FH JOANNEUM

CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

Eine Seminararbeit für die Lehrveranstaltung "E-SECURITY"

Vortragender: FH-Prof. DI Ewald Graif

Andreas Garger

Reinhard Kiesswetter

SS 05 - IMA 03

Vertiefungsrichtung: Systemtechnologien

Graz, 03.07.2005

Inhaltsverzeichnis

Abstract

Diese Seminararbeit befasst sich mit den Mitgliedern eines COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT), den weit reichenden Aufgabengebieten des Teams, mit der Implementierung des CSIRT – Prozesses in die Organisation, den Bedrohungspotenzialen, denen sich das CSIRT gegenüber sieht und einem wichtigen Werkzeug des Teams, der KNOWLEDGEBASE.

Die Motivation zu dieser Arbeit ergab sich aus der Aufgabenstellung der Lehrveranstaltung E-Security der Vertiefungsrichtung Systemtechnologien. Im Laufe der Recherchearbeit zu dieser Arbeit musste festgestellt, dass die Verbreitung der Idee von CSIRTs im mitteleuropäischen Raum noch nicht sehr ausgeprägt scheint oder nur in dementsprechend großen Organisationen verwirklicht wurde. Gerade angesichts der, zum Zeitpunkt der Verfassung dieser Arbeit, aktuellen Ereignisse um ein Dienstleistungsunternehmen einer namhaften Kreditkartenfirma, wo 40 Millionen (!) Kundendaten durch eine Sicherheitslücke entwendet wurden, erscheint die Notwendigkeit der Einführung eines derartigen Teams aber besonders wichtig.

Diese Arbeit sieht sich auch als Basis für mögliche weitere Betrachtungen zur Arbeit eines CSIRT im Zusammenhang mit der österreichischen Gesetzgebung im Allgemeinen und in der Ausforschung, Beweissicherung und Strafverfolgung von Computerkriminalität in Österreich im Speziellen.

1. Geschichte

Bevor 1988 der MORRIS INTERNET WORM sein Unwesen trieb, und geschätzte 10 % der damals vernetzten Rechner lahm legte, wurde Computersicherheit nicht viel Aufmerksamkeit geschenkt. Der MORRIS – oder INTERNET WORM wurde von Robert Tappan Morris, Jr. geschrieben. Laut seiner Aussage wollte er die Größe (die Anzahl der Hosts) des Internet feststellen und die Bösartigkeit des Viruses war ein Bug. Der Wurm nutze einen Bug im UNIX Programm SENDMAIL um sich zu verbreiten. Robert Morris, Jr. ist der erste Mensch der nach dem COMPUTER FRAUD AND ABUSE ACT angeklagt und verurteilt wurde.

Der Effekt des MORRIS WORM war aber auch, dass die Internetbenutzer und die Computerwelt im Allgemeinen auf das Thema COMPUTER SECURITY aufmerksam wurden und auch entsprechend reagierten. Das erste INCIDENT RESPONSE TEAM wurde 1988 von der Defense Applied Research Projects Agency (DARPA) (http://www.darpa.mil) gegründet. Das Team wurde COMPUTER EMERGENCY RESPONSE TEAM (CERT) (http://www.cert.org) genannt und ist im Software Engineering Insitute der Carnegie Mellon University angesiedelt. (Anm. der Autoren: Auf der gleichen Universität hat Morris studiert, gestartet hat er seinen Wurm aber vom Massachusetts Institute of Technology (MIT), wo er jetzt ein außerordentlicher Professor ist.) Der MORRIS WORM hat eine Unzahl von Berichten nach sich gezogen die, zusammengefasst, folgende Beobachtungen beinhalteten (vgl. Hare 2004, S 1850):

- Das Fehlen einer zentralen Stelle um internetweite Sicherheitsthemen bezogen auf Koordinations- und Kommunikationsprobleme während eines Sicherheitsnotfalls anzusprechen.
- An manchen Standorten existieren Sicherheitsschwachstellen.
- Nicht alle Systemmanager haben die Fähigkeiten und das Wissen um ihre Systeme richtig zu schützen
- Der Erfolg des MORRIS WORM beruht auf der Art des Angriffs, indem von bekannten Bugs, Vertrauensstellungen und PASSWORD GUESSING Gebrauch gemacht wurde.
- Es gibt Probleme beim Entwickeln und Verteilen von PATCHES und FIXES.

Obwohl diese Themen bereits 1988 nach dem MORRIS WORM aufgezeigt wurden, haben viele Organisationen im Bereich der Sicherheit noch ernstzunehmende Probleme.
Die Einführung eines COMPUTER SECURITY INCIDENT RESPONSE TEAM soll, vor allem in Bezug auf die oben erwähnten Defizite, Abhilfe schaffen.

