EINRICHTUNG EINES CSIRT SCHRITT FÜR SCHRITT

Resultat WP2006/5.1(CERT-D1/D2)

Index

1 Zusammenfassung ... 2

2 Rechtliche Hinweise ... 2

3 Danksagung ... 2

4 Einführung ... 3

4.1 Zielgruppen ... 5
4.2 Verwendung dieses Dokuments ... 5
4.3 In diesem Dokument verwendete Konventionen ... 6

5 Generelle Strategie für die Planung und Einrichtung eines CSIRT ... 7

5.1 Was ist ein CSIRT? ... 7
5.2 Mögliche Dienste eines CSIRT ... 12
5.3 Analyse der Klientel und Festlegung des Aufgabenbereichs ... 15

6 Ausarbeitung des Geschäftsplans ... 23

6.1 Festlegung des Finanzierungsmodells ... 23
6.2 Festlegung der Organisationsstruktur ... 25
6.3 Einstellung der richtigen Mitarbeiter ... 30
6.4 Nutzung und Ausstattung des Büros ... 32
6.5 Festlegung der Richtlinien für die Informationssicherheit ... 35
6.6 Suche nach Kooperationsmöglichkeiten zwischen anderen CSIRT-Teams und möglichen nationalen Initiativen ... 36

7 Förderung des Geschäftsplans ... 39

7.1 Beschreibung von Geschäftsplänen und Anstößen für die Geschäftsführung ... 42

8 Beispiele für betriebsspezifische und technische Verfahren (Arbeitsabläufe) ... 46

8.1 Analyse der bei der Klientel installierten IT-Systeme ... 47
8.2 Erstellung von Alarm- und Warnmeldungen und Bekanntgaben ... 48
8.3 Behandlung von Vorfällen ... 55
8.4 Beispiel für einen Reaktions-Zeitplan ... 61
8.5 Verfügbare CSIRT-Werkzeuge ... 62

9 CSIRT-Schulungsmaßnahmen ... 64

9.1 TRANSITS ... 64
9.2 CERT/CC ... 65

10 Praktische Übung: Erstellung eines Advisory ... 67

11 Schlussfolgerung ... 72

12 Beschreibung des Projektplans ... 73

ANHANG ... 75

A.1 Weiterführende Literatur ... 75
A.2 CSIRT-Dienste ... 76
A.3 Beispiele ... 86
A.4 Musterunterlagen aus CSIRT-Seminaren ... 90

1 Zusammenfassung

Im vorliegenden Dokument wird die Einrichtung eines CSIRT-Teams (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) unter Berücksichtigung aller relevanten Aspekte, wie Unternehmensführung und Prozessmanagement, und aus technischer Sicht beschrieben. Mit diesem Dokument werden zwei der im ENISA-Arbeitsprogramm 2006, Kapitel 5.1, beschriebenen Aufgaben umgesetzt:

- Das vorliegende Dokument: *Schriftlicher Bericht über die Einrichtung eines CERT oder ähnlicher Organe Schritt für Schritt, einschließlich Beispielen* (**CERT-D1**)
- Kapitel 12 und externe Dateien: *Auszug aus dem Zeitplan in aufgeschlüsselter Form zur leichten Anwendung des Zeitplans in der Praxis* (**CERT-D2**)

2 Rechtliche Hinweise

Sofern nichts anderes angegeben ist, wird darauf hingewiesen, dass diese Veröffentlichung die Auffassung und Interpretation der Verfasser und Herausgeber widerspiegelt. Die vorliegende Veröffentlichung ist nicht als eine Maßnahme der ENISA oder einer ihrer Gremien auszulegen, sofern diese nicht gemäß der Verordnung (EG) Nr. 460/2004 zur Einrichtung der ENISA angenommen wurde. Die vorliegende Veröffentlichung entspricht nicht unbedingt dem aktuellen Stand und kann von Zeit zu Zeit aktualisiert werden.

Externe Quellen bzw. Dritte werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt aus externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur zu Unterrichtungs- und Informationszwecken gedacht. Weder die ENISA noch ein Dritter, der in ihrem Auftrag handelt, haftet für die mögliche Nutzung der in dieser Veröffentlichung enthaltenen Informationen.

Alle Rechte vorbehalten. Ohne die vorherige schriftliche Genehmigung der ENISA bzw. nur sofern ausdrücklich gesetzlich zulässig oder nur gemäß den mit den entsprechenden Rechtsorganisationen vereinbarten Bedingungen darf kein Teil dieser Veröffentlichung vervielfältigt, in einem Datenabfragesystem gespeichert oder auf sonstige Weise elektronisch oder mechanisch übertragen, fotokopiert oder aufgezeichnet werden. Die Quelle ist jederzeit anzugeben. Vervielfältigungsanfragen können an die in dieser Veröffentlichung genannte Kontaktadresse gerichtet werden.

© Europäische Agentur für Netz- und Informationssicherheit (ENISA), 2006

3 Danksagung

Die ENISA dankt allen Institutionen und Personen, die am vorliegenden Dokument mitgewirkt haben. Ein spezieller Dank gilt den folgenden Personen bzw. Mitwirkenden:

- Henk Bronk, der als Berater die erste Fassung des vorliegenden Dokuments erstellt hat;

- CERT/CC und insbesondere dem CSIRT-Entwicklungsteam, das an äußerst nützlichen Unterlagen und den im Anhang enthaltenen Seminar-Musterunterlagen mitgewirkt hat;
- GovCERT.NL für seine Vorlage des *„CERT-in-a-box";*
- dem TRANSITS-Team, das an den im Anhang enthaltenen Seminar-Musterunterlagen mitgewirkt hat;
- den Kollegen aus dem Bereich Sicherheitsrichtlinien der Technischen Abteilung, die an Kapitel 6.6 mitgewirkt haben;
- den zahllosen Personen, die das vorliegende Dokument geprüft und Korrektur gelesen haben.

4 Einführung

Kommunikationsnetze und Informationssysteme sind zu einem wesentlichen Faktor der wirtschaftlichen und gesellschaftlichen Entwicklung geworden. Computer und Kommunikationsnetze werden wie Elektrizitäts- und Wasserversorgung zu unentbehrlichen Einrichtungen des täglichen Lebens.

Daher gewinnt die Sicherheit, vor allem aber die Verfügbarkeit von Kommunikationsnetzen und Informationssystemen, für die Gesellschaft mehr und mehr an Bedeutung. Dies gilt nicht zuletzt deshalb, weil sich aufgrund der Systemkomplexität sowie aufgrund von Unfällen, Bedienungsfehlern und unbefugten Eingriffen bei wichtigen Informationssystemen Probleme ergeben könnten, die sich auf die technische Infrastruktur von Diensten, die für das Wohlergehen der EU-Bürger von maßgeblicher Bedeutung sind, auswirken können.

Die Europäische Agentur für Netz- und Informationssicherheit wurde am 10. März 2004 errichtet[1]. Sie soll eine hohe und effektive Netz- und Informationssicherheit innerhalb der Gemeinschaft und die Entwicklung einer Kultur der Netz- und Informationssicherheit gewährleisten, die den Bürgern, Verbrauchern, Unternehmen und Organisationen des öffentlichen Sektors der Europäischen Union Nutzen bringt, und damit zum reibungslosen Funktionieren des Binnenmarkts beiträgt.

Seit mehreren Jahren haben einige Sicherheitseinrichtungen in Europa, wie CERT/CSIRT-, Abuse- und WARP-Teams, daran mitgewirkt, die Internet-Sicherheit zu erhöhen. Die ENISA möchte diese Einrichtungen bei ihren Bemühungen durch die Bereitstellung von Informationen über Maßnahmen zur Gewährleistung einer angemessenen Dienstgüte unterstützen. Darüber hinaus hat die ENISA die Absicht, die EU-Mitgliedstaaten und die Organe der EU bei Fragen in Bezug auf die Berücksichtigung bestimmter IT-Nutzergruppen mit entsprechenden Sicherheitsdiensten beratend zu unterstützen. Daher wird sich diese neue Arbeitsgruppe auf Basis der Feststellungen der 2005 eingerichteten Ad-hoc-Arbeitsgruppe „CERT Cooperation and

[1] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit. Eine „Agentur der Europäischen Gemeinschaft" ist ein von der EU eingerichtetes Organ zur Wahrnehmung spezieller technischer, wissenschaftlicher oder führungsrelevanter Aufgaben innerhalb des „Gemeinschaftsbereichs" („erste Säule") der EU.

Support“ mit Fragen der Bereitstellung adäquater Sicherheitsdienste („CERT-Dienste“) für bestimmte Benutzer (Benutzerkategorien oder -gruppen) befassen.

Durch die Veröffentlichung des vorliegenden Berichts *„Einrichtung eines CSIRT Schritt für Schritt mit zusätzlicher Prüfliste“*, der die Einrichtung eines eigenen CSIRT (Computer Security Incident Response Team, d. h. Reaktionsteam für Computersicherheitsverletzungen) erleichtern soll, unterstützt die ENISA die Einrichtung neuer CSIRT-Teams.

Zielgruppen

Die Zielgruppen für diesen Bericht sind in erster Linie staatliche und andere Institutionen, die die Einrichtung eines CSIRT beschließen, um ihre eigene IT-Infrastruktur oder die ihrer Interessengruppen zu schützen.

Verwendung dieses Dokuments

Das vorliegende Dokument enthält Informationen darüber, was ein CSIRT ist, welche Dienstleistungen von einem CSRIT angeboten werden können und welche vorbereitenden Maßnahmen erforderlich sind. Diese Informationen sollen dem Leser einen guten und pragmatischen Überblick über die Methode, Struktur und Aufgabe für die Einrichtung eines CSIRT vermitteln.

Kapitel 4 *„Einführung“*
Dieses Kapitel enthält eine Einführung zu diesem Bericht.

Kapitel 5 *„Generelle Strategie für die Planung und Einrichtung eines CSIRT“*
Der erste Abschnitt beschreibt, was ein CSIRT ist, und enthält Informationen über die verschiedenen Arbeitsumgebungen von CSIRT-Teams und die von ihnen angebotenen Dienstleistungen.

Kapitel 6 *„Ausarbeitung des Geschäftsplans“*
In diesem Kapitel wird der Geschäftsführungsansatz für die Einrichtung beschrieben.

Kapitel 7 *„Förderung des Geschäftsplans“*
Dieses Kapitel behandelt geschäftsfall- (Business Case) und finanzierungsspezifische Fragen.

Kapitel 8 *„Beispiele für betriebsspezifische und technische Verfahren“*
In diesem Kapitel wird das Verfahren beschrieben, wie Informationen gesammelt und in ein Sicherheitsbulletin (Security Bulletin) übertragen werden. Außerdem enthält dieses Kapitel eine Beschreibung des Arbeitsablaufes bei der Behandlung von Sicherheitsvorfällen.

Kapitel 9 *„CSIRT-Schulungsmaßnahmen“*
Dieses Kapitel gibt einen Überblick über die zur Verfügung stehenden CSIRT-Schulungsmaßnahmen. Die im Anhang enthaltenen Seminar-Musterunterlagen dienen zur Erläuterung.

Kapitel 10 *„Praktische Übung: Erstellung eines Advisory“*
Dieses Kapitel enthält eine praktische Übung für die Erbringung eines der grundlegenden CSIRT-Dienste (oder Hauptdienste), nämlich die Erstellung eines Sicherheitsbulletins (oder Advisory).

Kapitel 12 „Beschreibung des Projektplans“
Dieses Kapitel verweist auf den zusätzlichen Projektplan (Prüfliste), der mit diesem Leitfaden zur Verfügung gestellt wird. Dieser Plan dient als einfaches Instrument zur Umsetzung dieses Leitfadens.

In diesem Dokument verwendete Konventionen

Zur besseren Übersicht für den Leser beginnt jedes Kapitel mit einer Zusammenfassung der bislang bei der Einrichtung eines CSIRT unternommenen Schritte. Diese Zusammenfassungen werden in einem Kasten kurz erläutert, wie etwa:

Der erste Schritt wurde unternommen

Jedes Kapitel wird mit einer praktischen Übung der jeweils erläuterten Schritte abgeschlossen. Im vorliegenden Dokument ist das „fiktive CSIRT“ ein kleines, unabhängiges CSIRT für ein mittelständisches Unternehmen oder eine Einrichtung mittlerer Größe. Der Anhang enthält eine Zusammenfassung.

Fiktives CSIRT

5 Generelle Strategie für die Planung und Einrichtung eines CSIRT

Die erfolgreiche Inangriffnahme der Einrichtung eines CSIRT setzt eine klare Vorstellung über die möglichen Dienstleistungen voraus, die das Team seinen Kunden, in der „CSIRT-Welt“ auch besser unter dem Begriff „Constituents“ (zu Deutsch etwa Klientel) bekannt, anbieten kann. Daher muss man ihre Bedürfnisse genau kennen, um die entsprechenden Dienste zeitgerecht und in der adäquaten Qualität leisten zu können.

Was ist ein CSIRT?

CSIRT ist das Akronym für **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam (Reaktionsteam für Computersicherheitsverletzungen). Der Begriff CSIRT wird vorwiegend in Europa für den geschützten Begriff CERT verwendet, der in den USA vom CERT Coordination Center (CERT/CC) eingetragen ist.
Es gibt mehrere Akronyme, die für derartige Teams verwendet werden:

- CERT oder CERT/CC (**C**omputer **E**mergency **R**esponse **T**eam/**C**oordination **C**enter)
- CSIRT (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam)
- IRT (**I**ncident **R**esponse **T**eam)
- CIRT (**C**omputer **I**ncident **R**esponse **T**eam)
- SERT (**S**ecurity **E**mergency **R**esponse **T**eam)

Die erste größere Epidemie in der globalen IT-Infrastruktur wurde Ende der 80er Jahre durch einen Wurm ausgelöst. Dieser Wurm namens Morris[2] breitete sich rasch aus und infizierte eine Vielzahl von IT-Systemen rund um den Globus.

Dieser Vorfall wirkte wie ein Weckruf. Denn plötzlich erkannten die Menschen, wie wichtig die Zusammenarbeit und Koordination zwischen Systemadministratoren und IT-Managern für den Umgang mit derartigen Fällen ist. Aufgrund der Tatsache, dass Zeit ein kritischer Faktor war, musste ein besser organisierter und strukturierter Ansatz zur Behandlung von Sicherheitsvorfällen eingeführt werden. Daher wurde das erste CSIRT nur wenige Tage nach dem durch Morris ausgelösten Vorfall von der DARPA (**D**efence **A**dvanced **R**esearch **P**rojects **A**gency, einer Behörde des US-amerikanischen Verteidigungsministeriums zur Durchführung von Hightech-Forschungsprojekten), eingerichtet, nämlich das CERT Coordination Center (CERT/CC[3]) an der Carnegie Mellon-Universität von Pittsburgh (Pennsylvania).

Kurze Zeit später wurde dieses Modell in Europa übernommen. 1992 wurde das erste CSIRT namens SURFnet-CERT[4] in Europa von dem niederländischen Anbieter und Universitätsnetzwerk SURFnet eingeführt. In der Folgezeit wurden zahlreiche Teams eingerichtet. Derzeit umfasst das Verzeichnis der ENISA über CERT-Aktivitäten in Europa (*Inventory of CERT activities in Europe*[5]) über 100 bekannte Teams in Europa.

---

[2] Weitere Informationen über den Wurm Morris finden Sie auf der Website: http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC: http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

[5] ENISA-Verzeichnis: http://www.enisa.europa.eu/CERT_INVENTORY/

Im Laufe der Jahre haben die CERT-Teams ihre Kapazitäten ausgedehnt und sind nicht mehr nur reine Reaktionsteams, sondern Sicherheitsdienstanbieter, die auch präventive Dienste anbieten, wie Warnungen, Security Advisories (Sammlung von Hinweisen und Ratschlägen zu einem Problem), Schulungs- und Sicherheitsmanagementdienste. Schon bald wurde erkannt, dass der Begriff „CERT“ nicht ausreichend war. Daher wurde Ende der 90er Jahre der neue Begriff „CSIRT“ eingeführt. Derzeit werden beide Begriffe (CERT und CSIRT) synonym verwendet, wobei CSIRT der präzisere Begriff ist.

5..1 Der Begriff „*Constituency“* (Klientel)

Im Folgenden wird der (in CSIRT-Gemeinschaften) etablierte Begriff „Klientel“ (engl. „Constituency“) als Bezeichnung für den Kundenstamm eines CSIRT verwendet. Ein einzelner Kunde wird dabei als Klient, eine Gruppe von Kunden als Klienten bezeichnet.

5..2 Definition eines CSIRT

Ein CSIRT ist ein Team von IT-Sicherheitsexperten bzw. -sachverständigen, deren Hauptaufgabe darin besteht, auf Computersicherheitsverletzungen zu reagieren. Dieses Team bietet die zu ihrer Behandlung notwendigen Dienstleistungen und unterstützt seine Klientel bei der Wiederherstellung nach derartigen Sicherheitsverletzungen.

Um Risiken zu mindern und die Anzahl der erforderlichen Gegenmaßnahmen (Reaktionen) auf ein Minimum zu senken, bieten die meisten CSIRT-Teams auch Präventiv- und Schulungsdienste für ihre Klientel an. Sie veröffentlichen Advisories über Sicherheitslücken in der jeweils verwendeten Hardware und Software und informieren die Nutzer auch über Schwachstellen (Exploits) und Viren, die sich diese Lücken zunutze machen. Daher kann die Klientel schnell das erforderliche Patch (Korrekturprogramm) bzw. die erforderliche Aktualisierung auf ihrem System installieren. In Kapitel *5.2 Mögliche Dienste* finden Sie eine vollständige Liste aller denkbaren Dienstleistungen.

5..3 Vorzüge eines CSIRT

Mit einem speziellen IT-Sicherheitsteam kann ein Unternehmen die gravierendsten Vorfälle abschwächen und verhindern sowie seine wertvollen Anlagen besser schützen.

Zu den weiteren Vorzügen zählen:

- Zentrale Koordination aller IT-sicherheitsrelevanten Probleme innerhalb des Unternehmens (zentraler Ansprechpartner)
- Zentrale und sachkundige Behandlung von und Reaktion auf IT-Vorfälle
- Fachkenntnisse zur Unterstützung der Benutzer bei der raschen Wiederherstellung ihrer Systeme nach Sicherheitsvorfällen
- Behandlung von rechtlichen Problemen und Aufbewahrung von Nachweisen bei einem Rechtsstreit
- Verfolgung der Entwicklungen im Bereich der Sicherheit
- Förderung der Zusammenarbeit innerhalb der Klientel im Bereich der IT-Sicherheit (Sensibilisierung des Sicherheitsbewusstseins)

Fiktives CSIRT (Schritt 0)

Verstehen, was ein CSIRT ist:

Bei diesem Beispiel soll das CSIRT Dienste für eine Einrichtung mittlerer Größe mit etwa 200 Mitarbeitern leisten. Die Einrichtung hat eine eigene IT-Abteilung und zwei weitere Niederlassungen im gleichen Land. Der IT-Bereich spielt eine wesentliche Rolle für das Unternehmen, da die IT-Systeme für die interne Kommunikation, das Datennetz und den elektronischen Geschäftsverkehr rund um die Uhr (24x7) verwendet werden. Die Einrichtung hat ein eigenes Netzwerk und verfügt über einen redundanten Internetanschluss über zwei verschiedene ISP (Internet Service Provider, d. h. Internetdienstanbieter).

5..4 Beschreibung der unterschiedlichen CSIRT-Umgebungen

Der erste Schritt wurde unternommen

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.

>> Im nächsten Schritt ist die Frage zu beantworten: „Für welchen Bereich soll das CSIRT Dienste anbieten?"

Bei der Einrichtung eines CSIRT gilt es (wie bei jedem anderen Unternehmen auch), sich innerhalb kürzester Zeit darüber klar zu werden, wer zur Klientel gehört und für welche Umgebung die CSIRT-Dienste entwickelt werden sollen. Derzeit werden CSIRT-Teams für die folgenden Bereiche in alphabetischer Reihenfolge unterschieden:

- Anbieterbereich
- CIP/CIIP-Bereich
- Hochschulbereich
- Interner Bereich
- KMU-Bereich (kleine und mittlere Unternehmen)
- Kommerzieller Bereich
- Militärischer Bereich
- Nationaler Bereich
- Staatlicher Bereich

CSIRT für den Anbieterbereich
Ausrichtung
Ein CSIRT für diesen Bereich unterstützt vorwiegend anbieterspezifische Produkte. Es soll Lösungen zur Beseitigung von Sicherheitslücken und zur Abschwächung der negativen Auswirkungen solcher Lücken entwickeln und bereitstellen.

Klientel
Produkteigentümer

Wie im Absatz über CSIRT-Teams für den nationalen Bereich (s. u.) beschrieben, kann ein Team Dienste für mehrere Bereiche anbieten, was sich beispielsweise auf die Analyse der Klientel und deren Anforderungen auswirkt.

CSIRT für den CIP/CIIP-Bereich
Ausrichtung
Ein CSIRT-Team in diesem Bereich bietet seine Dienste in erster Linie zum Schutz kritischer Informationen (**C**ritical **I**nformation **P**rotection) und/oder zum Schutz kritischer Informationen und Infrastrukturen (**C**ritical **I**nformation and **I**nfrastructure **P**rotection) an. Meistens arbeitet dieses spezielle CSIRT-Team eng mit einer staatlichen CIIP-Abteilung zusammen. Es befasst sich mit allen kritischen IT-Bereichen des jeweiligen Landes und schützt die Bürger dieses Landes.

Klientel
Regierung; kritische, sicherheitsgefährdete IT-Unternehmen, Bürger

CSIRT für den Hochschulbereich
Ausrichtung
Ein CSIRT für den Hochschulbereich bietet CSIRT-Dienste für Hochschulen und Bildungseinrichtungen, wie Universitäten oder Forschungseinrichtungen, und deren Internetumgebung auf dem Campus.

Klientel
Zur typischen Klientel dieses CSIRT-Typs gehören Mitarbeiter und Studenten von Hochschulen und Universitäten.

CSIRT für den internen Bereich
Ausrichtung
Ein internes CSIRT bietet nur Dienste für seine Auftraggeberorganisation an. Dadurch wird also kein Bereich, sondern vielmehr die Funktionsweise beschrieben. Viele Telekommunikationsunternehmen und Banken verfügen über eigene interne CSIRT-Teams, die in der Regel keine öffentlich zugängliche Website haben.

Klientel
Interne Mitarbeiter und IT-Abteilung der Auftraggeberorganisation

CSIRT für den KMU-Bereich (kleine und mittlere Unternehmen)
Ausrichtung
Dieses CSIRT mit eigener Organisation bietet seine Dienstleistungen für den eigenen Geschäftszweig oder eine ähnliche Nutzergruppe an.

Klientel
Zur Klientel dieser CSIRT-Teams könnten KMU und deren Mitarbeiter oder spezielle Interessengruppen wie der „Verband der Städte und Stadtverwaltungen“ eines Landes gehören.

CSIRT für den kommerziellen Bereich
Ausrichtung
Ein CSIRT für den kommerziellen Bereich leistet kommerzielle CSIRT-Dienste für seine Klientel. Bei einem ISP bietet das CSIRT größtenteils missbrauchrelevante Dienste für Endbenutzerkunden (Einwahl, ADSL) und CSIRT-Dienste für deren professionelle Kunden.

Klientel
CSIRT-Teams für den kommerziellen Bereich leisten ihre Dienste für die Klientel in der Regel gegen Bezahlung.

CSIRT für den militärischen Bereich
Ausrichtung
Ein CSIRT für diesen Bereich bietet Dienste für militärische Organisationen an und ist für die IT-Infrastruktur verantwortlich, die zu Verteidigungszwecken erforderlich ist.

Klientel
Mitarbeiter von militärischen Einrichtungen oder eng verwandten Organisationen, beispielsweise des Verteidigungsministeriums.

CSIRT für den nationalen Bereich
Ausrichtung
Ein CSIRT mit nationaler Ausrichtung wird als Ansprechpartner für Sicherheitsfragen eines Landes angesehen. Manchmal fungiert ein CISRT für den staatlichen Bereich auch als nationaler Ansprechpartner (beispielsweise UNIRAS in Großbritannien).

Klientel
Normalerweise hat dieser CSIRT-Typ keine direkte Klientel, da das CSIRT für den nationalen Bereich nur eine (Ver-) Mittlerrolle für das gesamte Land spielt.

CSIRT für den staatlichen Bereich
Ausrichtung
Ein CSIRT für den staatlichen Bereich bietet Dienste für (staatliche) Behörden und in einigen Ländern auch für die Bürger an.

Klientel
Regierung und (staatliche) Behörden; in einigen Ländern (beispielsweise in Belgien, Ungarn, den Niederlanden, dem Vereinigten Königreich oder Deutschland) werden auch Warndienste für die Bürger erbracht.

Fiktives CSIRT (Schritt 1)
Startphase In der Startphase wird das neue CSIRT als internes CSIRT geplant und soll Dienste für die Auftraggeberorganisation, die lokale IT-Abteilung und die Mitarbeiter anbieten. Ferner soll es die Behandlung IT-sicherheitsrelevanter Vorfälle zwischen den einzelnen Niederlassungen unterstützen und koordinieren.

Mögliche Dienste eines CSIRT

Die beiden ersten Schritte wurden unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?

>> Im nächsten Schritt ist die Frage zu beantworten, *welche Dienste für die Klientel angeboten werden sollen.*

Ein CSIRT kann viele Dienste anbieten; doch bislang bietet noch kein etabliertes CSIRT alle Dienste an. Daher ist die Auswahl der richtigen Dienste eine ganz wesentliche Entscheidung. Nachstehend finden Sie einen kurzen Überblick über alle bekannten CSIRT-Dienste, die in dem vom CERT/CC[6] veröffentlichten Handbuch („Handbook for CSIRTs“) definiert sind.

