CarmentiS

- Frühe Warnung im deutschen Internet -

Jürgen Sander[1], Hans-Peter Jedlicka[2]
[1] PRESECURE Consulting GmbH
js@pre-secure.de
[2] Bundesamt für Sicherheit in der Informationstechnik,
Hans-Peter.Jedlicka@bsi.bund.de

Zusammenfassung: In diesem Beitrag wird das Projekt CarmentiS vorgestellt, das durch Mitglieder des deutschen CERT-Verbunds zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik umgesetzt wurde. Ziel des Projekts ist die Schaffung einer Basisinfrastruktur für die Erprobung verfügbarer Ansätze und Strategien zur Ermittlung von zeitnahen Informationen über aktuelle Bedrohungslagen im deutschen Internet.

1. Einleitung

Unsere Informationstechnik bietet mit ihrer zunehmenden Vernetzung eine Vielzahl von Angriffspunkten für feindliche Handlungen. Dies führt zu einer schleichend größer werdenden Bedrohung, die alle Bereiche der Wirtschaft, Industrie, der öffentlichen Verwaltung sowie die Privathaushalte betrifft. Herauszuheben indes sind Sektoren, die in der letzten Zeit als „kritische Infrastrukturen“ bezeichnet werden. Durch die Abhängigkeit vieler wichtiger Prozesse von funktionsfähigen IT- und TK-Systemen dieser Infrastrukturen, ist bei erheblichen Störungen eine Beeinträchtigung des öffentlichen oder wirtschaftlichen Lebens wahrscheinlich.

In den letzten Jahren ist die Anzahl der gemeldeten Sicherheitsvorfälle stark angestiegen. 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. Das IT-Sicherheitsmanagement ist heute in einer extrem schwierigen Situation. Ebenso ist zu verzeichnen, dass die Schadenswirkung durch kriminelle Handlungen (u.a. Phishing, Betrug, Erpressung) stark ansteigt. Einige Experten weisen auf einen Zusammenhang zur organisierten Kriminalität hin [BSI 2005]. Auch die Möglichkeit terroristischer Angriffe ist nicht ganz 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. Ein aus dem deutschen CERT-Verbund vorangetriebener gemeinschaftlicher Ansatz ist das Projekt CarmentiS. In enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden die Vorarbeiten aus dem Projekt „Frühe Warnung im deutschen Internet“ zusammen mit weiteren Komponenten in der Praxis erprobt und die Basis für ein nationales IT-Frühwarnsystem geschaffen. Ziel der gemeinsamen Anstrengungen war es, mit überschaubaren Mitteln in einem definierten Zeitraum eine Architektur zu entwickeln, die relativ einfach und mit überschaubarem Aufwand umgesetzt werden kann. Damit ist CarmentiS als Teil der Umsetzung des nationalen Plans [NPSI 2005] anzusehen, in dem der Aufbau eines Sensornetzwerks angekündigt wird, um IT-Sicherheitsvorfälle besser erkennen, erfassen und bewerten zu können.

1.1 IT-Frühwarnung

In den letzten 24 Monaten hat der Begriff „Frühwarnung“ nicht nur im Bereich IT-Sicherheit eine Inflation erlebt. Es werden sowohl Alarmierungssysteme – bei denen es nur um die rasche Information einer bestimmten Zielgruppe geht – als auch Forschungsarbeiten mit diesem publikumswirksamen Begriff in Zusammenhang gebracht. Dabei ist das zunehmende Interesse der Politik und Wirtschaft hierfür mit verantwortlich, da diese endlich die existierende Lücke erkannt haben und Lösungen einfordern.

Die Analogien, die für Frühwarnung jedoch oftmals bemüht werden, greifen auf Warnungen vor Naturkatastrophen zurück und fordern letztlich etwas – nicht nur für den Bereich der Computernetzwerke – technisch Unmögliches, nämlich das Verhalten von Menschen vorherzusagen. Bei Kenntnis neuer Sicherheitslücken kann mit einer fast 100%-igen Wahrscheinlichkeit davon ausgegangen werden, dass neue Angriffe erfolgen. Dies kann daher nicht der alleinige Maßstab sein, die Kernfragen sind anderes: Wann wird ein Schadprogramm das erste Mal eingesetzt? Wo wird es eingesetzt? Wird es in einem Wurm zu finden sein? Wird man einen solchen Angriff automatisiert erkennen können?

Trotz dieser ernüchternden Worte gibt es natürlich Verfahren, um Angriffe so wie früh wie möglich zu erfassen. Es ist jedoch unabdingbar, Frühwarnung sinnvoll zu definieren, um seriös über die technischen Möglichkeiten zu diskutieren. Daher muss ein Kompromiss zwischen Schnelligkeit und Genauigkeit gefunden werden:

Aufgrund eindeutiger Erkenntnisse, die noch möglichst wenige betreffen, sind Informationen zu verteilen, die vielen (noch nicht Betroffenen) helfen, und (insgesamt) Schlimmeres vermeiden!

1.2 Zielsetzung und Zielgruppen

Da dieser Ansatz geprägt ist durch eine enge inhaltliche Beziehung der IT-Frühwarnung mit der Arbeit der Computer-Notfallteams[1], sollten keine bereits bestehenden Strukturen des CERT-Bereichs ersetzt werden. Vielmehr sollten diese als mögliche Kooperationspartner sinnvoll in einen späteren Betrieb integriert werden. Dies galt insbesondere für Werkzeuge, Sensor-Netzwerke und in Hinblick auf die Betreuung der jeweiligen Zielgruppe sowie die Versorgung mit Informationen – für Warnungen bis hin zu Alarmierungen. Bei der Realisierung von CarmentiS standen die folgenden Vorgaben im Mittelpunkt:

- Aggregierte Informationen sollen für Nutzer zur Erstellung und Verbesserung von Lagebildern bzgl. der aktuellen Bedrohung zur Verfügung stehen (z. B. für Trendanalysen und vergleichende statistische Auswertungen).
- Bei der Analyse von neuen Sicherheitslücken sollen Experten zusammenarbeiten und hierbei Informationen, die über Angriffe im Netzwerk verfügbar sind, nutzen können. Entsprechend der aufgestellten Hypothesen soll gezielt nach neuen Angriffsmustern gesucht werden können.
- Angriffe im Netzwerk sollen für Nutzer möglichst früh erkennbar werden, damit
  1. Nutzer oder zuständige Verantwortliche ihre jeweilige Zielgruppe warnen können;
  2. Nutzer die Unterstützung der Betroffenen innerhalb ihrer jeweiligen Zielgruppe koordinieren können;
  3. Nutzer in ihrem eigenen Verantwortungsbereich weitere geeignete Gegenmaßnahmen initiieren können.

Sensornetze sind eine wichtige Komponente eines Systems, das dem Anspruch „Frühwarnung“ gerecht werden soll, jedoch muss vielmehr die Verknüpfung von menschlicher und (teil-) automatisierter Informationsverarbeitung gewährleistet sein, um alle Aspekte abdecken zu können.

1 In der englischen Sprache als Computer Emergency Response Team (CERT) bezeichnet.

Es gilt, durch ein gemeinsames Engagement möglichst vieler Kooperationspartner im Bereich Frühwarnung einen wesentlichen Mehrwert zu schaffen. Bei der Konzeption wurde zwischen den folgenden vier Nutzergruppen differenziert:

- **Operative Stellen auf nationaler Ebene**, die vor allem Interesse an Informationen zum Lagebild und zur Verbesserung des Krisenmanagements haben,
- **CERT-Teams**, die vor allem Interesse an der Betreuung der jeweils eigenen Zielgruppe, deren Alarmierung und der Aufklärung von Angriffen auf IT-Systeme der Zielgruppe haben,
- **Betreiber kritischer Infrastrukturen** erhalten ein aktuelles Lagebild, das ihnen ermöglicht, geeignete vorbeugende Maßnahmen zu ergreifen, sobald sich akute Gefahren abzeichnen,
- **Partner**, wobei hier insbesondere Organisationen zu nennen sind, die durch die Bereitstellung und Sammlung von Informationen oder Daten zu den Zielen eines Frühwarnsystems beitragen.