2. Die Mitglieder des CSIRT

Die Etablierung und die Arbeit des CSIRTs in einer Organisation erfolgen als Prozess (vgl. Hare 2004, S. 1855ff). Folgerichtig muss es einen Prozesseigner geben. In vielen Organisationen ist dies der CIO (CHIEF INFORMATION OFFICER / IT-Verantwortliche). Dies erscheint aufgrund der technischen Aufgaben des CSIRT als sinnvoll. Um jedoch jeglichen Interessenskonflikt zu vermeiden sollte als Prozesseigner laut Hare (2004) jedoch der CFO (CHIEF FINANCIAL OFFICER / Kaufmännische Direktor) oder der Verantwortliche für die Innenrevision gewählt werden. Der Prozesseigner bestimmt den Teamleiter oder die Teamleiterin des CSIRT.
Häufig werden die Mitarbeiter des CSIRT in zwei Gruppen unterteilt (vgl. Hare 2004, S. 1855ff):

- Kernteam
- Support-Team

Der Prozesseigner und der Teamleiter oder die Teamleiterin wählen gemeinsam die Mitglieder des Kernteams aus. Die Ermittlungen in einem Sicherheitsvorfall erfordern von den Mitgliedern des CSIRT weit reichende Erfahrungen und einiges an Hintergrundwissen. Besonders wichtig ist hierbei auch die Fähigkeit der einzelnen Mitglieder selbständig und trotzdem auch als Teil eines Teams arbeiten zu können. Speziell die Mitglieder des Kernteams sollten laut Hare (2004) folgenden Bereichen entstammen:

- Unternehmenssicherheit
- Innenrevision
- Informationssicherheit
- Rechtsangelegenheiten
- Technische Spezialisten, falls dies die Gegebenheiten erfordern

Die Aufgabe des Kernteams ist die Entscheidung, ob ein Vorfall den Einsatz des CSIRT erfordert, das Management auf erforderliche Maßnahmen hinzuweisen, die Zusammenstellung der erforderlichen Mitglieder des Supportteams und die Koordination der Ermittlungen, sowie die Erstellung eines Berichts.

Das gesamte CSIRT deckt im Idealfall die weiteren Bereiche

- Betrugsermittlung,
- Personalangelegenheiten,
- Daten- und Systemwiederherstellung,
- Öffentlichkeitsarbeit,
- Managementverantwortung und
- die Vertretung der betroffenen Unternehmensbereiche oder lokalen Teil-organisationen

ab (vgl. Hare 2004, S. 1856f).

Die Teammitglieder sind je nach Größe der Organisation einerseits und den Erfordernissen andererseits entweder ausschließlich dem CSIRT und seinen Aufgaben zugeordnet oder treten nur bei einem Sicherheitsvorfall in Aktion. Die Aktivierung des CSIRT ist dann Aufgabe des Prozesseigners.

Unerlässlich ist es, dass zumindest alle Mitglieder des Kernteams laufend Schulung zum Thema Infiltrationsmanagement, Ermittlungs- und Interviewtechniken und Computerforensik erhalten.

Hare (2004) meint, dass das CSIRT die Ermächtigung des Managements besitzen muss, im Falle einer Sicherheitsverletzung in dessen Namen zu agieren. Deshalb ist es wichtig, dass auch alle Mitarbeiter und Mitarbeiterinnen der Organisation die Weisung erhalten, mit dem CSIRT im Bedarfsfall so gut als möglich zu kooperieren.

3. Aufgabengebiet des CSIRT

In diesem Kapitel wird gezeigt, was ein CSIRT tut und wie es das tut. Die Hauptaufgaben werden dargestellt und herausgearbeitet wann das Team aktiv wird. Für ein CSIRT sehr zu empfehlen ist das Vorgehen nach einem LIFE-CYCLE-MODEL, wie es zum Beispiel von CERT verwendet wird. In diesem Modell ist abgebildet wer den Vorfall meldet und wie er weiter bearbeitet werden soll. In Abbildung 1 sehen wir das Modell von CERT. Wie schon aus dem Namen hervorgeht ist das Reagieren auf Vorfälle die Hauptaufgabe des CSIRTs. Das Team setzt hoch spezialisierte Experten an vorderste Front und ermöglicht so eine durchgängige Herangehensweise an die Lösung des Vorfalls. Das CSIRT führt die Untersuchung vom Start bis zum Ende durch und berichtet seine Ergebnisse in Form von Vorschlägen an das Management.

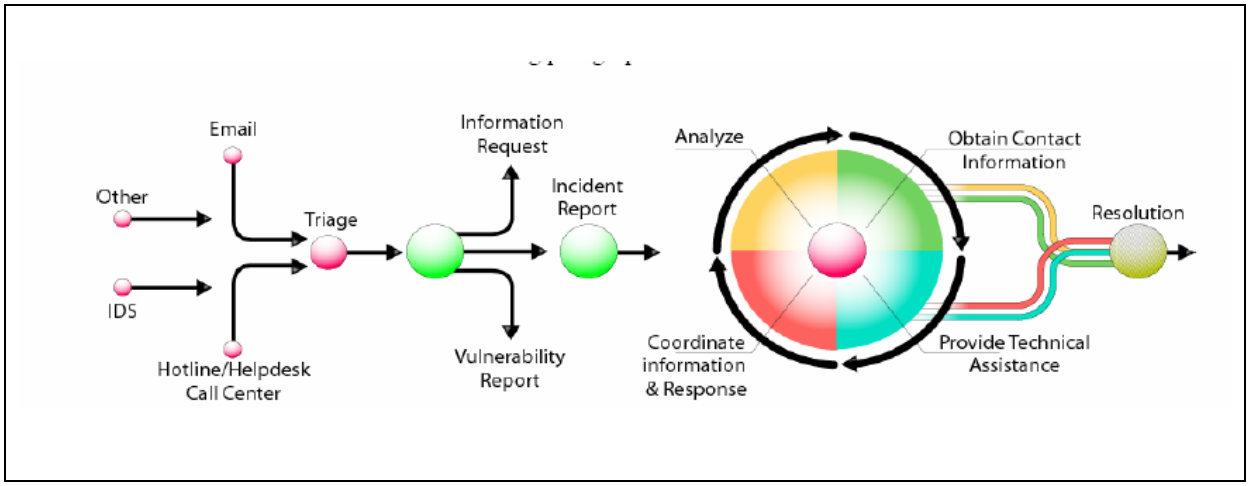

Abbildung 1: INCIDENT HANDLING LIFE CYCLE, entnommen aus West-Brown et al. (2003, S. 77)

Dieses Bild zeigt, dass ein Vorfall, mit allen dazugehörigen Informationen, mehrere Stadien durchläuft, bis keine weiteren Aktionen seitens des Teams notwendig sind. Wichtig ist, dass der LIFE CYCLE auch beendet wird (und somit der Vorfall als abgeschlossen gilt), wenn noch weitere Berichte über diesen Vorfall eintreffen, aber das Team keine weiteren Aktionen zur Beseitigung mehr setzten kann.

