenn dies nicht geschieht, kann für eine Übergangszeit durch starkes Engagement des Personals die Leistung aufrecht erhalten werden, dann allerdings wird eine Fortführung unter den gleichen Bedingungen nicht mehr möglich sein. Dies könnte, wenn es nicht rechtzeitig erkannt und adressiert wird, den Nutzen insgesamt gefährden.

4 Implementierungsmöglichkeiten für die KMU-CERT-Infrastruktur

Um die in dem vorherigen Kapitel ausgeführten Dienstleistungen anzubieten, bedarf es einer erfolgreichen Implementierung. Ein wichtiger Faktor für den Erfolg sind die Kosten, die für die Implementierung aufgewendet werden müssen. Es gibt aber auch andere Faktoren, die über Erfolg und Misserfolg entscheiden und daher nicht außer Acht gelassen werden dürfen.

Traditionell gibt es zwei Betreibermodelle für die Realisierung von CERT-Dienstleistungen:

1. Beauftragung eines etablierten Teams mit der Erbringung der Dienstleistung.
2. Aufbau eines neuen Teams speziell für diesen Zweck.

Beide Modelle werden im folgenden bewertet.

4.1 Erbringung durch ein etabliertes Team

Bisher gibt es immer noch relativ wenige etablierte "Player",[11] die sich zur Erbringung der Dienstleistungen grundsätzlich anbieten würden. Es gibt bei allen eine Reihe von mehr oder weniger gleichen Problemen, die hier kurz skizziert werden:

- **Es gibt (noch) kein eigenes Team:**

  Im Laufe des Jahres 2000 hat der BITKOM als Verband zusammen mit verschiedenen Mitgliedern eine Vision für ein BITKOM-CERT entwickelt. Aus mehreren Gründen, die an dieser Stelle nicht relevant sind, kam es bis jetzt nicht zum Aufbau eines eigenen Teams.

  Der BITKOM kommt zwar grundsätzlich in Frage, verfügt allerdings nicht über ein bestehendes Team. Damit würde sich für den BITKOM prinzipiell die Situation wie beim Aufbau eines eigenen Teams (siehe Abschnitt 4.2) darstellen.

  Gleiches gilt prinzipiell für die Deutsche Telekom AG, die derzeit ein eigenes Team aufbaut.[12]

- **Es gibt ein Team, dem allerdings eine feste Zielgruppe zugeordnet ist:**

  In Deutschland haben sich das DFN-CERT seit 1993 und das BSI-CERT seit 1995 als Dienstleister für eine jeweils feste und klar abgrenzbare Zielgruppe

---

[11] Der Begriff "Player" wird hier sehr frei benutzt. Er bezeichnet gleichfalls Entitäten, die bereits über ein eigenes Team verfügen, als auch solche, die entsprechende Aktivitäten angekündigt haben.

[12] Von dem internen Team zu unterscheiden sind Dienstleister im Umfeld der Deutschen Telekom, die kommerzielle Dienstleistungsangebote offerieren. Diese werden im folgenden behandelt.

positioniert. Dem entsprechend sind die Dienstleistungen und Strukturen, aber auch die Ausstattung der Teams, auf diese Zielgruppe ausgerichtet.

BSI-CERT und DFN-CERT kommen zwar grundsätzlich in Frage, verfügen allerdings im Moment nicht über die notwendige Ausstattung, um grundsätzlich neue Dienstleistungen sofort erbringen zu können. Damit würde sich auch für diese beiden Teams die Situation ähnlich wie beim Aufbau eines eigenen Teams darstellen.

Es ist jedoch anzumerken, dass im Gegensatz zum obigen Fall bereits eine lokale Infrastruktur für die Dienstleistung und erfahrenes Personal zur Verfügung steht, so dass die Chancen für eine erfolgreiche Implementierung höher eingeschätzt werden können.

Gleiche Aussagen gelten für interne Teams wie z. B. das SIEMENS CERT.

Hier muss beachtet werden, dass bei einem Betrieb durch ein internes Team eines großen Konzerns ein Anwender in der Regel nicht zwischen dem Anbieter/Hersteller/Konzern SIEMENS mit seinem SIEMENS-CERT und der - quasi extern vergebenen - Erbringung einer Dienstleistung unterscheiden wird. Wenn parallel kommerziell CERT-Dienstleistungen angeboten werden, wird diese Differenzierung noch schwieriger.

- **Es gibt kein entsprechendes Dienstleistungsangebot:**

  FIRST als neutraler Dachverband erbringt verschiedene Dienstleistungen für seine Mitglieder, die allerdings deutlich von dem für die KMU-CERT-Infrastruktur entwickelten Spektrum abweichen. Ebenso spricht die starke Internationalisierung gegen eine Einbindung von FIRST.

  FIRST kommt grundsätzlich nicht in Frage, stellt aber ein wichtiges Gremium dar, in das die KMU-CERT-Infrastruktur integriert werden muss.

  Weitgehend ähnliche Aussagen sprechen auch gegen eine Erbringung solcher Dienstleistungen durch TI.[13]

- **Es gibt ein kommerzielles Dienstleistungsangebot:**

  Inzwischen haben verschiedene Dienstleister (z. B. IBM ERS, debis IT Security Services) kommerzielle Angebote entwickelt, um Kunden bei der Bewältigung von Vorfällen oder aber bei der Vorbeugung von Vorfällen durch CERT-nahe Dienstleistungen zu unterstützen. Diese sind auf eine 1:1 Beziehung zwischen Dienstleister und Kunden ausgerichtet und geben dem Kunden einen vertraglich definierten Zugang zu bestimmten Dienstleistungen. Dieser Ansatz verfolgt also nicht, wie für die KMU-CERT-Infrastruktur festgelegt, das Interesse einer Solidargemeinschaft, was als 1:n Beziehung charakterisiert wurde.

[13] Zu berücksichtigen ist zusätzlich, dass sowohl FIRST als auch TI keinerlei Interesse für die Übernahme solcher Dienstleistungen gezeigt haben, sondern statt dessen den Ausbau ihrer speziellen Funktionen vorantreiben. Da jedoch verschiedentlich auf diese "Player" verwiesen wird, wurden sie in die Betrachtung miteinbezogen.

Die verschiedenen Dienstleister liegen miteinander im Wettbewerb und sehen in der Regel eine bestehende Kundenbeziehung als Möglichkeit, neue Aufträge zu gewinnen.

Seitens der Nutzer wird bei einer (alleinigen) Erbringung einer Dienstleistung durch einen der Anbieter die Frage aufkommen, ob tatsächlich eine neutrale und angemessene Beratung/Betreuung erfolgt. Insbesondere könnte befürchtet werden, dass die gewonnenen Informationen für interne Zwecke des Dienstleisters genutzt werden. Eine Neutralität wird ohne weitere Maßnahmen schwer zu kommunizieren sein.[14]

Bewertung: Keines der etablierten Teams befindet sich in einer Position, die die Übernahme der Verantwortung für die Zielgruppe der kleinen und mittleren Unternehmen als "natürlich" erscheinen lässt.

Von den anderen Instanzen, die im CERT-Umfeld eine Rolle spielen, aber noch keine CERT-Dienstleistungen anbieten, befindet sich keine in der Lage, kurzfristig ein entsprechendes Team aufzubauen (siehe dazu auch die Ausführungen des nächsten Abschnitts).