2. Architektur

Ziel der gemeinsamen Anstrengungen war eine substantielle Annäherung an die Vision einer „nationalen“ IT-Frühwarnung. Ein ehrgeiziges Ziel, denn es müssen Akteure in unterschiedlichen Rollen miteinander kooperieren und interdisziplinär zusammenarbeiten, Informationen und Daten aus einer Vielzahl von Quellen miteinander verknüpft und der gewonnene Mehrwert den unterschiedlichen Zielgruppen zur Verfügung gestellt werden.

2.1 Vorgehensweise

Um die Komplexität handhaben zu können, wurde das Gesamtsystem von unterschiedlichen Perspektiven aus betrachtet und so weit vertieft, wie es für eine Umsetzung erforderlich war.

- **Organisation:**
  CarmentiS geht von einem kooperativen Ansatz bei der Bereitstellung von Daten und der Analyse aus. Aufgrund der realen Gegebenheiten ist keine einzelne Organisation in der Lage, alle Daten für ein umfassendes Lagebild, geschweige denn für ein nationales IT-Frühwarnsystem, bereitzustellen, also muss von einer Zusammenarbeit verschiedener Organisationen ausgegangen werden, die zum gleichen Ziel beitragen wollen. In dieser Perspektive war vor allem die Verteilung der verschiedenen Aufgaben relevant. Daher musste die Rolle der Datenzulieferer, also Organisationen, die rechtlich unabhängig sind und die Daten in ihrem eigenen Bereich erheben, gesondert betrachtet werden. Dies erforderte eine differenzierte Betrachtung der:
  - Datenzulieferer – ebenso als „administrative Domänen“ bezeichnet:

    Eine administrative Domäne stellt sich aus Sicht der Frühwarnzentrale als schwarze Box dar, die Daten über Angriffe erhebt und für eine zentrale Auswertung zur Verfügung stellt. Aufgrund der Unabhängigkeit der administrativen Domänen mussten hier nur Vorgaben für die Schnittstellen und organisatorischen Regelungen gegeben werden.
  - Frühwarnzentrale:

    Diese stellt Komponenten bereit, die für die Aufgabe der Frühwarnung zentral aufgebaut und betrieben werden müssen. Alle Daten und Informationen fließen an dieser Stelle zusammen und können im Gesamtkontext durch Analysten ausgewertet werden.
- **Komponenten:**
  Hierunter sind die „Building Blocks“ der Frühwarnzentrale zu verstehen, die einen inhaltlich zusammenhängenden Aufgabenbereich übernehmen, wobei zunächst offen war, wie diese

Funktionen erbracht werden. Die folgenden Komponenten wurden identifiziert und inhaltlich erschlossen:

- Datenübergabe von Datenzulieferern: Die Übernahme der bereitgestellten Daten in den zentralen Datenbestand erfordert eine Synchronisation der technischen Kommunikation zwischen Datenzulieferer und der Frühwarnzentrale.
- Informationsmanagement: Diese Komponente hat eine zentrale Bedeutung für das Gesamtsystem. Sie dient der Aufbereitung und Speicherung von angereicherten Daten, Ergebnissen und Informationen, die zur Erbringung der Aufgabenstellung, z. B. die Erstellung eines Lagebildes und die Alarmierung bei besonderen Vorkommnissen, benötigt werden.
- Arbeitsumgebung für die Analyse: Kernaufgabe der Analyse ist die Wertschöpfung aus den im Gesamtsystem vorliegenden Daten und Informationen. Diese Wertschöpfung kann nicht durch Automatisierung allein erreicht werden, sondern erst durch die Verknüpfung von menschlicher mit automatisierter Informationsverarbeitung. Dies stellt auch eines der herausragenden Merkmale der Gesamtarchitektur dar, in der durch Kooperation die verteilte Analyse und Bearbeitung von neuen Sicherheitslücken sowie die Bewertung der aktuellen Sicherheitslage möglich wird.
- Bereitstellung der Ergebnisse: Präsentation der Resultate der internen Informationsverarbeitung für die jeweiligen Nutzer, wobei der Zugang reglementiert sein wird. Für die benötigten Funktionen werden technische Schnittstellen definiert, über die die jeweilige Repräsentation der benötigten Informationen (Sichten) verfügbar gemacht werden können.

- **Schnittstellen:**
  Die Kommunikation zwischen den verschiedenen Komponenten muss über vereinbarte Protokolle und Austauschformate erfolgen. Der Schwerpunkt der Architektur richtet sich naturgemäß auf die für Nutzer zur Verfügung gestellten Schnittstellen. Hierbei waren insbesondere folgende Fragestellungen relevant:

  A) Wie erhalten Analysten **Zugang zur Arbeitsumgebung** und zu den verfügbaren Daten und Informationen?

  B) Wie werden **Daten von den Datenzulieferern** bereitgestellt und entgegengenommen?

  C) Wie erhalten Nutzer **Zugang zu den Diensten** und bereitgestellten Ergebnissen?

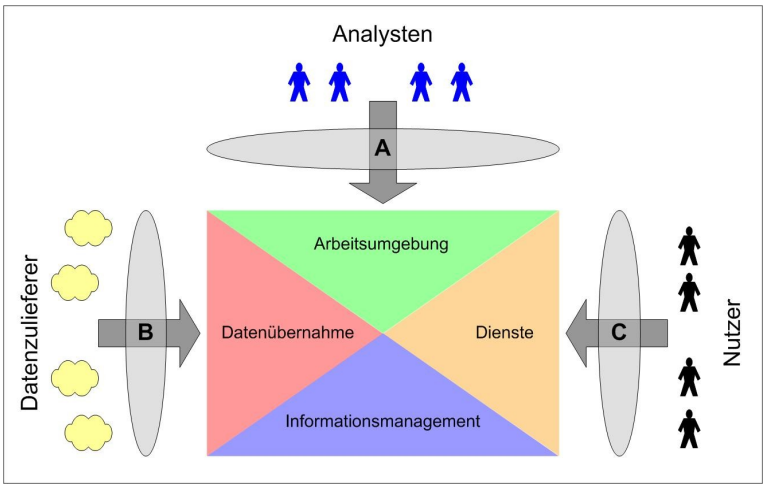


Abbildung 1: Schnittstellen der Frühwarnzentrale

3. Realisierung

Um die notwendigen Grundlagen für eine spätere Implementierung zu legen, wurden die spezifischen Anforderungen der Analysten und Nutzergruppen analysiert und benötigte Funktionen, Daten und Leistungsanforderungen identifiziert. Anschließend wurden bereits existierende Werkzeuge hinsichtlich einer Adaption evaluiert. Die einzelnen Funktionen wurden in Basis- und erweiterte Funktionen unterschieden und somit eine Priorisierung der Umsetzung vorgegeben. Diese Vorgehensweise wurde konsequent auf die Datenbeschreibungen übertragen, die aus einer logischen Sicht modelliert wurden. Abschließend wurden die spezifischen Leistungsanforderungen (u.a. barrierefreier Zugang zu den Systemen, Authentizität der Nutzer und Sicherheit der Kommunikationsverbindungen) der zu realisierenden Funktionen ermittelt.

3.1 Datenübergabe

Maßgeblich für den Erfolg eines IT-Frühwarnsystems ist eine ausreichende Erschließung von repräsentativen Daten für eine zentrale Analyse. Unter Daten werden im Kontext von CarmentiS Informationen über Verstöße gegen Sicherheitsrichtlinien verstanden. Da sich eine administrative Domäne durch ihre organisatorische Unabhängigkeit auszeichnet, beschränken sich die Gestaltungsvorgaben im Hinblick auf eine Datenübergabe ausschließlich auf die Definition der Schnittstellen zur Frühwarnzentrale. Um eine Übergabe von Sensordaten - einheitlich für alle - zu ermöglichen, wurden existierende Datenformate und Technologien evaluiert, Anforderungen an die Datenübergabe analysiert und letztendlich ein Übergabeformat spezifiziert. Dabei wurden verschiedene Fragestellungen erörtert, u.a. die Erfassung von Metadaten, ohne die eine korrekte Bewertung und eine automatisierte Vor-Verarbeitung nicht möglich ist. Das Hauptaugenmerk lag indes bei dem Schutz sensitiver Informationen.

Schutz sensitiver Information

Aus dem Blickwinkel der Frühwarnzentrale stellt sich die Situation wie folgt dar. Es muss davon ausgegangen werden, dass eine administrative Domäne nur solche Daten zur Verfügung stellt, die datenschutzrechtlich unbedenklich sind. Insbesondere sind dies Daten über unerwünschte Kommunikationsverbindungen, die von außen initiiert wurden und somit als Angriff zu bewerten sind. Es werden grundsätzlich keine Bestands- und Nutzungsdaten sowie Kommunikationsinhalte an die Frühwarnzentrale übermittelt.