Was ist ein Vorfall (INCIDENT)?

Da es beim CSIRT vorrangig um das Reagieren beziehungsweise Abwehren und Vermeiden von Vorfällen geht, ist natürlich primär zu klären: Was ist überhaupt ein Vorfall?

Dies passiert innerhalb des CSIRTs selber und kann grob als eine unerwartete Handlung, die eine unmittelbare oder mögliche Auswirkung auf die Organisation hat, definiert werden. Vorfälle sollten klassifiziert werden, und zwar nach dem Ausmaß indem sie die Organisation beeinflussen. Empfohlen wird eine Klassifizierung, wie im Kapitel Bedrohungsanalyse beschrieben.

Das CSIRT wird aber auch in den folgenden Fällen aktiv:

- Wenn nach einem VULNERABILITYTEST der Anlass besteht
- Auf Anfragen vom Help Desk, welche ein Angriffsmuster erkennen lassen
- Auf Anraten eines externen Sicherheitsaudits

(vgl. Hare 2004, S. 1854)

Weitere wichtige Aufgaben

Eine gute Übersicht über die Aufgaben eines CSIRTs gibt Moira J. West-Brown im Handbook for Computer Security Incident Response Teams (CSIRTs), welche in Abbildung 2 als Überblick gezeigt ist und einige näher erläutert werden:

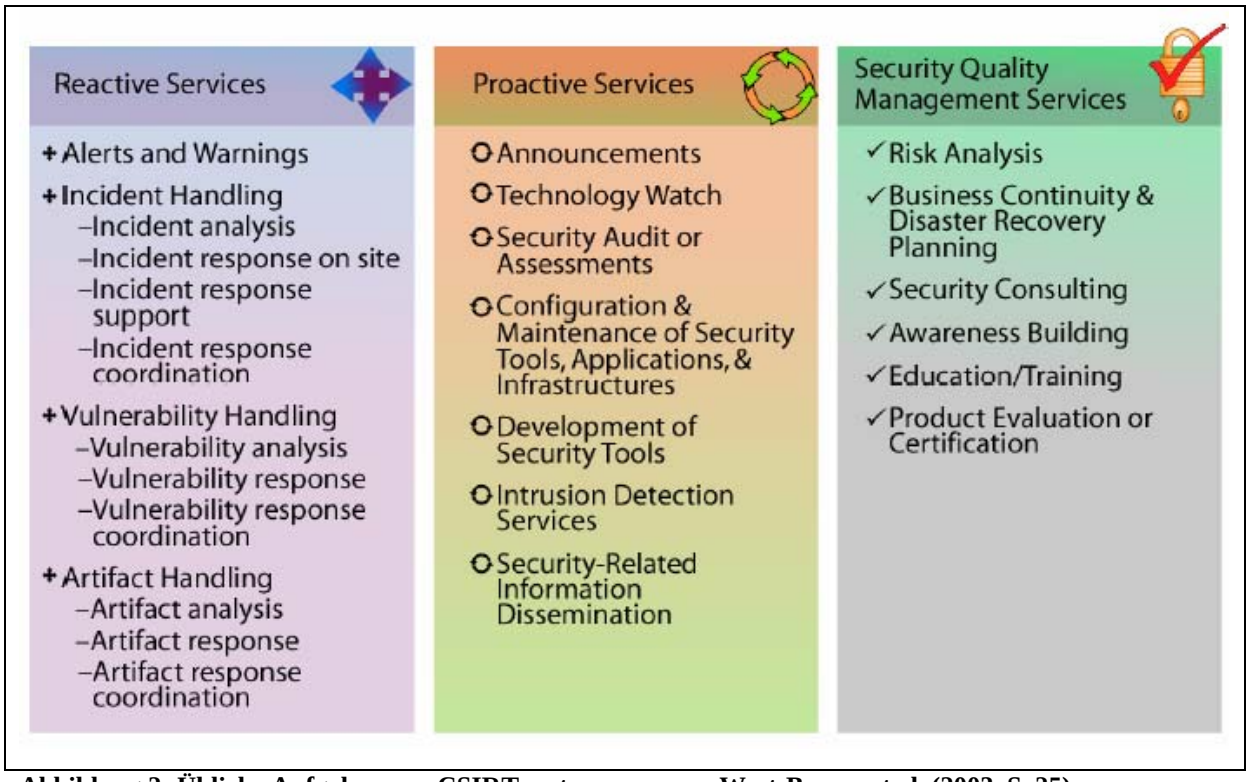

Abbildung 2: Übliche Aufgaben von CSIRT, entnommen aus West-Brown et al. (2003, S. 25)