[6] CERT/CC-Handbuch für CSIRT-Teams (in englischer Sprache): http://www.cert.org/archive/pdf/csirt-handbook.pdf

Reaktive Dienste	**Proaktive Dienste**	**Behandlung von Artefakten**
• **Alarm- und Warnmeldungen** • **Behandlung von Sicherheitsvorfällen** • **Analyse von Sicherheitsvorfällen** • **Unterstützung bei der Reaktion auf Sicherheitsvorfälle** • **Koordination der Reaktion auf Sicherheitsvorfälle** • Reaktion auf Sicherheitsvorfälle vor Ort • Behandlung von Sicherheitslücken • Analyse von Sicherheitslücken • Reaktion auf Sicherheitslücken • Koordination der Reaktion auf Sicherheitslücken	• **Bekanntgaben** • Technologieüberwachung • Sicherheitsaudits oder -analysen • Konfiguration und Pflege des Sicherheitssystems • Entwicklung von Sicherheitswerkzeugen • Dienste für die Erkennung von Angriffsversuchen • Verteilung von sicherheitsrelevanten Informationen	• *Analyse von Artefakten* • *Reaktion auf Artefakte* • *Koordination der Reaktion auf Artefakte*
		Sicherheitsqualitäts-management
		• *Risikoanalyse* • *Kontinuität des Geschäftsbetriebs und Wiederherstellung nach Notfällen* • *Beratung in Sicherheitsfragen* • *Sensibilisierung des Sicherheitsbewusstseins* • *Ausbildung/Schulung* • *Produktevaluierung oder -zertifizierung*

Abb. 1: Liste der CSIRT-Dienste von CERT/CC[7]

Die **Hauptdienste (in Fettdruck gekennzeichnet)**: Es wird zwischen reaktiven und proaktiven Diensten unterschieden. Durch die Sensibilisierung des Sicherheitsbewusstseins und Schulungsmaßnahmen zielen proaktive Dienste auf die Prävention von Vorfällen ab, während reaktive Dienste auf die Behandlung von Sicherheitsvorfällen und die Begrenzung des entstandenen Schadens ausgerichtet sind.

Die **Behandlung von Artefakten** umfasst die Analyse der in einem System erkannten Dateien oder Objekte, die u. U. an bösartigen Aktionen beteiligt sind, wie Reste von Viren, Würmern, Skripten, Trojanern usw. Sie sieht auch die Bearbeitung und Verteilung von entsprechenden Informationen an Anbieter und andere Interessenten vor, um die weitere Verbreitung der Malware zu vermeiden und die Risiken zu minimieren.

Dienste für das Sicherheits- und Qualitätsmanagement sind Dienstleistungen mit einer längerfristigen Zielsetzung und umfassen Beratung sowie Ausbildungs- und Schulungsmaßnahmen.

Im Anhang finden Sie eine detaillierte Erläuterung der CSIRT-Dienste.

Die Auswahl der richtigen Dienste für Ihre Klientel ist ein wichtiger Schritt und wird in Kapitel *6.1 Festlegung des Finanzierungsmodells* näher erläutert.

[7] Liste der CSIRT-Dienste von CERT/CC: http://www.cert.org/csirts/services.html

Die meisten CSIRT-Teams beginnen mit der Verteilung von „Alerts und Warnings“ (Alarm- und Warnmeldungen), machen „Announcements“ (Bekanntgaben) und bieten „Incident Handling“ (Behandlung von Sicherheitsvorfällen) für ihre Klientel an. Diese Hauptdienste bewirken normalerweise eine gute Sensibilisierung innerhalb der Klientel und werden hauptsächlich als echter „Mehrwert“ angesehen.

In der Praxis empfiehlt es sich, mit einer kleinen Gruppe von Pilotklienten zu beginnen, die Hauptdienste für einen Pilotzeitraum zu leisten und danach um Rückmeldungen zu bitten.
Interessierte Pilotnutzer geben in der Regel konstruktive Rückmeldungen und helfen bei der Entwicklung maßgeschneiderter Dienste.

Fiktives CSIRT (Schritt 2)

Auswahl der richtigen Dienste

In der Startphase wird beschlossen, dass das neue CSIRT hauptsächlich auf die Erbringung der Hauptdienste für die Mitarbeiter ausgerichtet sein soll.

Es wird beschlossen, dass man nach Abschluss der Pilotphase eine Erweiterung der Dienstpalette um einige „Sicherheitsmanagementdienste“ in Erwägung ziehen könnte. Diese Entscheidung soll auf Basis der Rückmeldungen vonseiten der Pilotklienten und in enger Zusammenarbeit mit der Abteilung für Qualitätssicherung getroffen werden.

Analyse der Klientel und Festlegung des Aufgabenbereichs

Die ersten drei Schritte wurden unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann.

>> Im nächsten Schritt ist die Frage zu beantworten, *welcher Ansatz für die Einrichtung des CSIRT gewählt werden sollte.*

Der nächste Schritt ist eine genauere Analyse der Klientel mit dem vorrangigen Ziel, die richtigen Kommunikationskanäle zu wählen:

- Festlegung der Kommunikationswege zur Klientel
- Festlegung des Aufgabenbereichs
- Erstellung eines realistischen Implementierungs-/Projektplans
- Festlegung der CSIRT-Dienste
- Festlegung der Organisationsstruktur
- Festlegung der Richtlinien für die Informationssicherheit
- Einstellung der richtigen Mitarbeiter
- Nutzung Ihres CSIRT-Büros

- Suche nach Kooperationsmöglichkeiten zwischen anderen CSIRT-Teams und möglichen nationalen Initiativen

Diese Schritte werden in den folgenden Absätzen näher beschrieben und können in den Geschäfts- und den Projektplan aufgenommen werden.

5..1 Kommunikationswege zur Klientel

Wie bereits erwähnt, ist es sehr wichtig, dass Sie die Anforderungen der Klientel sowie Ihre eigene Kommunikationsstrategie, einschließlich der am besten geeigneten Kommunikationskanäle für die Verteilung von Informationen an diese Klientel, genau kennen.

In der Managementtheorie sind mehrere methodische Ansätze für das Problem der Zielgruppenanalyse bekannt. Im vorliegenden Dokument werden zwei Ansätze beschrieben, nämlich die SWOT- und die PEST-Analyse.

SWOT-Analyse
Eine SWOT-Analyse (engl. Akronym für **S**trengths, **W**eaknesses, **O**pportunities und **T**hreats) ist ein strategisches Planungsinstrument zur Evaluierung der Stärken, Schwächen, Chancen und Gefahren eines Projekts, eines unternehmerischen Vorhabens oder einer anderen Situation, für das bzw. die eine Entscheidung erforderlich ist. Dieses Verfahren wurde von Albert Humphrey erfunden, der in den 60er und 70er Jahren ein Forschungsprojekt auf Basis von Daten der Fortune 500-Unternehmen an der Stanford-Universität leitete.[8]

Stärken	**Schwächen**
Chancen	**Gefahren**

Abb. 2: SWOT-Analyse

[8] SWOT-Analyse auf der Website von Wikipedia: http://de.wikipedia.org/wiki/SWOT-Analyse

PEST-Analyse

Die PEST-Analyse (engl. Akronym für **P**olitical, **E**conomic, **S**ocio-cultural und **T**echnological), auch STEP-Analyse genannt, ist ein anderes wichtiges und gängiges Werkzeug zur Analyse der Klientel mit dem Ziel, die politische, ökonomische, soziokulturelle und technologische Umgebung zu verstehen, in der ein CSIRT agiert. Dieses Instrument dient zur leichteren Ermittlung, ob die Planung noch auf die Umgebung abgestimmt ist, und zur Vermeidung von Maßnahmen auf Basis falscher Annahmen.

Politische Faktoren	**Ökonomische Faktoren**
• Ökologische/umweltschutzspezifische Fragen • Aktuelle Gesetzgebung im jeweiligen Land • Zukünftige Gesetzgebung • Europäische/internationale Gesetzgebung • Regulierungs-/Aufsichtsbehörden und Abläufe • Staatliche Richtlinien • Amtsdauer und Wechsel der Regierung • Handelsrichtlinien • Finanzierung, Subventionen, Beihilfen und Initiativen • Lobbys/Interessenverbände im jeweiligen Land • Internationale Interessenverbände	• Wirtschaftssituation im jeweiligen Land • Konjunkturentwicklung im jeweiligen Land • Konjunktur und Entwicklung im Ausland • Generelle steuerrechtliche Fragen • Besteuerung von Produkten/ Dienstleistungen • Saisonbedingte/witterungsbedingte Fragen • Markt- und Konjunkturzyklen • Branchenspezifische Faktoren • Vermarktungswege und Vertriebstrends • Treibende Faktoren für Kunden/ Endbenutzer • Zinssätze und Wechselkurse
Soziale Faktoren	**Technologische Faktoren**
• Lifestyle-Trends • Demografische Faktoren • Verbraucherverhalten und -meinungen • Ansichten in öffentlichen Medien • Gesetzesänderungen mit Auswirkung auf soziale Faktoren • Marken-, Firmen-, Technologieimage • Einkaufsverhalten von Verbrauchern • Mode und Rollenmodelle • Wesentliche Ereignisse und Einflüsse • Kaufmöglichkeiten und -trends • Ethnische/religiöse Faktoren • Werbung und Reklame	• Entwicklung von Wettbewerbertechnologien • Forschungsfinanzierung • Verwandte/abhängige Technologien • Ersatztechnologie/-lösungen • Reife der Technologie • Reife und Kapazität der Fertigung • Information und Kommunikation • Kaufmechanismen von Verbrauchern/ Technology • Technologiespezifische Gesetzgebung • Innovationspotenzial • Technologiezugang, Lizenzierung, Patente • Fragen in Bezug auf geistiges Eigentum

Abb. 3: Pest-Analysemodell

Die PEST-Analyse ist auf der Website von Wikipedia näher beschrieben[9].

Beide Instrumente geben einen umfassenden und strukturierten Überblick über die Anforderungen der Klientel. Die Ergebnisse dienen zur Ergänzung des Geschäftsplans und dadurch auch zur Beantragung der Finanzierungsmittel für die Einrichtung des CSIRT.

[9] PEST-Analyse auf der Website von Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis oder http://de.wikipedia.org/wiki/PEST-Analyse

Kommunikationskanäle
Ein wichtiges Thema, das bei der Analyse berücksichtigt werden sollte, sind die möglichen Methoden für die Kommunikation und Informationsverteilung (Kommunikation mit der Klientel).

Nach Möglichkeit sollten regelmäßige, persönliche Besuche der Klientel in Erwägung gezogen werden. Nachweislich erleichtern persönliche Gespräche die Zusammenarbeit. Wenn beide Seiten zur Zusammenarbeit bereit sind, führen solche Gespräche und Sitzungen zu einem offeneren Dialog.

Normalerweise nutzen CSIRT-Teams mehrere Kommunikationskanäle. Die folgenden Kanäle haben sich in der Praxis bewährt und sind erwägenswert:

- Öffentlich zugängliche Website
- Geschlossener Mitgliederbereich auf der Website
- Webformulare zur Meldung von Vorfällen
- Mailinglisten
- Persönliche E-Mail-Nachrichten
- Telefon / Fax
- SMS
- „Altmodische“ Korrespondenz (Schreiben)
- Monats- oder Jahresberichte

Abgesehen von der Verwendung von E-Mail, Webformularen, Telefon oder Fax zur leichteren Behandlung von Vorfällen (zum Erhalt von Berichten der Klientel über Vorfälle, zur Koordinierung mit anderen Teams oder zur Information und Unterstützung des Opfers) veröffentlichen die meisten CSIRT-Teams ihre Security Advisories (mit Hinweisen und Ratschlägen) auf einer öffentlich zugänglichen Website und über Mailinglisten.

! Nach Möglichkeit sollten Informationen auf sichere, geschützte Weise verteilt werden. E-Mail-Nachrichten lassen sich beispielsweise mit PGP (engl. Akronym für Pretty Good Privacy) digital signieren; vertrauliche Daten über Vorfälle sollten stets verschlüsselt werden.

Weitere Informationen finden Sie in Kapitel *8.5 Verfügbare CSIRT-Werkzeuge*. Siehe auch Kapitel *2.3* der *RFC2350*[10].

Fiktives CSIRT (Schritt 3a)
Analyse der Klientel und der geeigneten Kommunikationskanäle

Bei einer Brainstorming-Sitzung mit Schlüsselpersonen der Geschäftsführung und der Klientel werden genügend Daten für eine SWOT-Analyse zusammengestellt. Aufgrund dessen kommt man zu dem Schluss, dass die folgenden Hauptdienste erforderlich sind:

[10] http://www.ietf.org/rfc/rfc2350.txt

- Alarm- und Warnmeldungen
- Behandlung von Vorfällen (Analyse, Unterstützung bei der Reaktion und Koordination der Reaktion)
- Bekanntgaben

Es muss gewährleistet sein, dass die Informationen gut organisiert möglichst an einen Großteil der Klientel verteilt werden. Daher wird beschlossen, die Alarm- und Warnmeldungen und Bekanntgaben in Form von Security Advisories auf einer speziellen Website zu veröffentlichen und über eine Mailingliste zu verteilen. Das CSIRT ermöglicht E-Mail-Nachrichten, Telefonate und Faxmitteilungen für den Eingang von Berichten über Vorfälle. Für den nächsten Schritt wird ein einheitliches Webformular geplant.

Auf der nächsten Seite finden Sie ein Beispiel für eine SWOT-Analyse.

Stärken • Einige Kenntnisse im Unternehmen vorhanden • Befürwortung des Plans und Kooperationsbereitschaft • Unterstützung und Finanzierung seitens der Geschäftsführung	**Schwächen** • Kaum Kommunikation zwischen den einzelnen Abteilungen und Niederlassungen • Keine Koordination bei IT-Sicherheitsvorfällen • Vielzahl von „kleinen Abteilungen“
Chancen • Nicht strukturierte Informationsflut über Sicherheitslücken • Großer Koordinationsbedarf • Begrenzung der Schäden durch Vorfälle • Vielzahl an offenen Fragen in Bezug auf IT-Sicherheit • Schulung der Mitarbeiter im Bereich der IT-Sicherheit	**Gefahren** • Kaum Geld vorhanden • Personalengpässe • Hohe Erwartungen • Kultur

Abb. 4: Beispiel einer SWOT-Analyse

5..2 Aufgabenbereich

Nach der Analyse der klientelseitigen Anforderungen und Wünsche in Bezug auf die CSIRT-Dienste sollte im nächsten Schritt der Aufgabenbereich im Entwurf festgelegt werden.

Ein Aufgabenbereich beschreibt die grundlegende soziale Funktion des Unternehmens im Hinblick auf die der Klientel angebotenen Produkte und Dienstleistungen. Dadurch lassen sich Existenz und Funktion des neuen CSIRT klar und deutlich kommunizieren.

In der Praxis empfiehlt es sich, den Aufgabenbereich kurz, aber nicht zu knapp zu formulieren, weil er in der Regel mehrere Jahre lang unverändert bleibt.

Nachstehend finden Sie einige Beispiele für Aufgabenbereiche von aktiven CSIRT-Teams:

„<Name des CSIRT> bietet Informationen und Unterstützung für seine <Klientel (Klientel zu definieren)> bei der Umsetzung proaktiver Maßnahmen zur Verringerung der Risiken von Computersicherheitsverletzungen sowie bei der Reaktion auf derartige Verletzungen bzw. Vorfälle, sobald diese eintreten.“

„Unterstützung der <Klientel> bei der Prävention von und Reaktion auf IT-relevante Sicherheitsvorfälle“[11]

Die Festlegung des Aufgabenbereichs ist ein wichtiger und notwendiger Schritt. In Kapitel *2.1* der *RFC2350*[12] finden Sie eine nähere Beschreibung der Informationen, die von einem CSIRT veröffentlicht werden sollten.

Fiktives CSIRT (Schritt 3b)
Die Geschäftsführung des fiktiven CSIRT hat folgenden Aufgabenbereich festgelegt: *„Das fiktive CSIRT bietet den Mitarbeitern des Auftraggebers Informationen und Unterstützung zur Verringerung der Risiken von Computersicherheitsverletzungen sowie bei der Reaktion auf derartige Verletzungen bzw. Vorfälle, sobald diese eintreten.“* Dadurch stellt das fiktive CSIRT klar, dass es ein internes CSIRT ist und dass seine Hauptaufgaben in der Behandlung IT-sicherheitsrelevanter Probleme bestehen.

[11] Aufgabenbereich von Govcert.nl: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Ausarbeitung des Geschäftsplans

Die folgenden Schritte wurden bereits unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann.
4. Analyse der Umgebung und der Klientel
5. Festlegung des Aufgabenbereichs

>> Im nächsten Schritt ist der Geschäftsplan festzulegen.

Da Ihnen die Analyseergebnisse einen guten Überblick über die Anforderungen und (angenommenen) Schwächen der Klientel geben, können Sie diese beim nächsten Schritt berücksichtigen.

Festlegung des Finanzierungsmodells

Nach der Analyse werden einige Hauptdienste ausgewählt, mit denen begonnen werden soll. Im nächsten Schritt muss das Finanzmodell überdacht werden, d. h. welche Parameter der angebotenen Dienste geeignet sind und bezahlt werden können.

Im Idealfall wäre es möglich, die Finanzierung an die Bedürfnisse der Klientel anzupassen. In der Realität muss das Spektrum der angebotenen Dienste jedoch an ein bestimmtes Budget angepasst werden. Daher ist es realistischer, mit der Planung von finanzierungsspezifischen Fragen zu beginnen.

6..1 Kostenmodell

Die beiden Hauptfaktoren, die sich auf die Kosten auswirken, sind die Festlegung der Dienstzeiten und der Anzahl (und Qualität) der einzustellenden Mitarbeiter. Müssen die Reaktion auf Vorfälle und die technische Unterstützung rund um die Uhr (24x7) gewährleistet sein, oder sollen diese Dienste nur während der normalen Geschäftszeiten angeboten werden?

Abhängig von der jeweils gewünschten Verfügbarkeit und der Büroeinrichtung (können Mitarbeiter beispielsweise von zuhause arbeiten?) kann es von Vorteil sein, mit einem Bereitschaftsdienstplan oder einem festen Dienstplan zu arbeiten.

Denkbar ist ein Szenario, bei dem sowohl proaktive als auch reaktive Dienste während der normalen Geschäftszeiten angeboten werden. Außerhalb der normalen Geschäftszeiten werden bestimmte Dienste, beispielsweise bei extremen Notfällen und Vorfällen, nur von einem Mitarbeiter erbracht, der Dienstbereitschaft hat.

Eine andere Möglichkeit besteht darin, sich um die internationale Kooperation mit anderen CSIRT-Teams zu bemühen. Es gibt bereits Beispiele für eine gut

funktionierende Zusammenarbeit nach dem „Following the Sun“-Prinzip (Sonnenstand, Sonnenwanderung). So hat sich beispielsweise die Zusammenarbeit zwischen europäischen und amerikanischen Teams als nützliche und gute Möglichkeit erwiesen, um die vorhandenen Kapazitäten gegenseitig zu nutzen. So bietet das CSIRT von Sun Microsystems mit mehreren internationalen Niederlassungen in verschiedenen Zeitzonen (wobei alle Mitarbeiter jedoch zum gleichen CSIRT-Team gehören) weltweit Dienste rund um die Uhr (24x7) durch den Schichtbetrieb an. Dadurch werden die Kosten im Rahmen gehalten, weil die Teams stets nur während der üblichen Geschäftszeiten arbeiten und auch Dienste für den „schlafenden Teil“ der Welt anbieten.

Üblicherweise wird insbesondere der Bedarf für Dienste rund um die Uhr (24x7) mit der Klientel genauestens analysiert. Nachts ausgegebene Alarm- und Warnmeldungen sind wohl kaum sinnvoll, wenn der Empfänger sie erst am nächsten Morgen lesen kann. Zwischen „Dienstbedarf“ und „Dienstwunsch“ besteht ein feiner Unterschied. Insbesondere die Geschäftszeiten machen jedoch einen großen Unterschied im Hinblick auf den Personal- und Einrichtungsbedarf und wirken sich daher erheblich auf das Kostenmodell aus.

6..2 Ertragsmodell

Wenn die Kosten bekannt sind, sollte man im nächsten Schritt über mögliche Ertragsmodelle nachdenken, d. h. wie die geplanten Dienste finanziert werden können. Im Folgenden finden Sie einige Szenarios für die Evaluierung:

Nutzung vorhandener Ressourcen
Es ist immer von Vorteil, die in anderen Teilen des Unternehmens bereits vorhandenen Ressourcen zu analysieren. Gibt es bereits geeignete Mitarbeiter (z. B. in der bestehenden IT-Abteilung) mit dem erforderlichen Hintergrund- und Fachwissen? Denkbar wäre, dass die Geschäftsführung diese Mitarbeiter in der Startphase für das CSIRT abstellt oder dass diese Mitarbeiter das CSIRT auf Ad-hoc-Basis unterstützen.

Mitgliedsbeitrag
Eine andere Möglichkeit besteht darin, Ihre Dienste gegen Zahlung eines jährlichen/ vierteljährlichen Mitgliedsbeitrags zur Verfügung zu stellen. Zusätzliche Dienste, wie Beratungsdienste oder Sicherheitsaudits, könnten nach Inanspruchnahme bezahlt werden.

Andere denkbare Szenarios: Dienste für die (interne) Klientel werden unentgeltlich angeboten, während Dienste für externe Kunden bezahlt werden müssen. Eine andere Idee besteht darin, Advisories und Informationsbulletins auf der öffentlichen Website und spezielle, genauere Informationen in einem Bereich „Nur für Mitglieder“ zu veröffentlichen.

In der Praxis hat sich gezeigt, dass sich ein „Abonnement pro CSIRT-Dienst“ vor allem in der Startphase nur bedingt für die Bereitstellung ausreichender Finanzierungsmittel eignet. Feste Grundkosten für das Team und die Ausstattung müssen beispielsweise im Voraus gezahlt werden. Die Finanzierung dieser Kosten durch kostenpflichtige CSIRT-Dienste ist schwierig und erfordert eine sehr genaue Finanzanalyse, um den „Breakeven-Point“ (die Rentabilitätsschwelle) zu erreichen.

Subventionen
Eine andere überlegenswerte Möglichkeit bestünde darin, staatliche oder behördliche Subventionen zu beantragen, da die meisten Länder heutzutage Finanzmittel für IT-Sicherheitsprojekte zur Verfügung stellen. Eine Kontaktaufnahme mit dem Innenministerium könnte ein guter Anfang sein.

Natürlich ist auch eine Kombination unterschiedlicher Modelle denkbar.

Festlegung der Organisationsstruktur

Die geeignete Organisationsstruktur eines CSIRT hängt weitgehend von der vorhandenen Struktur der Auftraggeberorganisation und der Klientel ab. Sie hängt auch von der Verfügbarkeit der in Festanstellung oder auf Ad-hoc-Basis einzustellenden Fachkräfte ab.

Ein typisches CSIRT definiert die folgenden Funktionen innerhalb des Teams:

Intern
- General Manager

Mitarbeiter
- Büroleiter
- Buchhalter
- Kommunikationsberater
- Rechtsberater

Technisches Team (für den Betrieb)
- Leiter des technischen Teams
- Technische Sachverständige zur Erbringung der CSIRT-Dienste
- Forscher/Wissenschaftler

Externe Berater
- Inanspruchnahme bei Bedarf

Vor allem während der Startphase des CSIRT ist es extrem nützlich, einen Juristen im Team zu haben. Dadurch steigen zwar die Kosten, doch letzten Endes können Sie dadurch Zeit einsparen und sich rechtliche Schwierigkeiten ersparen.

Abhängig von dem innerhalb der Klientel vorhandenen Fachwissen und bei einem CSIRT mit einem hohen Medienprofil hat es sich auch bewährt, einen Kommunikationsexperten im Team zu haben. Diese Experten können schwierige technische Fragen ganz gezielt in Aussagen übertragen, die für die Klientel oder Medienpartner leichter zu verstehen sind. Außerdem soll der Kommunikationsexperte die Kommentare der Klientel an die technischen Experten weiterleiten und fungiert somit als „Übersetzer“ und „Vermittler“ zwischen diesen beiden Gruppen.

Nachstehend finden Sie einige Beispiele für Organisationsmodelle, die in aktiven CSIRT-Teams angewandt werden.

6..1 Das unabhängige Geschäftsmodell

Das CSIRT wird eingerichtet und fungiert als unabhängige Organisation mit eigener Geschäftsführung und eigenen Mitarbeitern.

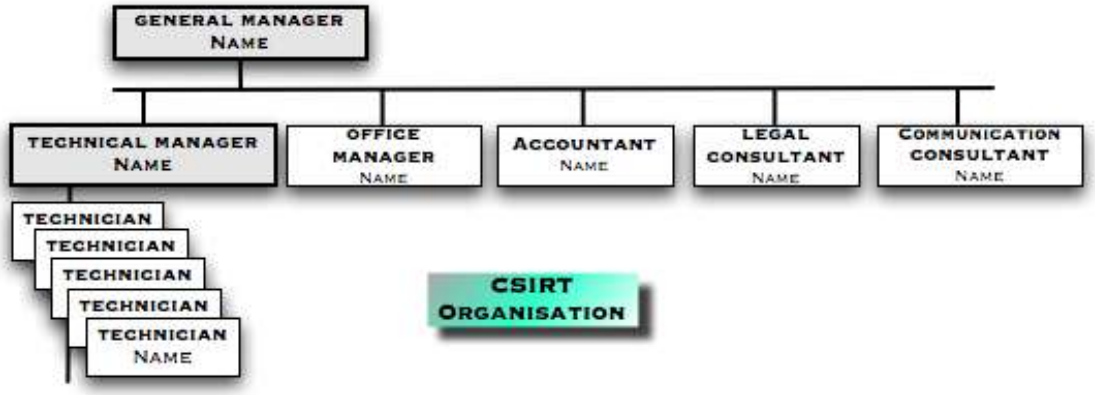


Abb. 5: Unabhängiges Geschäftsmodell

6..2 Das integrierte Geschäftsmodell

Dieses Modell kann angewandt werden, wenn ein CSIRT innerhalb einer bestehenden Organisation eingerichtet werden soll, beispielsweise durch die Nutzung einer bereits vorhandenen IT-Abteilung. Das CSIRT wird von einem Teamleiter geführt, der für die CSIRT-Aktivitäten verantwortlich ist. Bei der Behebung von Vorfällen oder CSIRT-Arbeit nimmt der Teamleiter die notwendigen technischen Fachkräfte in Anspruch. Er oder sie kann um Hilfe aus der bestehenden Organisation bitten, wenn spezielle fachliche Unterstützung erforderlich ist.

Dieses Modell lässt sich auch jeweils an spezielle Situationen anpassen. In diesem Fall wird dem Team eine bestimmte Anzahl von FTE (engl. Akronym für **F**ull **T**ime **E**quivalent; etwa Vollzeit-Arbeitskräfte) zugewiesen. Der Abuse-Desk (Helpdesk), beispielsweise bei einem ISP, ist zweifelsohne ein Vollzeitjob für ein oder (meist) mehrere FTE.