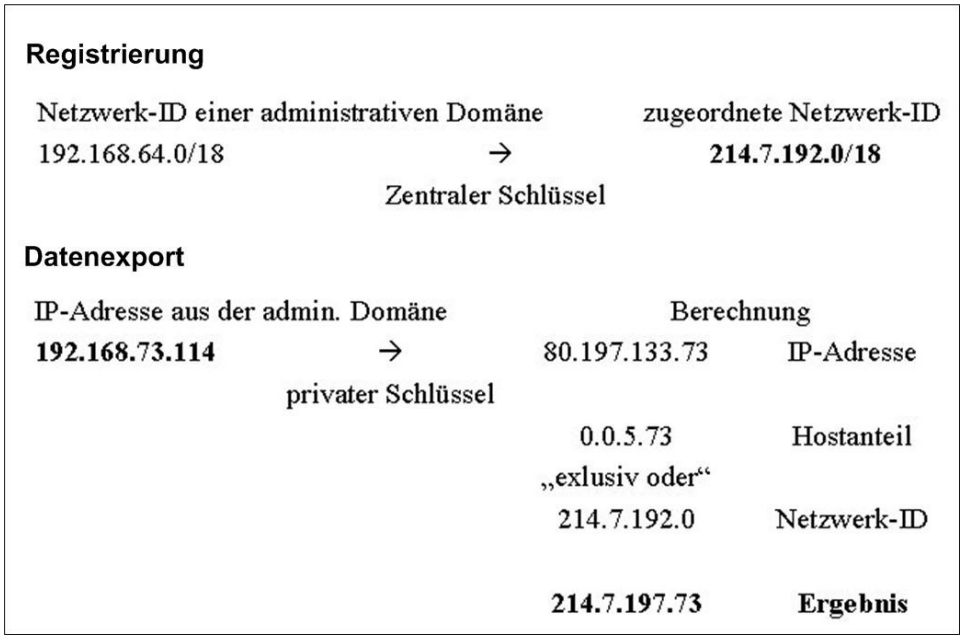


Abbildung 2: Pseudonymisierung

Um den berechtigten Anforderungen der administrativen Domänen bzgl. des Schutzes ihrer Belange gerecht zu werden und weiterhin eine aussagekräftige Analyse zu ermöglichen, wurde ein von Sicherheitsexperten akzeptiertes Verfahren [FAN 2004] zur Anonymisierung von sensitiven Datenfeldern (hier IP Adressen) adaptiert, das sich durch die folgenden Eigenschaften charakterisieren lässt:

- Die Informationen über die Netzwerkstruktur bleibt verfügbar (Präfix erhaltende Anonymisierung).
- Es erfolgt eine eindeutige Abbildung der IP-Adressen.
- Eine Auflösung der Anonymisierung kann ausschließlich durch die administrative Domäne erfolgen, welche die Daten bereitstellt.

Da eine vollständige Übergabe aller automatisch durch Sensoren gesammelten Daten mit den internen Belangen und Vorgaben einer administrativen Domäne nicht vereinbar ist, wurde ein Werkzeug implementiert, das neben einer Pseudonymisierung zusätzliche Funktionen zur Filterung und Verifikation der zum Export vorgesehenen Daten bereitstellt. Anschließend werden die Daten durch einen Transportdienst zur Frühwarnzentrale übermittelt, der die Vertraulichkeit, Integrität und Authentizität sicherstellt. Der Einsatz dieses Werkzeugs ist optional und nicht verpflichtend, es vereinfacht jedoch die Teilnahme am Frühwarnsystem erheblich. Sofern Daten zur Verfügung gestellt werden, die der Spezifikation entsprechen, können auch andere Werkzeuge durch die administrativen Domänen eingesetzt werden.

Da ein überwiegender Teil der im Bereich Netzwerksicherheit verfügbaren Werkzeuge, im Hinblick auf die hohen Anforderungen in Bezug auf die Performanz, auf Basis der Programmiersprache “C” entwickelt werden, wurde bei der Entwicklung der Software ebenfalls diese Umsetzungsoption gewählt. Die Entwicklung dieses Werkzeugs, wie auch aller weiteren Softwarekomponenten, erfolgte auf einem Linux-Betriebssystem.

3.2 Informationsmanagement

Für die Verarbeitung und die Präsentation der Informationen, die im Rahmen einer automatisierten Datensammlung durch Sensoren verfügbar werden, benötigt man besondere Funktionalitäten. Eine Design-Entscheidung mit einer weitreichenden Auswirkung betraf die Frage der zentralen Datenhaltung. Erkenntnisse aus anderen Projekten haben aufgezeigt, dass aufgrund der Menge der kontinuierlich zu verarbeitenden Daten und den damit verbundenen Anforderungen an die Verarbeitungszeit für Einfügungen oder Abfragen der alleinige Einsatz einer relationalen Datenbank nicht zielführend ist. Dies war ein wesentlicher Grund, warum die Werkzeugsammlung für die Verarbeitung von Netflow[2] Daten vom SWITCH-CERT [Haag 2005] als Basis für die Implementierung ausgewählt wurde. Diese Werkzeuge haben sich in der Praxis zur Überwachung der SWITCH Internet-Gateways ausgezeichnet bewährt und stellen ein hochperformantes und skalierbares Datei-basiertes Basissystem zur Verfügung, das in der Lage ist, große Datenmengen zu verarbeiten.

Das Kommandozeilen-orientierte Basissystem (*nfdump*) wurde hinsichtlich der Belange der Frühwarnzentrale adaptiert und um zusätzliche Funktionen erweitert. Schwerpunkte waren:

- Erweiterung des internen Datenformate um Meta- und IDS-Informationen
- Verarbeitung von IDS- und alternativen Flowformaten
- Normalisierung der Sensordaten
- Erzeugung zusätzlicher Statistiken
- Erweiterung der Filtersyntax

Ebenso wurde der Verarbeitungsablauf der Sensordaten hinsichtlich der Aufgabenstellung modifiziert. In der Abbildung 3 ist der Datenfluss der Sensordaten schematisch dargestellt. In der aktuellen Implementierung werden die Daten einer administrativen Domäne durch das Exportwerkzeug gefiltert, pseudonymisiert und an die Frühwarnzentrale übermittelt. Der Kollektor (eine mögliche Realisierung ist durch den Einsatz eines Prelude-Managers mit einem entsprechendem Plug-In gegeben[3]) nimmt die Daten in dem innerhalb des Projekts spezifizierten Format entgegen und legt die Daten in einem Spoolbereich ab. Im Gegensatz zur ursprünglichen Implementierung werden hier nicht einzelne Informationsquellen unterschieden, sondern entsprechend der integrierten Metainformationen verschiedene Kategorien von Daten zusammengefasst. Eine Kategorie wird durch die Art der Sensordaten (z.B. Flows oder IDS) und der Anordnung eines Sensors (u.a. Darknet, DMZ) definiert. Im folgenden Verarbeitungsschritt werden die Daten in ein internes Datenformat konvertiert oder normalisiert und in einem Arbeitsverzeichnis abgelegt. In diesem Verzeichnis werden alle eingehenden Daten vorgehalten, dies wird im weiteren als Live-Profil bezeichnet.