- REACTIVE SERVICES: Das sind die Hauptaufgaben des CSIRT und werden von einem Vorfall oder einem Bericht über einen Vorfall ausgelöst.
- PROAKTIVE SERVICES: Diese Dienste dienen der Unterstützung und Information um konsistente Systeme auf Angriffe vorzubereiten und zu schützen. Diese Dienste reduziere die Anzahl der zukünftigen Vorfälle.
- SECURITY QUALITY MANAGEMENT SERVICES: Diese Dienste sind eigentlich unabhängig vom Incident Handling und werden üblicherweise von anderen Stellen (IT, Schulungsabteilung oder Auditing) durchgeführt. Das CSIRT hilft bei diesen Diensten, Die Sichtweise des CSIRT und die Erfahrung helfen diese Dienste zu verbessern und verbessern so generell die Security einer Organisation

Bedrohungsanalyse

Die Bedrohungsanalyse oder THREAT ANALYSIS ist eine der wichtigsten Aufgaben eines CSIRTs, die auf der Seite der vorbeugenden Maßnahmen steht. Als Ergebnis liefert das Team Vorschläge was zu tun ist und wer dafür zuständig ist an das Management. In Zusammenhang mit Bedrohungsanalyse müssen vorab einmal 3 Begriffe definiert werden, die die Auswirkung eines Risikos beschreiben:

- THREAT (Bedrohung): Ist das Potenzial die Organisation zu beinträchtigen. Beispiele hierfür sind: Hacker, Industriespionage, und manchmal, eigene Angestellte.
- VULNERABILITY (Sicherheitslücke): Ist eine Schwäche oder eine Bedrohung der Vermögenswerte. Wenn es keine Sicherheitslücke gibt, kann die Bedrohung die Organisation nicht beeinflussen.
- IMPACT (Auswirkung): Beschreibt das Ausmaß der Bedrohung im Zusammenhang mit der Signifikanz des Problems und wie viel Auswirkung es auf die Organisation haben wird.

(vgl. Hare 2004, S. 1851)

In Abbildung 3 sieht man eine grafische Darstellung der Bedrohungsanalyse. Wie daraus hervorgeht, beeinflussen alle drei Faktoren das Risiko.

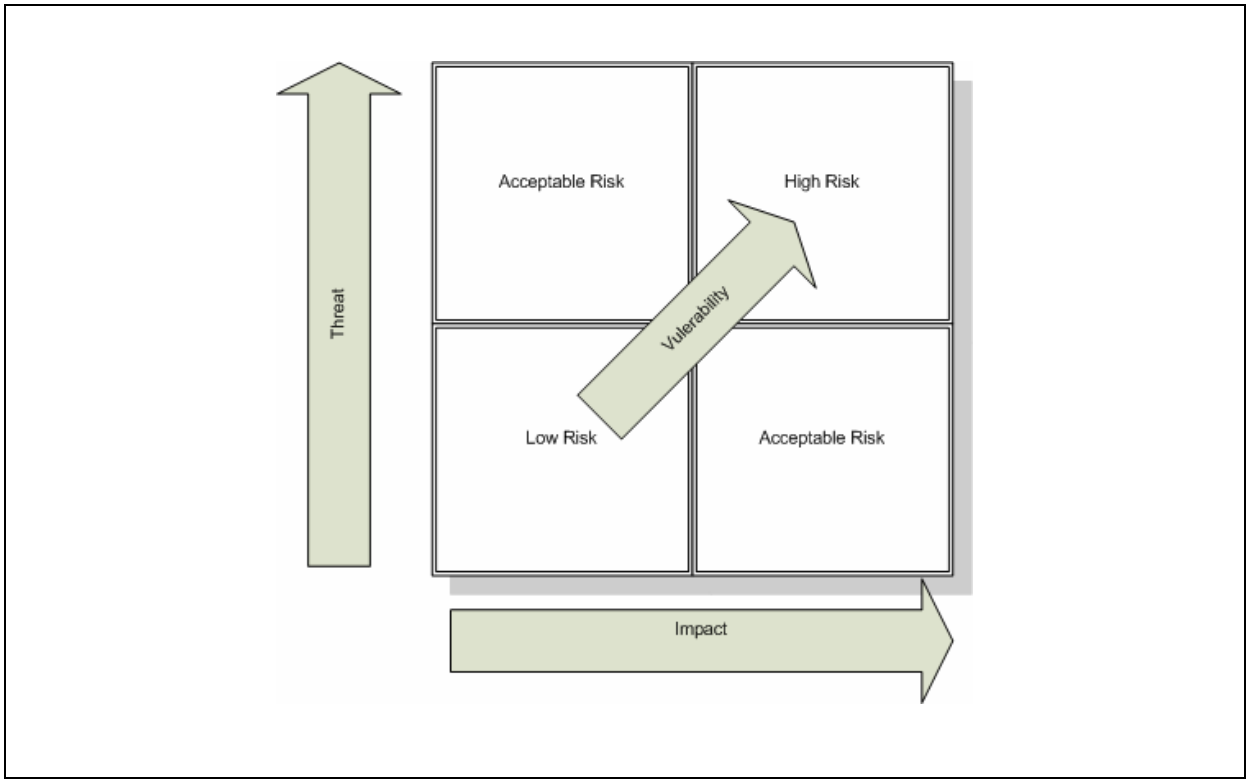

Abbildung 3: Threat graph, entnommen aus Hare (2004, S. 1851)

Bei dieser Grafik ist der Ausdruck des „akzeptablen Risikos“ hervorzustreichen. Darunter versteht man ein Risiko das die Organisation bewusst in Kauf nimmt, weil die Kosten zur Beseitigung höher sind als die Folgen wenn das Risiko eintrifft (THREAT größer als IMPACT) oder die Wahrscheinlichkeit das das Risiko eintrifft sehr gering ist (IMPACT größer als THREAT).