Bei der Überlegung, ob ein etablierter Dienstleister alleine die Versorgung mit CERT-Dienstleistungen übernehmen soll, wurde die Neutralität bereits angesprochen. Ebenso spielt die Frage nach einer Monopolstellung bzw. der daraus abzuleitenden Abhängigkeit oder Übermächtigkeit eines einzelnen Dienstleisters, eine wichtige Rolle.

Aus gesamtwirtschaftlicher Sicht beinahe ebenso wichtig wie die genannten Punkte ist bei der Wahl eines etablierten Dienstleisters der Effekt auf den gesamten CERT-Markt. Da dieser Markt sich gerade erst langsam öffnet, wäre die Auswahl eines einzelnen CERT-Dienstleisters erdrückend.[15] Ein erfolgreiches Konzept muss dies berücksichtigen.

4.2 Aufbau eines neuen Teams

Die Erfahrung zeigt, dass bei dem Aufbau eines neuen Teams einige Punkte beachtet werden müssen, um den Erfolg nicht in Frage zu stellen. Diese werden hier näher ausgeführt, um ein Verständnis für die mit dem Aufbau eines neuen Teams verbundenen Schwierigkeiten zu schaffen.

---

[14] Auch wenn dies vertraglich ausgeschlossen werden kann, verbleibt ein "ungutes" Gefühl, das die Akzeptanz und damit letztendlich den Nutzen deutlich einschränken wird.

[15] Bei der Definition des BITKOM-CERTs wurde immer wieder darauf hingewiesen, dass ein BITKOM-CERT den etablierten Dienstleistern keine Konkurrenz machen dürfe. Dies stellt jedoch in keinem Fall ein Problem dar, denn jedes eine Solidargemeinschaft betreuende Team kann auch potentiell keine Konkurrenz darstellen, da es weder über die notwendigen Ressourcen noch über die Ausrichtung auf ein Individualkundengeschäft verfügt. D. h. das Angebot von 1:n Dienstleistungen ist unkritisch und regt eher den Bedarf (durch Schaffung eines Problembewusstseins oder die Suche nach einem besseren Service-Level) für etablierte/neue 1:1 Dienstleistungen an.

- **Eigenes rechtliches Konstrukt notwendig:**

  In der Regel ist der Aufbau einer neuen rechtlichen Person erforderlich, wenn Dienstleistungen nicht nur intern angeboten werden. Die mit verschiedenen Dienstleistungen verbundenen Haftungsfragen machen in der Regel eine GmbH notwendig, um andere Funktionen oder Geschäftsbereiche nicht zu gefährden.

  Dies verzögert zum einen den Start der Dienstleistung und macht zum anderen nur dann einen Sinn, wenn die Dienstleistung langfristig angelegt ist. Für den Fall, dass eine neue rechtliche Person geschaffen werden muss, weil die Dienstleistung nicht anzugliedern ist, muss in jedem Fall mit Verzögerungen gerechnet werden.

- **Eigenes Personal notwendig:**

  Obwohl dieser Punkt zunächst trivial erscheint, stellt er doch eines der größten Probleme überhaupt dar. Bisher gibt es keinen Ausbildungsgang zum "Incident Handler" und nur durch "Training on the Job" oder durch Personal, das bei einem anderen Team bereits die notwendige Erfahrung gesammelt hat, kann das eigene Personal aufgebaut werden.

  Ohne persönliche Kontakte zu anderen CERTs, die wiederum an erfahrenes Personal gebunden sind, fällt die nationale und internationale Integration schwerer, wodurch wiederum Verzögerungen bei der effektiven Erbringung der Dienstleistungen auftreten.

  Auch wenn sich die Verfügbarkeit von grundsätzlich geeignetem Personal in den letzten Monaten etwas verbessert hat, ist für CERT-Aufgaben qualifiziertes Personal generell schwer zu finden.

  Viele der im vorherigen Kapitel identifizierten Dienstleistungen beruhen darauf, dass das Personal nicht nur technisch versiert ist, sondern auch vertraut ist mit dem Aufbau eines Teams, mit der Erbringung von Dienstleistungen und mit den Anforderungen anderer Zielgruppen. Nur so kann gewährleistet werden, dass die Dienstleistungen konkret und vor allem effektiv an die Bedürfnisse einerseits und die Möglichkeiten andererseits angepasst werden.

- **Verzögerungen bei dem Aufbau von Personal:**

  Selbst wenn ausreichend vorgebildetes Personal gewonnen werden kann, das in der Lage wäre, sich in die neuen Aufgaben einzuarbeiten, müssen Verzögerungen befürchtet werden. Diese werden in der Regel daraus resultieren, dass zeitgleich mit dem Aufbau des Teams bereits mit der Erbringung der Dienstleistungen begonnen werden muss. D. h., die für Training und Ausbildung des Personals notwendige Zeit steht nicht zur Verfügung. Neu hinzukommendes Personal kann ebenfalls nur unzureichend eingearbeitet werden, wodurch erneute Verzögerungen entstehen.

  Mit Definition und Erbringung der Dienstleistungen verbundene praktische Erfahrungen sind ebenfalls unerlässlich, wenn daraus resultierende Verzögerungen vermieden werden sollen. Im Umkehrschluss bedeutet dies, dass wenn kein entsprechendes Personal auf "Senior Level" angeworben werden kann, auch hierdurch Verzögerungen entstehen.

- **Verzögerungen bei dem Aufbau der Dienstleistungen:**

  Mit dem Startschuss für den Aufbau des Teams ist eine Periode verbunden, die für den Aufbau der Dienstleistungen genutzt werden kann. Kommt es hierbei zu Verzögerungen, zum Beispiel durch unzureichend vorgebildetes Personal oder Personalmangel, gibt es spätestens bei der Aufnahme der Dienstleistungen Probleme. Für die Definition adäquater Vorgaben und Vorgehensweisen gibt es generell nur sehr wenig Zeit, da die Zielgruppe sonst das Vertrauen in die Fähigkeit des Teams verliert.

  Dieses Problem kann entschärft werden, indem der offizielle Startschuss bis zur Erreichung eines ausreichenden Niveaus herausgeschoben wird. Da allerdings der Aufbau des Teams bekannt werden wird, ist auch der hierdurch gewonnene Spielraum begrenzt.

- **Risiken für die Verfügbarkeit und Qualität der Dienstleistungen:**

  Unzureichende Qualifikation des Personals und der ständige Druck, die jeweiligen Dienstleistungen erbringen zu müssen, gefährden deren Verfügbarkeit. Wenn die Dienstleistungen nicht ausreichend definiert sind, kann auch dies die Verfügbarkeit, aber noch mehr die Qualität bzw. das Service-Level, gefährden.[16]

  Gerade die Sicherstellung der Qualität erfordert mehr als das minimale Personal, so dass Redundanzen vorgesehen werden müssen.

- **„Unternehmerisches" Risiko:**

  Das Angebot einer Dienstleistung ist nur aufrecht zu erhalten, wenn die Finanzierung gesichert ist. Für den Aufbau eines Teams stellt sich also die Frage, wie dieses Team langfristig finanziert und ausgebaut werden kann. Neben dem Mehraufwand für eigenes Personal, wobei nicht unerheblich die technische Infrastruktur und deren Absicherung zu Buche schlägt, muss auch die Marktsituation bedacht werden. In jedem Fall ist ein Business Case zu erstellen, der generell nicht nur auf einer Einnahmequelle beruhen sollte. Erfahrungen haben gezeigt, dass Teams mit einer ungesicherten Finanzierung nicht das notwendige Personal einbinden und halten können. Hierdurch würden dann erneut Verzögerungen oder eine temporäre Verschlechterung der Dienstleistung drohen.