---

2 Netflow ist ein von CISCO entwickeltes Konzept (auch Datenformat) zur Erfassung von Kommunikationsverbindungen.

3 Prelude Homepage : http://www.prelude-ids.org

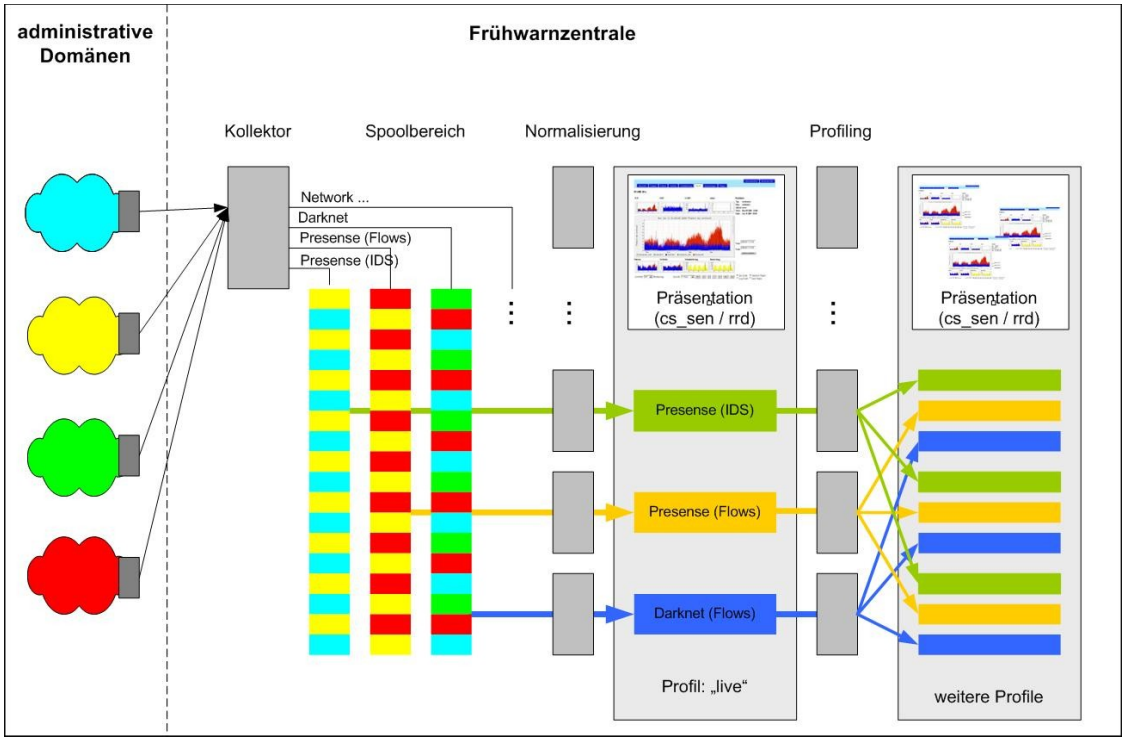


Abbildung 3: Informationsverarbeitung

Im Anschluss an die Normalisierung kann das so genannte Profiling erfolgen. Das Profiling ist eine automatische Informationsverarbeitung, die auf Basis von Filterregeln erfolgt, die ein Analyst über entsprechende Funktionen der Präsentationsschicht aktivieren kann.

3.3 Arbeitsumgebung für die Analyse

In einem zweiten Schritt wurde die Präsentationsschicht des Basissystems (*nfsen*) an die Belange der Frühwarnzentrale angepasst und erweitert. Die Präsentationsschicht arbeitet jedoch nicht direkt auf den Sensordaten, sondern nutzt Round-Robin-Datenbanken (RRD)[4], die alle fünf Minuten aktualisiert werden. Durch die Einbeziehung dieser Zwischenschicht bekommt ein Analyst jederzeit einen Einblick, wie der Status bzgl. Angriffen und Angriffsversuchen einzuschätzen ist. Neben den notwendigen Modifikationen der Datenbankschemata wurden weitere Visualisierungsmodule für Detailansichten (u.a. Schadwirkung und Bewertung von IDS Signaturen) implementiert und in das Navigationsschema des Analyse-Werkzeuges integriert. In der Abbildung 5 ist die obere Hälfte der Detailansicht für Sensordaten dargestellt, durch das die Daten eines Profils nach Protokoll, Schadwirkung und Bewertung selektiert in alternativen zeitlichen Abschnitten dynamisch dargestellt und bearbeitet werden können.

4 Homepage des Projekts: http://oss.oetiker.ch/rrdtool/

Abbildung 4: Benutzeroberfläche für Analysten

In der unteren Hälfte des Fensters (Abbildung 5) sind die Kontrollelemente angeordnet, die einen detaillierten Zugriff auf die selektierten Sensordaten ermöglichen. Hierdurch kann ein Analyst direkt auf die Sensordaten zugreifen, um auffällige Kommunikationsverbindungen im Detail zu analysieren oder spezifische Statistiken zu erzeugen. Die verwendete Filtersyntax ist an *tcpdump*[5] angelehnt, diese wurde jedoch um einige Optionen erweitert.

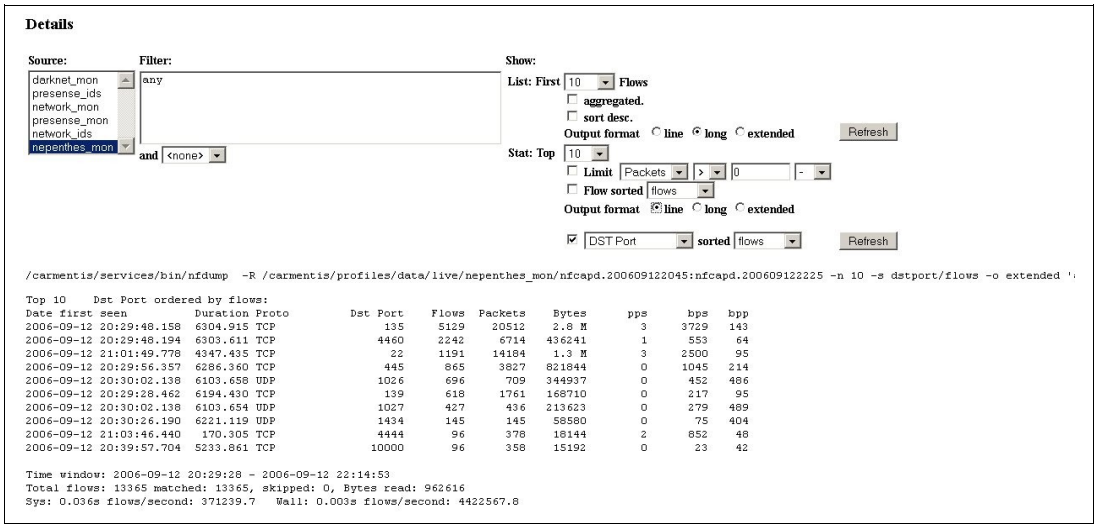


Abbildung 5: Detailzugriff auf die Sensordaten

Die Arbeitsumgebung für Analysten kann durch Plug-Ins erweitert und somit an spezifische Anforderungen angepasst werden. Ein Plug-In besteht aus einem Backend und einen optionalen Frontend für die Präsentation. Durch die Integration eines Plug-Ins kann z.B. auf wichtige statistische Auswertungen direkt zugegriffen werden oder es können neue Analysemethoden evaluiert und in die Arbeitsumgebung integriert werden. Folgende Plug-Ins werden derzeit verwendet:

5 TCPDump ist ein häufig zur Netzwerkanalyse genutztes Programm; es ist in fast allen Unix/Linux-Distributionen enthalten.

- Portstatistik

  Darstellung der angegriffenen Zielports (Top 10, Selektion und Unterdrückung einzelner Ports, tabellarische Zusammenfassung).