VULNERABILITY TESTS

Es gibt zwei Arten von Tests. Die erste verwendet automatisierte Tools, die vorgefertigte Tests durchführen um festzustellen, ob Sicherheitslücken vorliegen, die ein Angreifer ausnutzen könnte. Die zweite Art sind Tests, die die Sicherheitsimplementierung durch ausprobieren testen. Diese PENETRATIONS- oder PROTECTIONTESTS simulieren die unterschiedlichen Arten von Angriffen. Die Arten von Penetrationstests korrelieren mit den Arten von Angriffen und sind wie folgt untergliedert:

- LEVEL 1 ZERO-KNOWLEDGE: Dieser Versuch in das Netzwerk einzudringen wird von einer Stelle außerhalb des Netzwerkes ohne Wissen über die Architektur durchgeführt. Jedoch wird Information, die öffentlich zugänglich ist, verwendet.
- LEVEL 2 FULL KNOWLEDGE: Dieser Test versucht das Netzwerk von außerhalb, unter Ausnutzung des Wissens über die Architektur des Netzwerkes und der verwendet Software, zu penetrieren.
- LEVEL 3 INTERNAL: Bei diesem Versuch wird das Netzwerk von einem Rechner innerhalb des Netzwerkes angegriffen.

4. Der CSIRT Prozess

Nachdem das Team gebildet wurde, muss die Organisation sich darauf konzentrieren, wie das CSIRT arbeiten wird. Der Prozess, der entwickelt werden muss, definiert die genauen Schritte, die durchlaufen werden müssen, sobald das Team aktiviert wird. Neben den Schritten die notwendig sind um das Team zu schaffen, zu etablieren und mit der notwendigen Autorität zu versehen muss das Team auch:

- Seine eigenen Praktiken und Prozeduren dokumentieren
- Eine Datenbank mit Kontaktnamen und Informationen aufbauen und aktuell halten
- Hardware und Software, die während eines Vorfalls benötigt wird, organisieren

Das Team muss Wege entwickeln, wie es auf Vorfälle reagiert. Dazu gehören eine Vorfall Matrix und eine RESPONSE MATRIX. In der Vorfall oder INCIDENT MATRIX wird die Art des Vorfalls, das benötigte Personal, die benötigten finanziellen Ressourcen und die Quelle dieser Ressourcen aufgezeigt. In der RESPONSE MATRIX werden die Art des Vorfalls, die für diesen Vorfall angebrachte Reaktion, die geschätzten Ressourcen für diese Reaktion und wie eine Ausweitung des Vorfalls vermieden werden kann, dargelegt. (vergleiche Hare 2004, S. 1857f)

Finanzierung

Die Planung eines Budgets gestaltet sich beim CSIRT etwas schwieriger als bei anderen Prozessen. Zwar können die Personal- und Materialkosten für Ausrüstung im täglichen Gebrauch genau so geplant werden wie anders wo auch, aber die Kosten für speziell benötige Ausrüstung (Softwaretools, Hardware…) müssen über ein gesondertes Budgetkontingent gewährleistet sein. (vgl. Hare 2004, S. 1858)

4.1 Der CSIRT-Prozess im Zusammenhang mit INCIDENT RESPONSE MANAGEMENT

Das CSIRT ist nur ein Teil des INCIDENT RESPONSE MANAGEMENT und dieses Management gehört zum Risikomanagement einer Organisation. Risikomanagement ist

ebenfalls ein Prozess, der fortwährend und nachhaltig von einer Organisation durchgeführt werden muss. (vgl. Sterneckert 2004, S. 1861) Der Prozess selbst besteht aus mehreren Teilprozessen, die wir hier kurz erläutern wollen. Die Teilprozesse sind:

- PREPARE/SUSTAIN/IMPROVE (PREPARE)
- PROTECT INFRASTRUCTURE (PROTECT)
- DETECT EVENTS(DETECT)
- TRIAGE EVENTS (TRIAGE)
- RESPOND

(vgl. Alberts 2004, S. 8f)

PREPARE

Die Vorbereitungsphase sieht das Einsetzen oder Verbessern eines CSIRT vor, dient aber auch als Nachbereitungsphase eines abgeschlossenen Vorfalls.

- Planen und implementieren eines CSIRT
- Das CSIRT unterstützen
- Ein bestehendes CSIRT verbessern durch Evaluierung und Assessments
- Durchführen einer nachfolgenden Analyse von Aktionen
- Verbesserungen an den Protect-Prozess weiterleiten

PROTECT

In diesem Teilprozess geht es vorrangig um das Schützen der materiellen und immateriellen Werte der Organisation. Das CSIRT selbst wird hier nicht überall mitarbeiten, sondern mit Vorschlägen und Berichten helfen die Aufgaben bestmöglich zu lösen.

- Veränderungen an der Computerinfrastruktur vornehmen um einen Vorfall oder eine mögliche VULNERABILITY in der Hardware- oder Softwareinfrastruktur zu stoppen oder einzudämmen
- Implementierung von Infrastrukturschutzverbesserungen resultierend aus den Analysen des Vorprozesses oder anderen Prozessverbesserungsmechanismen

- Evaluierung der Computerinfrastruktur durch proaktives Scannen, Netzwerkmonitoring und SECURITY und Risikoevaluierung.
- Informationen über aktuelle Vorfälle, entdeckte VULNERABILITIES oder andere SECURITY bezogene Vorgänge die während der Evaluierung entdeckt wurden and den DETECT-Prozess melden

DETECT

Die Erkennung von Vorfällen und das Verfassen von Berichten an das Management sind in diesem Prozess angesiedelt und somit arbeitet das CSIRT hier sehr stark mit.