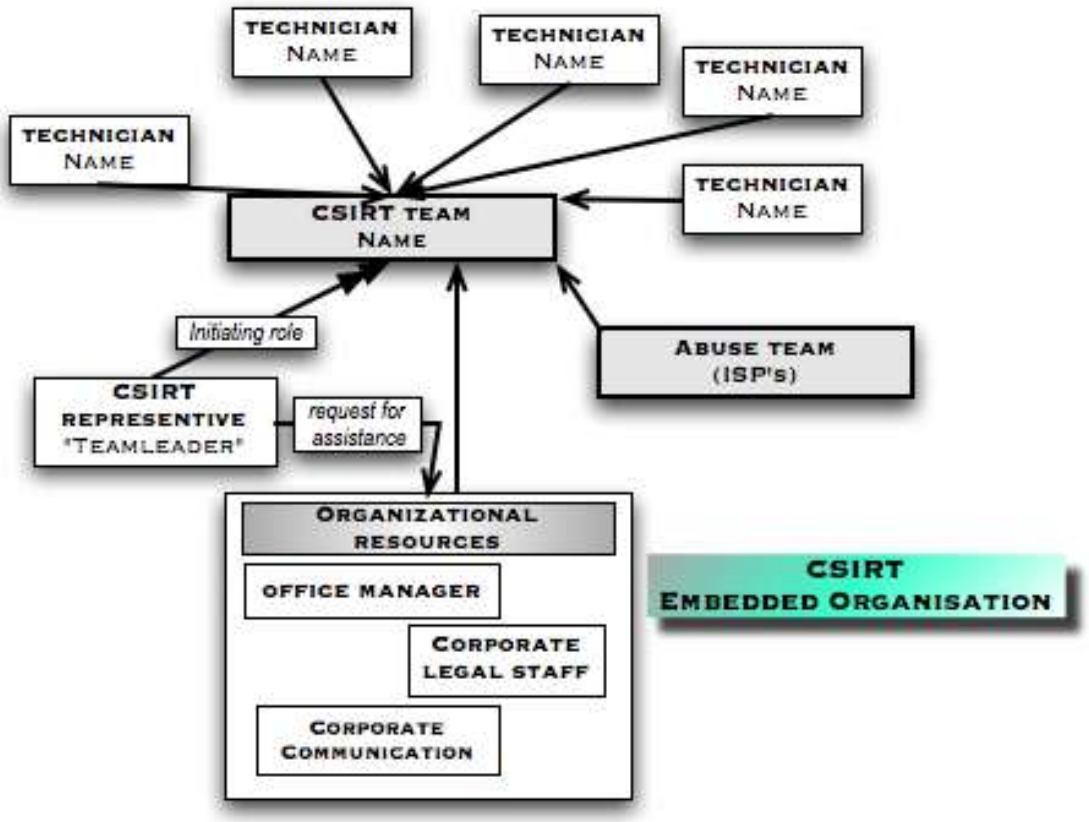


Abb. 6: Integriertes Organisationsmodell

6..3 Das Campus-Modell

Wie der Name bereits vermuten lässt, wird das Campus-Modell in erster Linie von CSIRT-Teams für den Hochschul- und Forschungsbereich angewandt. Die meisten Hochschul- und Forschungsorganisationen bestehen aus mehreren Universitäten und Campuseinrichtungen, die an verschiedenen Standorten innerhalb einer Region oder sogar eines ganzen Landes (wie bei den NREN (**N**ational **R**esearch and **E**ducation **N**etwork), den nationalen Forschungs- und Bildungsnetzen) verteilt sind. In der Regel sind diese Organisationen unabhängig voneinander und haben häufig ihr eigenes CSIRT. Diese CSIRT-Teams unterstehen normalerweise einem CSIRT-Dach- oder Hauptteam. Dieses CSIRT-Hauptteam fungiert als zentraler Koordinator und Ansprechpartner für die Außenwelt. In den meisten Fällen bietet das CSIRT-Hauptteam auch die CSIRT-Hauptdienste an und leitet vorfallspezifische Informationen an das entsprechende Campus-CSIRT weiter.

Einige CSIRT-Teams teilen sich ihre Hauptdienste mit den anderen CSIRT-Teams für den Campusbereich, wodurch die Gemeinkosten für das CSIRT-Hauptteam geringer sind.

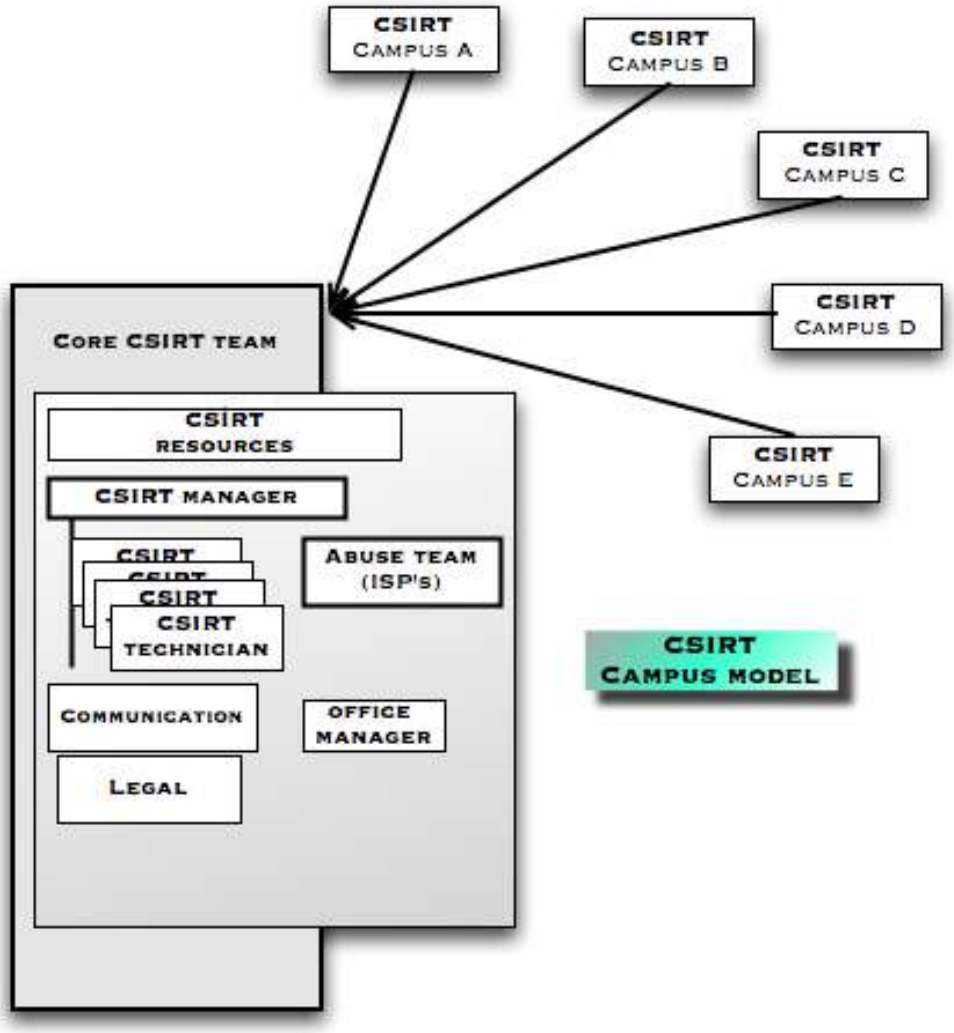


Abb. 7: Campus-Modell

6..4 Das freiwillige Modell

Dieses Organisationsmodell beschreibt eine Gruppe von Personen (Spezialisten), die sich auf freiwilliger Basis gegenseitig (und auch anderen) Ratschläge geben und unterstützen. Dabei handelt es sich um eine lose Gemeinschaft, die in starkem Maße auf die Motivation der Beteiligten angewiesen ist.

Dieses Modell wird beispielsweise von der WARP-Gemeinschaft (engl. Akronym für **W**arning, **A**dvice **R**eporting **P**oints)[13] angewandt.

[13] Die WARP-Initiative: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02_02.htm#12

Einstellung der richtigen Mitarbeiter

Nachdem beschlossen wurde, welche Dienste und Unterstützung angeboten werden sollen, und ein Organisationsmodell ausgewählt wurde, besteht der nächste Schritt darin, die richtige Anzahl von qualifizierten Fachkräften für die Arbeit zu finden.

Es ist fast unmöglich, verbindliche Angaben zu der jeweils erforderlichen Anzahl von Fachkräften zu machen. Doch in der Praxis haben sich die folgenden Schlüsselwerte als Richtschnur bewährt:

- Mindestens **4** FTE zur Erbringung von zwei Hauptdiensten, nämlich der Verteilung von Security Advisories und der Behandlung von Vorfällen

- Mindestens **6 bis 8** FTE für ein CSIRT, das sämtliche Dienste während der Geschäftszeiten anbietet und für die Systempflege verantwortlich ist

- Mindestens **12** FTE für ein CSIRT mit voller Personalstärke, das rund um die Uhr (24x7) im Schichtbetrieb arbeitet (2 Schichten außerhalb der Geschäftszeiten)

Diese Zahlenangaben enthalten auch Stellvertreter bei Krankheit, Urlaub usw. Dabei müssen auch die lokalen Tarifverträge geprüft werden. Bei Personen, die außerhalb der Geschäftszeiten arbeiten, können zusätzliche Kosten in Form von Zuschlägen anfallen.

Nachstehend finden Sie einen kurzen Überblick über die Kernkompetenzen für die technischen Fachkräfte in einem CSIRT.

Allgemeine Stellenbeschreibung für Fachkräfte:

Persönliche Kompetenzen
- Flexibilität, Kreativität und ausgeprägter Teamgeist
- Starke analytische Fähigkeiten
- Fähigkeit, schwierige technische Sachverhalte in einfachen Worten zu erklären
- Gutes Gespür für vertrauliche Angelegenheiten und strukturierte Arbeitsweise
- Gute organisatorische Fähigkeiten
- Hohe Belastbarkeit
- Ausgeprägte Kommunikationsfähigkeit (in Wort und Schrift)
- Aufgeschlossenheit und Lernbereitschaft

Fachliche Kompetenzen
- Umfassende Kenntnisse der Internettechnologie und -protokolle
- Kenntnisse der Betriebssysteme Linux und Unix (je nach den bei der Klientel vorhandenen Geräten)
- Kenntnisse der Windows-Betriebssysteme (je nach den bei der Klientel vorhandenen Geräten)
- Kenntnisse der Geräte in der Netzinfrastruktur (Router, Switches, DNS, Proxy, Mail usw.)
- Kenntnisse von Internetanwendungen (SMTP, HTTP(s), FTP, telnet, SSH usw.)
- Kenntnisse von Sicherheitsrisiken (DDoS, Phishing, Defacing, Sniffing usw.)
- Kenntnisse der Risikobewertung und praktischen Umsetzung

Zusätzliche Kompetenzen
- Bereitschaft zur Schichtarbeit rund um die Uhr (24x7) oder Rufbereitschaft (je nach Dienstmodell)
- Hohe Reisebereitschaft (bei Notdienst im Büro)
- Bildungsstand
- Arbeitserfahrung im Bereich IT-Sicherheit

Fiktives CSIRT (Schritt 4)

Festlegung des Geschäftsplans

Finanzierungsmodell

Aufgrund der Tatsache, dass es sich um ein eBusiness-Unternehmen handelt, das rund um die Uhr (24x7) arbeitet und eine IT-Abteilung (24x7) hat, wird beschlossen, sämtliche Dienste während der Geschäftszeiten und Rufbereitschaft außerhalb der Geschäftszeiten anzubieten. Die Dienste sollen für die Klientel unentgeltlich geleistet werden, wobei die Möglichkeit, Dienste für externe Kunden anzubieten, während der Pilot- und Evaluierungsphase geprüft werden soll.

Ertragsmodell

Während der Start- und Pilotphase soll das CSIRT vom Auftrag gebenden Unternehmen finanziert werden. In der Pilot- und Evaluierungsphase soll eine zusätzliche Finanzierung

erörtert werden, einschließlich der Möglichkeit, externen Kunden kostenpflichtige Dienste anzubieten.

Organisationsmodell
Da der Auftraggeber ein kleines Unternehmen ist, entscheidet man sich für das integrierte Modell.
Während der Geschäftszeiten sollen drei Mitarbeiter die Hauptdienste (Verteilung von Security Advisories sowie Behandlung/Koordination von Vorfällen) leisten.

Die IT-Abteilung des Unternehmens hat bereits adäquat qualifizierte Mitarbeiter. Mit dieser Abteilung wird vereinbart, dass das neue CSIRT bei Bedarf ad hoc Unterstützung anfordern kann. Auch die 2. Reihe von Technikern mit Rufbereitschaft kann in Anspruch genommen werden.
Das CSIRT-Hauptteam soll aus vier vollzeitbeschäftigten und fünf zusätzlichen CSIRT-Teammitgliedern bestehen, wovon ein Mitglied im wechselnden Schichtbetrieb zur Verfügung stehen soll.

Mitarbeiter
Der CSIRT-Teamleiter hat Erfahrung im Sicherheitsbereich und Support der 1. und 2. Ebene (1st und 2nd Level) und hat bereits im Krisenmanagement gearbeitet. Die anderen drei Teammitglieder sind Sicherheitsexperten. Die Teilzeitmitarbeiter im CSIRT-Team aus der IT-Abteilung sind Spezialisten für ihren jeweiligen Bereich der Unternehmens-infrastruktur.

Nutzung und Ausstattung des Büros

Die Nutzung und Ausstattung der Bürofläche und die physische Sicherheit sind sehr komplexe Themen und können daher in diesem Dokument nicht erschöpfend beschrieben werden. Dieses Kapitel soll einen kurzen Überblick über dieses Thema geben.

Weitere Informationen über physische Sicherheit finden Sie auf den folgenden Websites in englischer Sprache:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Schützen des Komplexes“
Da CSIRT-Teams normalerweise mit äußerst vertraulichen Informationen arbeiten, empfiehlt es sich, dass das Team für die physische Sicherheit des Büros verantwortlich ist. Diese Aufgabe hängt stark von der vorhandenen Ausstattung und Infrastruktur sowie von den geltenden Informationssicherheitsrichtlinien der Auftrag gebenden Organisation ab.

Regierungen arbeiten beispielsweise mit Geheimhaltungssystemen und haben sehr strenge Richtlinien für den Umgang mit vertraulichen Informationen. Prüfen Sie die lokalen Regeln und Richtlinien Ihres eigenen Unternehmens oder Ihrer Einrichtung.

Normalerweise ist ein neues CSIRT auf die Zusammenarbeit mit der Auftrag gebenden Organisation angewiesen, um Näheres über die lokalen Regeln und Richtlinien und sonstige Rechtsfragen zu erfahren.

Eine umfassende Beschreibung aller jeweils erforderlichen Geräte und Sicherheitsmaßnahmen würde den Rahmen dieses Dokuments sprengen. Nachstehend finden Sie jedoch eine kurze Liste der Grundausstattung für Ihr CSIRT:

Allgemeine Regeln für das Gebäude
- Nutzen Sie Zugangskontrollen.
- Achten Sie darauf, dass das CSIRT-Büro nur für CSIRT-Mitarbeiter zugänglich ist.
- Überwachen Sie die Büros und Eingänge mit Kameras.
- Archivieren Sie vertrauliche Informationen in Schließfächern oder einem Safe.
- Verwenden Sie sichere IT-Systeme.

Allgemeine Regeln für IT-Geräte
- Verwenden Sie Geräte, die von den Mitarbeitern unterstützt werden können.
- Schützen Sie sämtliche Systeme.
- Aktualisieren Sie alle Systeme (inkl. Patch), bevor Sie diese an das Internet anschließen.
- Verwenden Sie Sicherheitssoftware (Firewalls, mehrere Virenschutzprogramme, Spyware-Schutzprogramme usw.).

Verwaltung und Pflege der Kommunikationskanäle
- Öffentlich zugängliche Website
- Geschlossener Mitgliederbereich auf der Website
- Webformulare zur Meldung von Vorfällen
- E-Mail (mit Unterstützung für PGP / GPG / S/MIME)
- Software für Mailinglisten
- Separate Telefonnummer für die Klientel:
    - Telefon
    - Fax
    - SMS

Datenerfassungssystem(e)
- Kontaktdatenbank mit den persönlichen Daten von Teammitgliedern, anderen Teams usw.
- CRM-Tools (**C**ustomer **R**elationship **M**anagement)
- Ticketsystem für die Vorfallbehandlung

Einhaltung des „Unternehmensstils“ von Anfang an für:
- Layout von E-Mail-Standardnachrichten und Advisories/Bulletins
- „Altmodische“ Korrespondenz (Schreiben)
- Monats- oder Jahresberichte
- Formular für die Meldung von Vorfällen

Sonstiges

- Sehen Sie bandexterne (Out-of-Band) Kommunikation bei Angriffen vor.
- Sehen Sie Redundanz für Internetverbindungen vor.

Weitere Informationen über bestimmte CSIRT-Werkzeuge finden Sie in Kapitel *8.5 Verfügbare CSIRT-Werkzeuge.*

Festlegung der Richtlinien für die Informationssicherheit

Abhängig vom jeweiligen CSIRT-Typ gelten kunden- bzw. benutzerspezifische Richtlinien für die Informationssicherheit. Abgesehen von der Beschreibung des gewünschten Zustands aller betrieblichen und administrativen Abläufe und Verfahren müssen diese Richtlinien den geltenden Gesetzen und Standards entsprechen, insbesondere im Hinblick auf die Haftung des CSIRT. In der Regel ist das CSIRT zur Einhaltung nationaler Gesetze und Vorschriften verpflichtet, die häufig im Rahmen der europäischen Gesetzgebung (normalerweise Richtlinien) und anderer internationaler Vereinbarungen implementiert werden. Standards sind nicht unbedingt rechtsverbindlich, können jedoch durch Gesetze und Vorschriften angeordnet oder empfohlen werden.

Nachstehend finden Sie eine kurze Liste möglicher Gesetze und Richtlinien:

Auf nationaler Ebene
- Verschiedene Gesetze über Informationstechnologie, Telekommunikation, Medien
- Datenschutzgesetze
- Gesetze und Vorschriften über die Aufbewahrung von Daten
- Gesetzgebung zu Finanzwesen, Rechnungslegung und Unternehmensführung
- Verhaltenskodizes für „Corporate Governance“ (Grundsätze der Unternehmensführung) und „IT Governance“

Auf europäischer Ebene
- Richtlinie über elektronische Signaturen (1999/93/EG)
- Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1995/46/EG) und Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)
- Richtlinien über den Zugang zu elektronischen Kommunikationsnetzen und -diensten (2002/19/EG – 2002/22/EG)
- Richtlinien zum Gesellschaftsrecht (z. B. 8. Richtlinie zum Gesellschaftsrecht)

Auf internationaler Ebene
- Basel II-Abkommen (insbesondere im Hinblick auf das Betriebsrisikomanagement)
- Übereinkommen des Europarats über Cyberkriminalität
- Übereinkommen des Europarats über Menschenrechte (Artikel 8 zum Datenschutz)
- IAS (**I**nternational **A**ccounting **S**tandards, internationale Grundsätze der Rechnungslegung, in denen gewisse IT-Kontrollen angeordnet werden)

Standards
- Britischer Standard BS 7799 (Informationssicherheit)
- Internationale Standards ISO2700x (Managementsysteme für die Informationssicherheit)
- Deutsches IT-Grundschutzbuch, französische EBIOS-Methode und andere davon abgeleitete nationale Versionen

Zur Ermittlung, ob Ihr CSIRT nationale und internationale Gesetze und Vorschriften einhält, wenden Sie sich bitte an Ihren Rechtsberater.

Zu den grundlegenden Fragen, die im Zusammenhang mit Ihren Richtlinien für den Umgang mit Informationen zu beantworten sind, zählen:

- Wie werden eingehende Informationen „gekennzeichnet“ (Tags) oder „klassifiziert“?
- Wie werden Informationen behandelt, insbesondere in Bezug auf Vertraulichkeit?
- Welche Aspekte werden für die Offenlegung von Informationen berücksichtigt, insbesondere wenn vorfallbezogene Informationen an andere Teams oder Standorte weitergeleitet werden?
- Sind rechtliche Aspekte in Bezug auf den Umgang mit Informationen zu berücksichtigen?
- Haben Sie Richtlinien über die Verwendung kryptografischer Methoden zum Schutz von Exklusivität und Integrität in Archiven und/oder bei der Datenkommunikation, insbesondere E-Mail?
- Sehen diese Richtlinien rechtliche Randbedingungen vor, wie Schlüsselhinterlegung oder Durchsetzbarkeit der Entschlüsselung bei Rechtsstreiten?

Fiktives CSIRT (Schritt 6)

Büroausstattung und -standort

Da in dem Auftrag gebenden Unternehmen bereits eine effiziente physische Sicherheit vorhanden ist, ist das CSIRT in dieser Hinsicht gut abgedeckt. Für die Kommunikation in Notfällen wird ein so genannter „War Room” (Einsatzbesprechungsraum) vorgesehen. Für die Verschlüsselungsunterlagen und vertraulichen Dokumente wird ein Safe angeschafft. Es wird eine separate Telefonleitung, einschließlich Zentrale, für die Hotline während der Geschäftszeiten und die Rufbereitschaft (über Mobiltelefon) außerhalb der Geschäftszeiten mit der gleichen Telefonnummer, eingerichtet.

Die vorhandenen Geräte und die unternehmenseigene Website können ebenfalls zur Bekanntgabe von CSIRT-bezogenen Informationen verwendet werden. Eine Mailingliste ist installiert und wird gepflegt, wobei ein beschränkter Teil für die Kommunikation unter den Teammitgliedern und mit anderen Teams vorgesehen ist. Alle persönlichen Daten der Mitarbeiter sind in einer Datenbank gespeichert; im Safe wird ein Ausdruck aufbewahrt.

Richtlinien

Da das CSIRT in ein Unternehmen mit vorhandenen Richtlinien für die Informationssicherheit integriert ist, sind die entsprechenden Richtlinien für das CSIRT mit Unterstützung des unternehmenseigenen Rechtsberaters festgelegt worden.

Suche nach Kooperationsmöglichkeiten zwischen anderen CSIRT-Teams und möglichen nationalen Initiativen

Andere vorhandene CSIRT-Initiativen und der starke Kooperationsbedarf untereinander sind bereits mehrfach in diesem Dokument angesprochen worden. Es hat sich in der Praxis bewährt, dass sich ein CSIRT möglichst frühzeitig mit anderen CSIRT-Teams in Verbindung setzt, um die notwendigen Kontakte zu den CSIRT-Gemeinschaften

herzustellen. In der Regel sind andere CSIRT-Teams gerne bereit, neu eingerichteten Teams in der Anfangsphase zu helfen.

Das *Verzeichnis der ENISA für CERT-Aktivitäten in Europa*[14] bietet eine sehr gute Grundlage für die Suche nach anderen CSIRT-Teams im jeweiligen Land oder nach Kooperationsmöglichkeiten mit CSIRT-Teams auf nationaler Ebene.

Für weitere Fragen und Hilfe bei der Suche nach geeigneten CSIRT-Informationsquellen wenden Sie sich bitte an die CSIRT-Experten der ENISA:

CERT-Relations@enisa.europa.eu

[14] Verzeichnis der ENISA: http://www.enisa.europa.eu/CERT_INVENTORY

Nachstehend finden Sie einen Überblick über CSIRT-Gemeinschaftsaktivitäten. Eine umfassendere Beschreibung und weitere Informationen entnehmen Sie bitte dem *Verzeichnis*.

Europäsche CSIRT-Initiative

TF-CSIRT[15]
Die Task Force (Arbeitsgruppe) TF-CSIRT fördert die Zusammenarbeit zwischen den CSIRT-Teams (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eams; Reaktionsteams für Computersicherheitsverletzungen) in Europa. Die Hauptziele dieser Arbeitsgruppe bestehen darin, eine Plattform für den Erfahrungs- und Wissensaustausch zu bieten, Pilotdienste für die europäische CSIRT-Gemeinschaft einzurichten und bei der Einrichtung neuer CSIRT-Teams zu helfen.

Hauptziele der Arbeitsgruppe:
- Plattform für den Erfahrungs- und Wissensaustausch
- Einrichtung von Pilotdiensten für die europäische CSIRT-Gemeinschaft
- Förderung gemeinsamer Standards und Verfahren für die Reaktion auf Sicherheitsvorfälle
- Unterstützung bei der Einrichtung neuer CSIRT-Teams und Schulung der Mitarbeiter von CSIRT-Teams
- Gemäß den von der TERENA (**T**rans-**E**uropean **R**esearch and **E**ducation **N**etworking **A**ssociation) am 15. September 2004 genehmigten „Terms of Reference“ (Richtlinien) liegt der Schwerpunkt der Aktivitäten des TF-CSIRT in Europa und Nachbarländern.

Globale CSIRT-Initiative

FIRST[16]
FIRST (**F**orum of **I**ncident **R**esponse and **S**ecurity **T**eams) ist die weltweit anerkannte, führende Organisation bei der Reaktion auf Sicherheitsvorfälle. Durch ihre Mitgliedschaft bei FIRST können Notfall-Reaktionsteams effizienter auf Sicherheitsvorfälle reagieren, und zwar reaktiv und proaktiv.

FIRST ist der Zusammenschluss zahlreicher Reaktionsteams für Computersicherheitsverletzungen aus staatlichen, kommerziellen und Bildungsorganisationen. FIRST hat es sich zum Ziel gesetzt, die Kooperation und Koordination bei der Prävention von Sicherheitsvorfällen zu unterstützen und eine rasche Reaktion auf Vorfälle sowie den Informationsaustausch unter den Mitgliedern und in der Gemeinschaft insgesamt zu fördern.

Abgesehen von dem Vertrauensnetz, das FIRST innerhalb der internationalen Gemeinschaft zur Reaktion auf Sicherheitsvorfälle bildet, bietet FIRST auch Dienste mit Wertschöpfungspotenzial.