- IDS-Signaturen

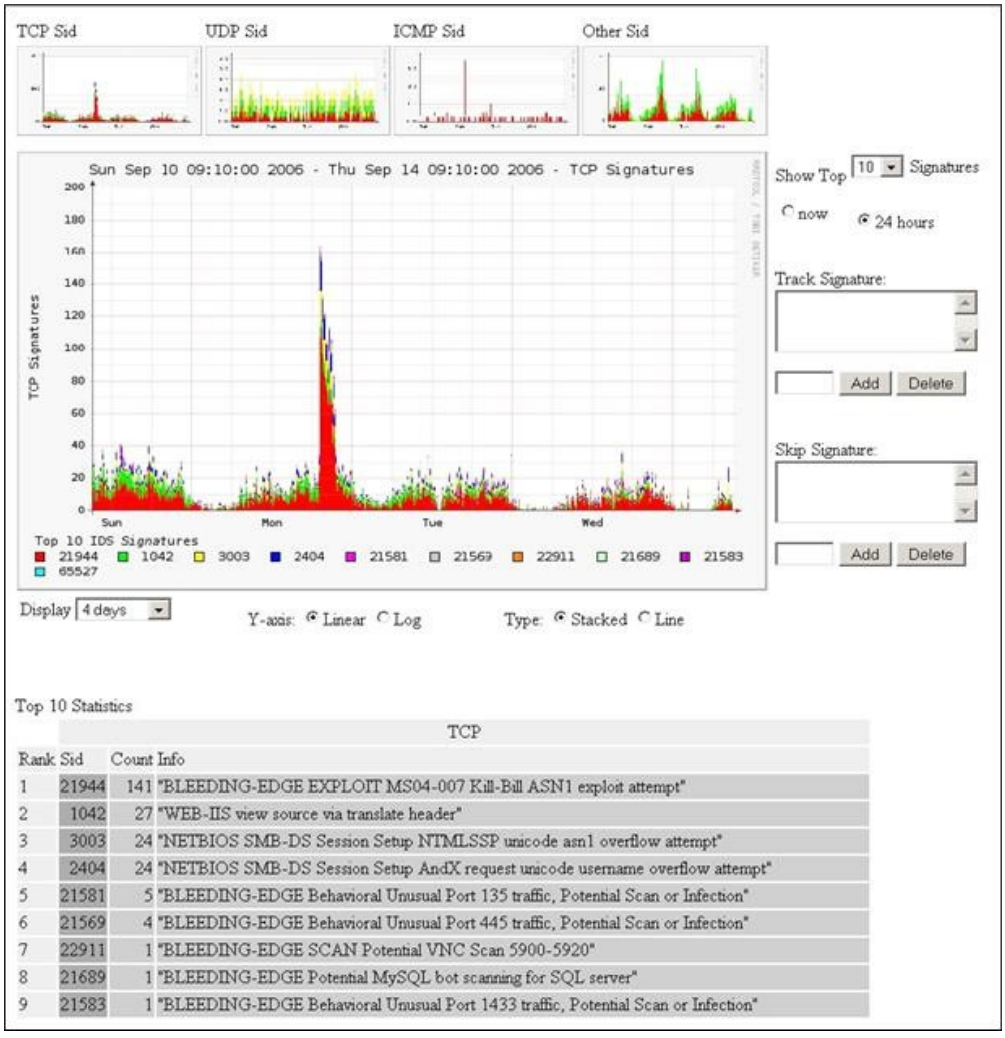
  Statistische Aufarbeitung erkannter IDS Angriffssignaturen (analog zur Portstatistik, dazu Abbildung 6)

- Metainformationen

  Angabe der Summe aller aktiven Quell- u. Ziel IP-Adressen für eine vorgegebene Zeiteinheit und Anzahl und Art der aktiven Datenquellen.

- Alarmierungsmodule

  Um den Analysten bei außergewöhnlichen Vorkommnissen oder Anomalien zeitnah informieren zu können, wurden zwei Verfahren zur Angriffserkennung integriert. Bei einem Modul werden statische Vorgaben (Schwellwerte) für verschiedene Alarmierungszustände definiert, deren Überschreitung innerhalb eines Zeitfensters zur Alarmierung führt. Das zweite Modul ermittelt durch ein bayesisches Verfahren [ISMO 2004] die Wahrscheinlichkeit von kritischen Zuständen.



Top 10 Statistics

		TCP	
Rank	Sid	Count	Info
1	21944	141	"BLEEDING-EDGE EXPLOIT MS04-007 Kill-Bill ASN1 exploit attempt"
2	1042	27	"WEB-IIS view source via translate header"
3	3003	24	"NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt"
4	2404	24	"NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt"
5	21581	5	"BLEEDING-EDGE Behavioral Unusual Port 135 traffic, Potential Scan or Infection"
6	21569	4	"BLEEDING-EDGE Behavioral Unusual Port 445 traffic, Potential Scan or Infection"
7	22911	1	"BLEEDING-EDGE SCAN Potential VNC Scan 5900-5920"
8	21689	1	"BLEEDING-EDGE Potential MySQL bot scanning for SQL server"
9	21583	1	"BLEEDING-EDGE Behavioral Unusual Port 1433 traffic, Potential Scan or Infection"

Abbildung 6: IDS Statistik

3.4 Nutzerschnittstelle

Die durch die manuelle und automatische Auswertung gewonnenen Erkenntnisse werden in einzelne Analysen zusammengefasst, mit weiteren Informationen verknüpft und zu einem Lagebild (Abbildung 7) verdichtet. Dieses wird verschiedenen Nutzergruppen (CERTs, operative Stellen auf nationaler Ebene) durch spezifische Sichten (Sektoren der kritischen Infrastrukturen) zugänglich gemacht. Dafür wurde als Ergänzung des Analysewerkzeugs ein kollaboratives System zur Wartung und Pflege von Lagebildern, Analysen, und Benutzergruppen der Frühwarnzentrale als PHP Web-Applikation realisiert. Diese Anwendung beinhaltet Verfahren zur automatisierten Verknüpfung von Daten der Frühwarnzentrale wie auch Möglichkeiten zur Verknüpfung externer, öffentlich verfügbaren Informationsquellen, um so Analysten und Nutzern die Recherche zu erleichtern.

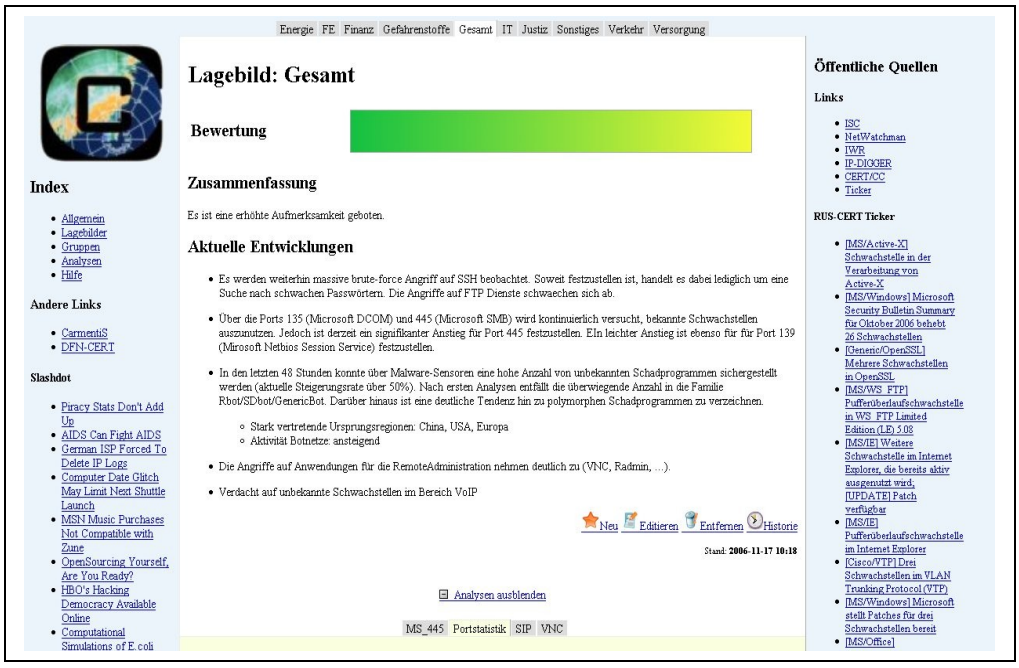


Abbildung 7: Lagebild / Nutzersicht

Die Lagebilder und vertiefende Untersuchungen werden dabei von Analysten unter Nutzung der in Abschnitt 3.3 beschriebenen Arbeitsumgebung manuell erstellt und im System für Nutzer bereitgestellt. Um die Benutzergruppen, Lagebilder und Analysen effektiv erzeugen und darstellen zu können werden entsprechende Webformulare unter Integration der Markdown-Formatsyntax[6] zur vereinfachten Erzeugung textueller Inhalte bereitgestellt und eine RSS[7]-Integration vorgenommen.

4. Erprobung und Tests

Bei einem Projektpartner, der über die notwendigen Voraussetzungen für den Betrieb (Fachpersonal und breitbandige Verbindung in das Internet) verfügt, wurde die Implementierung der Frühwarnzentrale im Frühsommer 2006 begonnen. Neben den zuvor beschriebenen primären Anwendungen der Frühwarnzentrale wurde eine Public Key Infrastruktur aufgebaut. Durch diese Basistechnologie werden zertifikatsbasierte Sicherheitsdienstleistungen für alle Entitäten

6 Markdown Homepage: http://daringfireball.net/projects/markdown/

7 RSS - Abkürzung für Really Simple Syndication. Eine Technik, die es dem Nutzer ermöglicht, die Inhalte einer Webseite zu abonnieren.

bereitgestellt. Auf dieser Grundlage wird die Absicherung der Kommunikationsplattform, eine hinreichende Sicherheit (Integrität und Vertraulichkeit) der Daten und eine aussagekräftige Authentizität (Identifikation und Unabstreitbarkeit) aller Nutzer erreicht.