- Vorfälle erkennen und Berichte darüber erstellen
- Die Berichte von Vorfällen erhalten
- Indikatoren wie Netzwerkmonitoring, IDS oder Technologieüberwachungssysteme proaktiv beobachten
- Die Indikatoren analysieren (um Aktivitäten festzustellen, die bösartiges Verhalten andeuten oder um Risiken und Bedrohungen für die Organisation festzustellen)
- Jede verdächtige oder erkennbare Aktivität an den TRIAGE-Prozess weiterleiten
- Alle Vorfälle, welche nicht an den TRIAGE-Prozess weitergeleitet werden oder neu zugeordnet werden, abschließen

TRIAGE

Der TRIAGE Prozess wird überwiegend vom CSIRT durchgeführt, da er ja auch ein Kernstück des INCIDENT-HANDLING-LIFE-CYCLE ist. Wichtig dabei ist, dass für die Meldung von Vorfällen eine zentrale Stelle für die gesamte Organisation zur Verfügung steht.

- Vorfälle kategorisieren und korrelieren
- Vorfälle priorisieren
- Vorfälle für Handhabung und Responds zuordnen
- Relevanten Daten und Informationen an den Respond-Prozess weiterleiten
- Vorfälle auf Gebiete außerhalb des Incident Management Prozesses neu zuordnen wenn möglich

- Alle Vorfälle die nicht an den Respond-Prozess weitergeleitet werden oder neu zugeordnet werden abschließen

RESPOND

In diesem Prozess liegt die Kernkompetenz des CSIRT. Mit der Kontaktdatenbank und den vorbereiteten Matrizen ist hier ein schnelles Reagieren möglich. Die Erfahrungen werden in die KNOWLEDGEBASE eingearbeitet, um erlangte Kompetenzen nicht neu erarbeiten zu müssen.

- Den Vorfall analysieren
- Eine Response Strategie planen
- Mit Externen kommunizieren
- Technische, Management- und rechtliche Verantwortung koordinieren und zur Verfügung stellen
- Die Erfahrungen und „lessons learned" an den PREPARE-Prozess weiterleiten, um sie in einer nachfolgenden Analyse zu bearbeiten

(vgl. Alberts 2004, S. 16f)

Wie zu erkennen ist, gibt es hier einige Punkte die direkt vom CSIRT durchgeführt werden und in dessen Aufgabengebiet fallen und andere Punkte die über dessen Aufgabengebiet hinausgehen. In Abbildung 4 ist zu sehen, wie diese Prozesse zusammenwirken.

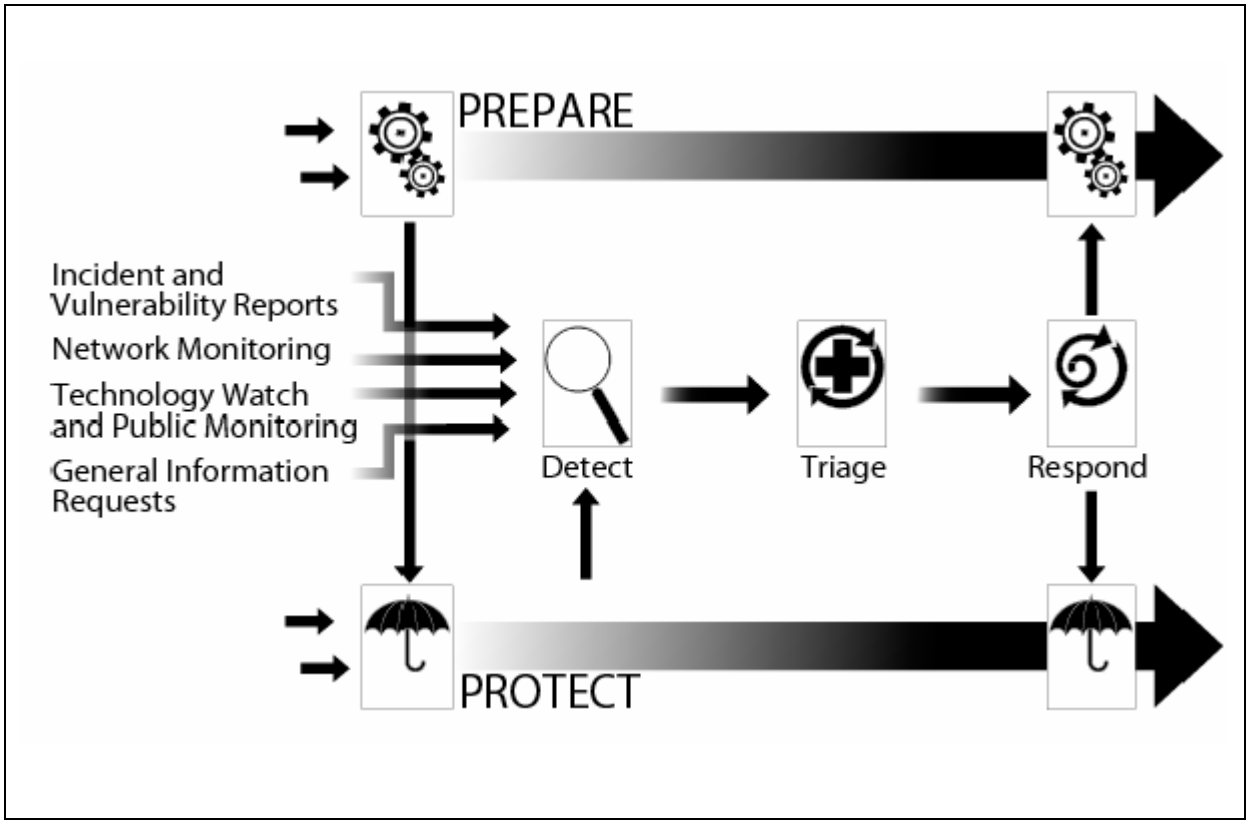

Abbildung 4:INCIDENT MANAGEMENT Prozesse, entnommen aus Alberts (2004, S. 18)