[15] TF-CSIRT: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/CERT_INVENTORY/pages/05_02.htm

Fiktives CSIRT (Schritt 6)

Suche nach Kooperationsmöglichkeiten

Auf Basis des Verzeichnisses der ENISA wurden rasch einige CSIRT-Teams im gleichen Land ausfindig gemacht und kontaktiert. Für den neu eingestellten Teamleiter wurde ein Besuch bei einem dieser CSIRT-Teams arrangiert. Im Rahmen dieses Besuchs erfuhr er Näheres über nationale CSIRT-Aktivitäten und nahm an einer Sitzung teil.

Diese Sitzung erwies sich als äußerst nützlich, weil er Beispiele für Arbeitsmethoden sammeln konnte und weil ihm die Unterstützung einiger anderer Teams zugesichert wurde.

7 Förderung des Geschäftsplans

Bislang wurden die folgenden Schritte unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann.
4. Analyse der Umgebung und der Klientel
5. Festlegung des Aufgabenbereichs
6. Ausarbeitung des Geschäftsplans
    a. Festlegung des Finanzierungsmodells
    b. Festlegung der Organisationsstruktur
    c. Einstellung von Mitarbeitern
    d. Nutzung und Ausstattung des Büros
    e. Festlegung der Richtlinien für die Informationssicherheit
    f. Suche nach Kooperationspartnern

>> Der nächste Schritt besteht darin, die o. g. Komponenten in einen Projektplan aufzunehmen und zu implementieren!

Ein Geschäftsfall bietet einen guten Einstieg zur Definition Ihres Projekts. Dieser Geschäftsfall dient auch als Grundlage für den Projektplan und zur Beantragung von Unterstützung seitens der Unternehmensführung und von Finanzmitteln oder sonstigen Ressourcen.

Es hat sich als nützlich erwiesen, die Unternehmensführung immer auf dem Laufenden zu halten, um das Bewusstsein für IT-Sicherheitsprobleme und dadurch auch für die kontinuierliche Unterstützung des eigenen CSIRT zu sensibilisieren.

Ein Geschäftsfall beginnt mit der Analyse der Probleme und Chancen anhand eines Analysemodells, das in Kapitel *5.3 Analyse der Klientel* beschrieben ist, und der Suche nach engen Kontakten zu der potenziellen Klientel.

Wie bereits oben erwähnt, sind bei der Einrichtung eines CSIRT viele Aspekte zu bedenken. Es empfiehlt sich, die o. g. Aspekte und Komponenten an die jeweiligen Anforderungen des CSIRT anzupassen.

Bei der Unterrichtung der Unternehmensführung empfiehlt es sich, den eigenen Fall durch die Verwendung aktueller Artikel aus Tageszeitungen oder dem Internet so aktuell wie möglich zu gestalten und zu erklären, warum die Dienste des CSIRT und die interne Koordination von Vorfällen zum Schutz der Vermögensgegenstände des Unternehmens von ausschlaggebender Bedeutung sind. Es muss auch klar darauf hingewiesen werden, dass nur die kontinuierliche Unterstützung bei IT-Sicherheitsfragen zu einem soliden Unternehmen beiträgt, insbesondere bei einem Unternehmen oder einer Einrichtung, das bzw. die auf den IT-Bereich angewiesen ist.

(Ein berühmter Satz von Bruce Schneier bringt diese Aussage auf den Punkt: *„Sicherheit ist ein Prozess und kein Produkt[17]!“)*

Ein anerkanntes Werkzeug zur Erläuterung von Sicherheitsproblemen ist die folgende Grafik vom CERT/CC:

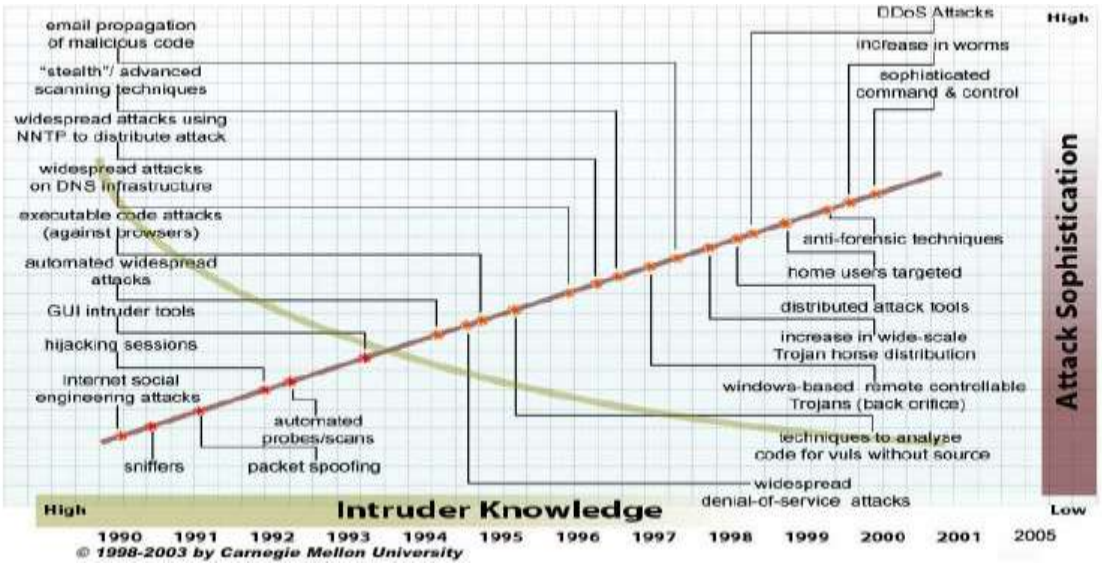


Abb. 8: Wissen von Eindringlingen bzw. Angreifern im Vergleich zur Raffinesse des Angriffs (Quelle: CERT-CC[18])

Diese Grafik stellt die Trends im Bereich der IT-Sicherheit dar, insbesondere die Tatsache, dass immer weniger Fähigkeiten zur Durchführung von zunehmend raffinierten Angriffen erforderlich sind.

Erwähnenswert ist auch der immer kürzere Zeitraum zwischen der Verfügbarkeit von Softwareaktualisierungen zum Schließen von Sicherheitslücken und Angriffsversuchen gegen sie:

[17] Bruce Schneier: http://www.schneier.com/ und http://www.schneier.com/news-014-de.pdf

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

Patch -> Exploit		**Verbreitungsgeschwindigkeit**	
Nimda:	11 Monate	Code red:	Tage
Slammer:	6 Monate	Nimda:	Stunden
Nachi:	5 Monate	Slammer:	Minuten
Blaster:	3 Wochen		
Witty:	1 Tag (!)		

Die Sammlung von Vorfalldaten, mögliche Verbesserungen und Erfahrungen dienen auch zur Darstellung dieses Sachverhalts.

Beschreibung von Geschäftsplänen und Anstößen für die Geschäftsführung

Eine Präsentation für die Geschäftsführung, einschließlich der Werbung für das CSIRT, macht allein noch keinen Geschäftsfall aus. Bei richtiger Ausführung führt sie meist jedoch dazu, dass das CSIRT von der Geschäftsführung unterstützt wird. Andererseits sollte der Geschäftsfall auch nicht nur als reine Managementübung angesehen werden, sondern auch als Grundlage für die Kommunikation mit dem Team und der Klientel dienen. Der Begriff „Geschäftsfall" mag zwar sehr kommerziell und weit entfernt von der täglichen CSIRT-Praxis klingen, er bietet jedoch einen guten Anhaltspunkt bei der Einrichtung eines CSIRT.

Die Antworten auf die folgenden Fragen können als Grundlage für die Ausarbeitung eines guten Geschäftsfalls dienen. (Die genannten Beispiele sind rein hypothetisch und dienen nur zur Erläuterung. Die „tatsächlichen" Antworten hängen stark von den „tatsächlichen" Umständen ab.)

- Worin besteht das Problem?
- Welche Ziele sollen mit der Klientel erreicht werden?
- Was geschieht, wenn Sie nichts unternehmen?
- Was geschieht, wenn Sie etwas unternehmen?
- Wie hoch sind die Kosten?
- Wie hoch ist der Gewinn?
- Wann ist der Startzeitpunkt, und wann ist der Endzeitpunkt?

Worin besteht das Problem?
In den meisten Fällen entsteht die Idee zur Einrichtung eines CSIRT, wenn die IT-Sicherheit ein wesentlicher Bestandteil des Kerngeschäfts eines Unternehmens oder einer Einrichtung geworden ist oder wenn IT-Sicherheitsvorfälle zu einem Geschäftsrisiko werden, wodurch geeignete Sicherheitsmaßnahmen zu einem normalen Geschäftsvorgang werden.

Die meisten Unternehmen oder Einrichtungen haben eine eigenständige Supportabteilung oder einen Helpdesk, doch meistens werden Sicherheitsvorfälle nicht ausreichend und nicht so strukturiert behandelt, wie es eigentlich der Fall sein sollte. In den meisten Fällen erfordert der Umgang mit Sicherheitsvorfällen eine besondere Qualifikation und Aufmerksamkeit. Ein strukturierterer Ansatz ist förderlich und dient zur Verringerung der Geschäftsrisiken und Schäden für das Unternehmen.

Vielfach besteht das Problem in der mangelnden Koordination und in der Tatsache, dass vorhandenes Wissen nicht zur Behandlung von Vorfällen genutzt wird, wodurch weitere Vorfälle ähnlicher Art und mögliche finanzielle Verluste und/oder eine mögliche Rufschädigung für eine Einrichtung vermieden werden könnten.

Welche Ziele sollen mit der Klientel erreicht werden?
Wie bereits oben erwähnt, soll Ihr CSIRT Dienste für die Klientel leisten und diese bei der Behebung von IT-Sicherheitsvorfällen und Lösung von Problemen unterstützen.

Weitere Ziele sind die Verbesserung des Sicherheitswissens im IT-Bereich und die Realisierung einer sicherheitsbewussten Unternehmenskultur.

Eine derartige Kultur fördert von Beginn an proaktive und präventive Maßnahmen, wodurch die Betriebskosten gesenkt werden.

Die Einführung einer durch Kooperations- und Hilfsbereitschaft geprägten Unternehmenskultur ist meist auch förderlich für die Effizienz im Allgemeinen.

Was geschieht, wenn nichts unternommen wird?
Eine nicht strukturierte Behandlung von IT-Sicherheitsproblemen kann zu weiteren Schäden führen, zumindest zu einer Rufschädigung für das Unternehmen oder die Einrichtung. Finanzielle Verluste und rechtliche Auswirkungen könnten andere Folgen sein.

Was geschieht, wenn etwas unternommen wird?
Das Bewusstsein für Sicherheitsprobleme wird sensibilisiert. Dadurch können sie effizienter gelöst und weitere Verluste vermieden werden.

Wie hoch sind die Kosten?
Je nach Organisationsmodell fallen Personalkosten für die CSIRT-Teammitglieder und -organisation sowie Kosten für Geräte, Werkzeuge und Softwarelizenzen an.

Wie hoch ist der Gewinn?
Abhängig vom jeweiligen Geschäftszweig und den in der Vergangenheit erlittenen Verlusten lassen sich Verfahren und Sicherheitspraktiken transparenter gestalten, wodurch wichtige Vermögensgegenstände des Unternehmens geschützt werden.

Wie sieht der Zeitrahmen aus?
In Kapitel *12. Beschreibung des Projektplans* finden Sie die Beschreibung eines Musterprojektplans.

Beispiele für vorhandene Geschäftsfälle und Ansätze
Nachstehend finden Sie einige Beispiele für CSIRT-Geschäftsfälle, die Sie sich genauer ansehen sollten:

- http://www.cert.org/csirts/AFI_case-study.html
  „Creating a Financial Institution CSIRT: A Case Study“ (Einrichtung eines CSIRT für ein Finanzinstitut: Fallstudie)

  Durch dieses Dokument sollen die Erfahrungen eines Finanzinstituts (das in diesem Dokument als AFI bezeichnet wird) bei der Ausarbeitung und Implementierung eines Plans zur Lösung von Sicherheitsproblemen und zur Einrichtung eines Reaktionsteams für Computersicherheitsverletzungen (CSIRT) ausgetauscht werden. (Übersetzung aus dem Englischen)

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Zusammenfassung des Geschäftsfalls von CERT POLSKA (Folienpräsentation im PDF-Format).

- http://www.auscert.org.au/render.html?it=2252
  Die Einrichtung eines IRT (**I**ncident **R**esponse **T**eam) in den 90er Jahren kann eine gewaltige, schier unlösbare Aufgabe sein. Viele, die ein IRT bilden, haben damit überhaupt keine Erfahrung. In diesem Dokument werden die Rolle, die ein IRT in der Gemeinschaft spielen kann, sowie die Aspekte erläutert, die sowohl bei der Einrichtung als auch nach der Aufnahme der Tätigkeit berücksichtigt werden sollten. Es dient auch zum Nutzen von bestehenden IRT-Teams, da ihr Bewusstsein für bislang nicht berücksichtigte Aspekte sensibilisiert wird. (Übersetzung aus dem Englischen)

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  „Case Study in Information Security: Securing the Enterprise“ (Fallstudie im Bereich Informationssicherheit: Unternehmensweite Sicherheit); Verfasser: Roger Benton

  Dieses Praxisbeispiel ist eine Fallstudie über die Migration einer Versicherungsgesellschaft auf ein unternehmensweites Sicherheitssystem. Es soll einen Pfad aufzeigen, der bei der Einrichtung eines oder Migration auf ein Sicherheitssystem verfolgt werden sollte. Zunächst war ein ganz einfaches Online-Sicherheitssystem der einzige Mechanismus zur Überwachung des Zugriffs auf die unternehmenseigenen Daten. Die Sicherheitsrisiken waren gravierend; es gab keine Integritätskontrollen außerhalb der Online-Umgebung. Jeder mit Programmierungsgundkenntnissen wäre in der Lage gewesen, Produktionsdaten hinzuzufügen, zu ändern und/oder zu löschen. (Übersetzung aus dem Englischen)

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  „Marriott's e-security strategy: business-IT collaboration“ (Elektronische Sicherheitsstrategie von Marriott: Zusammenarbeit zwischen Unternehmen und IT-Bereich)

  Nach den Erfahrungen, die Chris Zoladz von Marriott International, Inc. gemacht hat, ist die Sicherheit beim elektronischen Geschäftsverkehr (E-Business) kein Projekt, sondern ein Prozess. Diese Aussage machte Zoladz kürzlich bei der Konferenz „E-Security Conference and Expo“ in Boston, die von der Intermedia Group gesponsert wurde. Als Vizepräsident für den Bereich Informations- und Datenschutz bei Marriott ist Zoladz der Rechtsabteilung unterstellt, obwohl er kein Jurist ist. Seine Aufgabe besteht darin zu erkennen, wo die wichtigsten Geschäftsdaten von Marriott gespeichert sind und wie der Datenfluss innerhalb und außerhalb des Unternehmens abläuft. Marriott hat einen eigenen Aufgabenbereich für die technische Infrastruktur zur Unterstützung der Sicherheit, der dem IT-Sicherheitsarchitekten untersteht.

Fiktives CSIRT (Schritt 7)
Förderung des Geschäftsplans

Es wird beschlossen, Zahlen und Fakten aus der Vergangenheit des Unternehmens zu sammeln, was wirklich sehr nützlich ist, um sich einen statistischen Überblick über die Sicherheitssituation im IT-Bereich zu verschaffen. Diese Datenerfassung soll nach Einrichtung des CSIRT fortgesetzt werden, damit die statistischen Daten immer auf dem neuesten Stand sind.

Andere nationale CSIRT-Teams wurden kontaktiert und zu ihren Geschäftsfällen befragt. Durch die Zusammenstellung von Folien mit Informationen über die jüngsten Entwicklungen bei IT-Sicherheitsvorfällen und über die Kosten dieser Vorfälle leisteten diese CSIRT-Teams Unterstützung.

Bei diesem Beispielfall mit dem fiktiven CSIRT musste die Unternehmensführung nicht von der Bedeutung des IT-Bereichs überzeugt werden. Daher war es nicht schwierig, die Genehmigung für den ersten Schritt zu erhalten. Es wurden ein Geschäftsfall und ein Projektplan ausgearbeitet, einschließlich der geschätzten Einrichtungs- und Betriebskosten.

8 Beispiele für betriebsspezifische und technische Verfahren (Arbeitsabläufe)

Bislang wurden die folgenden Schritte unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann.
4. Analyse der Umgebung und der Klientel
5. Festlegung des Aufgabenbereichs
6. Ausarbeitung des Geschäftsplans
   a. Festlegung des Finanzierungsmodells
   b. Festlegung der Organisationsstruktur
   c. Einstellung von Mitarbeitern
   d. Nutzung und Ausstattung des Büros
   e. Festlegung der Richtlinien für die Informationssicherheit
   f. Suche nach Kooperationspartnern
7. Förderung des Geschäftsplans
   a. Einholung der Genehmigung des Geschäftsfalls
   b. Aufnahme aller Komponenten in einen Projektplan

>> Im nächsten Schritt soll das CSIRT seine Arbeit aufnehmen.

Gut definierte Arbeitsabläufe tragen dazu bei, die Qualität zu erhöhen und den Zeitaufwand für jeden Vorfall oder jede Sicherheitslücke zu verringern.

Wie oben beschrieben, soll das fiktive CSIRT die folgenden grundlegenden Hauptdienste anbieten:

- Alarm- und Warnmeldungen
- Behandlung von Vorfällen
- Bekanntgaben

Dieses Kapitel gibt Beispiele für Arbeitsabläufe, die die Hauptdienste eines CSIRT beschreiben. Ferner enthält dieses Kapitel Informationen über das Sammeln von Informationen aus verschiedenen Quellen, wobei diese auf ihre Relevanz und Authentizität hin geprüft und dann wieder an die Klientel verteilt werden. Abschließend enthält dieses Kapitel Beispiele für ganz grundlegende Verfahren und CSIRT-spezifische Werkzeuge.

Analyse der bei der Klientel installierten IT-Systeme

Der erste Schritt besteht darin, sich einen Überblick über die bei der Klientel installierten IT-Systeme zu verschaffen. Dadurch kann das CSIRT die Relevanz der eingehenden Informationen evaluieren und diese vor der Weiterleitung filtern, damit die Klientel nicht mit nutzlosen Informationen überhäuft wird.

Dabei hat sich eine einfache Vorgehensweise in der Praxis bewährt, beispielsweise die Verwendung einer Excel-Tabelle, die wie folgt aussehen könnte:

Kategorie	Anwendung	Software-produkt	Version	Betriebs-system	Version	Klient
Desktop	Office	Excel	x-x-x	Microsoft	XP Prof.	A
Desktop	Browser	IE	x-x-	Microsoft	XP Prof.	A
Netzwerk	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Dienste	Webserver	Apache		Unix	x-x-x	B

Mit der in Excel integrierten Filterfunktion lässt sich leicht die richtige Software auswählen und erkennen, welche Software von den einzelnen Mitgliedern der Klientel verwendet wird.

Erstellung von Alarm- und Warnmeldungen und Bekanntgaben

Die Erstellung von Alarm- und Warnmeldungen und Bekanntgaben basiert auf den folgenden Arbeitsabläufen:

- Sammlung von Informationen
- Evaluierung der Informationen in Bezug auf ihre Relevanz und Quelle
- Risikobewertung anhand der gesammelten Informationen
- Verteilung der Informationen

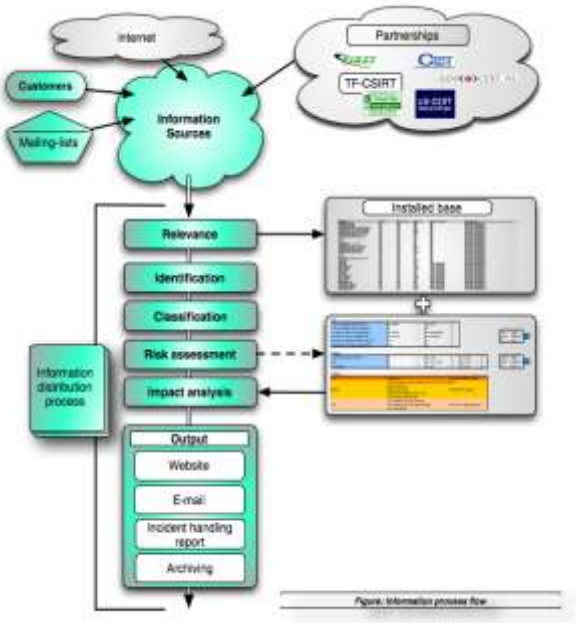


Abb. 9: Ablauf bei der Informationsverarbeitung

In den folgenden Absätzen wird dieser Arbeitsablauf im Einzelnen beschrieben.

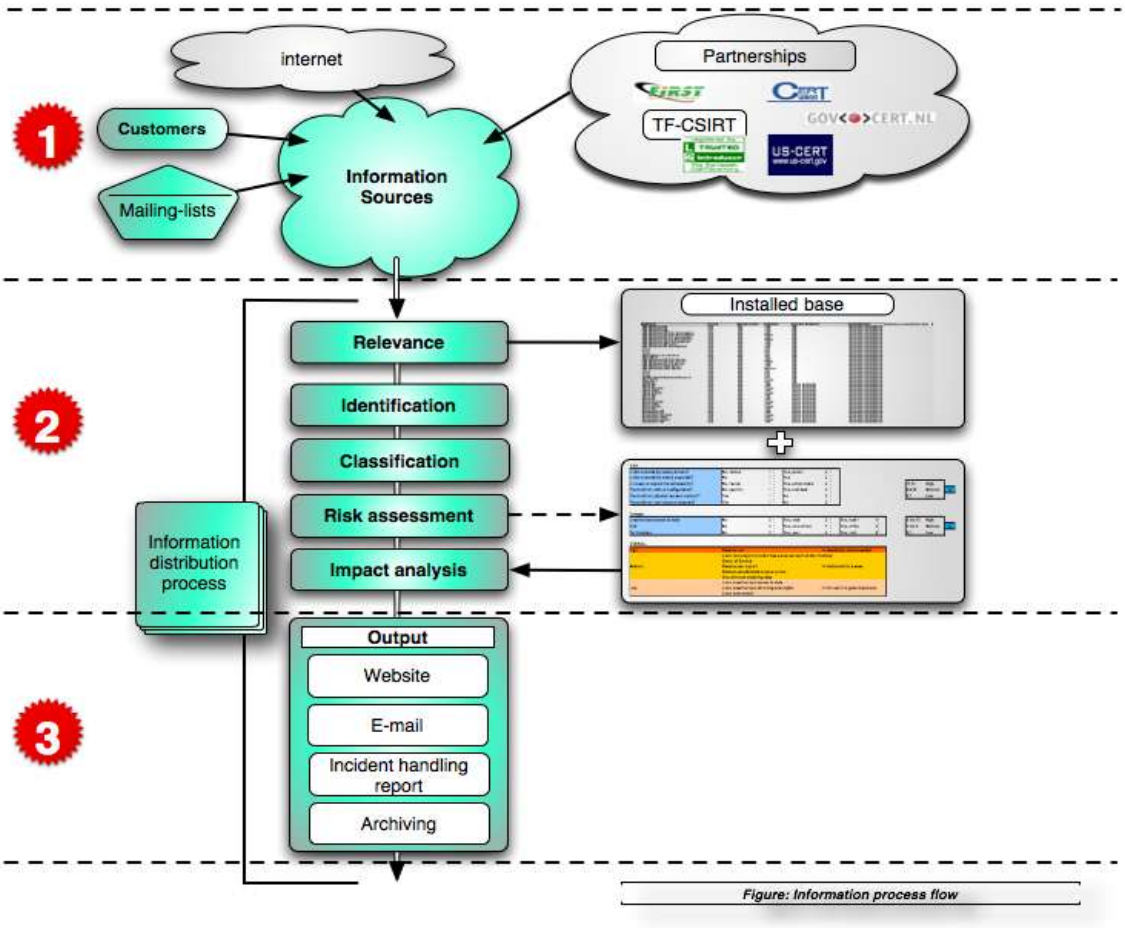


Figure: Information process flow

Schritt 1: Sammlung von sicherheitskritischen Informationen

Normalerweise gibt es zwei Hauptinformationsquellen, die für CSIRT-Dienste interessant sind:

- Informationen über Sicherheitslücken in (Ihren) IT-Systemen
- Berichte über Sicherheitsvorfälle

Es gibt viele öffentlich und beschränkt zugängliche Quellen für Informationen über Sicherheitslücken, was vom jeweiligen Geschäftszweig und von der IT-Infrastruktur abhängt:

- Öffentliche und geschlossene Mailinglisten
- Anbieterseitige Produktinformationen über Sicherheitslücken
- Websites
- Informationen im Internet (Google usw.)
- Öffentliche und private Vereinigungen, die Informationen über Sicherheitslücken bieten (FIRST, TF-CSIRT, CERT-CC, US-CERT usw.)

All diese Informationen tragen zum Wissensstand über bestimmte Sicherheitslücken in IT-Systemen bei.

Wie bereits erwähnt, bietet das Internet eine Fülle von guten und leicht zugänglichen Informationsquellen zu sicherheitsrelevanten Fragen. Zeitgleich zur Abfassung des vorliegenden Dokuments arbeitet die Ad-hoc-Arbeitsgruppe „CERT Services“ (CERT-Dienste) der ENISA an der Ausarbeitung einer umfassenderen Liste, die Ende 2006 vorliegen soll[19].

Schritt 2: Evaluierung der Informationen und Risikobewertung

Im Ergebnis führt dieser Schritt zu einer Analyse, wie sich eine bestimmte Sicherheitslücke in der IT-Infrastruktur auf die Klientel auswirkt.

Identifizierung
Eingehende Informationen über Sicherheitslücken müssen anhand ihrer Quelle identifiziert werden. Vor der Weiterleitung von Informationen an die Klientel muss ermittelt werden, ob die Quelle vertrauenswürdig ist. Andernfalls werden Benutzer u. U. irrtümlicherweise gewarnt, was zu unnötigen Störungen der Geschäftsabläufe führen und letztendlich dem Ruf von CSIRT-Teams schaden könnte.

[19] Ad-hoc-Arbeitsgruppe CERT Services: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Das folgende Verfahren zeigt ein Beispiel für die Erkennung der Authentizität einer Nachricht:

Verfahren zur Erkennung der Authentizität einer Nachricht und ihrer Quelle

Allgemeine Prüfliste

1. Ist die Quelle bekannt und als solche registriert?
2. Ist die Information über einen normalen Kanal eingegangen?
3. Enthält die Nachricht „seltsame“, „vom Gefühl her“ falsche Informationen?
4. Folgen Sie Ihrem Gefühl, wenn Sie eine Information in Zweifel ziehen. Sie sollten nicht handeln, sondern eine erneute Prüfung vornehmen!

