Frühe Warnung im deutschen Internet

Kooperation im Bereich IT-Frühwarnung

Stand März 2007

1. Warum eine frühe Warnung?

Die gegenwärtig eingesetzte Informations- und Telekommunikationstechnologie (ITK) bietet mit ihrer zunehmenden Vernetzung und der damit einhergehenden Komplexität eine Vielzahl von Angriffspunkten. Dies führt zu einer schleichend größer werdenden Bedrohung, die alle Bereiche der Wirtschaft, Industrie, der öffentlichen Verwaltung sowie die Privathaushalte betrifft. Herauszuheben sind indes die Sektoren, die als „kritische Infrastrukturen" bezeichnet werden. Durch die Abhängigkeit vieler wichtiger Prozesse von funktionsfähigen ITK-Infrastrukturen wird eine Beeinträchtigung des öffentlichen und wirtschaftlichen Lebens durch kritische Angriffe auf diese Strukturen – und in der Folge dann auch durch eintretende Sicherheitsvorfälle – immer wahrscheinlicher. Ein Angriff wird dabei als eine Handlung mit der gezielten Absicht, einen Vorteil für Angreifer (oder Dritte) bzw. Nachteile für Betroffene (oder Dritte) zu bewirken, definiert. Er bedingt immer Vorsatz oder Anstrengungen, um das angestrebte Ziel zu erreichen. Diese können dabei direkter oder indirekter, offener oder versteckter Art sein.

Die Anzahl der identifizierten Sicherheitslücken von IT-Systemen ist seit den Neunzigern mit wenigen hundert pro Jahr stetig angestiegen und verharrt seit 2002 auf einem hohen Niveau von jährlich ca. 4.000 neuen Verwundbarkeiten. Diese Stagnation gilt jedoch nicht für die Anzahl der bekannten Sicherheitsvorfälle, hier sind die Steigerungsraten weiterhin überproportional, wobei von einer hohen Dunkelziffer ausgegangen werden muss. Neben dem hohen Grad der Vernetzung, der steigenden Konvergenz bislang getrennt betriebener ITK-Infrastrukturen sowie der Komplexität insgesamt, sind folgende Gründe für diesen Anstieg zu nennen:

- Einsatz leistungsfähiger Werkzeuge zur Analyse von Systemprogrammen und Anwendungen und mit der zumindest teilautomatisierten Ableitung von Schadprogrammen, die gefundene Sicherheitslücken ausnutzen können.
- Steigende Automatisierung für die Durchführung von Angriffen insgesamt und Verfügbarkeit modularer „Baukästen" zur schnellen Entwicklung neuer Schadprogramme.
- Zunahme der Komplexität der Angriffsformen durch Nutzung mehrerer Angriffsmöglichkeiten und Integration vielfältiger Schadensfunktionen in die eingesetzten Schadprogramme.

Aus Angriffen resultierende Schäden haben oft gravierende Folgen, auch der Zeitraum zwischen dem Bekanntwerden einer Schwachstelle und dem Eintritt eines Sicherheitsvorfalls wird immer geringer, so dass kaum Zeit für umfangreiche Analysen und vorbeugende Maßnahmen verbleibt. Ebenso ist zu verzeichnen, dass der Anteil kriminell motivierter Handlungen mit dem Ziel der finanziellen Bereicherung ansteigt und in der Öffentlichkeit große Aufmerksamkeit erhalten hat. Einige Experten weisen auf einen Zusammenhang zur organisierten Kriminalität hin. Auch die Möglichkeit terroristischer Angriffen ist nicht auszuschließen.