Durch die Erprobung und Tests unter Produktionsbedingungen konnte nicht nur die Tragfähigkeit dieses Ansatzes demonstriert werden, sondern bereits konkret mit realistischen Daten gearbeitet werden.

4.1 Analyse realistischer Daten

In diesem Abschnitt soll der Leistungsumfang der Analyseplattform exemplarisch dargestellt werden. Zwar konnten für die Erprobungsphase nur wenige Datenquellen erschlossen werden, aber auch anhand der nur für wenige Bereiche repräsentativen Daten konnte die Funktionsweise der Analysewerkzeuge erfolgreich demonstriert werden. Auch wird das Potential aufgezeigt, das durch die Weiterentwicklung der aktuell verfügbaren Komponenten erschlossen werden kann, um sich der Zielsetzung eines national geprägten IT-Frühwarnsystems zu nähern.

Ausnutzung von Schwachstellen

Im Mai 2006 warnte u.a. das DFN-CERT vor potentiellen Schwachstellen im VNC-Server[8]. Dieser wird in der Standardinstallation über den TCP Port 5900 angesprochen. Nachdem im September vereinzelt Zugriffe auf dem Port registriert werden konnten, wurde ein entsprechendes Analyseprofil (Abbildung 8) angelegt. Diesem Profil war eine deutliche Zunahme der Angriffe seit dem 07.10.2006 zu entnehmen, deutlich vor dem Termin weiterer Warnmeldungen vom 11.10.2006, in der die Ausnutzung der Schwachstellen präzisiert wurde. (CIAC[9] - RealVNC Authentication Bypass)

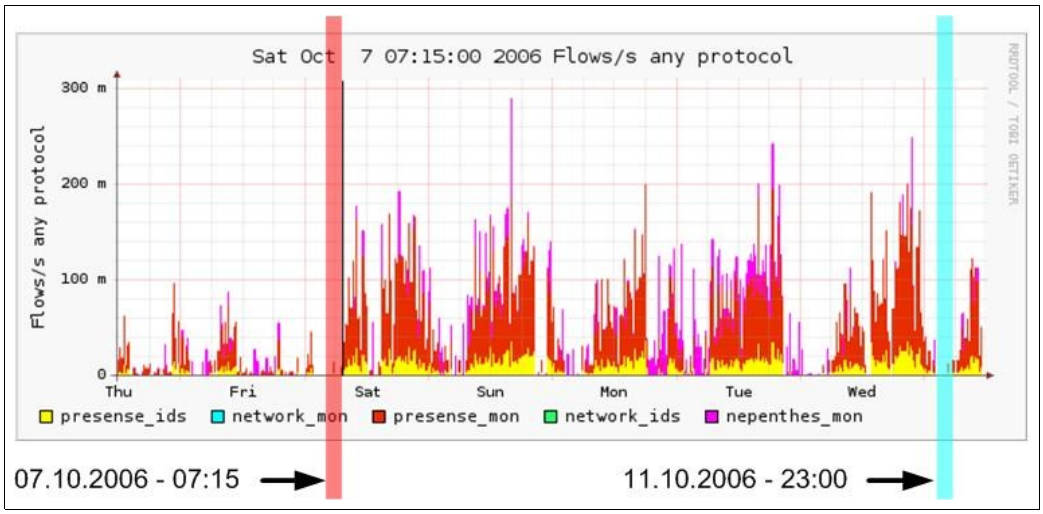


Abbildung 8: Schwachstellen im VNC-Server

8 Software für die Fernwartung von IT-Systemen.

9 The U.S. Department of Energy - Computer Incident Advisory Capability

Anhand dieses Beispiels kann auch die Wirkungsweise des Alarmierungsmoduls gezeigt werden. Am 07.10.2006 wurde durch das Modul ein Alarm ausgelöst.

Je nach Konfiguration der Schwellwerte, hätte eine Alarmierung der Analysten auch schon ein paar Tage früher erfolgen können (Abbildung 9).

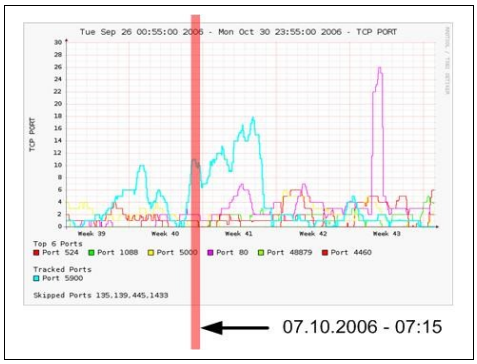


Abbildung 9: Alarmierungsmodul

Ausbreitung von Schadsoftware

Ende Oktober konnte die Ausbreitung einer neuen Schadsoftware[10] beobachtet werden. Ausgewertet wurden die Anfragen an den Port 48879 TCP (Backdoor[11] des Schadprogramms), die vereinzelt seit dem 17.10.2006 registriert werden konnten (Abbildung 10 – 1). In diesem Fall erfolgte jedoch keine großflächige Verbreitung. Die Anfragen an die Backdoor der Schadsoftware kamen zu über 90 % aus zwei Netzbereichen. Dies erklärt den Verlauf der Infektion in dem betreffenden Analyseprofil. Am 22.10.2006 wurde ein Netz in Polen (2) befallen, in den folgenden Tagen wurden insgesamt ca. 500 verschiedene Quell-IPs registriert. Ab dem 23.10.2006 war ein Netz in Deutschland (3) betroffen, verbunden mit starken horizontalen Portscans[12] (Anzahl der Quell IPs 26).

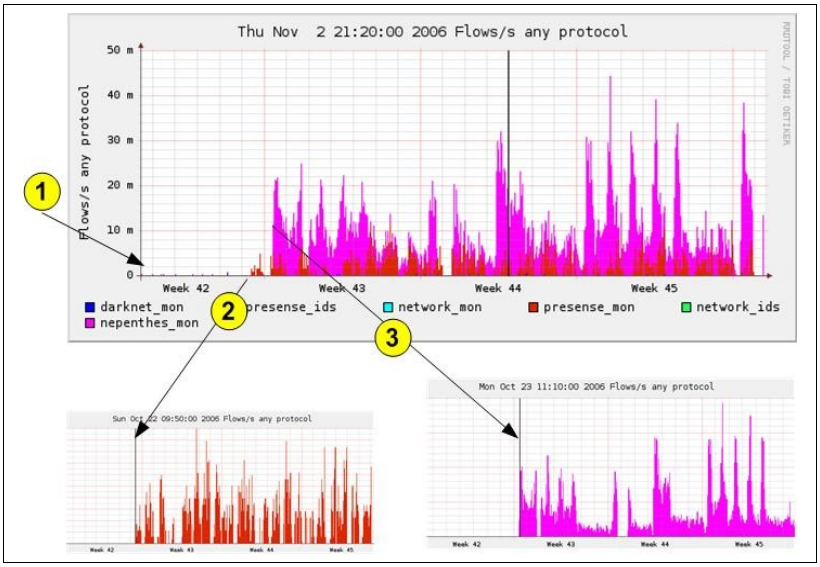


Abbildung 10: Ausbreitung eines Schadsoftware

---

10 Sammelbegriff für alle Arten von Software, die vom Anwender unerwünschte (schädliche) Funktionen ausführen (u.a. Würmer, Viren, Trojaner, Rootkits); häufig auch als Malware (malicious Software) bezeichnet.

11 Als Hintertür oder Backdoor bezeichnet man einen Teil eines Programms, durch den ein Zugang zu einem Computer - unter Umgehung der normalen Zugriffssicherung - ermöglicht wird.

12 Durch einen Portscan – oder auch einfach Scan - wird mittels eines Portscanners abgefragt, welche Dienste ein IT-System anbietet. Oft werden von einem Portscanner Zusatzfunktionen angeboten, z.B. Betriebssystemkennung. Bei einem horizontalen Portscan wird ein bestimmter Port über alle IP-Adressen eines Netzbereichs systematisch abgefragt.