Bewertung: Der Aufbau eines neuen Teams ist grundsätzlich möglich, birgt aber große Risiken, die die Verfügbarkeit der Dienstleistungen generell gefährden. In Kenntnis der aktuellen Personalsituation muss mit erheblichen Verzögerungen beim Aufbau eines eigenen Teams oder mit Einschränkungen bei der Erbringung der Dienstleistungen gerechnet werden.

[16] Hierbei muss auch die Vergleichbarkeit der Diensterbringung bedacht werden. Es kommt weniger darauf an, eine von zehn Fragen sehr gut und ausführlich zu beantworten, als vielmehr alle zehn Fragen angemessen und vergleichbar zu beantworten.

Daher ist dieses Modell nur dann zu empfehlen, wenn dem Aufbau eines "eigenen" Teams eine besondere Bedeutung zukommt oder wenn nur durch das Team ein Zusatznutzen entsteht, der anders nicht erreicht werden kann. Ein solcher Zusatznutzen müsste dann gegenüber den Risiken und Verzögerungen abgewogen werden.

Zusammenfassend ist festzustellen, dass beim Aufbau einer KMU-CERT-Infrastruktur die Risiken minimiert werden müssen und ein Zusatznutzen durch ein eigenes Team nicht zu erkennen ist. Statt dessen sollten nach einer Entscheidung Verzögerungen für den Aufbau vermieden werden. Wenn später ein langfristiger Bedarf für ein eigenes Team erkannt wird, kann dieses parallel aufgebaut werden. Hierdurch relativieren sich viele der angesprochenen Probleme, da dann genügend Zeit für den Personalaufbau vorhanden ist.

4.3 Schlussfolgerungen

Die Ausführungen dieses Kapitels haben gezeigt, dass für den Aufbau der KMU-CERT-Infrastruktur keine "traditionelle" Form der Implementierung als erfolgversprechend anzusehen ist. Sowohl der Aufbau eines eigenen Teams als auch die Übertragung der Verantwortung für die Dienstleistungen auf ein etabliertes Team oder einen Dienstleister haben signifikante Probleme und Defizite.

Anhand der Ausführungen kann allerdings abgeleitet werden, welche Ansätze für eine erfolgreiche Implementierung genutzt werden können:

- **Einsatz von mehreren Dienstleistern:**

  Um die in Abschnitt 4.2 aufgezeigten Risiken zu vermeiden, müssen Dienstleister, die bereits das entsprechende Personal und Expertise aufgebaut haben, genutzt werden. Hierdurch wird auch die Verfügbarkeit der Dienstleistungen erheblich verbessert. Durch die unabhängige Realisierung der einzelnen Dienstleistungen durch verschiedene Dienstleister wird die Verfügbarkeit weiter verbessert. Außerdem können neue Dienstleistungen rasch integriert werden, aber auch die Ausgliederung nicht mehr benötigter Dienstleistungen ist möglich.

  Insgesamt werden durch den Einsatz von mehreren externen Dienstleistern folgende Vorteile erreicht:

  - Eigenes Personal für die operativen Dienstleistungen wird unnötig.
  - Ein eigenes rechtliches Konstrukt wird nicht benötigt.
  - Es wird auf erfahrenes Personal zurückgegriffen.
  - Redundanz wird auf Seiten der Dienstleister sichergestellt.

- **Vorbereitungsphase definieren und klar kommunizieren:**

  Erfahrungen mit anderen CERTs haben gezeigt, dass die Ausrichtung auf die Zielgruppe entscheidend für den Erfolg und die Akzeptanz der Dienstleistung ist. Daher sollen in einer ausreichend dimensionierten Vorbereitungsphase folgende Aufgaben durchgeführt werden:

  - Erschließung der Zielgruppe sowie derer Anforderungen.

- Abstimmung der Dienstleistung mit der Zielgruppe und Definition der erweiterten Basisdienstleistungen.
- Einbeziehung der Schlüsselexpertise der Dienstleister.

Weitere Aspekte, die teilweise bereits angesprochen wurden, müssen in Hinblick auf diese Ansätze neu bewertet werden:

- **Konkurrenz zu kommerziellen Dienstleistern:**

  Alle potentiell in Frage kommenden Dienstleister werden bei der Auswahl berücksichtigt. Es sollten mehrere Dienstleister für unterschiedliche Dienstleistungen ausgewählt werden, um die Konzentration auf einen Dienstleister im Rahmen der Möglichkeiten zu vermeiden.

  Da die im Rahmen der KMU-CERT-Infrastruktur zu erbringenden Dienstleistungen jeweils 1:n Dienstleistungen darstellen und auf eine relativ große Zielgruppe ausgerichtet sind, werden die kommerziellen Dienstleistungsangebote nicht verdrängt oder überflüssig.

- **Marktöffnung:**

  Mit der Etablierung der Dienstleistung für KMUs wird nicht nur die Sicherheit innerhalb dieser Zielgruppe positiv beeinflusst. Über die Grenzen der Zielgruppe hinweg wird die Bedeutung eines CERTs betont und verdeutlicht. Dies dient letztendlich allen Dienstleistern und Beratungsunternehmen, die am Markt agieren. Zugleich wird der sich nur sehr langsam öffnende Markt weiter geöffnet, da die angebotenen 1:n Dienstleistungen nicht alle Bedürfnisse zufrieden stellen können, so dass auch 1:1 Dienstleister zum Zuge kommen.

- **Neutralität der Dienstleistung:**

  Durch die starke Einbindung von kommerziellen Dienstleistern kommt der Wahrung der Neutralität eine große Bedeutung bei. Diese muss mit adäquaten Mitteln gewährleistet werden.

- **Durchführung der Dienstleistung wird kontrolliert:**

  Im Sinne der Zielgruppe muss die Erbringung der Dienstleistung kontrolliert werden. Adäquate Kontrollmechanismen müssen vereinbart und etabliert werden.

Diese hier nur als Grundaussagen wiedergegebenen Überlegungen werden im folgenden Kapitel aufgegriffen, um ein Erfolg versprechendes Betreibermodell für eine KMU-CERT-Infrastruktur zu entwickeln, für das auch die Frage der Aufwände beantwortet wird.

5 Empfohlenes Betreibermodell für die KMU-CERT-Infrastruktur

Die beiden nahe liegenden Betreibermodelle für die KMU-CERT-Infrastruktur wurden im letzten Kapitel vorgestellt und bewertet.

- Eine Erbringung durch ein einzelnes etabliertes Team kann, wie in Abschnitt 4.1 ausgeführt, nicht empfohlen werden.
- Der Aufbau eines neuen Teams, wie in Abschnitt 4.2 ausgeführt, ist grundsätzlich möglich, birgt aber große Risiken, die die Verfügbarkeit der Dienstleistung generell gefährden. Daher ist auch dieses Modell nicht zu empfehlen, sofern nicht dem Aufbau eines "eigenen" Teams eine besondere Bedeutung zukommt. Diese ist jedoch für die hier untersuchte KMU-CERT-Infrastruktur nicht zu erkennen.