E-Mail-Quellen

1. Ist die Quelladresse der Organisation und der Quellliste bekannt?
2. Ist the PGP-Signatur richtig?
3. Im Zweifelsfall sollten Sie den vollständigen Nachrichtenkopf (Header) prüfen.
4. Im Zweifelsfall sollten Sie eine Abfrage („nslookup“ oder „dig“) zur Überprüfung der Absenderdomäne vornehmen[20].

Internet-Quellen

1. Prüfen Sie Browserzertifikate beim Herstellen einer Verbindung zu einer geschützten Website (https ://).
2. Prüfen Sie Inhalt und Gültigkeit (in technischer Hinsicht) einer Quelle.
3. Im Zweifelsfall sollten Sie auf keinen Link klicken bzw. keine Software herunterladen.
4. Im Zweifelsfall sollten Sie eine Abfrage („lookup“ und „dig“) vornehmen und den Befehl „traceroute“ (Route verfolgen) ausführen.

Telefon

1. Achten Sie genau auf den Namen.
2. Erkennen Sie die Stimme?
3. Bitten Sie den Anrufer um eine Telefonnummer, damit Sie ihn zurückrufen können.

Abb. 10: Beispiel für ein Verfahren zur Erkennung der Authentizität von Informationen

Relevanz

Die zuvor erstellte Übersicht über die installierte Hard- und Software kann zum Filtern der eingehenden Informationen über Sicherheitslücken nach Relevanz verwendet werden, um eine Antwort auf die folgenden Fragen zu erhalten: „Wird diese spezielle Software von der Klientel auch tatsächlich genutzt?“ „Sind die Informationen für die Klientel auch wirklich relevant?“

Klassifizierung

Manche eingehenden Informationen können als vertrauliche Informationen klassifiziert oder gekennzeichnet sein (beispielsweise Berichte über Sicherheitsvorfälle von anderen Teams). Sämtliche Informationen müssen nach den Anweisungen des Absenders und den eigenen Richtlinien für die Informationssicherheit behandelt werden. Eine gute

[20] Werkzeuge für die Identitätsprüfung im CHIHT: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02.htm#04

Faustregel lautet: *„Verteilen Sie keine Informationen, wenn unklar ist, ob sie weitergeleitet werden dürfen. Im Zweifelsfall sollten Sie den Absender um Erlaubnis bitten."*

Risikobewertung und Analyse der Auswirkungen
Es gibt mehrere Methoden zur Ermittlung der Risiken und Auswirkungen einer (potenziellen) Sicherheitslücke.

Ein Risiko wird definiert als die potenzielle Gefahr, dass sich eine Sicherheitslücke ausnutzen lässt. Dabei sind einige wichtige Faktoren zu berücksichtigen, wie u. a.:

- Ist die Sicherheitslücke allgemein bekannt?
- Ist die Sicherheitslücke weit verbreitet?
- Lässt sich die Sicherheitslücke leicht ausnutzen?
- Lässt sich die Sicherheitslücke von extern ausnutzen?

All diese Fragen und Antworten geben ein gutes Gespür dafür, wie bedenklich eine Sicherheitslücke ist.
Das Risiko lässt sich anhand der folgenden Formel sehr leicht berechnen:

Auswirkungen = Risiko x potenzieller Schaden

Der potenzielle Schaden könnte wie folgt aussehen:

- Unbefugter Datenzugriff
- Denial of Service (DOS)
- Erwerb oder Ausdehnung von Zugriffsberechtigungen

(Am Ende dieses Kapitels finden Sie nähere Informationen über Klassifizierungssysteme.)

Nach der Beantwortung dieser Fragen kann eine generelle Bewertung in das Advisory mit Informationen über potenzielle Risiken und Schäden aufgenommen werden. Dabei werden häufig Begriffe wie NIEDRIG, MITTEL und HOCH verwendet.

Zu den umfassenderen Risikobewertungssystemen zählen u. a.:

Bewertungssystem von GOVCERT.NL[21]

In seiner Startphase hat das CSIRT GOVCERT.NL der niederländischen Regierung eine Matrix für die Risikobewertung entwickelt, die unter Berücksichtigung der neuesten Trends ständig aktualisiert wird.

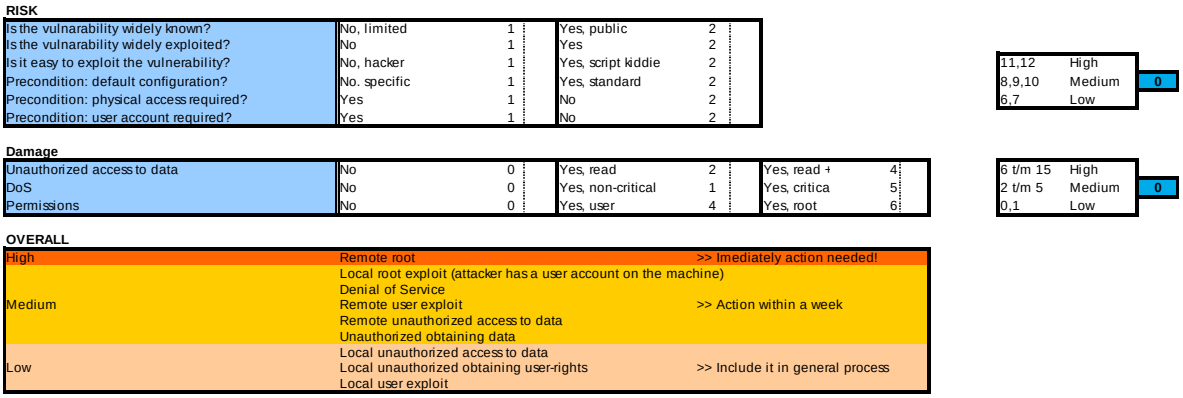


Abb. 11: Bewertungssystem von GOVCERT.NL

Beschreibung des EISSP-Austauschformats für Advisories[22]

Das EISPP (**E**uropean **I**nformation **S**ecurity **P**romotion **P**rogramme) ist ein Projekt, das nach dem Fünften Rahmenprogramm von der Europäischen Gemeinschaft mitfinanziert wird. Über das EISPP soll ein europäisches System nicht nur für den Austausch von Sicherheitsinformationen, sondern auch für den Inhalt und die Methoden zur Verteilung von Sicherheitsinformationen an KMU entwickelt werden. Durch die Bereitstellung der notwendigen IT-Sicherheitsdienste werden KMU in Europa mehr Vertrauen in den elektronischen Handel (E-Commerce) entwickeln und sein Potenzial zur Erschließung neuer und besserer Geschäftsmöglichkeiten stärker nutzen. Das EISPP ist ein Vorreiterprojekt für die Vision der Europäischen Kommission zur Schaffung eines europäischen Wissensnetzwerks innerhalb der Europäischen Union.

DAF (Deutsches Advisory Format)[23]

DAF ist eine Initiative vom deutschen CERT-Verbund und die Kernkomponente einer Infrastruktur für die Erstellung und den Austausch von Security Advisories von unterschiedlichen Teams. DAF ist speziell auf die Bedürfnisse von deutschen CERT-Teams zugeschnitten. Der Standard wird von CERT-Bund, DFN-CERT, PRESECURE und Siemens-CERT entwickelt und gepflegt.

[21] Risikomatrix für Sicherheitslücken: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_03.htm#02

Schritt 3: Verteilung der Informationen

Je nach den Wünschen der Klientel und Ihrer Kommunikationsstrategie hat ein CSIRT die Auswahl zwischen mehreren Verteilungsmethoden.

- Website
- E-Mail
- Berichte
- Archivierung und Forschung

Die von einem CSIRT verteilten Security Advisories sollten stets gleich strukturiert sein, damit sie besser verständlich sind und der Leser rasch alle relevanten Informationen finden kann.

Ein Advisory sollte zumindest die folgenden Informationen enthalten:

Titel des Advisory
……

Referenznummer
……
Betroffene Systeme
- ……
- ……

Jeweiliges Betriebssystem und Version
……
Risiko (Hoch - Mittel - Niedrig)
……
Auswirkungen/potenzieller Schaden (Hoch - Mittel - Niedrig)
……
Externe IDs: (CVE, IDs von Bulletins über Sicherheitslücken)
……

Übersicht über die Sicherheitslücke
……

Auswirkungen
……

Lösung
……

Beschreibung (Details)
……

Anhang
……

Abb. 12: Beispiel für ein Advisory-Format

In Kapitel *10. Praktische Übung* finden Sie ein vollständiges Beispiel für ein Security Advisory.

Behandlung von Vorfällen

Wie bereits in der Einführung zu diesem Kapitel erwähnt, ist die Informationsbearbeitung bei der Behandlung von Sicherheitsvorfällen im Wesentlichen identisch mit dem Prozess bei der Erstellung von Alarm- und Warnmeldungen und Bekanntgaben. Die Informationssammlung läuft normalerweise jedoch auf andere Weise ab, weil vorfallbezogene Daten entweder aus den von der Klientel oder anderen Teams weitergeleiteten Berichten über Vorfälle oder aus Kommentaren von den an der Behandlung von Vorfällen beteiligten Personen entnommen werden. In der Regel werden die Informationen per (verschlüsselter) E-Mail weitergeleitet; manchmal sind auch Telefon oder Fax als Kommunikationsmittel erforderlich.

Bei telefonischer Übermittlung von Informationen empfiehlt es sich, sämtliche Details sofort in einem Werkzeug für die Behandlung von Vorfällen/Erstellung von Berichten über Vorfälle oder in einem Memo zu notieren. Es sollte sofort (noch vor Beendigung des Telefonats) eine Vorfallnummer erstellt (sofern noch keine Nummer für diesen Vorfall vorhanden ist) und der Bericht erstattenden Person am Telefon (oder später durch eine kurze E-Mail) als Referenznummer für weitere Mitteilungen bekannt gegeben werden.

Im Folgenden wird der grundsätzliche Ablauf bei der Behandlung von Vorfällen beschrieben. Eine detaillierte Analyse des kompletten Vorfallsmanagements und aller an diesem Prozess beteiligten Arbeitsabläufe ist in der vom CERT/CC unter dem Titel „*Defining Incident Management processes for CSIRTs*[24] veröffentlichten Dokumentation zu finden.

[24] Defining Incident Management Processes: http://www.cert.org/archive/pdf/04tr015.pdf

Im Wesentlichen läuft die Vorfallbehandlung wie folgt ab:

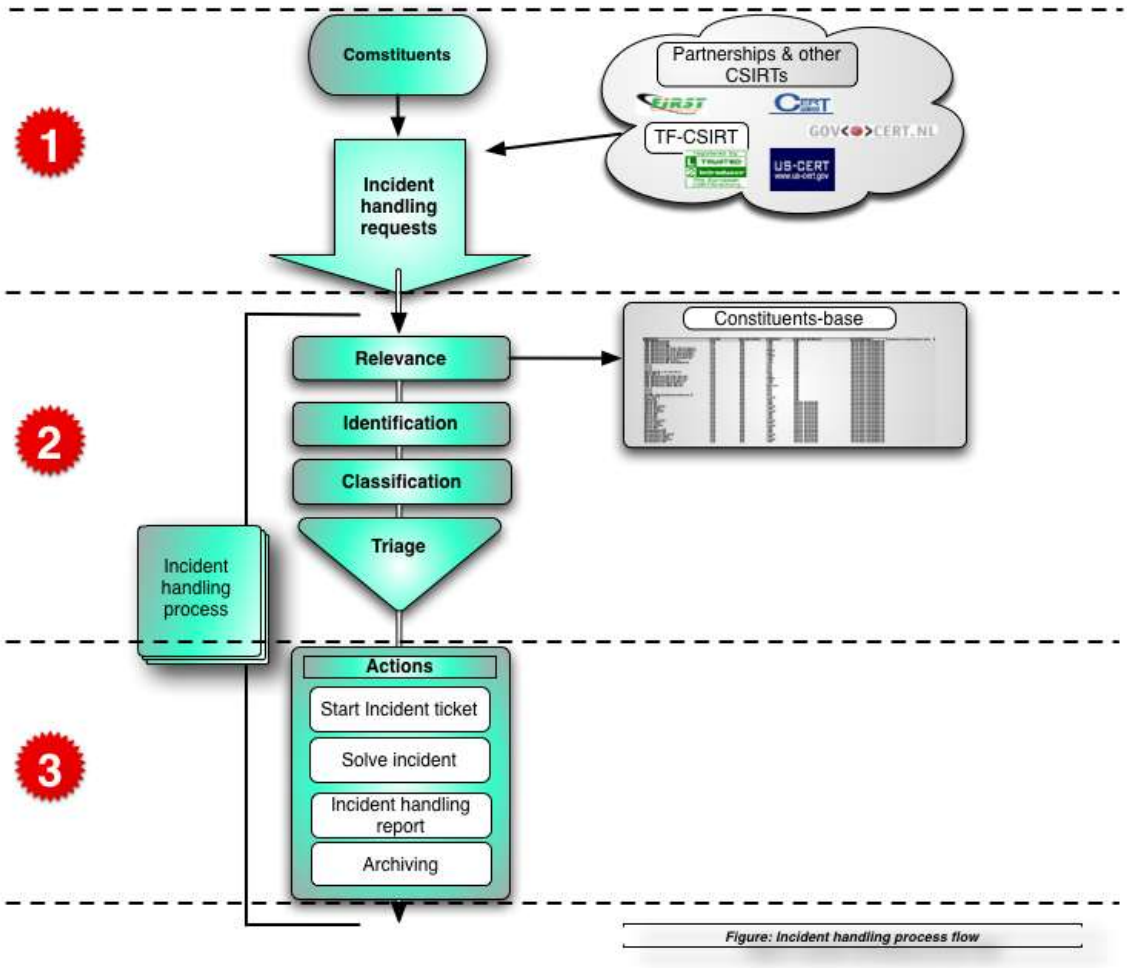


Abb. 13: Ablauf bei der Behandlung von Vorfällen

Schritt 1: Eingang von Vorfallberichten

Wie bereits erwähnt, gehen Vorfallberichte über mehrere Kanäle bei einem CSIRT ein, meist per E-Mail, doch auch per Telefon oder Fax.

Wie bereits erwähnt, empfiehlt es sich, bei Eingang eines Vorfallberichts alle Einzelheiten in einem bestimmten (festen) Format zu notieren. Dadurch ist gewährleistet, dass wichtige Informationen nicht außer Acht gelassen werden. Nachstehend finden Sie ein Beispielformular:

FORMULAR FÜR VORFALLBERICHTE

Bitte füllen Sie dieses Formular aus, und senden Sie es per Fax oder E-Mail an: ……..
*In den mit * gekennzeichneten Zeilen ist eine Angabe zwingend erforderlich.*

Name und Organisation
1. Name*:
2. Name der Organisation*:
3. Bereichstyp:
4. Land*:
5. Ort:
6. E-Mail-Adresse*:
7. Telefonnummer*:
8. Sonstiges:

Betroffene(r) Host(s)
9. Anzahl der Hosts:
10. Hostname & IP*:
11. Host-Funktion*:
12. Zeitzone:
13. Hardware:
14. Betriebssystem:
15. Betroffene Software:
16. Betroffene Dateien:
17. Sicherheit:
18. Hostname & IP:
19. Protokoll/Port:

Vorfall
20. Referenznummer (Nr.):
21. Vorfalltyp:
22. Startzeit des Vorfalls:
23. Kontinuierlicher Vorfall: JA NEIN
24. Uhrzeit und Methode der Erkennung:
25. Bekannte Sicherheitslücken:
26. Verdächtige Dateien:
27. Gegenmaßnahmen:
28. Detaillierte Beschreibung*:

Abb. 14: Informationen in einem Vorfallbericht

Schritt 2: Evaluierung des Vorfalls

Bei diesem Schritt gilt es, die Authentizität und Relevanz des gemeldeten Vorfalls zu prüfen und den Vorfall zu klassifizieren.

Identifizierung

Zur Vermeidung unnötiger Aktionen empfiehlt es sich zu prüfen, ob der Urheber vertrauenswürdig ist und zu Ihrer CSIRT-Klientel oder der Klientel eines verwandten CSIRT gehört. Es gelten ähnliche Regeln wie in Kapitel *8.2 Erstellung von Alarmmeldungen* beschrieben.

Relevanz

Bei diesem Schritt prüfen Sie, ob die Anforderung zur Behandlung des Vorfalls von der Klientel des CSIRT stammt oder ob IT-Systeme der Klientel am gemeldeten Vorfall beteiligt sind. Wenn keine dieser beiden Bedingungen zutrifft, wird der Bericht normalerweise an das entsprechende CSIRT weitergeleitet[25].

Klassifizierung

Bei diesem Schritt wird die Triage (Selektierung) vorbereitet, indem der Schweregrad des Vorfalls klassifiziert wird. Eine detaillierte Erläuterung der Klassifizierung von Vorfällen würde den Rahmen dieses Dokuments sprengen. Das CSIRT-Fallklassifikationssystem bietet eine gute Grundlage (Beispiel für ein Unternehmens-CSIRT):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

* - Sensitivity will vary depending on circumstances. Guidelines are provided.

Abb. 15: Vorfall-Klassifikationssystem (Quelle: FIRST)[26]

[25] Werkzeuge für die Identitätsprüfung im CHIHT: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02.htm#04

[26] CSIRT Case Classification: http://www.first.org/resources/guides/csirt_case_classification.html

Triage (Selektierung)
Die Triage ist ein aus der Militärmedizin herrührender Begriff für die Aufgabe, bei einem Massenunfall von Verletzten/Kranken darüber zu entscheiden, wie die knappen Mittel (personelle und materielle Ressourcen) auf sie aufzuteilen sind[27].

Das CERT/CC gibt die folgende Beschreibung (aus dem Englischen übersetzt):

Triage ist eine wesentliche Komponente jeder Vorfallbehandlungsfunktion, insbesondere für ein etabliertes CSIRT. Triage ist unerlässlich, um verstehen zu können, worüber Berichte in der gesamten Organisation erstellt werden. Sie fungiert als Vehikel, mit dessen Hilfe sämtliche Informationen an eine zentrale Kontaktstelle weitergeleitet werden, und ermöglicht dadurch eine unternehmensweite Ansicht der laufenden Aktivitäten und eine umfassende Korrelation aller Berichtsdaten. Die Triage ermöglicht die erste Analyse eines eingehenden Berichts und stellt diesen zur weiteren Bearbeitung in eine Warteschlange. Darüber hinaus bietet sie eine Plattform für die erste Dokumentation und Dateneingabe für einen Bericht oder eine Anforderung, sofern dies noch nicht beim Erkennungsprozess erfolgt ist.

Die Triage-Funktion bietet einen sofortigen Schnappschuss des aktuellen Status aller gemeldeten Aktivitäten, d. h. welche Berichte offen bzw. geschlossen (erledigt) sind, welche Aktionen noch anstehen und wie viele Berichte eines bestimmten Typs bereits eingegangen sind. Dieser Prozess erleichtert die Erkennung von potenziellen Sicherheitsproblemen und Festlegung von Prioritäten für die anstehende Arbeit. Die bei der Triage gesammelten Informationen dienen auch zum Erstellen von Trends und Statistiken über Sicherheitslücken und -vorfälle für die Geschäftsführung[28].

Die Triage sollte nur von äußerst erfahrenen Teammitgliedern vorgenommen werden, weil sie fundierte Kenntnisse der potenziellen Auswirkungen von Vorfällen auf bestimmte Teile der Klientel und die Fähigkeit voraussetzt, zu entscheiden, welches Teammitglied für die Bearbeitung des jeweiligen Vorfalls am besten geeignet sein könnte.

[27] Triage auf der Website von Wikipedia: http://de.wikipedia.org/wiki/Triage oder http://en.wikipedia.org/wiki/Triage (engl.)

[28] Defining Incident Management Processes: http://www.cert.org/archive/pdf/04tr015.pdf

Schritt 3: Aktionen

Normalerweise werden Vorfälle nach der Triage in eine Anforderungswarteschlange in einem Werkzeug zur Vorfallbearbeitung gestellt, das von einem oder mehreren Bearbeitern verwendet wird, die im Wesentlichen die folgenden Schritte ausführen.

Erstellen des Vorfalltickets
Die Vorfall-Ticketnummer wurde u. U. bereits im vorigen Schritt erstellt (beispielsweise wenn der Vorfall telefonisch gemeldet wurde). Andernfalls besteht der erste Schritt darin, diese Nummer zu erstellen, die für die weitere Kommunikation über diesen Vorfall verwendet wird.

Vorfalllebenszyklus
Die Behandlung eines Vorfalls basiert nicht auf einer bestimmte Schrittabfolge, die schließlich zu einer Lösung führt, sondern vielmehr auf einem Zyklus von Schritten, die wiederholt ausgeführt werden, bis der Vorfall endgültig behoben ist und alle beteiligten Parteien über alle erforderlichen Informationen verfügen. Dieser Zyklus, oft auch „Vorfalllebenszyklus“ genannt, umfasst die folgenden Prozesse:

Analyse:	Alle Details des gemeldeten Vorfalls werden analysiert.
Anforderung von Kontaktinformationen:	Zur weiteren Information aller beteiligten Parteien über den Vorfall, wie anderer CSIRT-Teams, Opfer und vermutlich auch der Eigentümer der missbräuchlich angegriffenen Systeme.
Technische Unterstützung:	Unterstützung der Opfer, um sich rasch von den Auswirkungen des Vorfalls zu erholen und weitere Informationen über den Angriff zu sammeln.
Koordination:	Information anderer beteiligter Parteien, wie des verantwortlichen CSIRT für das angegriffene IT-System, oder anderer Opfer.

Diese Struktur wird „Lebenszyklus“ genannt, weil ein Schritt jeweils zum nächsten führt und der letzte Schritt, d. h. die Koordination, zu einer neuen Analyse führen könnte, wodurch der Zyklus wieder neu beginnt. Der Prozess ist beendet, sobald alle beteiligten Parteien alle erforderlichen Informationen erhalten und gemeldet haben.

Im CERT/CC CSIRT-Handbuch finden Sie eine genauere Beschreibung des Vorfalllebenszyklus[29].

Bericht über die Vorfallbehandlung
Seien Sie auf Fragen der Geschäftsführung über Vorfälle vorbereitet, indem Sie einen Bericht zusammenstellen. Es empfiehlt sich, ein Dokument (nur zur internen Verwendung) über die gesammelten Erfahrungen zu verfassen, um die Mitarbeiter zu unterrichten und Fehler bei der Behandlung künftiger Vorfälle zu vermeiden.

[29] CSIRT-Handbuch (in engl. Sprache): http://www.cert.org/archive/pdf/csirt-handbook.pdf

Archivierung
Schauen Sie sich die die Kapitel *6.5 Festlegung der Richtlinien für die Informationssicherheit* oben bereits beschriebenen Richtlinien für die Archivierung an.

In Anhang *A.1 Weiterführende Literatur* finden Sie umfassende Hinweise zur Vorfallbearbeitung und zum Vorfalllebenszyklus.

Beispiel für einen Reaktions-Zeitplan

Die Festlegung der Reaktionszeiten wird häufig außer Acht gelassen, sollte jedoch ein fester Bestandteil jedes guten SLA-Vertrages (**S**ervice **L**evel **A**greement) zwischen einem CSIRT und seiner Klientel sein. Zeitgerechte Rückmeldungen an die Klientel während der Behandlung eines Vorfalls sind für die Pflichten der Klientel und für den Ruf des Teams von ausschlaggebender Bedeutung.
Um falsche Erwartungen zu vermeiden, sollte die Klientel unmissverständlich über die Reaktionszeiten informiert werden. Der folgende, nur grob skizzierte Zeitplan kann als Grundlage für einen detaillierten SLA mit der Klientel eines CSIRT verwendet werden.

Nachstehend finden Sie ein Beispiel für einen praktischen Reaktions-Zeitplan, angefangen vom Eingang der Hilfeanforderung:

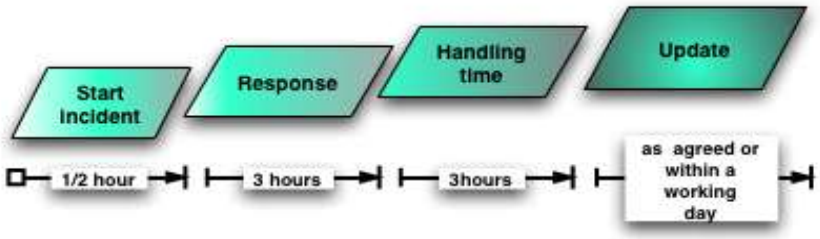


Abb. 16: Beispiel für einen Reaktions-Zeitplan

Es empfiehlt sich auch, der Klientel genaue Anweisungen für ihre eigenen Reaktionszeiten zu geben, insbesondere wann das CSIRT bei Eintreten eines Notfalls zu kontaktieren ist. Meist ist die frühzeitige Kontaktaufnahme mit dem CSIRT ratsam. Daher sollte die Klientel dazu ermutigt werden, sich im Zweifelsfall frühzeitig an das CSIRT zu wenden.

Verfügbare CSIRT-Werkzeuge

Dieses Kapitel enthält einige Hinweise auf gängige Werkzeuge, die von CSIRT-Teams verwendet werden. Es enthält nur Beispiele. Weitere Hinweise können Sie im *Clearinghouse of Incident Handling Tools*[30] (CHIHT) finden.

Software zur Verschlüsselung von E-Mails und Nachrichten

- GNUPG http://www.gnupg.org/
  GnuPG ist die komplette und kostenlose Implementierung des OpenPGP-Standards des GNU-Projekts, wie im RFC2440 festgelegt. Mit GnuPG können Sie Ihre Daten und Kommunikation verschlüsseln und signieren.

- PGP http://www.pgp.com/
  Kommerzielle Version

Werkzeug zur Behandlung von Vorfällen

Verwalten Sie Vorfälle und ihre weitere Bearbeitung, und verfolgen Sie alle Aktionen.

- RTIR http://www.bestpractical.com/rtir/
  RTIR ist ein kostenfreies Open-Source-System zur Behandlung von Vorfällen, das speziell auf die Bedürfnisse von CERT-Teams und anderen IRT-Teams (Vorfall-Reaktionsteams) zugeschnitten ist.