Verfügbarkeit von Exploits

Mit der Analyseplattform lässt sich ebenfalls gezielt die Annahme und Verbreitung von publizierten Exploits[13] beobachten. Am 28. u. 30.10.2006 wurden über die Internetseite http://www.mailw0rm.com Exploits (Buffer und Stack overflow) für den Novell eDirectory Server veröffentlicht. In einem engen Zusammenhang mit der Publikation konnten massive Scans auf dem entsprechenden Serverport (8028 TCP) festgestellt werden. Diese konnten ca. eine Woche lang beobachtet werden (Abbildung 11 – großes Bild), über einen längeren Zeitraum waren anschließend eher verdeckte Scans auf einzelne IP-Adressen (kleines Bild) festzustellen.

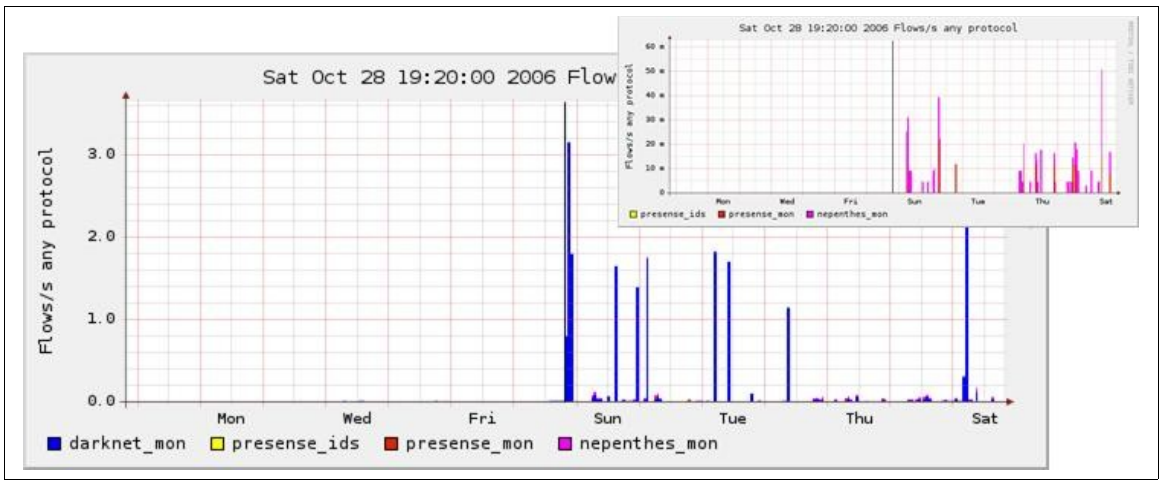


Abbildung 11: Exploit für Novells eDirectory Server

Weitere detaillierte Beispiele würden den Rahmen dieses Beitrags sprengen, daher nur eine kurze Aufzählung wichtiger Analyseergebnisse:

- **Unbekannte Kommunikationsverbindungen**

  Nach der Veröffentlichung von Exploits oder nach der Analyse von Malware können bislang nicht zugeordnete Kommunikationsverbindungen einer bestimmten Schwachstelle oder einem Schadprogramm zugeordnet werden. Hier wären z.B. die Ports der „Control and Command“ Server von Botnetzen[14] oder die Ports der Backdoors von Trojanern zu nennen. Durch die Analyse unbekannter Kommunikationsverbindungen, die erst durch die Installation einer Frühwarnzentrale überhaupt sinnvoll möglich ist, kann ein wichtiger Beitrag zur Gefahrenabwehr geleistet werden.

- **Beobachtung bekannter Schwachstellen und Schadsoftware**

  Durch die Einrichtung von Analyseprofilen kann auch das Bedrohungspotential bekannter Schadsoftware ständig beobachtet werden. Einerseits haben auch „ältere“ Schwachstellen und Schadsoftware einen nicht unbeträchtlichen Anteil an den aktuellen Angriffen, andererseits ist diese Kategorie von Schadsoftware gerade wegen ihrer Bekanntheit und Verbreitung in den einschlägigen Täterkreisen gefährlich, da mit jedem neuen Exploit die Verbreitung der Schadfunktion stark ansteigen kann.

---

13 Ein Exploit ist ein Programm oder ein Script, welches zur Demonstration einer Sicherheitslücke geschrieben und veröffentlich wurde.

14 Der Begriff "Bot" ist von dem Wort "Robot" abgeleitet, im technischen Umfeld wird darunter ein Programm verstanden, das ohne menschlichen Eingriff Aktionen ausführt. Als Botnetz versteht man einen virtuellen Verbund kompromittierter Client-Systeme, die ferngesteuert werden. Dies können z.B. für die Verbreitung weiterer Schadprogramme oder für Angriffe verwendet werden.

- **Backscatter**

  Wie bei DoS oder DDoS Angriffen üblich, werden die Quelladressen in den Datenpaketen gefälscht, so dass unerwartete Datenpakete – auch Backscatter[15] genannt – in Teilbereichen oder im gesamten Internet die Folge sind. Somit ist es wahrscheinlich, dass beim Angriff auch IP Adressen verwendet werden, die auch von den Sensoren des Frühwarnsystems erfasst werden. Backscatter zeichnet sich beispielsweise durch einen Quell-Port 22, 80 und 6667 TCP mit Syn/Ack Flags aus und können daher recht zuverlässig aus den Gesamtdaten extrahiert werden.

- **Ausnutzung von schwachen Passwörtern**

  Eine in der letzten Zeit sehr weit verbreitete Angriffsmethode ist das Raten von schwachen Passwörtern bei Secure-Shell (SSH)- oder FTP-Servern. Diese Angriffsform wird dabei durch zwei prinzipielle Sicherheitsprobleme ermöglicht. Das erste Problem besteht aufgrund von Passwörtern, die fest bei der Installation der Software oder des Hardwareproduktes vorgegeben sind. Da diese Default-Passwörter in einigen Fällen nicht geändert werden, sind sie ein beliebtes Angriffsziel. Weiterhin werden speziell von unerfahrenen Benutzern in einigen Fällen unsichere Passwörter gewählt, die leicht erraten werden können.

- **IDS Signaturen**

  Daten, die von IDS-Sensoren geliefert werden, können grundsätzlich nur ein aktuelles Bild über die Ausnutzung von Schwachstellen mittels bereits bekannter Angriffsmethoden vermitteln. Dies muss im Kontext von Frühwarnung zwar kritisch hinterfragt werden, aber auch diese Kategorie von Daten liefert trotz des offensichtlichen Mangels an Aktualität einen unmittelbaren Mehrwert.

  Ebenso wie bei allen anderen Datenquellen wird durch die Zusammenführung von Informationen aus verschiedenen Organisationen aus unterschiedlichen Kritis-Sektoren eine vergleichende Betrachtung ermöglicht.

  1) Die Kenntnis über die aktuelle Verteilung der Angriffsmethoden liefert einen wertvollen Beitrag für die Aussagekraft eines nationalen IT-Lagebilds. Veränderungen in der Verwendung bekannter Methoden lassen fundierte Aussagen über Trends zu. Ähnlich wie bei den Portstatistiken, lassen verstärkt auftretende oder abnehmende Angriffssignaturen auf eine Veränderung der Bedrohungslage schließen.
  2) Schwerpunkte beim zukünftigen Ausbau der Frühwarnzentrale ist die Etablierung einer kooperativen Analyse von Schwachstellen und Malware durch ein virtuelles Analystenteam und die Integration von Werkzeugen für eine automatische Analyse von Schadprogrammen. Auf dieser Basis kann nachfolgend eine automatisierte bzw. teilautomatisierte und zugleich zeitnahe Erstellung von Angriffssignaturen erfolgen. Dadurch bekommt der Einsatz von IDS eine neue Qualität; so dass die Verbreitung von neuen Angriffsmethoden kurzfristig erfasst und visualisiert werden kann. Ein weiterer Mehrwert dürfte durch die künftige Korrelation von Flow- und IDS-Daten beim Einsatz der „Presense-Sensoren[16]“ gegeben sein, da hier der Anteil von nicht zuordenbaren Kommunikationsverbindungen verringert werden kann und somit eine Konzentration auf den verbleibenden Rest erfolgt.

---

15 Eine häufig verwendete Vorgehensweise bei verteilten Denial of Service (DDoS) Angriffen ist es, möglichst viele halb-offene Verbindungen zu einem Dienst des angegriffenen Systems aufzubauen. Halb-offen ist eine TCP-Verbindung, wenn der Client nach der Bestätigung des Verbindungsaufbaus durch den Server keine weiteren Daten zum Server sendet. Ziel des Angriffs ist dabei, eine so hohe Anzahl von Ressourcen des Servers zu binden, so dass dieser keine Anfragen von anderen Systemen mehr bearbeiten kann. Fälscht der Angreifer die eigene Absenderadresse, sendet der Server das Bestätigungspaket an die gefälschte Absenderadresse. Diese Pakete werden als Backscatter bezeichnet.