Dennoch gibt es eine Alternative, die die identifizierten Nachteile und Schwachpunkte ausschließt und die in Abschnitt 4.3 aufgestellten Anforderungen erfüllt. Dieses empfohlene Betreibermodell bietet darüber hinaus zahlreiche Vorteile, die durch Synergieeffekte und Modularisierung gewonnen werden. Das empfohlene Betreibermodell ist in Abbildung 5-1 dargestellt.

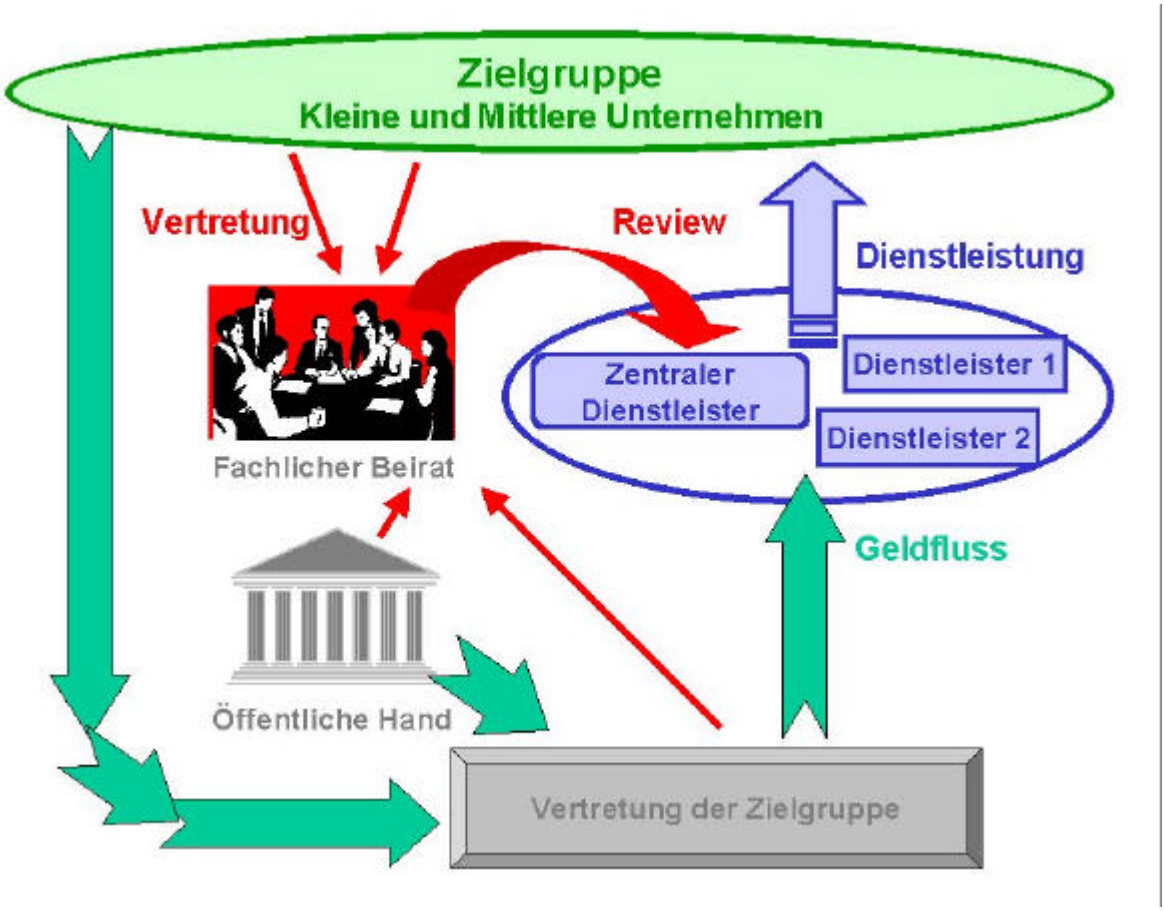

Abbildung 5-1: Empfohlenes Betreibermodell

5.1 Darstellung des empfohlenen Betreibermodells

Die zentrale, koordinierende Rolle im empfohlenen Betreibermodell nimmt der **zentrale Dienstleister** ein. Dieser hat die wesentliche Aufgabe, die Versorgung der Zielgruppe mit Dienstleistungen sicherzustellen. Dies erfolgt zum einen dadurch, dass er die zentralen Basisdienstleistungen selber erbringt. . Zum anderen hat er die Aufgabe, die erweiterten Basisdienstleistungen und die Zusatzdienstleistungen zunächst in Kooperation mit der Zielgruppe zu spezifizieren und auszuwählen und diese anschließend am Markt einzukaufen. Hierzu werden Ausschreibungen durchgeführt, an denen sich etablierte Dienstleister beteiligen können. Unterschiedliche Dienstleistungen können auch von unterschiedlichen Dienstleistern erbracht werden. Über das Mittel der Ausschreibung wird sichergestellt, dass eine möglichst wirtschaftliche Lösung gewählt wird.

Um die inhaltliche Arbeit aller Dienstleister zu kontrollieren, wird ein **fachlicher Beirat** eingerichtet. Dieser setzt sich aus Vertretern der Zielgruppe, der Geldgeber und verschiedener anerkannter CERTs zusammen. Durch den Beirat wird auch die Neutralität der Diensterbringung sichergestellt. Zusätzlich unterstützt der Beirat den zentralen Dienstleister bei der Definition der erweiterten Basis- sowie der Zusatzdienstleistungen.

Die Finanzierung des empfohlenen Betreibermodells wird über eine **Vertretung der Zielgruppe** gewährleistet. Diese Vertretung nimmt quasi als finanzielle Clearingstelle Finanzmittel ein, die aus potentiell mehreren Quellen kommen können. Über die erhaltenen Finanzmittel wird dann die Erbringung der zentralen Basisdienstleistungen sowie eine Finanzierung der ausgeschriebenen Dienstleistungen sichergestellt. Darüber hinaus hat die Vertretung der Zielgruppe die Aufgabe, den zentralen Dienstleister bei der Erschließung der Zielgruppe zu unterstützen. Dies kann z. B. durch Etablierung von Kontakten, Wahrnehmung von Interessensvertretung und einer Legitimierung der CERT-Dienstleistung in der Zielgruppe erfolgen.

Als **Dienstleister** kommen sowohl Firmen in Betracht, die bereits heute entsprechende Dienste am Markt anbieten, als auch Firmen, die durch eine entsprechende Nachfrage motiviert werden, eigene neue Dienstleistungsangebote zu entwickeln.[17] Dieses modulare und verteilte Dienstleistungsprinzip wirkt marktöffnend und erlaubt darüber hinaus die Partizipation kleinerer Unternehmen. Durch die Einbindung mehrerer Anbieter wird verhindert, dass ein einziger Dienstleister eine übermächtige Position einnehmen kann.

Für die **Zielgruppe** kann somit durch den zentralen Dienstleister über eine Koordinierung verschiedener Dienstleister, die zusammen die Dienstleistung erbringen, ein auf die Zielgruppe und die finanziellen Ressourcen zugeschnittenes Dienstleistungspaket erbracht werden.