Die Abbildung zeigt deutlich, dass PREPARE und PROTECT Prozess zwei wesentliche, kontinuierliche Prozesse sind, die von den anderen Teilprozessen unterstützt werden. Da das CSIRT vor allem in den unterstützenden Prozessen tätig ist, sieht man hier sehr gut, dass ein CSIRT als Herz von INCIDENT MANAGEMENT gesehen werden kann.

5. Bedrohungspotenziale

Jedes System ist verwundbar. Auch die umsichtigste Vorgangsweise beim Einsatz von Hard- und Software im IT-Bereich kann diese Tatsache nicht verändern. Aber durch eine genaue Planung, technischem Wissen und anderen Vorsichtsmaßnahmen kann der Grad der Verwundbarkeit beziehungsweise die Auswirkungen eines Angriffs minimiert werden.
Im zeitgemäßen IT-Management geht das Hauptaugenmerk weg von der rein physikalischen Sicherung und Backupmaßnahmen hin zu der schnellen und effizienten Reaktion auf Sicherheitsvorfälle. Das CSIRT ist ein Teil dieser Maßnahmen.

5.1 Die Angreifer

Auch die Charakteristik der Angriffe sowie die Profile der Angreifer haben sich in den letzten Jahren stark verändert. Man unterscheidet zwischen folgenden Angreiferprofilen:

- *Der Ahnungslose:* Dieser Angreifer besitzt wenig Wissen und Erfahrung. Besitzt wenig bis kein Bewusstsein über die Konsequenzen seiner Handlung.
- *Der Brutale:* Besitzt ebenfalls wenig an Wissen, nutzt jedoch intensiv die bereits vorhandenen ATTACK TOOLS. Angriffe dieser Art werden auf überwachten Systemen relativ schnell entdeckt.
- *Der Wissende:* Dieser Typus von Angreifern besitzt einiges an Fachwissen und beherrscht eine Reihe von Techniken um sich Zugang zu Systemen zu verschaffen. Seine Angriffe sind generell raffinierter und schwerer zu entdecken.
- *Der Geschickte:* Diese Gruppe gehört zu den Computerkriminellen des 21. Jahrhunderts. Sie wissen, welche Informationen sie wollen, wissen wer für diese bezahlt, wie sie Zugang zu einem System bekommen und wie sie sich in dem System bewegen müssen. Sie hinterlassen wenig bis gar keine Spuren in dem angegriffenem System.

(vgl. Hare 2004, S. 1848)

Aufgrund ihrer Motivation lassen sich die die Angreifer in

- *Jugendliche Angreifer* (Angriffe aus Spaß, Ehrgeiz, Mutprobe oder Geltungsdrang und in der Regel mit mehr oder weniger bekannten Methoden),
- *Insider* (Z.B.: Angestellte im Unternehmen, mit der Berechtigung auf mehr oder weniger sensible Informationen im Netzwerk zuzugreifen – Gefahr der Schädigung von Daten und Systemen durch unzufriedene Mitarbeiter oder Diebstahl von Informationen um diese der Konkurrenz zu verkaufen oder den Medien zu zuspielen) und
- *Industriespione* (Meist gefürchtete Angreifergruppe – Meist entweder von Konkurrenzunternehmen oder regierungsnahen Spionagediensten angeheuerte Hacker mit guter Ausbildung, durch welche sie in der Lage sind, die gesamte Bandbreite der Angriffsarten zu verwenden)

unterteilen (vgl. Hare 2004, S. 1848f).

5.2 Die Angriffe

Die Angreifer verwenden zumeist eine Auswahl von ATTACK TOOLS und nutzen die steigende Anzahl von Schwachstellen in der heutigen Software. Abhängig von ihren Absichten und Zielen verwenden die Angreifer verschiedene Werkzeuge.

Die Reichweite der ATTACK TOOLS geht von recht einfachen, von beinahe jedermann verwendbaren Softwareapplikationen bis hin zu C-Programmen oder komplexen Scan- und Analysetools wie zum Beispiel nmap. Viren und ACTIVE CODE werden verwendet um Information zu zerstören, Zugang zu einem System herzustellen, um Informationen über Systeme zu sammeln, Dienste zu beeinträchtigen bzw. zu blockieren oder Computer zu zerstören.