CRM-Werkzeuge

Wenn Sie eine große, breit gefächerte Klientel haben und alle Termine und Details genau verfolgen möchten, ist eine CRM-Datenbank hilfreich. In dieser Hinsicht wird eine große Palette unterschiedlicher Versionen angeboten. Hier nur einige Beispiele:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (Kostenlose Open-Source-Version) http://www.sugarforge.org/

Prüfung von Informationen

- WebSite-Watcher http://www.aignes.com/de/index.htm
  Dieses Programm ermöglicht das automatisierte Prüfen von Internet-Seiten auf Updates und Änderungen.

- WatchThatPage http://www.watchthatpage.com/
  Dieser Dienst sendet Informationen über Änderungen in Websites per E-Mail (kostenlos und kommerziell).

[30] CHIHT: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02.htm#04

Suche von Kontaktinformationen
Es ist wahrlich nicht einfach, den richtigen Ansprechpartner zur Meldung von Vorfällen zu finden. Es stehen einige Informationsquellen zur Verfügung, die hierfür verwendet werden können:

- RIPE[31]
- IRT-Objekt[32]
- TI[33]

Darüber hinaus enthält das CHIHT eine Liste einiger Werkzeuge für das Suchen von Kontaktinformationen[34].

Fiktives CSIRT (Schritt 8)

Festlegung der Arbeitsabläufe und der betriebsspezifischen und technischen Verfahren
Das fiktive CSIRT konzentriert sich auf seine Hauptdienste:

- Alarm- und Warnmeldungen
- Bekanntgaben
- Behandlung von Vorfällen

Das Team hat gut funktionierende und für jedes Teammitglied leicht verständliche Verfahren entwickelt. Das fiktive CSIRT hat auch einen Rechtsexperten eingestellt, der sich mit Haftungsfragen und den Richtlinien für die Informationssicherheit befassen soll. Ferner hat das Team einige nützliche Werkzeuge verwendet und durch die Diskussion mit anderen CSIRT-Teams hilfreiche Informationen über betriebsspezifische Fragen erhalten.

Es wurde eine (feste) Vorlage für Security Advisories und Vorfallberichte erstellt. Das Team verwendet RTIR (**R**equest **T**racker for **I**ncident **R**esponse) zur Behandlung von Vorfällen.

[31] RIPE whois: http://www.ripe.net/whois

[32] IRT-Objekt in der RIPE-Datenbank: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_01_03.htm#07

[34] Werkzeuge für die Identitätsprüfung im CHIHT: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02.htm#04

9 CSIRT-Schulungsmaßnahmen

Bislang wurden die folgenden Schritte unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann
4. Analyse der Umgebung und der Klientel
5. Festlegung des Aufgabenbereichs
6. Ausarbeitung des Geschäftsplans
   a. Festlegung des Finanzierungsmodells
   b. Festlegung der Organisationsstruktur
   c. Einstellung von Mitarbeitern
   d. Nutzung und Ausstattung des Büros
   e. Festlegung der Richtlinien für die Informationssicherheit
   f. Suche nach Kooperationspartnern
7. Förderung des Geschäftsplans
   a. Einholung der Genehmigung des Geschäftsfalls
   b. Aufnahme aller Komponenten in einen Projektplan
8. Gewährleistung der Funktionsfähigkeit des CSIRT
   a. Erstellung von Arbeitsabläufen
   b. Implementierung von CSIRT-Werkzeugen

>> Der nächste Schritt besteht in der Mitarbeiterschulung.

In diesem Kapitel werden die beiden Hauptquellen für spezielle CSIRT-Schulungsmaßnahmen genannt, nämlich Seminare von TRANSITS und dem CERT/CC.

TRANSITS

TRANSITS (**Tra**ining of **N**etwork **S**ecurity **I**ncident **T**eams **S**taff) war ein europäisches Projekt, das die Einrichtung von CSIRT-Teams (Computer Security Incident Response Teams; Reaktionsteams für Computersicherheitsverletzungen) und die Verbesserung von bereits bestehenden CSIRT-Teams durch die Behebung des Fachkräftemangels für CSIRT-Teams fördern sollte. Dieses Ziel wurde durch das Angebot spezieller Schulungsseminare zur Ausbildung von (neuen) CSIRT-Mitarbeitern in organisatorischen, betriebsspezifischen, technischen, marktspezifischen und juristischen Fragen erreicht, die bei der Erbringung von CSIRT-Diensten auftreten können.

Das Angebotsspektrum von TRANSITS sah insbesondere vor:

- Entwicklung, Aktualisierung und regelmäßige Überprüfung der modular aufgebauten Schulungsunterlagen
- Organisation von Workshops, bei denen die Schulungsunterlagen ausgehändigt wurden
- Einladung der Mitarbeiter von (neuen) CSIRT-Teams zur Teilnahme an diesen Workshops, insbesondere auch von Mitarbeitern aus den EU-Beitrittsländern

- Verteilung der Schulungsunterlagen und Gewährleistung der optimalen Nutzung der Ergebnisse[35].

Die ENISA fördert und unterstützt die TRANSITS-Seminare. Bei Fragen zur Anmeldung für Seminare oder zu den Anforderungen und Kosten wenden Sie sich bitte an die CSIRT-Experten der ENISA:

CERT-Relations@enisa.europa.eu

Im Anhang zu diesem Dokument finden Sie Seminarmusterunterlagen!

CERT/CC

Aufgrund der Komplexität der Computer- und Netzinfrastrukturen und administrativer Probleme ist es schwierig, die Netzsicherheit richtig zu verwalten. Netzwerk- und Systemadministratoren haben nicht genügend Personal und keine ausreichenden Sicherheitsmaßnahmen, um sich gegen Angriffe zu schützen und mögliche Schäden auf ein Minimum zu reduzieren. Aus diesem Grunde nimmt die Anzahl der Computer-sicherheitsverletzungen immer mehr zu.
Bei Auftreten von Computersicherheitsverletzungen müssen Organisationen rasch und effizient reagieren. Je schneller eine Organisation einen Sicherheitsvorfall erkennt, analysiert und darauf reagiert, desto besser kann sie den Schaden begrenzen und die Kosten für die Wiederherstellung verringern. Zur raschen Reaktion und Vermeidung zukünftiger Vorfälle bietet sich die Einrichtung eines CSIRT (Reaktionsteam für Computersicherheitsverletzungen) an.

CERT-CC bietet Seminare für Führungs- und Fachkräfte u. a. in folgenden Bereichen an: Einrichtung und Führung von CSIRT-Teams, Reaktion auf und Analyse von Sicherheitsvorfällen und Verbesserung der Netzsicherheit. Sofern nichts anderes angegeben ist, finden alle Seminare in Pittsburgh, PA, statt. Mitglieder aus unserem Team geben auch Sicherheitsseminare an der Carnegie Mellon-Universität.

Speziell für CSIRT-Teams angebotene CERT/CC-Seminare[36] (Seminartitel aus dem Englischen übersetzt)

Einrichtung eines Computer Security Incident Response Teams (CSIRT)
Führung von Computer Security Incident Response Teams (CSIRT)
Grundlagenwissen für die Behandlung von Vorfällen
Erweiterte Behandlung von Vorfällen für technische Fachkräfte

Im Anhang zu diesem Dokument finden Sie Seminarmusterunterlagen!

[35] TRANSITS: http://www.enisa.europa.eu/CERT_INVENTORY/pages/04_02_02.htm#11

[36] Seminare des CERT/CC: http://www.sei.cmu.edu/products/courses

Fiktives CSIRT (Schritt 9)

Ausbildung und Schulung der Mitarbeiter

Das fiktive CSIRT beschließt, alle technischen Fachkräfte für die nächsten TRANSITS-Seminare anzumelden. Ferner soll der Teamleiter am CERT/CC-Seminar *Führung eines CSIRT* teilnehmen.

10 Praktische Übung: Erstellung eines Advisory

Bislang wurden die folgenden Schritte unternommen:

1. Verstehen, was ein CSIRT ist und welche Vorteile es bieten könnte.
2. Für welchen Bereich soll das neue Team seine Dienste anbieten?
3. Welche Dienste ein CSIRT für seine Klientel anbieten kann
4. Analyse der Umgebung und der Klientel
5. Festlegung des Aufgabenbereichs
6. Ausarbeitung des Geschäftsplans
   a. Festlegung des Finanzierungsmodells
   b. Festlegung der Organisationsstruktur
   c. Einstellung von Mitarbeitern
   d. Nutzung und Ausstattung des Büros
   e. Festlegung der Richtlinien für die Informationssicherheit
   f. Suche nach Kooperationspartnern
7. Förderung des Geschäftsplans.
   a. Einholung der Genehmigung des Geschäftsfalls
   b. Aufnahme aller Komponenten in einen Projektplan
8. Gewährleistung der Funktionsfähigkeit des CSIRT
   a. Erstellung von Arbeitsabläufen
   b. Implementierung von CSIRT-Werkzeugen
9. Ausbildung und Schulung Ihrer Mitarbeiter

>> Der nächste Schritt ist eine praktische Übung, damit Sie für die echte Praxis gut gerüstet sind!

Als Beispiel wird eine ganz alltägliche Aufgabe aus der Arbeit eines CSIRT in diesem Kapitel beschrieben, nämlich das Erstellen eines Security Advisory.

Auslöser war das folgende von Microsoft veröffentlichte Security Advisory:

Kennung des Bulletins	**Microsoft Security Bulletin MS06-042**
Titel des Bulletins	**Kumulatives Sicherheitsupdate für Internet Explorer (918899)**
Kurzzusammen-fassung	Dieses Update behebt mehrere Sicherheitsanfälligkeiten in Internet Explorer, die eine Codeausführung von Remotestandorten aus ermöglichen können.
Bewertung des maximalen Schweregrads	Kritisch
Auswirkung der Sicherheitsanfälligkeit	Remotecodeausführung
Betroffene Software	**Windows, Internet Explorer.** Weitere Informationen finden Sie im Abschnitt „Betroffene Software und Download Locations“.

Dieses anbieterseitige Bulletin bezieht sich auf eine kürzlich in Internet Explorer erkannte Sicherheitslücke. Der Anbieter veröffentlicht mehrere Korrekturen für diese Software für mehrere Versionen von Microsoft Windows.

Nach Eingang dieser sicherheitsrelevanten Informationen über eine Mailingliste beginnt das CSIRT den in Kapitel *8.2 Erstellung von Alarm- und Warnmeldungen und Bekanntgaben* beschriebenen Arbeitsablauf.

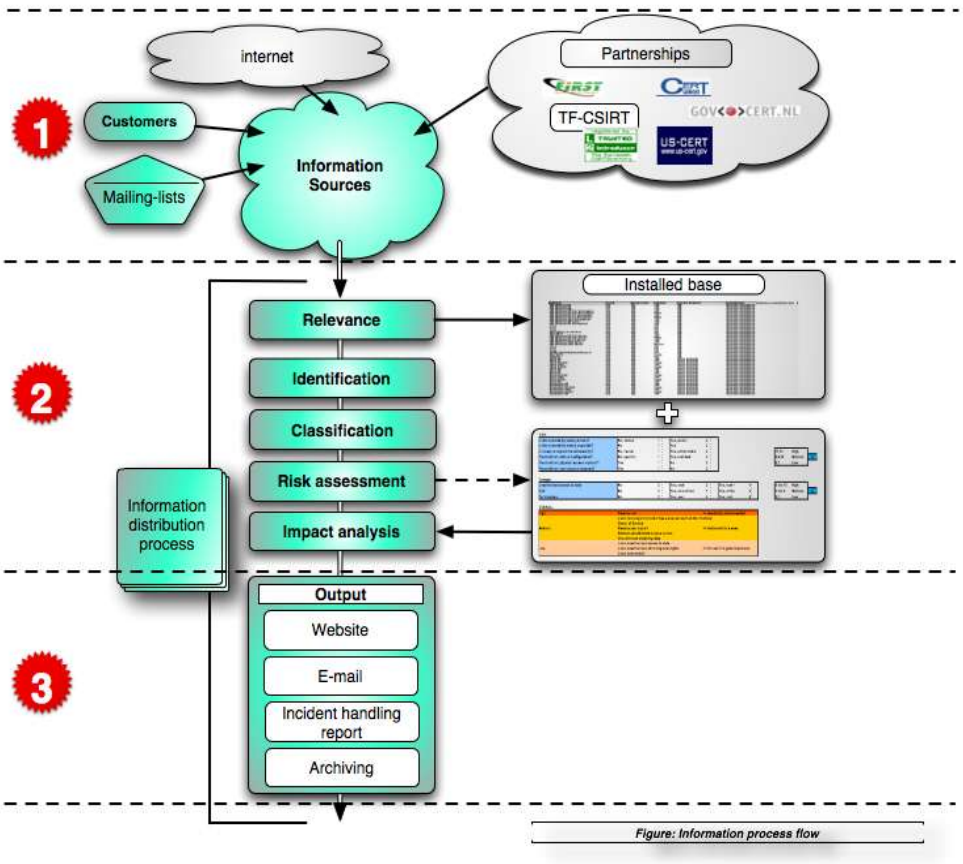


Figure: Information process flow

Schritt 1: Sammlung von Informationen über Schwachstellen

Der erste Schritt besteht darin, dass das fiktive CSIRT die Website des Anbieters aufruft, um die Authentizität der Informationen zu prüfen und weitere Einzelheiten über die Schwachstelle und die betroffenen IT-Systeme zu sammeln.

Schritt 2: Evaluierung der Informationen und Risikobewertung

Identifizierung
Durch den Vergleich der per E-Mail eingegangenen Informationen über Schwachstellen und Sicherheitslücken mit dem betreffenden, auf der Website des Anbieters veröffentlichten Wortlaut wurden die Informationen bereits geprüft.

Relevanz
Das fiktive CSIRT vergleicht die auf der Website veröffentlichte Liste der betroffenen Systeme mit den Systemen, die bei der Klientel im Einsatz sind, und stellt fest, dass mindestens ein Klient mit Internet Explorer arbeitet. Demzufolge sind die Informationen über die Sicherheitslücke tatsächlich relevant.

Kategorie	Anwendung	Software produkt	Version	Betriebs-system	Version	Klient
Desktop	Browser	IE	x-x-	Microsoft	XP Prof.	A

Klassifizierung
Da die Informationen öffentlich zugänglich sind, können sie genutzt und weiter verteilt werden.

Risikobewertung und Analyse der Auswirkungen
Durch die Beantwortung der Fragen wird klar, dass die Risiken und Auswirkungen *hoch* sind (von Microsoft als *kritisch* bewertet).

RISIKO

Ist die Sicherheitslücke allgemein bekannt?	Ja
Ist die Sicherheitslücke weit verbreitet?	Ja
Lässt sich die Sicherheitslücke leicht auszunutzen?	Ja
Lässt sich die Sicherheitslücke von extern ausnutzen?	Ja

SCHADEN
Mögliche Auswirkungen sind die externe Zugriffsmöglichkeit und die potenzielle Remotecodeausführung. Da diese Schwachstelle mehrere Probleme nach sich zieht, ist das Schadensrisiko als *hoch* einzustufen.

Schritt 3: Verteilung

Das fiktive CSIRT ist ein internes CSIRT und verfügt über die Kommunikationskanäle E-Mail, Telefon und die interne Website. Auf Basis der Vorlage in Kapitel *8.2 Erstellung von Alarm- und Warnmeldungen und Bekanntgaben* erstellt das CSIRT das folgende Advisory.

Titel des Advisory
Feststellung mehrerer Sicherheitslücken in Internet Explorer

Referenznummer
082006-1

Betroffene Systeme
- Alle Desktop-Systeme, auf denen Microsoft ausgeführt wird

Betroffenes Betriebssystem und Betriebssystemversion
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 und Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 und Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 für Itanium-basierte Systeme und Microsoft Windows Server 2003 mit SP1 für Itanium-basierte Systeme
- Microsoft Windows Server 2003 x64 Edition

Risiko (Hoch-Mittel-Niedrig)
HOCH

Auswirkung/potenzieller Schaden (Hoch-Mittel-Niedrig)
HOCH

Externe ID: (CVE, ID des Bulletins über die Sicherheitslücke)
MS-06-42

Übersicht über die Sicherheitslücke
Microsoft hat mehrere kritische Sicherheitslücken in Internet Explorer gefunden, die eine Codeausführung von Remotestandorten ermöglichen können.

Auswirkung
Wenn ein Benutzer mit Administratorrechten angemeldet ist, könnte ein Angreifer die vollständige Kontrolle über das System erlangen. Er könnte Programme installieren, Benutzer hinzufügen sowie Daten anzeigen, ändern oder löschen. Für Benutzer, deren Konten mit weniger Rechten konfiguriert sind, kann dies geringere Auswirkungen haben als für Benutzer, die mit Administratorrechten arbeiten.

Lösung
Sofortige Installation eines Patch in Internet Explorer

Beschreibung (Details)
Nähere Informationen finden Sie auf der Website:
http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms06-aug.mspx

Anhang
Nähere Informationen finden Sie auf der Website:
http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms06-aug.mspx

Jetzt kann dieses Advisory verteilt werden. Da es sich um ein kritisches Bulletin handelt, empfiehlt es sich, die Klientel nach Möglichkeit auch telefonisch zu informieren.

Fiktives CSIRT (Schritt 10)

Praktische Übungen

In den ersten Wochen nach Aufnahme seines Dienstes verwendet das fiktive CSIRT einige fiktive Fallbeispiele (von anderen CSIRT-Teams) für praktische Übungen. Außerdem werden einige Security Advisories auf Basis der von den Hardware- und Softwareanbietern verteilten Informationen über Sicherheitslücken und Schwachstellen nach Anpassung an die Bedürfnisse der Klientel veröffentlicht.

11 Schlussfolgerung

Damit ist dieser Leitfaden abgeschlossen. Das vorliegende Dokument soll nur einen knapp gefassten Überblick über die zur Einrichtung eines CSIRT notwendigen Abläufe geben und erhebt keinen Anspruch auf Vollständigkeit. In Anhang *A.1 Weiterführende Literatur* finden Sie weitere Informationen zu lesenswerter Literatur über dieses Thema.

Die folgenden wichtigen Schritte müssten von dem fiktiven CSIRT als Nächstes ausgeführt werden:

- Sammlung von Rückmeldungen seitens der Klientel zur Feinabstimmung der angebotenen Dienste
- Routine bei der alltäglichen Arbeit
- Praktische Erprobung von Notsituationen
- Enge Zusammenarbeit mit den verschiedenen CSIRT-Gemeinschaften mit dem Ziel, eines Tages auch einen Beitrag zu ihrer freiwilligen Arbeit zu leisten

12 Beschreibung des Projektplans

Hinweis: Der Projektplan ist eine erste Schätzung des Zeitaufwands. Die tatsächliche Dauer eines Projekts hängt von den zur Verfügung stehenden Ressourcen ab.

Der Projektplan steht auf einer CD-ROM und auf der ENISA-Website in verschiedenen Formaten zur Verfügung. Er deckt alle im vorliegenden Dokument beschriebenen Abläufe ab.

Als Hauptformat lässt sich Microsoft Project direkt bei diesem Projektmanagement-Werkzeug verwenden.

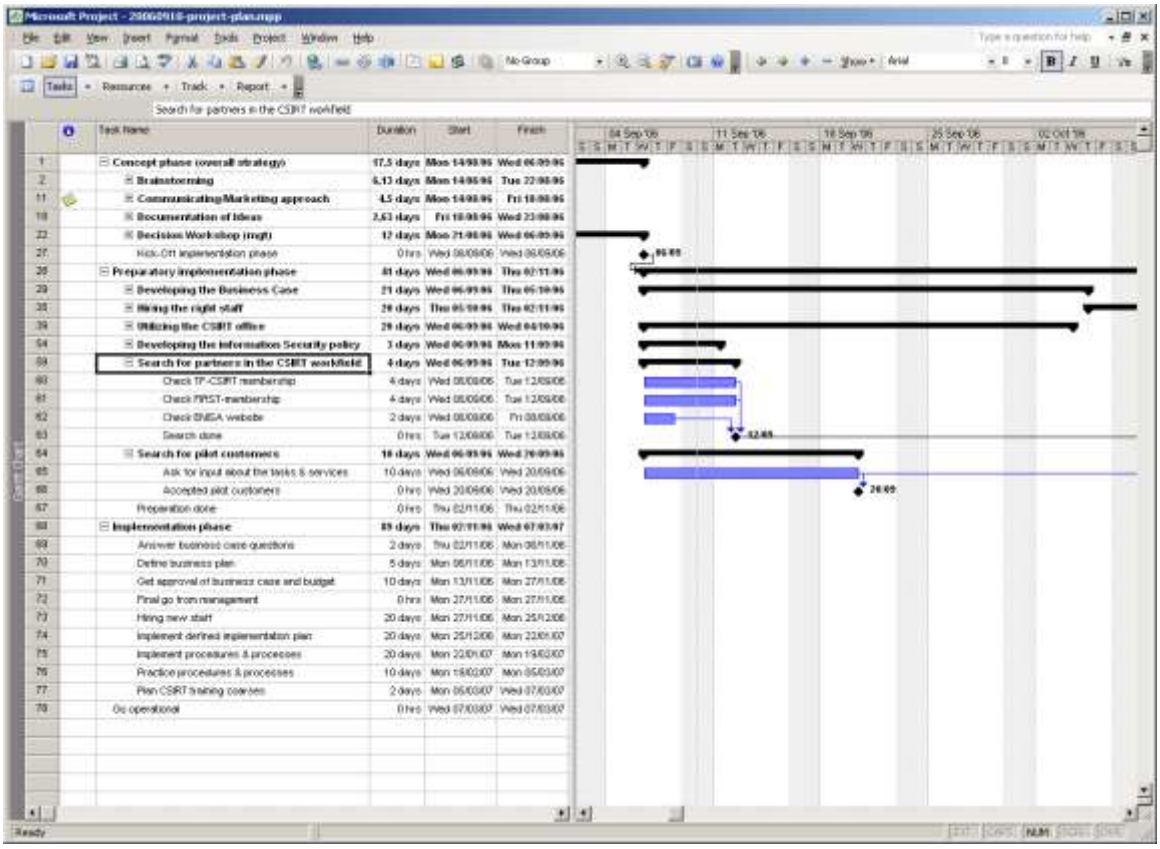


Abb. 17: Projektplan

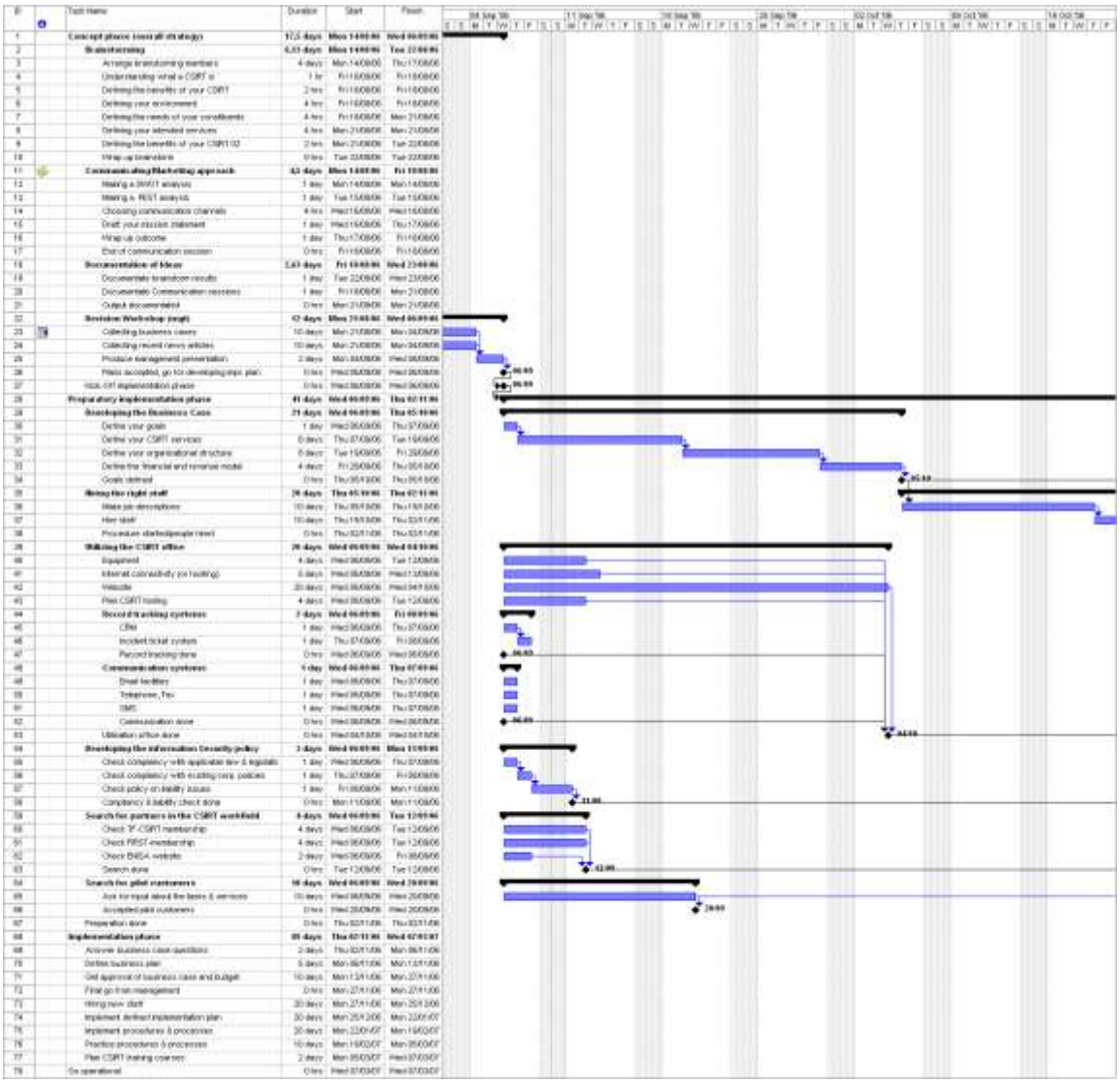


Abb. 18: Projektplan mit allen Aufgaben und einem Gant-Diagramm

Der Projektplan steht auch im CVS- und XML-Format zur Verfügung. Für Rückfragen zur Verwendung wenden Sie sich bitte an die CSIRT-Experten der ENISA: CERT-Relations@enisa.europa.eu

ANHANG

A.1 Weiterführende Literatur

„Handbook for CSIRTs (CERT/CC)“ (in englischer Sprache)
Ein Handbuch und sehr umfangreiches Nachschlagewerk zu allen Themen, die für die Arbeit eines CSIRT von Belang sind
Quelle: http://www.cert.org/archive/pdf/csirt-handbook.pdf

„Defining Incident Management Processes for CSIRTs: A Work in Progress“ (in englischer Sprache)
Eine detaillierte Analyse der Behandlung von Sicherheitsvorfällen
Quelle: http://www.cert.org/archive/pdf/04tr015.pdf

„State of the Practice of Computer Security Incident Response Teams (CSIRTs)“ (in englischer Sprache)
Eine eingehende Analyse der tatsächlichen Gegebenheiten der weltweiten CSIRT-Umgebung, einschließlich historischen Informationen, statistischen Daten usw.
Quelle: http://www.cert.org/archive/pdf/03tr001.pdf

„CERT-in-a-box“ (in englischer Sprache)
Eine detaillierte Beschreibung der Erfahrungen, die bei der Einrichtung von „GOVCERT.NL“ und „De Waarschuwingsdienst“, dem Warndienst in den Niederlanden, gemacht wurden
Quelle: http://www.govcert.nl/render.html?it=69

RFC 2350: „Expectations for Computer Security Incident Response“ (in englischer Sprache)
Quelle: http://www.ietf.org/rfc/rfc2350.txt

„NIST[37] Computer Security Incident Handling Guide“ (in englischer Sprache)
Quelle: http://www.securityunit.com/publications/sp800-61.pdf

„ENISA Inventory of CERT activities in Europe“ (in englischer Sprache)
Ein Verzeichnis mit Informationen über CSIRT-Teams in Europa und ihre diversen Aktivitäten
Quelle: http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] NIST: National Institute of Standards and Technologies (Nationales Institut für Standardisierung und Technologie in den USA)

A.2 CSIRT-Dienste

Ein besonderer Dank gilt dem CERT/CC, das diese Liste vorgelegt hat.