Aufgrund der wichtigen Rolle des zentralen Dienstleisters muss dieser zum einen in der Lage sein, durch Fachkenntnis ein möglichst gutes Dienstleistungsspektrum zusammenzustellen und an die Bedürfnisse der Zielgruppe anzupassen. Zum anderen sollte es sich um einen nicht im Wettbewerb stehenden und daher neutralen

[17] Dabei ist zu beachten, dass die Dienstleistungen durch die Dienstleister im Namen und Auftrag der KMU-CERT-Infrastruktur erbracht werden und nicht unter eigenen Namen.

sowie etablierten Partner handeln, um von Anfang an ein entsprechendes (Grund)Vertrauen bei der Zielgruppe zu erreichen.

5.2 Erfolgsfaktoren für das empfohlene Betreibermodell

Für das empfohlene Betreibermodell gibt es eine Reihe von Erfolgsfaktoren:

- Relativ niedrige Basiskosten für den zentralen Dienstleister (Basisdienstleistung).
- Durch Einkauf der Dienstleistungen am Markt entfallen der zeitliche und der finanzielle Aufwand zur Ausbildung eigenen Personals (was heutzutage sowieso kaum zur Verfügung steht).
- Anderer Overhead entfällt.
- Bereits durch die Realisierung der Basisdienstleistungen wird der Zielgruppe eine Hilfe erbracht.
- Zusätzliche Finanzmittel können (nach Prioritätenliste) dynamisch für neue Zusatzdienstleistungen verwendet werden.
- Das unternehmerische Risiko bei Nichtannahme des Angebots wird minimiert.

5.3 Realisierung des empfohlenen Betreibermodells

Nach Darstellung der zu erbringenden Dienstleistungen in Abschnitt 3.3 und des empfohlenen Betreibermodells in Abschnitt 5.1 soll nun dargestellt werden, wie eine praktische Realisierung der KMU-CERT-Infrastruktur erfolgen soll.

Es wird dabei von einer Laufzeit von zunächst drei Jahren ausgegangen. Wie die Erfahrung beim Aufbau anderer CERT-Infrastrukturen zeigt, ist dies ein Zeitraum, der mindestens nötig ist, um die Dienstleistungen aufzubauen und in der Zielgruppe zu verankern.[18] Ein kürzerer Zeitraum birgt die Gefahr, dass eine Umsetzung in der Zielgruppe nicht erfolgt und somit getätigte Investitionen verloren gehen. Der Zeitraum ist im wesentlichen durch drei Faktoren begründet. Erstens gilt es die (sehr heterogene) Zielgruppe organisatorisch zu erschließen und ihr die Bedeutung der neuen CERT-Infrastruktur zu vermitteln. Zweitens müssen die Dienstleistungen detailliert formuliert und aufgebaut werden. Und schließlich müssen die neuen Dienstleistungen so in der Zielgruppe etabliert werden, dass diese in die unternehmenseigenen Prozesse integriert werden, bzw. dass eigene Ressourcen aufgewendet werden, um konkret mit erhaltenen Informationen sachgerecht umzugehen.

Bevor mit den eigentlichen Dienstleistungen begonnen werden kann, sind einige Vorarbeiten erforderlich:

- Finanzierung sicherstellen: Es muss geklärt werden, wer sich in welcher Höhe an der Finanzierung der Arbeiten beteiligt. Dabei muss mindestens der Betrag für die Realisierung der Basisdienstleistungen gesichert werden,

[18] Erfahrungen etablierter Teams haben wiederholt gezeigt, dass von der Bereitstellung einer Meldemöglichkeit von Vorfällen bis zu einer regelmäßigen Nutzung ein Zeitraum von ca. neun Monaten vergeht.

wünschenswert ist jedoch mittelfristig ein höherer Betrag, der auch die Realisierung von Zusatzdienstleistungen ermöglicht.

- Vertretung der Zielgruppe finden: Es muss eine Instanz gefunden werden, die die Interessen der Zielgruppe vertritt und zugleich die Sicherstellung der finanziellen Transaktionen garantiert.
- Zentralen Dienstleister finden: Da dem zentralen Dienstleister die zentrale Rolle im empfohlenen Betreibermodell zukommt, muss diese Position kompetent besetzt werden (Fachkenntnis, Neutralität, potentielle Akzeptanz in der Zielgruppe). Auf Basis von konkreten Angeboten kann diese Funktion entweder über eine beschränkte Ausschreibung oder über eine freihändige Vergabe erfolgen.

Nach erfolgreicher Erledigung dieser Vorarbeiten kann zum Zeitpunkt T_0 mit der Umsetzung des zeitlichen Ablaufplanes und somit mit den inhaltlichen Arbeiten begonnen werden. Eine Darstellung des zeitlichen Ablaufs gibt Tabelle 5-1, basierend auf einem 6-monatigen Zeitraster. Dabei werden - soweit nicht anders angegeben - die Arbeiten vom zentralen Dienstleister durchgeführt.

Angegeben ist jeweils der erste Zeitpunkt, zu dem mit der Realisierung einer Dienstleistung begonnen wird. Bei den meisten Dienstleistungen schließt sich daran eine kontinuierliche Fortführung dieser Arbeiten an (z. B. Pflege der Informationssysteme, Erschließung der Zielgruppe, Beantwortung von Sicherheitsfragen, Erstellung der Newsletter, usw.). Insofern nehmen die Initialtätigkeiten des zentralen Dienstleisters mit Projektverlauf ab, während die laufenden Tätigkeiten deutlich zunehmen. Der Beginn neuer Arbeiten in den letzten Quartalen hängt insbesondere davon ab, ob eine Fortführung der Arbeiten über die Laufzeit von drei Jahren hinaus gesichert werden kann.

Zeitpunkt	Neu zu beginnende Arbeiten
T_0	- KMU-CERT-Infrastruktur international positionieren (FIRST, Europäisches CERT-Verzeichnis) - Organisation des fachlichen Beirats durch die Vertretung der Zielgruppe in Zusammenarbeit mit dem zentralen Dienstleister - Erstellung von Informationsmaterial über Ziele der KMU-CERT-Infrastruktur - Organisation eines "Roundtables" mit CERTs im Industrie- und Wirtschaftsbereich - Aufbau von Kontakten zu nationalen CERTs - Konzeption und Aufbau der gesicherten technischen Infrastruktur (Web-Server, Mailinglisten)
T_0 + 6 Monate	- Zentraler Dienstleister ist per Mail, Telefon, Fax erreichbar - Auf dem Web-Server sind für die Zielgruppe nützliche Informationen vorhanden - Beginn der konkreten Maßnahmen zur Erschließung der Zielgruppe: zentraler Dienstleister und die Vertretung der Zielgruppe treten an die Zielgruppe heran

Zeitpunkt	Neu zu beginnende Arbeiten
	- Konzeption der 1. erweiterten Basisdienstleistung - Einführung der Mailingliste für Sicherheitsfragen - Vorbereitung des 1. KMU-CERT Workshops - Ausschreibung der 1. erweiterten Basisdienstleistung - Konzeption der Austauschstelle für Vorfallsinformationen - Beginn der Maßnahmen zum "Awareness Building" - Angebot des 1. Monatlichen Newsletters
T_0 + 12 Monate	- Zuschlagserteilung für die 1. erweiterte Basisdienstleistung - Konzeption der 2. erweiterten Basisdienstleistung - Durchführung des 1. KMU-CERT Workshops - Austauschstelle für Vorfallsinformationen nimmt ihren Dienst auf - Angebot der 1. erweiterten Basisdienstleistung - Ausschreibung der 2. erweiterten Basisdienstleistung
T_0 + 18 Monate	- Zuschlagserteilung für die 2. erweiterte Basisdienstleistung - Vorbereitung des 2. KMU-CERT Workshops - Angebot der 2. erweiterten Basisdienstleistung
T_0 + 24 Monate	- Durchführung des 2. KMU-CERT Workshops
T_0 + 30 Monate bis T_0 + 36 Monate	- In Abhängigkeit der Frage der Fortführung der KMU-CERT-Infrastruktur können hier weitere (Zusatz)Dienstleistungen begonnen werden. Dies macht jedoch nur Sinn, wenn eine Fortführung gesichert ist.