Bereits die kurze Skizzierung der Bedrohungssituation macht deutlich, dass neue Arbeitsweisen und Methoden entwickelt werden müssen, um dieser Situation letztendlich nicht nur reaktiv, sondern weiterhin auch vorbeugend begegnen zu können. In der Abbildung 1 wird diese Situation durch den

schraffierten Bereich graphisch hervorgehoben. Es gilt durch geeignete Maßnahmen dem Bedrohungspotential entgegenzuwirken. Eine Schadensminimierung kann nachweislich durch die rechtzeitige Verteilung von Informationen über aktuelle Bedrohungen und Risiken erreicht werden[1]. Es ist jedoch nicht ausreichend, lediglich öffentliche Quellen auszuwerten. Für die Validierung nicht verifizierbarer Informationen oder etwaiger Verdachtsmomente sind Daten erforderlich, die in den Informationsinfrastrukturen gewonnen werden müssen, die es zu schützen gilt. Eine frühe Warnung erscheint nur erfolgversprechend, wenn verschiedene Ansätze miteinander sinnvoll kombiniert werden, diese sind u.a.:

- Auswertung öffentlicher Informationsquellen
- Erfassung und (teil)automatisierte Verarbeitung von Sensordaten
- Analyse und Korrelation der Informationen und Sensordaten durch Analysten

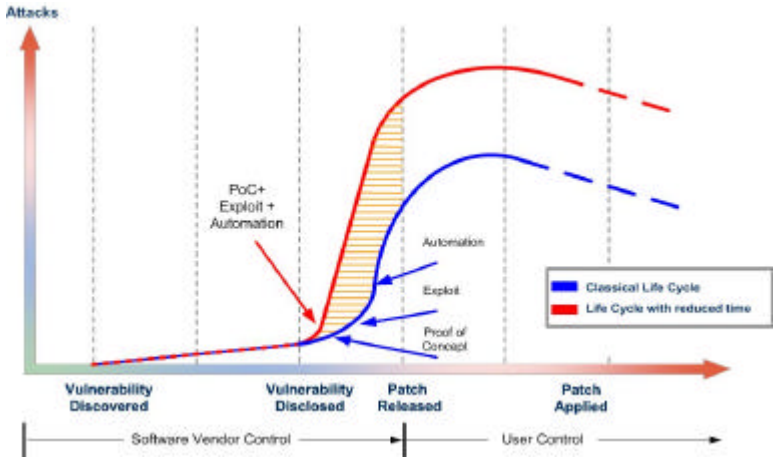

Abbildung 1: Lebenszyklus von Schwachstellen

Zum Schutz kritischer Informationsinfrastrukturen, wurden innerhalb des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erste Vorarbeiten für ein nationales IT-Frühwarnsystem durchgeführt. Durch das Projekt „Frühe Warnung im deutschen Internet“ konnten Fortschritte auf dem Weg hin zu einem deutschen IT-Frühwarnsystem aufgezeigt werden. Ziel des Projekts war es, mit überschaubaren Mitteln in einem definierten Zeitraum eine Architektur zu entwickeln, die relativ einfach und mit überschaubarem Aufwand umgesetzt werden.

2. Status der Arbeiten

Unter dem Arbeitstitel „CarmentiS“ konnte von Mitgliedern des deutschen CERT-Verbunds die Tragfähigkeit des vom BSI geförderten Konzeptes durch eine prototypische Implementierung unter Beweis gestellt werden. Dabei konnten wichtige Erkenntnisse bezüglich der Gestaltung eines nationalen Frühwarnsystem gewonnen werden, u.a:

- Durch die Sammlung und Auswertung von Daten aus unterschiedlichster Datenquellen, wie z. B. Fows aus Darknets und Ereignissen aus Intrusuion Detection Systemen (IDS), konnte unter realistischen Einsatzumgebungen erfolgreich in der Praxis getestet werden. Darüber hinaus konnte demonstriert werden, dass die Pseudonymisierungs- und Export-Funktionen die datenschutzrechtlichen Anforderungen eines datenliefernden Partners erfüllen kann.
- Mit dem Test der Pseudonymisierungs- und Export-Funktion entstand ein erster Datenpool, der zur Evaluierung der für die Analyse eingesetzten Methoden genutzt werden konnte. Es hat

---

1 Ebenso deutlich geht aus der Abbildung hervor, dass auch den Herstellem eine besondere Verantwortung zukommt.

sich deutlich gezeigt, dass ein Datenpool von realen Netzwerkbeobachtungen eine kritische Voraussetzung zur Entwicklung und Evaluation von jedweden Analyse- und Korrelationsmethoden ist.