Reaktive Dienste	***Proaktive Dienste***	***Behandlung von Artefakten***
• Alarm- und Warnmeldungen • Behandlung von Sicherheitsvorfällen • Analyse von Sicherheitsvorfällen • Reaktion auf Sicherheitsvorfälle vor Ort • Unterstützung bei der Reaktion auf Sicherheitsvorfälle • Koordination der Reaktion auf Sicherheitsvorfälle • Behandlung von Sicherheitslücken • Analyse von Sicherheitslücken • Reaktion auf Sicherheitslücken • Koordination der Reaktion auf Sicherheitslücken	• Bekanntgaben • Technologieüberwachung • Sicherheitsaudits oder -analysen • Konfiguration und Pflege des Sicherheitssystems • Entwicklung von Sicherheitswerkzeugen • Dienste für die Erkennung von Angriffsversuchen • Verteilung von sicherheitsrelevanten Informationen	• Analyse von Artefakten • Reaktion auf Artefakte • Koordination der Reaktion auf Artefakte ***Sicherheitsqualitäts-management*** • Risikoanalyse • Kontinuität des Geschäftsbetriebs und Wiederherstellung nach Notfällen • Beratung in Sicherheitsfragen • Sensibilisierung des Sicherheitsbewusstseins • Ausbildung/Schulung • Produktevaluierung oder -zertifizierung

Abb. 19: Liste der CSIRT-Dienste von CERT/CC

Beschreibung der Dienste

Reaktive Dienste

Reaktive Dienste dienen als Reaktion auf Hilfeersuchen, Berichte vonseiten der CSIRT-Klientel über Sicherheitsvorfälle und jegliche Gefahren für bzw. Angriffe auf CSIRT-Systeme. Einige Dienste können durch die Benachrichtigung von Dritten oder durch die Anzeige von Überwachungs- oder IDS-Protokollen und Alarmmeldungen eingeleitet werden.

Alarm- und Warnmeldungen

Dieser Dienst umfasst die Weiterleitung von Informationen, in denen ein Angriffsversuch, eine Sicherheitslücke, eine Warnmeldung über einen Eindringversuch, ein Computervirus oder eine Hoax-Nachricht beschrieben wird, und die Empfehlung kurzfristiger Maßnahmen für den Umgang mit dem dadurch entstehenden Problem. Als Reaktion auf das aktuelle Problem wird eine Alarm- oder Warnmeldung oder ein Advisory versandt, um die Klientel von den jeweiligen Aktivitäten zu benachrichtigen und Anleitungen für den Schutz ihrer Systeme oder die Wiederherstellung von betroffenen Systemen zu geben. Die Informationen können vom CSIRT erstellt oder von Anbietern,

anderen CSIRT-Teams, Sicherheitsexperten oder anderen Teilen der Klientel weitergeleitet werden.

Behandlung von Sicherheitsvorfällen

Die Behandlung von Sicherheitsvorfällen umfasst den Eingang, die Triage von und Reaktion auf Anfragen und Berichte sowie die Analyse von Sicherheitsvorfällen und Ereignissen. Zu den Gegenmaßnahmen (Reaktion) zählen insbesondere:

- Maßnahmen zum Schutz der betroffenen oder von Angreifern bedrohten Systeme und Netzwerke
- Ausarbeitung von Lösungen und Migrationsstrategien anhand von relevanten Advisories oder Warnmeldungen
- Suche nach möglichen Angriffen auf andere Teile des Netzwerks
- Filterung des Netzverkehrs
- Wiederherstellung von Systemen
- Korrektur (Patch) oder Reparatur von Systemen
- Ausarbeitung anderer Reaktions- oder Abhilfestrategien

Da die Behandlungsmaßnahmen für Sicherheitsvorfälle auf unterschiedliche Weise von verschiedenen CSIRT-Teams durchgeführt werden, wird dieser Dienst auf Basis der jeweils durchgeführten Maßnahmen und geleisteten Hilfe wie folgt kategorisiert:

Analyse von Sicherheitsvorfällen

Die Vorfallanalyse erfolgt auf vielen Ebenen, wobei viele Teildienste geleistet werden. Im Wesentlichen ist die Vorfallanalyse eine Prüfung aller verfügbaren Informationen und Nachweise oder Artefakte, die sich auf einen Vorfall oder ein Ereignis beziehen. Der Zweck der Analyse besteht darin, den Umfang des Vorfalls, das Ausmaß des durch den Vorfall verursachten Schadens, die Art des Vorfalls und mögliche Reaktionsstrategien oder Abhilfemaßnahmen zu ermitteln. Anhand der Ergebnisse der (nachstehend beschriebenen) Schwachstellen- und Artefaktanalyse kann das CSIRT eine detaillierte und aktuelle Analyse der in einem bestimmten System aufgetretenen Ereignisse durchführen. Dabei wird eine Korrelation zwischen Vorfällen hergestellt, um mögliche Zusammenhänge, Trends, Muster oder Angreifersignaturen zu ermitteln. Je nach Aufgabenstellung, Zielsetzung und Arbeitsabläufen des CSIRT werden u. U. zwei Teildienste im Rahmen der Vorfallanalyse geleistet:

Sammlung von forensischen Beweismitteln

Mit der Sammlung, Aufbewahrung, Dokumentation und Analyse von Beweismitteln aus einem betroffenen Computersystem lassen sich die am System vorgenommenen Änderungen feststellen und die zur Sicherheitsgefährdung führenden Ereignisse leichter rekonstruieren. Diese Sammlung von Informationen und Beweismitteln muss eine lückenlose, nach den Vorschriften des Beweisrechts gerichtlich zulässige Nachweisführung gewährleisten. Zu den Aufgaben bei der Sammlung forensischer Beweismittel zählen u. a. (jedoch nicht ausschließlich): Erstellung einer exakten Kopie des Festplattenlaufwerks des betroffenen Systems; Prüfung auf Änderungen, die am System vorgenommen wurden, wie neue Programme, Dateien, Dienste und Benutzer; Suche nach laufenden Prozessen und offenen Ports; Prüfung auf Trojanische Pferde und Toolkits. Mitarbeiter von CSIRT-Teams, die diese Aufgabe wahrnehmen, müssen

u. U. auch darauf vorbereitet sein, als sachverständige Zeugen bei Gerichtsverhandlungen aufzutreten.

Verfolgung oder Spurensicherung

Diese Aktivität dient zur Sicherung der Spuren eines Angreifers (Eindringlings) oder zur Erkennung der Systeme, auf die der Angreifer Zugriff hatte. Dabei wird u. a. verfolgt, wie sich der Angreifer den Zugang zu den betroffenen Systemen und zugehörigen Netzwerken verschafft hat, welche Systeme für diesen Zugang verwendet wurden, woher der Angriff stammte und welche anderen Systeme und Netzwerke im Rahmen des Angriffs genutzt wurden. Bei dieser Aktivität wird u. U. auch der Versuch unternommen, die Identität des Angreifers zu ermitteln. Diese Ermittlertätigkeit kann allein erfolgen, wird in der Regel jedoch in Zusammenarbeit mit Strafverfolgungsbehörden, Internetdienstanbietern (ISP) oder anderen beteiligten Organisationen durchgeführt.

Reaktion auf Sicherheitsvorfälle vor Ort

Das CSIRT hilft der Klientel vor Ort direkt bei der Wiederherstellung nach einem Vorfall. Dabei führt das CSIRT selbst eine physische Analyse der betroffenen Systeme durch und nimmt die Reparatur und Wiederherstellung der Systeme vor, leistet also nicht nur Unterstützung per Telefon oder E-Mail (s. u.) als Reaktion auf derartige Vorfälle. Dieser Dienst umfasst alle vor Ort notwendigen Maßnahmen, wenn sich ein Vorfall mutmaßlich oder tatsächlich ereignet. Wenn sich das CSIRT nicht am betroffenen Standort befindet, würden Mitglieder des Teams anreisen und die entsprechenden Maßnahmen durchführen. In anderen Fällen könnte sich ein lokales Team bereits vor Ort befinden und die entsprechenden Maßnahmen als Reaktion auf den Vorfall im Rahmen seiner Routinearbeiten durchführen. Dies trifft insbesondere zu, wenn die Vorfallbehandlung zu den normalen Aufgaben von System-, Netzwerk- oder Sicherheitsadministratoren gehört, also nicht die Aufgabe eines eigens dafür eingerichteten CSIRT ist.

Unterstützung bei der Reaktion auf Sicherheitsvorfälle

Per Telefon, E-Mail, Fax oder auf sonstige Weise (Dokumentation) hilft das CSIRT dem (den) Opfer(n) des Angriffs bei der Wiederherstellung nach einem Vorfall. Diese Unterstützung kann technische Hilfe bei der Interpretation der erfassten Daten, die Bereitstellung von Kontaktinformationen oder Anleitungen für Schadensminderungs- und Wiederherstellungsstrategien umfassen. Dabei werden jedoch nicht die oben beschriebenen direkten Gegenmaßnahmen (Reaktion) vor Ort durchgeführt. Stattdessen leistet das CSIRT externe Hilfe, damit die Mitarbeiter vor Ort die Wiederherstellung selbst vornehmen können.

Koordination der Reaktion auf Sicherheitsvorfälle

Das CSIRT koordiniert die Reaktionsbemühungen zwischen den am Vorfall beteiligten Parteien. Dazu zählen in der Regel das Opfer des Angriffs, andere am Angriff beteiligte Standorte sowie Standorte, die Hilfe bei der Analyse des Angriffs benötigen. Dazu können auch Parteien zählen, die IT-Unterstützung (Support) für das Opfer leisten, wie Internetdienstanbieter (ISP), andere CSIRT-Teams sowie System- und Netzwerkadministratoren vor Ort. Die Koordinationstätigkeit kann die Sammlung von Kontaktinformationen, die Benachrichtigung von Standorten über ihre potenzielle Beteiligung (als Opfer oder Quelle eines Angriffs), die Sammlung statistischer Daten zur

Zahl der betroffenen Standorte sowie den Austausch und die Analyse von Informationen umfassen. Im Rahmen der Koordinationstätigkeit sind u. U. auch die Unterrichtung und Zusammenarbeit mit dem Rechtsanwalt, der Personal- oder PR-Abteilung eines Unternehmens vorgesehen; sie kann ferner die Koordinierung mit Strafverfolgungsbehörden umfassen. Bei diesem Dienst ist jedoch keine direkte Reaktion auf Sicherheitsvorfälle vor Ort vorgesehen.

Behandlung von Sicherheitslücken

Die Behandlung von Sicherheitslücken umfasst die Entgegennahme von Informationen und Berichten über Schwachstellen in Hardware und Software, eine Analyse der Art, Mechanismen und Auswirkungen der Sicherheitslücken sowie die Entwicklung von Reaktionsstrategien zur Erkennung und Behebung von Sicherheitslücken. Da die Aktivitäten zur Behandlung von Sicherheitslücken auf unterschiedliche Weise von den verschiedenen CSIRT-Teams implementiert werden, wird dieser Dienst zudem auf Basis der jeweils durchgeführten Aktivitäten und geleisteten Hilfe wie folgt kategorisiert:

Analyse von Sicherheitslücken

Das CSIRT nimmt eine technische Analyse und Prüfung der in der Hardware oder Software vorhandenen Schwachstellen vor, wie u. a. die Überprüfung mutmaßlicher Sicherheitsrisiken und die technische Prüfung der Hardware oder Software auf Sicherheitslücken, um festzustellen, wo sie vorhanden sind und wie sie sich ausnutzen lassen. Bei der Analyse wird u. U. auch der Quellcode mithilfe eines Debuggers (Werkzeug zur Fehlerbereinigung) geprüft, um festzustellen, wo die Sicherheitslücke auftritt, oder der Versuch unternommen, das Problem auf einem Testsystem zu reproduzieren.

Reaktion auf Sicherheitslücken

Bei diesem Dienst werden geeignete Gegenmaßnahmen (Reaktion) zur Verringerung oder Beseitigung der Sicherheitslücken ermittelt. Dazu zählen u. a. die Entwicklung von Patchprogrammen, Korrekturen und Abhilfemaßnahmen sowie die Benachrichtigung von Dritten über Abhilfestrategien, u. U. durch die Erstellung und Verteilung von Advisories oder Warnmeldungen. Bei diesem Dienst sind u. U. auch Gegenmaßnahmen wie die Installation von Patchprogrammen, Korrekturen oder Abhilfemaßnahmen vorgesehen.

Koordination der Reaktion auf Sicherheitslücken

Das CSIRT setzt die verschiedenen Bereiche des Unternehmens oder der Klientel von den Sicherheitslücken in Kenntnis und verteilt Informationen darüber, wie die Sicherheitslücke behoben oder verringert werden kann. Das CSIRT prüft, ob die Reaktionsstrategie mit Erfolg umgesetzt wurde. Zu diesem Dienst zählt u. U. auch die Kommunikation mit Anbietern, anderen CSIRT-Teams, technischen Sachverständigen, Mitgliedern der Klientel sowie Einzelpersonen oder Gruppen, die die Sicherheitslücke zuerst festgestellt oder gemeldet haben. Zu den weiteren Aktivitäten zählen die Analyse eines Sicherheitsrisikos oder die Erstellung eines Berichts über ein Sicherheitsrisiko, die Koordination bei der Veröffentlichung der betreffenden Dokumente, Patchprogramme Abhilfemaßnahmen sowie die Synthese der von den verschiedenen Parteien durchgeführten technischen Analyse. Bei diesem Dienst kann auch die Pflege eines öffentlichen oder privaten Archivs oder einer Wissensdatenbank mit Informationen über Sicherheitslücken und entsprechende Reaktionsstrategien vorgesehen werden.

Behandlung von Artefakten

Artefakte sind in einem System erkannte Dateien oder Objekte, die an der Erkundung von oder einem Angriff auf Systeme und Netzwerke beteiligt sein können oder zur Umgehung der Sicherheitsmaßnahmen gedacht sind. Zu Artefakten zählen u. a. Computerviren, Trojanische Pferde, Würmer, Exploit-Skripte und Toolkits.
Zur Behandlung von Artefakten zählen die Sammlung von Informationen über und Kopien von Artefakten, die bei Eindringversuchen und Angriffen verwendet werden, Reconnaissance und sonstige unzulässige oder störende Aktivitäten. Bei der anschließenden Prüfung werden Art, Mechanismen, Version und Verwendung der Artefakte analysiert und Reaktionsstrategien zur Erkennung, Beseitigung und Abwehr dieser Artefakte entwickelt (oder vorgeschlagen). Da Artefakte auf unterschiedliche Weise von den verschiedenen CSIRT-Teams behandelt werden, wird dieser Dienst zudem auf Basis der jeweils durchgeführten Aktivitäten und geleisteten Hilfe wie folgt kategorisiert:

Analyse von Artefakten

Das CSIRT nimmt eine technische Prüfung und Analyse der in einem System festgestellten Artefakte vor. Diese Analyse könnte Folgendes umfassen: Identifizierung des Dateityps und der Struktur des Artefakts; Vergleich eines neuen Artefakts mit vorhandenen Artefakten oder anderen Versionen des gleichen Artefakts, um Ähnlichkeiten und Unterschiede zu erkennen; Rückentwicklung oder Disassemblierung des Codes, um den Zweck und die Funktion des Artefakts zu ermitteln.

Reaktion auf Artefakte

Bei diesem Dienst werden geeignete Maßnahmen zur Erkennung und Beseitigung von Artefakten aus einem System sowie Maßnahmen ausfindig gemacht, mit denen die Installation von Artefakten vermieden wird. Dazu zählt u. a. das Erstellen von Signaturen, die sich zu Virenschutzprogrammen oder IDS hinzufügen lassen.

Koordination der Reaktion auf Artefakte

Dieser Dienst umfasst die Synthese und den Austausch von artefaktspezifischen Analyseergebnissen und Reaktionsstrategien mit anderen Wissenschaftlern, CSIRT-Teams, Anbietern und sonstigen Sicherheitsexperten. Zu den Aktivitäten zählen die Benachrichtigung von Dritten und die Synthese der technischen Analyseergebnisse aus einer Vielzahl von Quellen. Bei diesen Aktivitäten kann auch die Pflege eines öffentlichen oder klienteleigenen Archivs über bekannte Artefakte und ihre Auswirkungen und entsprechende Reaktionsstrategien vorgesehen werden.

Proaktive Dienste

Mit proaktiven Diensten sollen die Infrastruktur und Sicherheitsabläufe der Klientel verbessert werden, bevor ein Vorfall oder Ereignis auftritt oder erkannt wird. Zu den vorrangigen Zielen zählen die Vermeidung von Vorfällen und die Verringerung ihrer Auswirkungen bzw. ihres Ausmaßes bei tatsächlichem Eintreten.

Bekanntgaben (Announcements)

Dazu zählen u. a. Warnhinweise auf mögliche Angriffe, Warnmeldungen über Sicherheitslücken und Security Advisories. Bei derartigen Bekanntgaben wird die Klientel über neue Entwicklungen mit mittel- bis langfristigen Auswirkungen informiert, beispielsweise über neu festgestellte Sicherheitslücken oder Angriffswerkzeuge. Auf Basis von Bekanntgaben kann die Klientel ihre Systeme und Netzwerke vor neu erkannten Problemen schützen, bevor sie ausgenutzt werden können.

Technologieüberwachung (Technology watch)

Das CSIRT überwacht und beobachtet neue technische Entwicklungen, Aktivitäten von Angreifern und zugehörige Trends, um zukünftige Risiken leichter erkennen zu können. Die geprüften Themengebiete können auf gesetzliche und legislative Bestimmungen, soziale oder politische Risiken sowie neue Technologien ausgedehnt werden. Dieser Dienst umfasst die Lektüre von sicherheitsspezifischen Mailinglisten und Websites sowie von aktuellen Zeitungs- und Zeitschriftenartikeln zu den Themenbereichen Wissenschaft, Technologie, Politik und Staatswesen, um sicherheitsrelevante Informationen für die Systeme und Netzwerke der Klientel zu extrahieren. Bei diesem Dienst kann auch die Kommunikation mit Dritten, d. h. mit Behörden vorgesehen werden, um eine optimale und möglichst genaue Unterrichtung oder Interpretation zu gewährleisten. Aus dieser Dienstleistung können Bekanntgaben, Richtlinien oder Empfehlungen hervorgehen, die sich eher mit mittel- oder langfristigen Sicherheitsproblemen befassen.

Sicherheitsaudits oder -analysen

Auf Basis der von einer Organisation oder durch andere gültige Industriestandards festgelegten Anforderungen bietet dieser Dienst eine detaillierte Prüfung und Analyse der Sicherheitsinfrastruktur der jeweiligen Organisation. Er kann auch eine Prüfung der organisationsinternen Sicherheitspraktiken umfassen. Dabei können unterschiedliche Audits (Prüfungen) oder Analysen vorgenommen werden, wie u. a.:

Prüfung der Infrastruktur

Dabei werden die Hardware- und Softwarekonfiguration, Router, Firewalls, Server und Desktopgeräte manuell geprüft, um zu gewährleisten, dass diese mit den organisationsinternen oder branchenspezifisch bewährten Sicherheitsrichtlinien und Standardkonfigurationen übereinstimmen.

Prüfung bewährter Verfahren

Mitarbeiter sowie System- und Netzwerkadministratoren werden befragt, um festzustellen, ob ihre Sicherheitspraktiken mit den organisationsintern festgelegten Sicherheitsrichtlinien oder bestimmten Industriestandards übereinstimmen.

Scannen

Dabei werden Sicherheits- oder Virenscanner verwendet, um festzustellen, welche Systeme und Netzwerke Sicherheitslücken haben.

Penetrationstests

Dabei wird die Sicherheit eines Standorts durch einen absichtlichen Angriff auf die zugehörigen Systeme und Netzwerke geprüft.
Für die Durchführung dieser Audits oder Bewertungen ist die Genehmigung der Geschäftsführung erforderlich. Aufgrund der organisationsinternen Richtlinien sind einige dieser Methoden u. U. untersagt. Dieser Dienst kann die Entwicklung einiger Verfahren, auf deren Grundlage die Prüfungen oder Bewertungen vorgenommen werden, sowie die Ausarbeitung der Qualifizierungs- und Zertifizierungsanforderungen für die Mitarbeiter umfassen, die die Tests, Bewertungen, Audits oder Prüfungen durchführen. Dieser Dienst könnte auch extern an einen Subunternehmer oder Sicherheitsdienstanbieter mit dem erforderlichen Fachwissen zur Durchführung solcher Audits und Bewertungen vergeben werden.

Konfiguration und Pflege von Sicherheitswerkzeugen, Anwendungen, Infrastrukturen und Diensten

Bei diesem Dienst sollen zweckdienliche Anweisungen zur sicheren Konfiguration und Pflege der Werkzeuge, Anwendungen und generellen Computerinfrastruktur gegeben werden, die bei der Klientel des CSIRT oder beim CSIRT selbst im Einsatz sind. Abgesehen von Anweisungen kann das CSIRT die Konfiguration von Sicherheitswerkzeugen und Diensten aktualisieren und pflegen, beispielsweise IDS, das Scannen von Netzwerken oder das Überwachen von Systemen, Wrappern, Firewalls, virtuellen privaten Netzwerken (VPN) oder Authentifzierungsmechanismen. Das CSIRT kann diese Dienste sogar im Rahmen ihrer Hauptfunktion anbieten. Außerdem kann das CSIRT Server, Desktops, Laptops, PDAs (persönliche digitale Assistenten) und andere drahtlose Geräte nach den Sicherheitsrichtlinien konfigurieren und pflegen. Dieser Dienst umfasst die Eskalierung von Problemen mit der Konfiguration oder Nutzung von Werkzeugen und Anwendungen an die Geschäftsführung, die die Sicherheit eines Systems nach Auffassung des CSIRT gefährden können.

Entwicklung von Sicherheitswerkzeugen

Dieser Dienst umfasst die Entwicklung von neuen, klientelspezifischen Werkzeugen, die nach Maßgabe der Klientel oder des CSIRT selbst erforderlich oder wünschenswert sind. Dazu zählt beispielsweise die Entwicklung von Sicherheitspatches für benutzerspezifische Software, die bei der Klientel im Einsatz ist, oder von Methoden für die sichere Verteilung von Software, die zur Wiederherstellung von gefährdeten Hosts angewandt werden können. Dieser Dienst kann auch die Entwicklung von Tools oder Skripten umfassen, mit denen sich die Funktionen vorhandener Sicherheitstools erweitern lassen, beispielsweise ein neues Plug-In (Zusatzmodul) für einen Sicherheits- oder Netzwerkscanner, Skripte zur leichteren Verwendung der Verschlüsselungstechnologie oder Mechanismen zur automatischen Patchverteilung.

Dienste für die Erkennung von Angriffsversuchen

CSIRT-Teams, die diesen Dienst anbieten, prüfen vorhandene IDS-Protokolle, analysieren und initiieren eine Gegenmaßnahme (Reaktion) auf Ereignisse, die ihren definierten Schwellenwert erreichen, oder leiten Warnhinweise nach einem vordefinierten SLA-Vertrag oder einer vordefinierten Eskalationsstrategie weiter. Die Erkennung von Angriffsversuchen und Analyse der zugehörigen Sicherheitsprotokolle kann eine schier unlösbare Aufgabe sein, und zwar nicht nur in Bezug auf die genaue Positionierung der Sensoren in der Umgebung, sondern auch in Bezug auf die Sammlung und anschließende Analyse der Vielzahl der erfassten Daten. Häufig sind für die Synthese und Interpretation der Daten spezielle Werkzeuge oder Fachkenntnisse erforderlich, um Fehlalarme, Angriffe oder Netzwerkereignisse erkennen und Strategien zur Beseitigung oder Verringerung dieser Ereignisse implementieren zu können. Einige Organisation entscheiden sich dafür, diese Aktivitäten im Wege des Outsourcing an Dritte zu vergeben, die mehr Erfahrung mit diesen Dienstleistungen haben, wie etwa Sicherheitsdienstanbieter.