Tabelle 5-1: Zeitlicher Ablauf der inhaltlichen Arbeiten

5.4 Aufwände zur Realisierung des empfohlenen Betreibermodells

Durch das mehrstufige Dienstkonzept ergibt sich ein flexibles Finanzierungskonzept. Als untere Schranke zur Realisierung des empfohlenen Betreibermodells ist die Finanzierung der zentralen Basisdienstleistungen zu sehen, die mit ca. 300 TDM pro Jahr abgeschätzt werden kann, wobei dieser Wert im dritten Jahr leicht ansteigt, da die Menge der kontinuierlich zu erbringenden Dienstleistungen zunimmt. Sinkt die Finanzierung unter dieses Niveau, kann vom zentralen Dienstleister lediglich ein Teil der zentralen Basisdienstleistungen erbracht werden, wodurch sich ein für die Zielgruppe nicht wirkungsvolles Leistungsspektrum ergäbe und die Beteiligung der Unternehmen und somit der Erfolg der Arbeiten grundlegend in Frage gestellt wäre.

Die Kosten für die Realisierung der erweiterten Basisdienstleistungen steigen mit zunehmender Laufzeit des Projektes an. Während im ersten Jahr keine Mittel dafür

einzuplanen sind (hier wird zunächst die Zielgruppe erschlossen), ist im zweiten Jahr mit Kosten von ca. 300 TDM zu planen und im dritten Jahr mit ca. 400 TDM.[19]

	1. Jahr	2. Jahr	3. Jahr	Gesamt
zentrale Basisdienstleistungen (zentraler Dienstleister)	300 TDM	300 TDM	350 TDM	950 TDM
erweiterte Basisdienstleistungen (div. Dienstleister am Markt)	0 TDM	300 TDM	400 TDM	700 TDM
Summe	**300 TDM**	**600 TDM**	**750 TDM**	**1.650 TDM**

Tabelle 5-2: Finanzieller Aufwand für das empfohlene Betreibermodell

Eine zusammenfassende Darstellung der Kosten gibt Tabelle 5-2. Für den Zeitraum von drei Jahren belaufen sich die Kosten für die zentralen Basisdienstleistungen auf ca. 950 TDM und für die erweiterten Basisdienstleistungen, die über einen Zeitraum von 24 Monaten angeboten werden, auf ca. 700 TDM. Somit sind für den Gesamtzeitraum für die CERT-Basisdienstleistungen Kosten in Höhe von ca. 1.650 TDM einzuplanen.

Sollten darüber hinaus Finanzmittel zur Verfügung stehen, so können diese flexibel genutzt werden, um das Konzept der modularen Zusatzdienstleistungen zu realisieren. Dies gilt ebenso für Einsparungen, die sich bedingt durch den Mechanismus der Ausschreibung sowie durch den festgelegten Service-Level ergeben können.

5.5 Eckpunkte für ein Finanzierungskonzept

Zur Finanzierung der Dienstleistung kommen im wesentlichen zwei Konzepte in Betracht: die Finanzierung über Einzelbeiträge und die zentrale Finanzierung durch Verbände der Zielgruppe (evtl. mit Unterstützung Dritter).

Aufgrund der Erfahrungen bei anderen CERTs lässt sich absehen, dass eine Einzelabrechnung von Mitgliedern der Zielgruppe nicht erfolgreich sein kann. Da diese mit den neuen Dienstleistungen noch nicht vertraut sind und somit auch deren Wert noch nicht erkennen können, wird es grundsätzlich keine Bereitschaft zur Einzelfinanzierung geben. Aber auch aus Sicht der KMU-CERT-Infrastruktur wäre dieser Ansatz nachteilig, da er einen erheblichen administrativen und somit auch finanziellen Mehraufwand bedeuten würde.

Für die Realisierung der KMU-CERT-Infrastruktur wird statt dessen empfohlen, die Finanzierung auf zwei wesentliche Säulen zu basieren: zum einen auf die öffentliche Hand, z.B. in Form einer Anschubfinanzierung und zum anderen auf Verbände, die als Interessenvertreter der Zielgruppe deren finanzielle Beiträge in gebündelter Form weitergeben.

[19] Bei diesen Werten wird davon ausgegangen, dass die erweiterten Basisdienstleistungen nur Mitgliedern der Zielgruppe direkt zur Verfügung stehen. Eine erlaubte Weitergabe der Dienstleistung an Dritte (z.B. durch ISPs) würde zu deutlich höheren Kosten führen.

Darüber hinaus können mittelfristig Mittel durch Sponsoring (Sicherheitsfirmen, Hersteller) oder durch das Angebot kostenpflichtiger Dienstleistungen (0190-Rufnummer) erzielt werden.

Eine entscheidende Voraussetzung für eine solide finanzielle Ausstattung ist jedoch eine feste Zusage der beiden wesentlichen Geldgeber für drei Jahre.

6 Zusammenfassung und Empfehlungen

Im Rahmen der im Mai 2000 von BM Dr. Müller gegründeten "Partnerschaft sichere Internet-Wirtschaft" ist auch die Verbesserung der Alarmierung über sicherheitsrelevante Vorfälle erörtert worden. Ziel dieses Gutachtens ist es, in diesem Zusammenhang den Nutzen und die Rolle von CERT-Dienstleistungen für kleine und mittlere Unternehmen zu identifizieren.

Empfehlung 1: Der Aufbau einer KMU-CERT-Infrastruktur wird empfohlen.

CERTs - im Deutschen bekannt als Computer-Notfallteams - sind eine der wichtigsten Neuerungen im Risiko- und Sicherheitsmanagement. Gerade bei einer übergreifenden Koordinierung ergibt sich durch sie die angestrebte Vorwarnfunktion, d. h. die Verteilung proaktiver Informationen, durch die Vorfälle verhindert werden können.

Es gibt in Deutschland in diesem Bereich erhebliche Kompetenz, allerdings existieren bisher in der deutschen Wirtschaft bis auf wenige Ausnahmen (Siemens, Sparkassen-Finanzgruppe) keine institutionalisierten Teams. Insbesondere fehlt dem Bereich der kleinen und mittleren Unternehmen eine geeignete Unterstützung, wie sie durch das DFN-CERT für die Wissenschaft oder durch das aus dem BSI-CERT entstehende CERT-BUND für die Bundesbehörden verfügbar ist bzw. sein wird.

Empfehlung 2: Die Vorbildfunktion der KMU-CERT-Infrastruktur für die Wirtschaft sollte genutzt werden.