16 Eine Weiterentwicklung der aus dem eCSIRT.net Projekt bekannten Sensoren [eCSIRT.net 2003].

- **Abgleich mit anderen Warnsystemen**

  Ein wesentliches Leistungsmerkmal der Analyseplattform ist die Bereitstellung von Statistiken, auf deren Basis vergleichende Betrachtungen mit Warnsystemen z.B. aus Asien und den USA vorgenommen werden können. Trotz der vergleichsweise geringen Datenbasis, konnten bereits in der Erprobungs- und Testphase im direkten Vergleich Gemeinsamkeiten und Unterschiede festgestellt werden. Diese Informationen standen bislang nicht zur Verfügung und bieten damit einen direkten Mehrwert.

5. Fazit

Die Zusammenführung von Sensordaten und der nachfolgenden Analyse stellt einen hohen Mehrwert dar, wie alle beteiligten Analysten konstatierten. Ein wichtiger Punkt ist dabei die Möglichkeit einer vergleichenden Betrachtung der aktuellen Situation in den einzelnen Organisationen mit der durch die Frühwarnzentrale gebildeten nationalen Sicht. Bislang war dies nur über öffentlich verfügbare Informationen möglich, die jedoch nicht über den erforderlichen Detaillierungsgrad verfügen. Diese Aussage ist hingegen nicht auf die Anbieter kommerzieller Dienste zu übertragen, jedoch fehlt hier die nationale Sichtweise.

Folgende Punkte stellen zentrale Erkenntnisse dar:

- Die Sammlung von relevanten Daten unterschiedlichster Datenquellen, wie z. B. Darknets, Netflows und IDS, konnte erfolgreich unter realistischen Einsatzumgebungen in der Praxis getestet werden. Darüber hinaus konnte demonstriert werden, dass die entwickelte Policy gesteuerte Pseudonymisierungs- und Export-Funktion sämtliche datenschutzrechtliche Anforderungen eines datenliefernden Partners berücksichtigen 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 sich deutlich gezeigt, dass ein Datenpool von realen Netzwerkbeobachtungen eine kritische Voraussetzung für die Entwicklung und Evaluation von jedweden Analyse- und Korrelationsmethoden ist.
- Der dem Projekt zugrunde liegende Ansatz, unterschiedliche Datenquellen von unterschiedlichen Partnern zu korrelieren, liefert bereits jetzt mit den bestehenden Standardmethoden qualitativ hochwertige Analysen. Zukünftig zu entwickelnde spezifischere Methoden zur Korrelation und Analyse, die mehrere Datenquellen von verschiedenen Partnern explizit berücksichtigen, lassen noch bessere Analyseergebnisse erwarten.

5.1 Weiterentwicklung und Forschungsbedarf

Die Funktionsweise der Analysewerkzeuge konnte in der Erprobungsphase erfolgreich demonstriert werden. In den vorangegangenen Abschnitten wurde eine Auswahl der Einsatzmöglichkeiten dargestellt und das Potential ist aufgezeigt worden, wenn aus weiteren Bereichen repräsentative Daten bereitgestellt werden. Durch die Erprobungsphase wurden auch Bereiche identifiziert, die durch eine konsequente Weiterentwicklung erschlossen werden müssen:

- Automatisierung der Analyse von Malware und Integration der Ergebnisse
- Auswertung von Metadaten und Kennzahlen für künftige Analysealgorithmen
- Bereitstellung von zusätzlichen Datenbanken (u.a. Schwachstellen, Kontakt, Ports) zur Unterstützung der Analysten

- Automatisches und manuelles Erstellen von Signaturen für die IDS Sensoren und deren Verteilung
- Integration von Geoinformationen für eine bessere Darstellung der Angriffssituation

Die Realisierung eines Teils der zuvor aufgeführten Analysewerkzeuge ist jedoch erst auf Basis von künftigen Forschungsergebnissen sinnvoll möglich. Sehr erfolgversprechend waren die Experimente mit einem Malware-Sensor[17], der bei einem Partner installiert wurde. Insbesondere das Verhalten einer bisher nicht identifizierten Malware nach einem erfolgreichen Angriff ist von zentraler Bedeutung, um insbesondere so genannte Botnetze aufspüren und weiter verfolgen zu können. Hier müssen jedoch weitere Anstrengungen unternommen werden, um die Analyse von Malware zu automatisieren und die Ergebnisse integrieren zu können.

Besondere Bedeutung hat auch die Einbindung weiterer, bereits eigenständig vorangetriebener Sensoren, so dass hierdurch bestehende Projekte und Kooperationen zur Datensammlung ebenfalls synergetisch genutzt werden können. Hier wären zunächst die durch eine Forschungsgruppe den Niederlande entwickelten „High Interaction Honeypots“ [ARGOS] zu nennen, die eine Simulation gängiger Closed-Source Betriebssysteme[18] realisieren und Angriffe ohne feste IDS-Signaturen erkennen können.

5.2 Kooperation mit Computer Emergency Response Teams

Bei der Erprobung der Arbeitsumgebung hat sich gezeigt, dass eine enge Kooperation mit CERTs für beide Seiten große Vorteile bietet. Zuerst profitieren CERTs von den Daten des Frühwarnsystems für verschiedene Dienstleistungen. Ein nicht unerheblicher Teil der unerwünschten Kommunikationsverbindungen, die von dem Frühwarnsystem erfasst werden, stammen von kompromittierten IT-Systemen. Sofern die Quell IP-Adressen nicht anonymisiert sind, kann ein CERT entsprechend gewarnt werden. Ein weiterer Vorteil für das CERT ist, dass die Daten des Frühwarnsystems strukturiert sind. Das ermöglicht dem CERT, die Daten weitgehend automatisch zu verarbeiten und so den Aufwand für die Bearbeitung zu minimieren.

Weiterhin veröffentlichen viele CERTs Sicherheitswarnungen für Schwachstellen in Softwareprodukten. Dafür ist es wichtig, das Risiko abschätzen zu können, das von den Sicherheitslücken ausgeht. Das Risiko hängt insbesondere davon ab, ob und in wie weit die Schwachstelle bereits in der Praxis ausgenutzt wird. Diese Informationen kann ein Frühwarnsystem liefern.

17 Derzeit wird ein Nepenthes-Sensor (Nepenthes Homepage: http://nepenthes.mwcollect.org) verwendet, jedoch stellt der Einsatz keine grundsätzliche Präferenz dar. Es eignen sich ebenso andere Sensoren, eine Übersicht über vergleichbare Projekte ist in [BSI 2006-3] enthalten.

18 Betriebssysteme, die ohne Quellcode ausgeliefert werden, z.B. Microsoft Windows.

6. Literaturverweise

[ARGOS] Argos: an Emulator for Fingerprinting Zero-Day Attacks / Georigios Portokalidis, Asia Slowinska, Herbert Bos / ACM SIGOPS EUROSYS 2006

[BSI 2005] BSI-Lagebericht IT-Sicherheit 2005/ BSI. – Bonn 2005 [http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf]

[ISMO 2004] Internet Threat Detection System Using Bayesian Estimation / Masaki Ishigiro, Hironobu Suzuki, Ichiro Murase, Hiroyuki Ohno – Budapest: 2004. [Vortrag auf der FIRST Konferenz 2004]

[eCSIRT.net 2003] Abschlussbericht des EU-Projekts eCSIRT.net / PRESECURE Consulting GmbH et al. – [In englischer Sprache; verfügbar über https://www.ecsirt.net/]

[FAN 2004] Prefix-preserving IP address anonymization / Jinliang Fan, Jun Xu, Mostafa H. Ammar and Sue B. Moon. Computer Networks, Volume 46: 2004.

[Haag 2005] NfSen and NFDUMP / Peter Haag. – Lissabon 2005. [Vortrag auf der 16. TF-CSIRT Tagung]

[NPSI 2005] Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI) / BMI. – Berlin 2005 / [http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/Nationaler__Plan__Schutz__Informationsinfrastrukturen,templateId=raw,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informationsinfrastrukturen]