- Der dem Projekt zugrunde liegende Ansatz, unterschiedliche Datenquellen von unterschiedlichen Partnern zu korrelieren, lieferte bereits in der Entwicklungsphase wertvolle Erkenntnisse.

Die Weiterentwicklung der Basiskomponenten des IT-Frühwarnsystems und die Überführung der prototypischen Implementierung in einen Pilotbetrieb erfolgt in der bewährten Form durch das BSI und Mitgliedern des deutschen CERT-Verbunds[2].

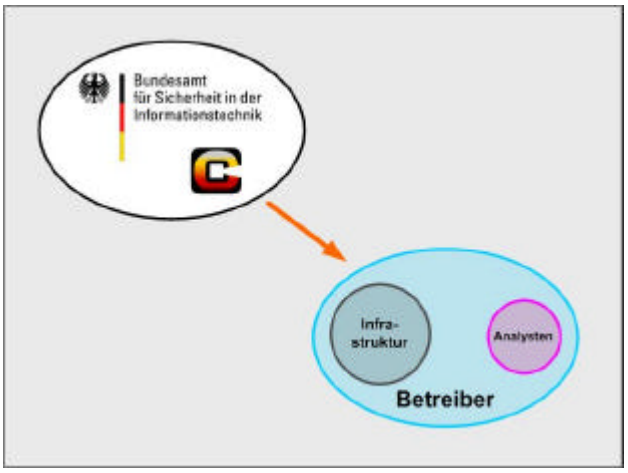

Abbildung 2: Betriebsmodell

In der Erprobungsphase konnten zunächst nur wenige Datenquellen erschlossen werden, aber auch anhand - der nur für wenige Bereiche - repräsentativen Daten, konnte die Funktionsweise der Analysewerkzeuge erfolgreich demonstriert werden. Ebenso wurde das Potential aufgezeigt, welches durch die konsequente Weiterentwicklung der aktuell verfügbaren Komponenten erschlossen werden kann, um sich der Zielsetzung eines national geprägten IT-Frühwarnsystems substantiell zu nähern.

Der Nutzen eines IT-Frühwarnsystems ist offensichtlich und liefert einen wichtigen Beitrag zum Schutz der ITK-Infrastrukturen. Die Implementierung von Frühwarnkapazitäten kann indes nicht die Aufgabe weniger sein, sondern muss als eine gemeinschaftliche Aufgabe gesehen werden. Derzeit haben folgende Organisationen Beiträge zu einem Frühwarnsystem geliefert:

- Staatliche Stellen
  - Schaffung politischer Rahmenbedingungen
  - Durchführung von Grundlagenarbeiten durch das BSI (unter Beteiligung von Forschungseinrichtungen)
- CERT-Verbund
  - Initiierung von Pilotprojekten
  - Betrieb der Infrastruktur
  - Bereitstellung von Analysekapazitäten

Damit die Aussagekraft eines solchen Systems verbessert, die Analysen und Trends präzisiert und letztendliche eine frühe Warnung bei Ereignissen, die ein hohes Schadenpotential aufweisen, realisiert werden kann, bedarf es einer ausreichenden Datenbasis. Bei der Bereitstellung dieser Datenbasis sind

---

[2] Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computer-Notfallteams, stellt jedoch kein Rechtssubjekt dar, d.h. er kann nicht Träger von Rechten und Pflichten sein. Der Betrieb der Infrastruktur wird daher durch die PRESECURE Consulting GmbH realisiert.

zunächst alle Wirtschaftsunternehmen und Verwaltungseinheiten gefordert, die ein elementares Interesse an einer funktionierenden ITK Infrastruktur haben.