Anders als bei den traditionellen Maßnahmen der Rechner- und Netzwerksicherheit werden in einer CERT-Infrastruktur Angriffe und Vorfälle nicht einfach ignoriert, sondern gezielt als Ansatzpunkt verstanden, um den Betroffenen zu helfen. Außerdem wird das Wissen über Angriffe und Vorfälle genutzt, um potentielle Betroffene zu warnen und so weitere Schäden zu begrenzen oder ganz abzuwehren.

In diesem Sinne dient eine KMU-CERT-Infrastruktur auch als positiver Multiplikator für vorbeugende Maßnahmen, die die Sicherheit wirksam erhöhen. Durch die empfohlenen Verfahren werden Angriffe und Vorfälle erkennbar und somit mögliche Schäden verringert. Sie erlauben damit effiziente Gegenmaßnahmen und tragen so ebenfalls wirksam zu dem globalen Ziel bei, die kleinen und mittleren Unternehmen zu schützen.

Dieser Effekt der KMU-CERT-Infrastruktur wird über die Zielgruppe der KMUs hinaus auch für die gesamte deutsche Wirtschaft positive Auswirkungen haben.

Empfehlung 3: Nur zentrale und erweiterte Basisdienstleistungen zusammen bilden ein CERT.

Basierend auf nationalen und internationalen Erfahrungen und Erkenntnissen wurden die verschiedenen Basisdienstleistungen identifiziert, die minimal benötigt werden. Darüber hinaus gehende Zusatzdienstleistungen sind möglich.

Die Basisdienstleistungen können differenziert werden: Zentrale Basisdienstleistungen sind die Grundlage für eine erfolgreiche Etablierung der KMU-CERT-Infrastruktur. Sie stellen die Erschließung der Zielgruppe sowie deren Versorgung mit elementaren Informationen sicher. Bereits hierdurch kann die Sicherheit bei KMUs deutlich verbessert werden.

Die erweiterten Basisdienstleistungen ergänzen das Dienstleistungsangebot, indem sie die konkrete Unterstützung bei Angriffen und Vorfällen ermöglichen.

Empfehlung 4: Für den Aufbau wird ein Zeitraum von drei Jahren empfohlen.

Die Aufteilung der Basisdienstleistungen erlaubt ein stufenweises Vorgehen, bei dem zunächst die zentralen Basisdienstleistungen aufgebaut werden. Die Erschließung der Zielgruppe bildet dann die Voraussetzung für den erfolgreichen Aufbau der weiteren Dienstleistungen, da eine Anpassung an die spezifischen Anforderungen der KMUs möglich wird.

Um die CERT-Dienstleistungen und ihre Akzeptanz in der Zielgruppe zu verankern, ist eine längerfristige Kontinuität sicherzustellen.

Empfehlung 5: Die KMU-CERT-Infrastruktur soll durch verschiedene Dienstleister aufgebaut werden.

Abweichend von der Vorgehensweise bei vielen CERT-Gründungen wird empfohlen, zunächst auf den Aufbau eigenen Personals zu verzichten. Statt dessen sollen verschiedene Dienstleister ausgewählt werden, die ihre jeweilige Kernkompetenz einbringen und koordiniert durch eine zentrale Instanz die KMU-CERT-Infrastruktur bilden.

Da durch die KMU-CERT-Infrastruktur nur auf die gesamte Zielgruppe ausgerichtete Dienstleistungen angeboten werden, besteht keine Konkurrenz zu den etablierten und neu gegründeten Dienstleistern, die unternehmensspezifische Leistungen anbieten. Vielmehr wird die Arbeit der KMU-CERT-Infrastruktur zu einer gesteigerten Nachfrage für weitere CERT-Dienstleistungen führen, so dass hier die Entwicklung eines gerade entstehenden Marktes gefördert wird.

Empfehlung 6: Im Rahmen des empfohlenen Betreibermodells sind Qualität und Neutralität der KMU-CERT-Infrastruktur sicherzustellen.

Um die Neutralität und Qualität der Dienstleistung sicherzustellen, soll ein fachlicher Beirat etabliert werden. Dieser soll zusammen mit einer Vertretung der Zielgruppe die Dienstleister überwachen und zudem die Anpassung an die spezifischen Anforderungen der Zielgruppe unterstützen.

Empfehlung 7: Der Aufbau der KMU-CERT-Infrastruktur sollte durch die öffentliche Hand unterstützt werden.

Die Finanzierung der KMU-CERT-Infrastruktur muss durch die Vertretung der Zielgruppe koordiniert und gesichert werden. Aufgrund der Ausrichtung auf eine Solidargemeinschaft bietet sich ein Umlageverfahren an, das auf möglichst viele Zahlende verteilt werden muss. Hier ist die Einbindung der Verbände ein wichtiger

Gesichtspunkt. Es sollten darüber hinaus Möglichkeiten genutzt werden, Finanzmittel einzuwerben bzw. aufwändige Dienstleistungskomponenten separat abzurechnen.

Wie oben ausgeführt, gibt es vielfältige positive Auswirkungen des Aufbaus einer KMU-CERT-Infrastruktur, die den KMUs aber auch der gesamten deutschen Wirtschaft zugute kommen. Dies bedingt ein starkes Interesse der öffentlichen Hand an einem erfolgreichen Aufbau.

Empfehlung 8: Die KMU-CERT-Infrastruktur stellt einen gleichberechtigten Partner für andere CERTs dar.

Die Präsenz der KMU-CERT-Infrastruktur erlaubt die nationale und internationale Einbindung in existierende CERT-Strukturen. Hier ist besonders die gleichberechtigte Position in Deutschland neben DFN-CERT und CERT-BUND zu betonen.

Gleichzeitig wird die Grundlage für eine verbesserte Arbeit aller im Bereich der Wirtschaft etablierten CERTs geschaffen, für die eine informelle Zusammenarbeit koordiniert werden kann.

7 Nationale Positionierung der KMU-CERT-Infrastruktur

Eine weitere Schlüsselfrage für die Rolle der KMU-CERT-Infrastruktur in Deutschland ist die Frage der Koordinierung. Diese Frage ist nicht Hauptgegenstand dieses Gutachtens, hat jedoch Auswirkungen auf die KMU-CERT-Infrastruktur und muss daher abschließend angesprochen werden.

Wie bei der Darstellung des CERT-Umfeldes deutlich wurde, ist heute eine informelle Kooperation der nationalen CERTs ausreichend. Es ist jedoch nicht zu erwarten, dass auch in Zukunft eine flache Struktur mit sehr vielen gleichberechtigten CERTs geeignet ist, um effizient und effektiv zu arbeiten. Die bisherige Entwicklung in Deutschland und verschiedenen europäischen Ländern zeigt eine Aufteilung in mehrere große Zielgruppen, innerhalb derer ein hohes Maß an Übereinstimmung bezüglich Sicherheitsanforderungen, Risiken, etc. vorgefunden werden kann. Typisch ist hier die Aufteilung in einzelne Sparten:[20] Forschung, Behörden, Militär, Wirtschaft und eventuell davon getrennt die Kreditwirtschaft. Dabei werden für diese Sparten Teams wie das DFN-CERT für die Forschung, das BSI-CERT in Zukunft als CERT-BUND für Bundesbehörden und auch die KMU-CERT-Infrastruktur tätig. Ihre Aufgabe ist es, die Abläufe innerhalb "ihrer" Sparte zu koordinieren und sich wiederum mit den "anderen" CERTs abzustimmen.