Definition eines Sicherheitsvorfalls

„ … an incident can be defined as any unexpected action that as an immediate or potential effect on the organization.“ (Zitat: Hare 2004, S. 1853)

Diese Definition beinhaltet laut Hare (2004, S. 1853) zum Beispiel folgende Vorfälle:

- Ausbreitung von Viren
- Nicht-Autorisierter Zugriff, ohne Unterscheidung von welcher Quelle
- Diebstahl von Information oder der Verlust der Geheimhaltung
- Angriffe gegen spezifische Systeme
- DoS (DENIAL OF SERVICE) Angriff
- Datenfälschungen

Sicherheitsvorfälle können weiters nach ihren Auswirkungen (Impact) auf die Organisation klassifiziert werden.
Ein Klassifikationsvorschlag nach Hare (2004, S. 1853) lautet wie folgt:

Klasse 1: GLOBAL
Diese Sicherheitsvorfälle haben die schwerwiegendsten Auswirkungen auf die gesamte Organisation. Vorfälle dieser Klasse können, z.B. durch einen „Bruch" der FIREWALL oder einer epidemische Ausbreitung eines schädlichen Virus, einen finanziellen Verlust oder eine Kredit- bzw. Rufschädigung des Unternehmens etc. verursachen. Derartige Sicherheitsprobleme fallen immer in den Aufgabenbereich des CSIRT.

Klasse 2: Regional
Diese Vorfälle sind auf bestimmte Regionen oder Bereiche beschränkt und es besteht die Möglichkeit einer Ausbreitung auf die gesamte Organisation. Verursacht könnte ein derartiger Vorfall durch logische Bomben oder Attacken auf spezifische Systeme in der betroffenen Region oder des angegriffenen Bereiches werden. In diesen Situationen handelt das CSIRT in Kooperation mit den regionalen Verantwortlichen und auf deren Anforderung.

Klasse 3: Lokal
Dies sind Sicherheitsvorfälle im lokalen Rahmen, wie einer einzelnen Abteilung oder einem Desktop-Rechner mit keinen oder vernachlässigbaren Auswirkungen auf die Gesamtorganisation. Keine Aktivierung des CSIRT, außer auf explizite Anforderung des oder der Abteilungsverantwortlichen.

6. CSIRT Knowledgebase

Ein wichtiges Werkzeug des CSIRT ist die Dokumentation jedes Sicherheitsvorfalles. Die Dokumentation beginnt mit der Erkennung eines Vorfalles und endet mit seiner Schließung. Somit sind alle gesammelten Informationen schon vom Beginn des Einschreitens des CSIRT an vorhanden und können von allen berechtigten Personen eingesehen werden. Gerade für zukünftige, wo möglich ähnliche oder gleiche Vorfälle, ist diese Dokumentation eine wichtige Wissensdatenbank.

Der Dokumentationsvorschlag von Rollason-Reese (2003, S. 100f) enthält folgende Informationen:

- *Vorfallsnummer und Datum*
- *Art des Vorfalls:* Z.B.: Virusattacke, Nicht autorisierter Zugriff, Ausfall einer Hardware, usw.
- *Schweregrad:* Einstufung nach dem festgelegten Kategorisierungssystem
- *CSIRT – Mitglieder:* Alle Personen, welche im Laufe der Vorfallsbehandlung mitgewirkt haben
- *Vorfallsstatus:* (Offen/Geschlossen)
- *Autor* (In der Regel der Teamleiter)
- *Verteilerkreis:* Welcher Personenkreis wurde zur Kommentierung bzw. Korrektur eingeladen? Die finale Version dieser Dokumentation erhält unter anderen der IT - Verantwortliche (CIO).
- *Beschreibung des Vorfalls*
- *Beschreibung der Nachforschungsprozedur:* Detaillierte Informationen über die Art und Weise der Nachforschungen und die verwendeten Werkzeuge
- *Ergebnis der Analyse:* Darstellung der Ursache des Problems
- *Lösungsansatz*
- *Auswirkungen auf Systeme*
- *Empfohlene Handlungsweise:* Konfigurationsänderungen, Upgrades, usw. Wenn die Sicherheitslücke nach wie vor besteht, eine Präventivmaßnahme vorschlagen.

Der Detailgrad der Aufzeichnung variiert von Team zu Team und ist abhängig von den spezifischen Anforderungen und der Tiefe der Analyse des Vorfalls. Weiters können statische Auswertungen oder Trendanalysen beinhaltet sein (vgl. West-Brown et al. 2003, S. 91).

Literaturverzeichnis

ALBERTS C. / Killcrece G. / Ruefle R. / Zajicek M. / Dorofee A. - Software Engineering Institute Carnegie Mellon University Pittsburgh (2004): Defining Incident Management Processes for CSIRTs: A Work in Progress, http://www.cert.org/archive/pdf/04tr015.pdf (Stand: 07.06.2005, 19:00)

HARE C. (2004): CIRT: Responding to Attack, in Tipton H. F. / Krause M. (Hrsg.): Information Security Management Handbook, Fifth Edition, Auerbach Publications, Boca Raton, 1847 – 1859

ROLLASON-REESE R.L. - Eastern Connecticut State University (2003): Incident handling: an orderly response to unexpected events, in Proceedings of the 31st annual ACM SIGUCCS conference on User services San Antonio (USA), ACM Press (Hrsg.), New York, 97 – 102

STERNECKERT A. (2004): Incident Response Management, in Tipton H. F. / Krause M. (Hrsg.): Information Security Management Handbook, Fifth Edition, Auerbach Publications, Boca Raton, 1861 – 1870

WEST-BROWN M.J. / Stikvoort D. / Kossakowski K. / Killcrece G. / Ruefle R. / Zajicek M. - Software Engineering Institute Carnegie Mellon University Pittsburgh (2003): Handbook for Computer Security Incident Response Teams (CSIRTs), http://www.cert.org/archive/pdf/csirt-handbook.pdf (Stand: 07.06.2005, 18:00)