3. Ebenen der Kooperation

Die Voraussetzungen für eine Kooperation im Bereich Frühwarnungen sind angemessene technische und organisatorische Schnittstellen notwendig, die bereits im Rahmen des Pilotprojekts geschaffen worden sind:

- Technische Schnittstellen:
  - Web-basierte Anwendungen
  - Kommunikationsinfrastruktur, die die Authentizität aller Benutzer und IT-Systeme sicherstellt und darüber hinaus die Vertraulichkeit der Kommunikation gewährleistet.
- Organisatorische Schnittstellen:
  - Kooperationsvereinbarungen zwischen Betreiber, Datenzulieferern, Analysten und Nutzern.
  - Regelungen in Bezug auf Vertraulichkeit und Verwendungszweck
  - Public Key Infrastruktur

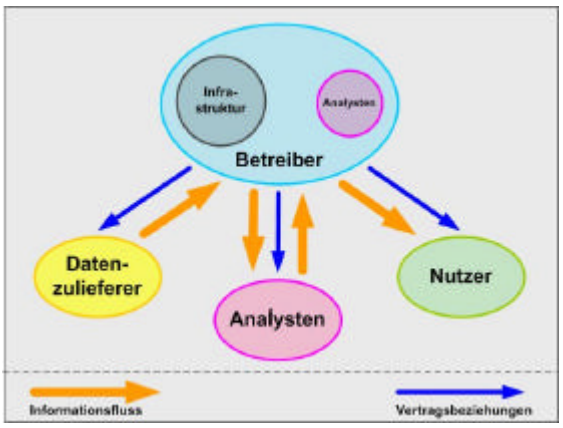

Abbildung 3: Ebenen der Kooperation

4. Wie können Sensordaten bereitgestellt werden?

Im Rahmen des Pilotbetriebs konnten vielfältige Erfahrungen bei der Integration von Datenquellen gemacht werden. Dabei hat sich eine Anzahl von unterschiedlichen Optionen als sinnvoll erweisen. Diese werden in den nachfolgenden Abschnitten kurz erläutert.

4.1 Bereitstellung von Daten, die bereits anderen Frühwarnsystemen zur Verfügung gestellt werden

Diese Form der Datenzulieferung bietet sich für alle Organisationen an, die sich bereits an bestehenden Analyse- und Warnsystemen beteiligen. Die Realisierung einer technischen Schnittstelle muss hier nur durch den Betreiber eines zuvor genannten Systems geleistet werden. Derzeit konnte dies bereits für eCSIRT.net umgesetzt werden. An der Integration weiterer Systeme, wie z.B. das Internet Analyse System (IAS) der Fachhochschule Gelsenkirchen und verschiedener Netzwerke zur Sammlung von Malware, wird derzeit gearbeitet.

Alle IP-Adressen der Datenzulieferer werden dabei durch den Betreiber vor Übergabe der Daten an die Frühwarnzentrale pseudonymisiert.