Wenn eine informelle Koordinierung und Kooperation nicht mehr ausreicht - und dies wird sich in der Praxis zeigen und kann an dieser Stelle nicht zeitlich abgeschätzt werden - müssen andere Lösungen entwickelt werden. Dies kann nur in der Diskussion mit allen Beteiligten von Anfang an erfolgen und muss zu einem Konsens führen, um eine wirkliche Verbesserung zu erreichen. Wichtig scheint hier die Einbindung verfügbarer Expertise, um bekannte Fehler zu vermeiden und schnell zu Lösungen zu kommen, die in der Praxis funktionieren.

Spätestens bei einer etablierten, wenn auch informellen Koordinierung und Kooperation können wichtige Erkenntnisse über die Verletzlichkeit der Anwender und Netze gewonnen werden. Die Gewinnung und Aufbereitung entsprechender Daten kann dabei nur Aufgabe der einzelnen CERTs jeweils für ihren Bereich sein, jedoch ist eine geeignete, anonymisierte Zusammenführung der Erkenntnisse für die Gewinnung einer realistischeren Einschätzung von Risikofaktoren, Bedrohungen und tatsächlichen Angriffen und Vorfällen entscheidend. Dies muss bei der Diskussion der Zusammenarbeit und der Vereinbarung abgestimmter Verfahren berücksichtigt werden.

Außer dass CERTs die Möglichkeit bieten, die bei ihnen vorliegenden Daten zusammenzuführen und so zu der öffentlichen Bewusstseinsbildung beizutragen, verfügen diese insgesamt über eine erhebliche Erfahrung mit Angriffsverfahren, Vorgehensweisen von Angreifern, Analyse von Vorfällen, etc. Diese Kenntnisse sollten in andere Bereiche, z. B. in die Diskussion über kritische Infrastrukturen, eingebracht werden. Bei einer entsprechenden Beteiligung können die CERTs dann wiederum als positiver Multiplikator hinein in ihre jeweilige Zielgruppe wirksam

[20] Ähnliche Gedanke werden auch in anderen Arbeitsgruppen, u. a. innerhalb der Initiative D21, diskutiert.

werden. Dies würde dann im Falle der KMU-CERT-Infrastruktur die Schaffung eines adäquaten Problembewusstseins in (einem Bereich) der Wirtschaft weiter unterstützen.

Wie aus den obigen Ausführungen auch deutlich wird, wird es über kurz oder lang einen konkreten Bedarf für ein "CERT-Wirtschaft" geben. Es bleibt bereits hier festzuhalten, dass ein solches Team auf den gleichen Grundsätzen wie die KMU-CERT-Infrastruktur aufgebaut werden kann - und sollte. Die Dienstleistungen werden ebenfalls sehr große Überschneidungen aufweisen, wobei bei dem "CERT-Wirtschaft" die Koordinierung aller innerhalb der deutschen Wirtschaft etablierten CERTs eine wesentliche Ergänzung darstellen muss. Ob dann die Versorgung der KMUs innerhalb eines "CERT-Wirtschaft" aufgenommen wird, ob ganz natürlich aus der KMU-CERT-Infrastruktur das "CERT-Wirtschaft" entsteht oder ob sich beide Dienstleistungsangebote unabhängig voneinander entwickeln, bleibt abzuwarten. Eine Entscheidung hängt nicht zuletzt von der Gründung neuer CERTs in der Wirtschaft, sowie von politischen Faktoren und letztendlich auch von den weiteren Entscheidungen bezüglich einer KMU-CERT-Infrastruktur ab.

Literaturhinweise

[CSIHW 1/1989] Invitational Workshop on Computer Security Incident Response / Carnegie Mellon University, Software Engineering Institute. - Pittsburgh, PA, August 1991.

[KOM(2001)298] Sicherheit der Netze und Informationen : Vorschlag für einen europäischen Politikansatz / Kommission der europäischen Gemeinschaften. - Brüssel, Juni 2001. - KOM(2001)298 endgültig.

[Kossakowski 1992] Klassifikation und Abwehr von Computer-Würmern in Netzwerken / Klaus-Peter Kossakowski. - Diplomarbeit am Fachbereich Informatik, Universität Hamburg. - August 1992.

[Kossakowski et al. 1999] Responding to Intrusions / Klaus-Peter Kossakowski ; Julia Allen ; Christopher Alberts ; Cory Cohen ; Gary Ford ; Barbara Fraser ; Eric Hayes ; John Kochmar ; Suresh Konda ; William Wilson. - Security Improvement Module CMU/SEI-SIM-006. - Pittsburgh, PA: Carnegie Mellon University, 1999.

[Kossakowski 2000] Information Technology Incident Response Capabilities / Klaus-Peter Kossakowski. - Doctoral Thesis. - January 2000. - ISBN: 3-8311-0059-4.

[Kossakowski, Stikvoort 2000] A Trusted CSIRT Introducer in Europe - An empirical approach towards trust inside the European Incident Response scene - the replacement of trust by expectations / Klaus-Peter Kossakowski ; Don Stikvoort. - Amersfoort, NL: M&I/Stelvio, 2000.

[Pethia van Wyk] Computer Emergency Response : An International Problem / Richard D. Pethia ; K. R. van Wyk. - CERT Coordination Center. - Pittsburgh, PA, o. J.

[Salus 1995] Early Insecurity / Peter H. Salus. - Vortrag auf der *UNIX Network Security Conference* in Washington DC, November 1995. [Tagungsunterlagen]

[Scherlis et al. 1990] Computer Emergency Response / W. L. Scherlis ; S. L. Squires ; Richard D. Pethia. - In: *Computers Under Attack* / Peter J. Denning (Hrsg.). - Reading, MA: Addison-Wesley, 1990. [S. 495-504]

[Schultz Jr. 1990] The Computer Incident Advisory Capability / E. Eugene Schultz Jr. - September 1990. [Eingereicht für die *Office Information Management Conference (OIM)*, New Orleans, LA, 24.-26. Oktober 1990]

[Schultz Jr. et al. 1990a] Computer Emergency Response Teams : Lessons Learned / E. Eugene Schultz Jr. ; Richard D. Pethia ; J. R. Dalton. - Vortrag auf der *13. National Computer Security Conference*. - S. 634-640. [Tagungsunterlagen]

[Schultz Jr. 1991] The Computer Emergency Response Team System (CERT-SYSTEM) / E. Eugene Schultz Jr. - Livermore, Calif., Oktober 1991. [Eingereicht für die *14th National Computer Security Conference (NCSC)*, Washington DC, 1.-4. Oktober 1991]

[RFC 2350] Expectations for Computer Security Incident Response / Nevil Brownlee ; Erik Guttman. - Request For Comments 2350. - Juni 1998. - [Elektronisch veröffentlicht unter http://ds.internic.net/rfc/rfc2350.txt]

[West-Brown et al. 1998] Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J. West-Brown ; Don Stikvoort ; Klaus-Peter Kossakowski. - CMU/SEI-98-HB-001. - Pittsburgh, PA: Carnegie Mellon University, 1998.

[West-Brown, Kossakowski 1999] International Infrastructure for Global Security Incident Response / Moira J. West-Brown ; Klaus-Peter Kossakowski. - Pittsburgh, PA: Carnegie Mellon University, 1999.