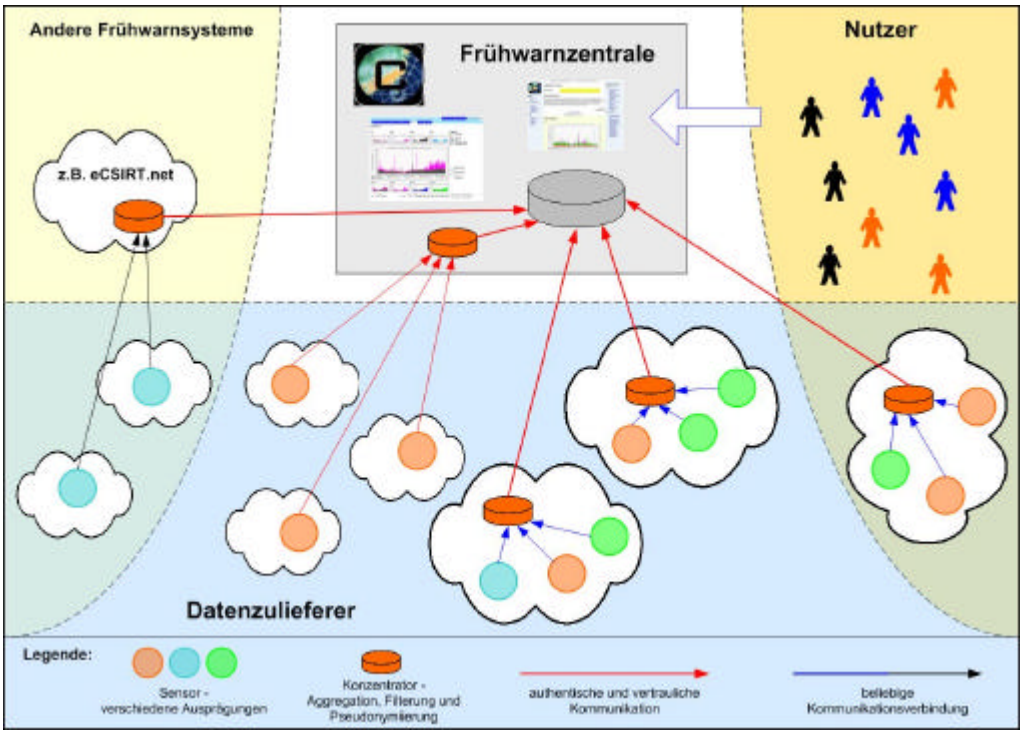

Abbildung 4: Optionen bei der Datenzulieferung

4.2 Betrieb eines CarmentiS-Sensors

Die Notwendigkeit dieser Option hat sich aus einer Vielzahl von Gesprächen mit Unternehmen ergeben, die aus verschiedenen Gründen keine eigenen IDS oder Monitoring-Systeme betreiben bzw. die erfassten Daten aufgrund bestehender Richtlinien nicht weitergeben dürfen.

Der so genannte CarmentiS-Sensor simuliert ein typisches Angriffziel (u.a. Windows und Linux basierte Serversysteme, die häufig verwendete Dienste zur Verfügung stellen) und verwendet dabei eine oder mehrere nicht genutzte IP-Adressen aus dem Adressbereich einer Organisation. Bei dieser Anordnung sind alle Verbindungsversuche als Angriffe zu bewerten. Grundsätzlich werden im Rahmen von CarmentiS keine Inhalte, Bestands- und Nutzungsdaten erhoben, was bei dieser Konstellation ohnehin nicht zutreffend ist. Personenbezogene Daten werden von den Sensoren nicht erfasst. Da dieser Sensor außerhalb des Intranets oder der DMZ platziert wird, können selbst bei einer Fehlfunktion, keine Kommunikationsverbindungen aus anderen Netzwerken erfasst und aufgezeichnet werden.

Alternativ bietet sich auch die Nutzung eines zu diesem Zweck betriebenen DSL-Anschlusses an.

- Die Software für einen Sensor wird kostenlos zu Verfügung gestellt; die einmalige Installationszeit beträgt ca. 30 – 60 Minuten.
- Alternativ kann - unter Beteiligung an den Kosten - eine Sensor-Appliance bereitgestellt werden. Sofern die Konfigurationsdaten vorab geliefert wurden, beschränken sich die Tätigkeiten auf Anschließen und Einschalten der Appliance.

Die Sensordaten werden unter Nutzung der vorhandenen Kommunikationsinfrastruktur verschlüsselt und an einen ausgezeichneten Konzentrator[3] der Frühwarnzentrale übermittelt. Alle IP-Adressen der Datenzulieferer werden vor Übergabe der Daten an die Frühwarnzentrale pseudonymisiert.

---

[3] Ein Konzentrator erfasst die Daten von mehreren Sensoren und stellt Funktionen zur Filterung, Pseudonymisierung, Export und ggf. zur Aggregation und Korrelation zur Verfügung.

4.3 Betrieb eigener Sensoren

Eine Vielzahl von Unternehmen betreiben zur Gewährleistung eines ordnungsgemäßen Betriebs ihrer ITK Infrastruktur und zum Schutz vor Angriffen aus dem Internet IDS/IPS und/oder Netzwerkmonitoringsysteme. Bei diesen Organisationen sind demnach eine oder mehrere Klassen von Sensoren bereits installiert, die auch Informationen erfassen, die für eine Frühwarnung genutzt werden können. Für die Anbindung an die Frühwarnzentrale werden in diesen Fällen die folgenden Funktionen benötigt:

- Exportfilter

  Da die Sensoren nicht nur Angriffe aufzeichnen können, muss sichergestellt werden, dass gewünschte Kommunikationsverbindungen gemäß einer Exportrichtlinie des Datenzulieferers beim Export unterdrückt werden.

- Pseudonymisierung

  Durch diese Funktion können sensitiven Daten (z.B. die Zieladresse) verschleiert werden. Das eingesetzte Verfahren basiert auf einem etablierten kryptographischen Mechanismus, welcher für den Einsatz im Rahmen von CarmentiS modifiziert wurde, um der spezifischen Anforderungen im Rahmen der IT-Frühwarnung zu genügen. Dabei wird ein nur dem Datenzulieferer bekannter Schlüsselpostfix eingesetzt, so dass der Betreiber ohne Mithilfe des Datenzulieferers die pseudonymisierten Originaladressen nicht auflösen kann.

- Anbindung an die Kommunikationsinfrastruktur

  Bereitstellung von Mechanismen für die Etablierung eines verschlüsselten und stark authentisierten Kommunikationskanals zum Betreiber der Frühwarnzentrale.

Diese Funktionen sind in Form von Softwaremodulen verfügbar und werden den Kooperationspartnern kostenfrei zur Verfügung gestellt. Ebenfalls kann - unter Beteiligung an den Kosten - eine Appliance bereitgestellt werden, die zukünftig noch mit weiteren Modulen ausgestattet werden kann (Präsentationsschicht, erweiterte Aggregations- und Korrelationsverfahren). Diese Form der Unterstützung wurde von vielen potentiellen Datenzulieferern eingefordert, um die Aufwände für die Installation beim Datenzulieferer und die Supportleistungen der Frühwarnzentral zu reduzieren.

Eine belastbare Aussage über die zu erwartenden Aufwände für die Integration kann an dieser Stelle nicht gegeben werden, da hier sehr unterschiedliche Ausgangslagen vorzufinden sind. Nach ersten Erfahrungen in der Erprobungsphase gestaltet sich die Integration problemlos, wenn Flowdaten oder OpenSource Intrusion Detection Systeme vorhanden sind. Bei der Integration von kommerziellen Monitoring, IDS oder Intrusion Prevention Systemen ist nicht auszuschließen,, dass Schnittstellenmodule realisiert werden müssen, weil propritäre Datenformate zum Einsatz kommen.

5. Zugang für Nutzer und Analysten

Ein wichtiges Ziel des Projekts ist die Schaffung eines Institutionen und Unternehmen übergreifenden Lagebilds zur Sicherheit im deutschen Internet. Dieses Lagebild wird über eine Web-Schnittstelle berechtigten Nutzern zur Verfügung gestellt. An dieser Stelle muss noch einmal mit Nachdruck darauf hingewiesen werden, dass in der aktuellen Situation die Datenbasis für ein belastbares Lagebild noch nicht ausreichend ist, daher können Dienste wie z. B. die Alarmierung derzeit noch nicht einer breiten Nutzergruppe zur Verfügung gestellt werden.

Trotz der zuvor genannten Einschränkungen in Bezug auf die Aussagekraft des Gesamtstatus („Ampel“) liefern die Analyseergebnisse bereits einen unmittelbaren Nutzen. Hier sind u.a. zu nennen:

- Trendanalysen
- Vergleichende Betrachtungen
  - mit Informationen anderer Systeme (z.B. aus Europa, USA und Asien)
  - und eigenen Erkenntnissen.

- Identifizierung und Alarmierung bei
  - ungewöhnlichen Ereignissen
  - neuer Schadsoftware
  - neuen Angriffsvektoren
  - aktuellen Angriffen

Bei ausreichender Unterstützung sind dann auch sektorspezifische Analysen und Auswertungen möglich. Abbildung 5 zeigt die aktuell verfügbare Benutzerschnittstelle. Diese enthält neben dem aktuellen Lagebild, zugehörigen Analyseergebnissen und statistischen Auswertungen auch zwei konfigurierbaren Menüleisten, in denen Verweise auf öffentliche Informationsquellen, News-Ticker, RSS-Feeds und sonstige relevante Informationen dem Benutzer zur Verfügung gestellt werden.

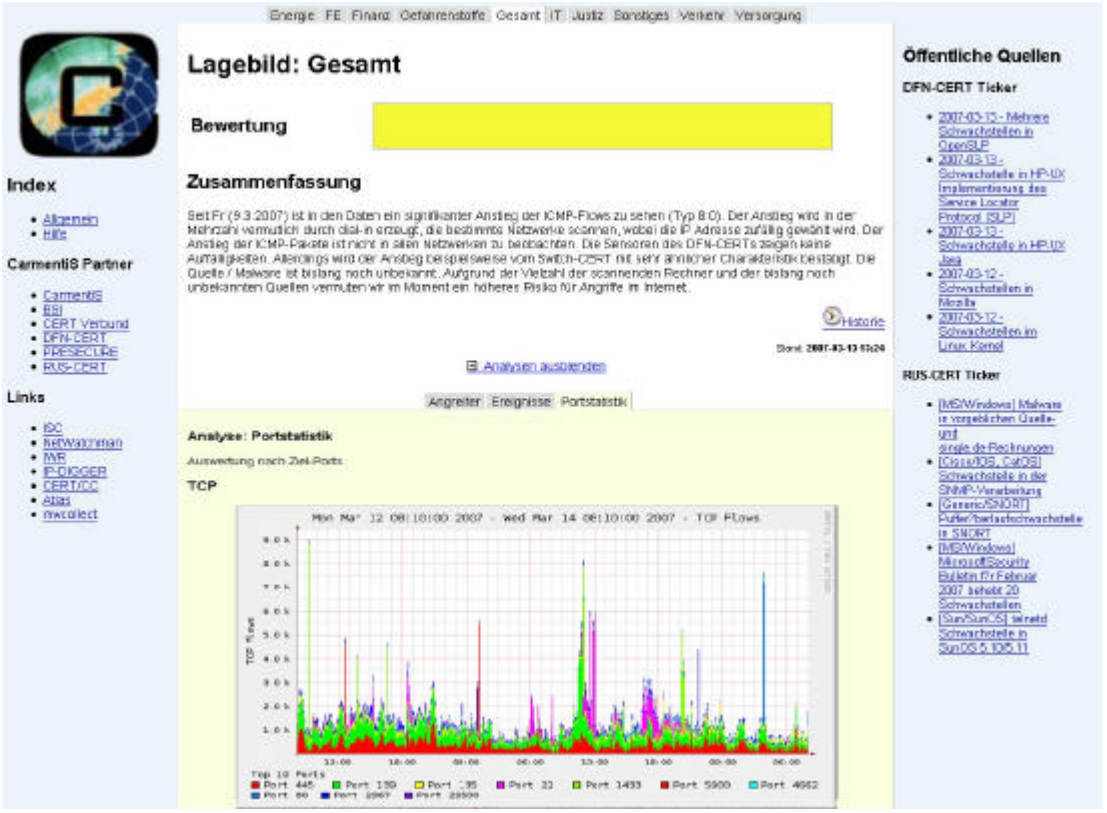

Abbildung 5: Benutzerschnittstelle

Wesentliche Punkte der Nutzungsvereinbarung sind:

- Nutzung der Informationen und Warnmeldungen nur für den eigenen Bereich
- keine kommerzielle Nutzung der Informationen
- Zeichnung einer Vertraulichkeitserklärung
- Beteiligung bzw. Mitarbeit bei der Realisierung eines nationalen IT-Frühwarnsystems

Eine Beteiligung an der Aufgabe IT-Frühwarnung durch die Stellung eines Analystenteams ist ebenfalls möglich und wird grundsätzlich angestrebt. In der gegenwärtigen Phase – Aufnahme des Pilotbetriebs – tritt die Aufnahme weiterer Analystenteams jedoch zunächst gegenüber der Integration von Datenquellen in den Hintergrund.

Für weitere Informationen stehen die nachfolgend genannten Ansprechpartner zur Verfügung.

Ansprechpartner

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Hans-Peter Jedlicka
Referat 121 – CERT-Bund
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888 9582-5822
Fax: +49 (0)1888 9582-905822

certbund@bsi.bund.de
http://www.bsi.bund.de
http://www.cert-bund.de

CERT-Verbund /
PRESECURE Consulting GmbH

Klaus-Peter Kossakowski
Tel: (+49) 0171 5767010
kpk@pre-secure.de

Jürgen Sander
Tel: (+49) 0171 7820685
js@pre-secure.de

http://www.carmentis.org