Verteilung von sicherheitsrelevanten Informationen

Durch diesen Dienst verfügt die Klientel über eine umfassende und übersichtliche Sammlung von nützlichen Informationen, die zur Erhöhung der Sicherheit beitragen. Zu diesen Informationen zählen u. a.:

- Richtlinien für Berichte und Kontaktinformationen für das CSIRT
- Archive mit Alarm- und Warnmeldungen und sonstigen Bekanntgaben
- Dokumentation über aktuelle bewährte Verfahren
- Generelle Richtlinien für die Sicherheit von Computern
- Richtlinien, Verfahren und Prüflisten
- Patch-Entwicklung und Verteilung von Informationen
- Links zu Anbietern
- Aktuelle Statistiken und Trends bei der Berichterstattung über Vorfälle
- Sonstige Informationen zur Verbesserung der sicherheitsrelevanten Praktiken

Diese Informationen können vom CSIRT oder von einem anderen Bereich der Organisation oder des Unternehmens (IT-, Personal-, PR-Abteilung) entwickelt und veröffentlicht werden und Informationen aus externen Quellen, wie von anderen CSIRT-Teams, Anbietern und Sicherheitsexperten, einschließen.

Dienste für das Sicherheitsqualitätsmanagement

Dienste, die unter diese Kategorie fallen, beziehen sich nicht nur auf die Vorfallbehandlung oder CSIRT-Teams im Besonderen. Mit diesen allgemein anerkannten Diensten soll die Sicherheit einer Organisation insgesamt verbessert werden. Auf Basis der bei den oben beschriebenen reaktiven und proaktiven Diensten gesammelten Erfahrungen kann ein CSIRT neue Perspektiven für diese Qualitätsmanagementdienste eröffnen, die ansonsten nicht zur Verfügung stünden. Bei diesen Diensten sollen die Rückmeldungen und die bei der Reaktion auf Vorfälle, Sicherheitslücken und Angriffe gesammelten Erfahrungen berücksichtigt werden. Durch die Berücksichtigung dieser Erfahrungen bei den (unten beschriebenen) etablierten, herkömmlichen Diensten als Bestandteil des Sicherheitsqualitätsmanagementprozesses können die langfristigen Sicherheitsanstrengungen einer Organisation verbessert werden. Je nach Organisationsstruktur und Aufgabenbereich kann ein CSIRT diese

Dienste anbieten oder im Rahmen einer breiter angelegten Zusammenarbeit innerhalb der Organisation an diesen Diensten mitwirken.
Die nachstehenden Beschreibungen erläutern, wie sich das Fachwissen eines CSIRT auf diese Dienste für das Sicherheitsqualitätsmanagement förderlich auswirken kann.

Risikoanalyse

CSIRT-Teams können zu einer Wertschöpfung für die Risikoanalyse und -bewertung beitragen. Dadurch kann eine Organisation bzw. ein Unternehmen echte Risiken besser bewerten, die Risiken für den Informationsbestand (Assets) in qualitativer und quantitativer Hinsicht realistischer bewerten sowie Schutz- und Reaktionsstrategien besser beurteilen. CSIRT-Teams, die diese Dienstleistung anbieten, würden für neue Systeme oder Geschäftsabläufe entsprechende Risikoanalysen für die Informationssicherheit durchführen oder bei ihrer Durchführung behilflich sein oder Risiken für bzw. Angriffe auf die bei der Klientel vorhandenen Einrichtungen (Assets) und Systeme evaluieren.

Kontinuität des Geschäftsbetriebs und Planung der Wiederherstellung nach Notfällen

Auf Basis von früheren Ereignissen oder Zukunftsprognosen über neue Sicherheitsvorfälle oder -trends bergen Sicherheitsvorfälle zunehmend die Gefahr, dass der Geschäftsbetrieb ernsthaft gestört wird. Daher sollten die Erfahrungen und Empfehlungen von CSIRT-Teams bei der Planung berücksichtigt werden, wie man optimal auf derartige Vorfälle reagieren sollte, um die Kontinuität des Geschäftsbetriebs zu gewährleisten. CSIRT-Teams, die diese Dienstleistung anbieten, sind an der Planung zur Gewährleistung der Kontinuität des Geschäftsbetriebs und Wiederherstellung nach Notfällen aufgrund von Vorfällen und Angriffen beteiligt, die die Sicherheit von Computern gefährden.

Beratung in Sicherheitsfragen

CSIRT-Teams dienen als Ratgeber für bewährte Sicherheitsmethoden zur Gewährleistung des Geschäftsbetriebs der Klientel. Ein CSIRT, das diese Dienstleistung anbietet, ist an der Ausarbeitung von Empfehlungen oder eines Anforderungskatalogs für die Anschaffung, die Installation oder den Schutz neuer Systeme, Netzgeräte, Softwareanwendungen oder unternehmensinterner Geschäftsabläufe aktiv beteiligt. Diese Dienstleistung schließt Hilfestellung und Unterstützung bei der Entwicklung von Sicherheitsrichtlinien für das Unternehmen oder die Klientel ein. Sie kann auch Erklärungen oder Ratschläge gegenüber gesetzgebenden Körperschaften oder sonstigen Behörden umfassen.

Sensibilisierung des Sicherheitsbewusstseins

CSIRT-Teams können einen Informations- und Hilfebedarf aufseiten der Klientel erkennen, damit diese allgemein anerkannte Sicherheitsverfahren und organisationsinterne Sicherheitsrichtlinien besser einhalten kann. Eine stärkere Sensibilisierung des allgemeinen Sicherheitsbewusstseins der Klientel trägt nicht nur zu ihrem besseren Verständnis der Sicherheitsprobleme, sondern auch zu einem sichereren Geschäftsbetrieb bei. Dadurch lässt sich die Anzahl der erfolgreichen Angriffe verringern und die Wahrscheinlichkeit erhöhen, dass die Klientel Angriffe erkennt und meldet,

wodurch der Zeitaufwand für die Wiederherstellung verringert wird und Verluste auf ein Minimum reduziert oder gänzlich vermieden werden.
CSIRT-Teams, die diese Dienstleistung anbieten, suchen nach Möglichkeiten zur Sensibilisierung des Sicherheitsbewusstseins, indem sie Artikel, Poster, Newsletter, Websites oder andere Informationsquellen zur Erläuterung bewährter Sicherheitspraktiken und für Ratschläge zu Vorsichtsmaßnahmen entwickeln. Zu diesen Aktivitäten zählt auch die Planung von Sitzungen und Seminaren, bei denen die Klientel über laufende Sicherheitsverfahren und potenzielle Risiken für die organisationsinternen Systeme informiert wird.

Ausbildung/Schulung

Dieser Dienst umfasst die Bereitstellung von Informationen über Computersicherheitsprobleme im Rahmen von Seminaren, Workshops, Schulungskursen und Lernprogrammen für Klienten. Zu den Themen zählen u. a. Richtlinien für die Berichterstattung über Sicherheitsvorfälle, geeignete Reaktions- bzw. Gegenmaßnahmen, Werkzeuge für die Reaktion auf Sicherheitsvorfälle, Methoden zur Prävention von Sicherheitsvorfällen und sonstige Informationen, die zur Vermeidung, Erkennung und Meldung von und Reaktion auf Computersicherheitsverletzungen erforderlich sind.

Produktevaluierung oder -zertifizierung

Bei diesem Dienst kann das CSIRT Produktevaluierungen für Werkzeuge (Tools), Anwendungen oder sonstige Dienste durchführen, um die Sicherheit der Produkte und deren Konformität mit CSIRT- oder organisationsinternen Sicherheitsverfahren zu gewährleisten. Bei den geprüften Tools und Anwendungen kann es sich um Open Source- oder kommerzielle Produkte handeln. Abhängig von den in der Organisation oder im CSIRT gültigen Standards kann diese Dienstleistung in Form einer Evaluierung oder über ein Zertifizierungsprogramm erbracht werden.

A.3 Beispiele

Fiktives CSIRT

Schritt 0: Verstehen, was ein CSIRT ist

Bei diesem Beispiel soll das CSIRT Dienste für eine Einrichtung mittlerer Größe mit etwa 200 Mitarbeitern leisten. Die Einrichtung hat eine eigene IT-Abteilung und zwei weitere Niederlassungen im gleichen Land. Der IT-Bereich spielt eine wesentliche Rolle für das Unternehmen, da die IT-Systeme für die interne Kommunikation, das Datennetz und den elektronischen Geschäftsverkehr rund um die Uhr (24x7) verwendet werden. Die Einrichtung hat ein eigenes Netzwerk und verfügt über einen redundanten Internetanschluss über zwei verschiedene ISP (Internetdienstanbieter).

- -

Schritt 1: Startphase

In der Startphase wird das neue CSIRT als internes CSIRT geplant und soll Dienste für die Auftraggeberorganisation, die lokale IT-Abteilung und die Mitarbeiter anbieten. Ferner soll es die Behandlung IT-sicherheitsrelevanter Vorfälle zwischen den einzelnen Niederlassungen unterstützen und koordinieren.

- -

Schritt 2: Auswahl der richtigen Dienste

In der Startphase wird beschlossen, dass das neue CSIRT hauptsächlich auf die Erbringung der Hauptdienste für die Mitarbeiter ausgerichtet sein soll.

Es wird beschlossen, dass man nach Abschluss der Pilotphase eine Erweiterung der Dienstpalette um einige „Sicherheitsmanagementdienste“ in Erwägung ziehen könnte. Diese Entscheidung soll auf Basis der Rückmeldungen vonseiten der Pilotklienten und in enger Zusammenarbeit mit der Abteilung für Qualitätssicherung getroffen werden.

- -

Schritt 3: Analyse der Klientel und der geeigneten Kommunikationskanäle

Bei einer Brainstorming-Sitzung mit Schlüsselpersonen der Geschäftsführung und der Klientel werden genügend Daten für eine SWOT-Analyse zusammengestellt. Aufgrund dessen kommt man zu dem Schluss, dass die folgenden Hauptdienste erforderlich sind:

- Alarm- und Warnmeldungen
- Behandlung von Vorfällen (Analyse, Unterstützung bei der Reaktion und Koordination der Reaktion)
- Bekanntgaben

Es muss gewährleistet sein, dass die Informationen gut organisiert möglichst an einen Großteil der Klientel verteilt werden. Daher wird beschlossen, die Alarm- und Warnmeldungen und Bekanntgaben in Form von Security Advisories auf einer speziellen Website zu veröffentlichen und über eine Mailingliste zu verteilen. Das CSIRT ermöglicht E-Mail-Nachrichten, Telefonate und Faxmitteilungen für den Eingang von Berichten über Vorfälle. Für den nächsten Schritt wird ein einheitliches Webformular geplant.

Schritt 4: Festlegung des Aufgabenbereichs

Die Geschäftsführung des fiktiven CSIRT hat folgenden Aufgabenbereich festgelegt:
„Das fiktive CSIRT bietet den Mitarbeitern des Auftraggebers Informationen und Unterstützung zur Verringerung der Risiken von Computersicherheitsverletzungen sowie bei der Reaktion auf derartige Verletzungen bzw. Vorfälle, sobald diese eintreten."

Dadurch stellt das fiktive CSIRT klar, dass es ein internes CSIRT ist und dass seine Hauptaufgaben in der Behandlung IT-sicherheitsrelevanter Probleme bestehen.

- -

Schritt 5: Festlegung des Geschäftsplans

Finanzierungsmodell
Aufgrund der Tatsache, dass es sich um ein eBusiness-Unternehmen handelt, das rund um die Uhr (24x7) arbeitet und eine IT-Abteilung (24x7) hat, wird beschlossen, sämtliche Dienste während der Geschäftszeiten und Rufbereitschaft außerhalb der Geschäftszeiten anzubieten. Die Dienste sollen für die Klientel unentgeltlich geleistet werden, wobei die Möglichkeit, Dienste für externe Kunden anzubieten, während der Pilot- und Evaluierungsphase geprüft werden soll.

Ertragsmodell
Während der Start- und Pilotphase soll das CSIRT vom Auftrag gebenden Unternehmen finanziert werden. In der Pilot- und Evaluierungsphase soll eine zusätzliche Finanzierung erörtert werden, einschließlich der Möglichkeit, externen Kunden kostenpflichtige Dienste anzubieten.

Organisationsmodell
Da der Auftraggeber ein kleines Unternehmen ist, entscheidet man sich für das integrierte Modell.
Während der Geschäftszeiten sollen drei Mitarbeiter die Hauptdienste (Verteilung von Security Advisories sowie Behandlung/Koordination von Vorfällen) leisten.

Die IT-Abteilung des Unternehmens hat bereits adäquat qualifizierte Mitarbeiter. Mit dieser Abteilung wird vereinbart, dass das neue CSIRT bei Bedarf ad hoc Unterstützung anfordern kann. Auch die 2. Reihe von Technikern mit Rufbereitschaft kann in Anspruch genommen werden.
Das CSIRT-Hauptteam soll aus vier vollzeitbeschäftigten und fünf zusätzlichen CSIRT-Teammitgliedern bestehen, wovon ein Mitglied im wechselnden Schichtbetrieb zur Verfügung stehen soll.

Mitarbeiter
Der CSIRT-Teamleiter hat Erfahrung im Sicherheitsbereich und Support der 1. und 2. Ebene (1^{st} und 2^{nd} Level) und hat bereits im Krisenmanagement gearbeitet. Die anderen drei Teammitglieder sind Sicherheitsexperten. Die Teilzeitmitarbeiter im CSIRT-Team aus der IT-Abteilung sind Spezialisten für ihren jeweiligen Bereich der Unternehmens-infrastruktur.

Schritt 6: Nutzung des Büros und Richtlinien für die Informationssicherheit
Büroausstattung und -standort
Da in dem Auftrag gebenden Unternehmen bereits eine effiziente physische Sicherheit vorhanden ist, ist das CSIRT in dieser Hinsicht gut abgedeckt. Für die Kommunikation in Notfällen wird ein so genannter „War Room" (Einsatzbesprechungsraum) vorgesehen. Für die Verschlüsselungsunterlagen und vertraulichen Dokumente wird ein Safe angeschafft. Es wird eine separate Telefonleitung, einschließlich Zentrale, für die Hotline während der Geschäftszeiten und die Rufbereitschaft (über Mobiltelefon) außerhalb der Geschäftszeiten mit der gleichen Telefonnummer, eingerichtet.

Die vorhandenen Geräte und die unternehmenseigene Website können ebenfalls zur Bekanntgabe von CSIRT-bezogenen Informationen verwendet werden. Eine Mailingliste ist installiert und wird gepflegt, wobei ein beschränkter Teil für die Kommunikation unter den Teammitgliedern und mit anderen Teams vorgesehen ist. Alle persönlichen Daten der Mitarbeiter sind in einer Datenbank gespeichert; im Safe wird ein Ausdruck aufbewahrt.

Richtlinien
Da das CSIRT in ein Unternehmen mit vorhandenen Richtlinien für die Informations-sicherheit integriert ist, sind die entsprechenden Richtlinien für das CSIRT mit Unterstützung des unternehmenseigenen Rechtsberaters festgelegt worden.

- -

Schritt 7: Suche nach Kooperationsmöglichkeiten
Auf Basis des Verzeichnisses der ENISA wurden rasch einige CSIRT-Teams im gleichen Land ausfindig gemacht und kontaktiert. Für den neu eingestellten Teamleiter wurde ein Besuch bei einem dieser CSIRT-Teams arrangiert. Im Rahmen dieses Besuchs erfuhr er Näheres über nationale CSIRT-Aktivitäten und nahm an einer Sitzung teil.
Diese Sitzung erwies sich als äußerst nützlich, weil er Beispiele für Arbeitsmethoden sammeln konnte und weil ihm die Unterstützung einiger anderer Teams zugesichert wurde.

- -

Schritt 8: Förderung des Geschäftsplans

Es wird beschlossen, Zahlen und Fakten aus der Vergangenheit des Unternehmens zu sammeln, was wirklich sehr nützlich ist, um sich einen statistischen Überblick über die Sicherheitssituation im IT-Bereich zu verschaffen. Diese Datenerfassung soll nach Einrichtung des CSIRT fortgesetzt werden, damit die statistischen Daten immer auf dem neuesten Stand sind.

Andere nationale CSIRT-Teams wurden kontaktiert und zu ihren Geschäftsfällen befragt. Durch die Zusammenstellung von Folien mit Informationen über die jüngsten Entwicklungen bei IT-Sicherheitsvorfällen und über die Kosten dieser Vorfälle leisteten diese CSIRT-Teams Unterstützung.

Bei diesem Beispielfall mit dem fiktiven CSIRT musste die Unternehmensführung nicht von der Bedeutung des IT-Bereichs überzeugt werden. Daher war es nicht schwierig, die Genehmigung für den ersten Schritt zu erhalten. Es wurden ein Geschäftsfall und ein

Projektplan ausgearbeitet, einschließlich der geschätzten Einrichtungs- und Betriebskosten.

- -

Schritt 9: Festlegung der Arbeitsabläufe und der betriebsspezifischen und technischen Verfahren

Das fiktive CSIRT konzentriert sich auf seine Hauptdienste:

- Alarm- und Warnmeldungen
- Bekanntgaben
- Behandlung von Sicherheitsvorfällen

Das Team hat gut funktionierende und für jedes Teammitglied leicht verständliche Verfahren entwickelt. Das fiktive CSIRT hat auch einen Rechtsexperten eingestellt, der sich mit Haftungsfragen und den Richtlinien für die Informationssicherheit befassen soll. Ferner hat das Team einige nützliche Werkzeuge verwendet und durch die Diskussion mit anderen CSIRT-Teams hilfreiche Informationen über betriebsspezifische Fragen erhalten.

Es wurde eine (feste) Vorlage für Security Advisories und Vorfallberichte erstellt. Das Team verwendet RTIR (**R**equest **T**racker for **I**ncident **R**esponse) zur Behandlung von Vorfällen.

- -

Schritt 10: Ausbildung und Schulung der Mitarbeiter

Das fiktive CSIRT beschließt, alle technischen Fachkräfte für die nächsten TRANSITS-Seminare anzumelden. Ferner soll der Teamleiter am CERT/CC-Seminar *Führung eines CSIRT* teilnehmen.

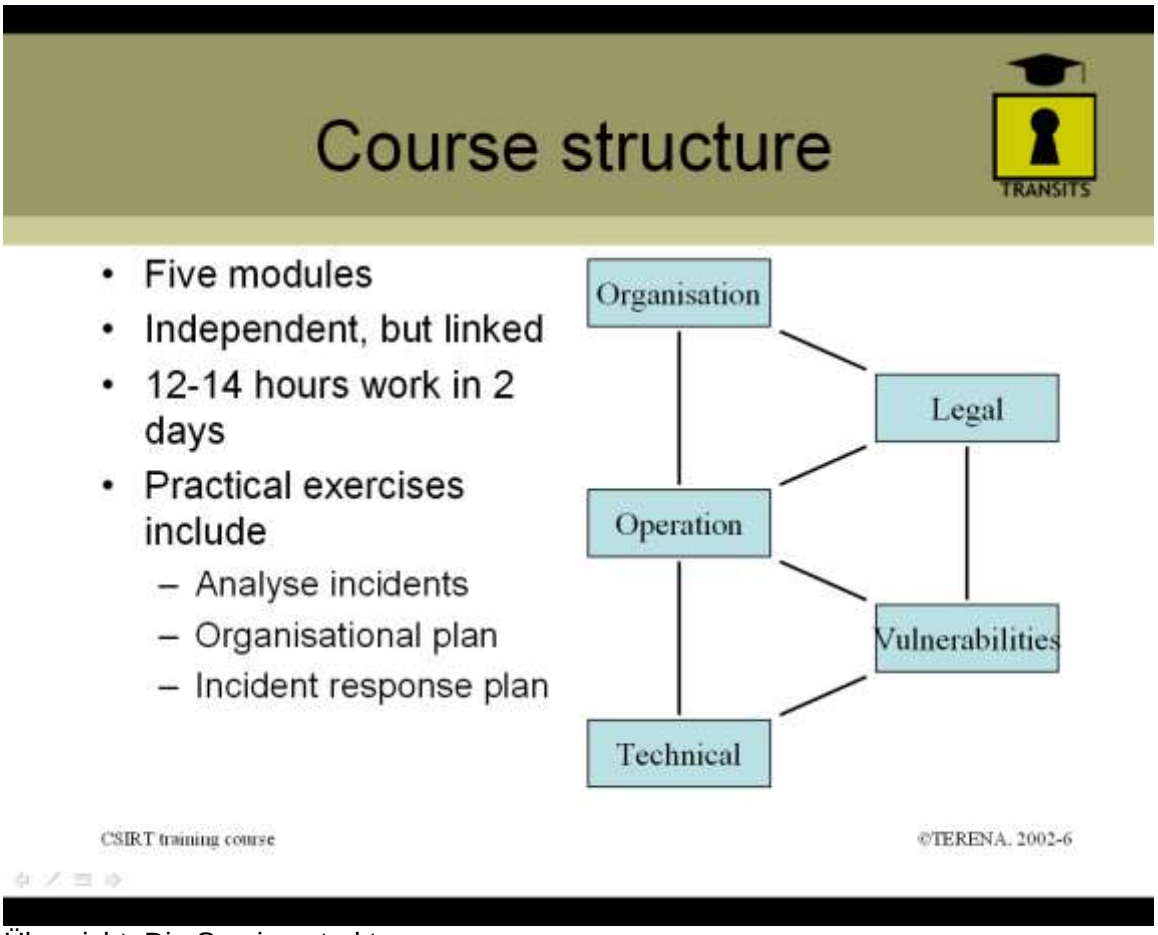
- -

Schritt 11: Praktische Übungen

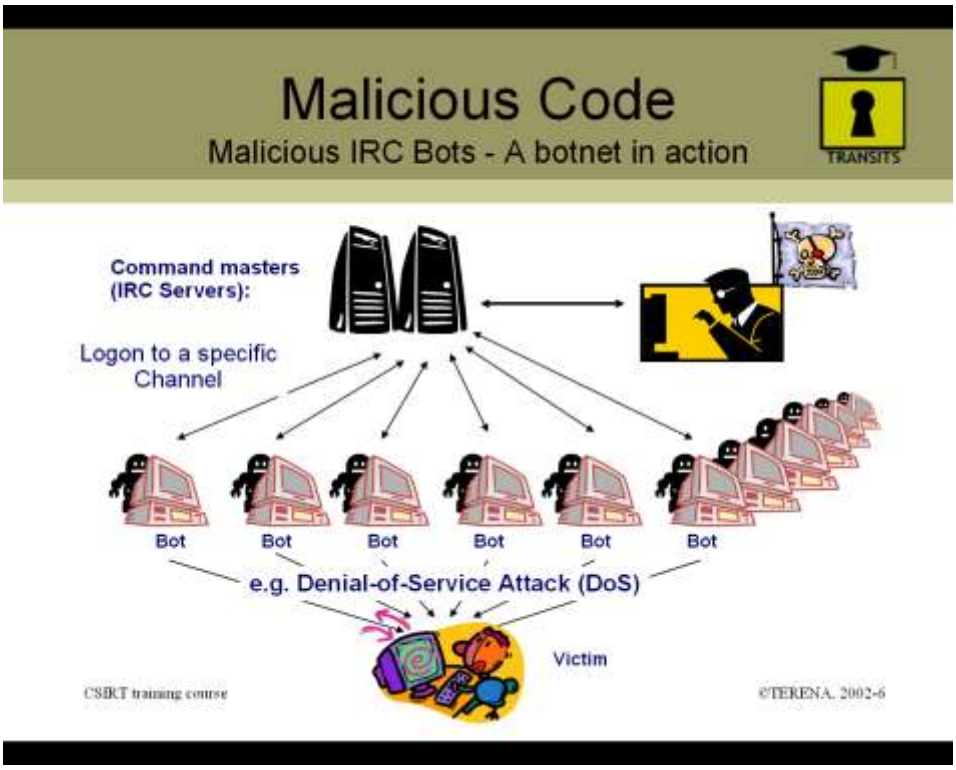
In den ersten Wochen nach Aufnahme seines Dienstes verwendet das fiktive CSIRT einige fiktive Fallbeispiele (von anderen CSIRT-Teams) für praktische Übungen. Außerdem werden einige Security Advisories auf Basis der von den Hardware- und Softwareanbietern verteilten Informationen über Sicherheitslücken und Schwachstellen nach Anpassung an die Bedürfnisse der Klientel veröffentlicht.

A.4 Musterunterlagen aus CSIRT-Seminaren

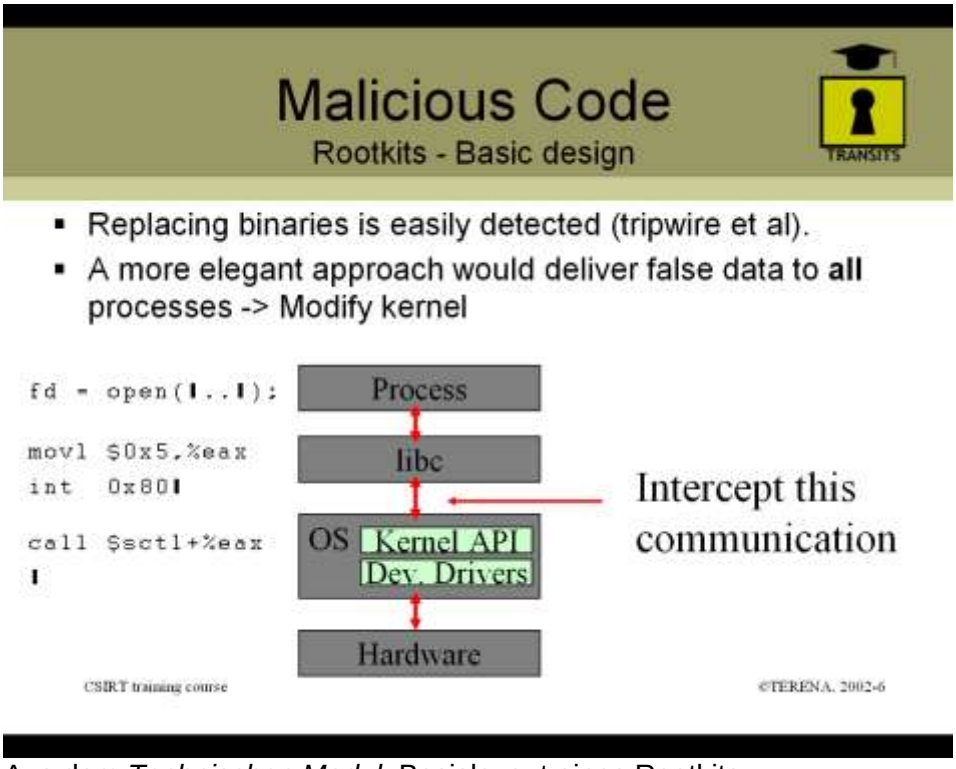
TRANSITS (mit freundlicher Genehmigung von Terena, http://www.terena.nl)



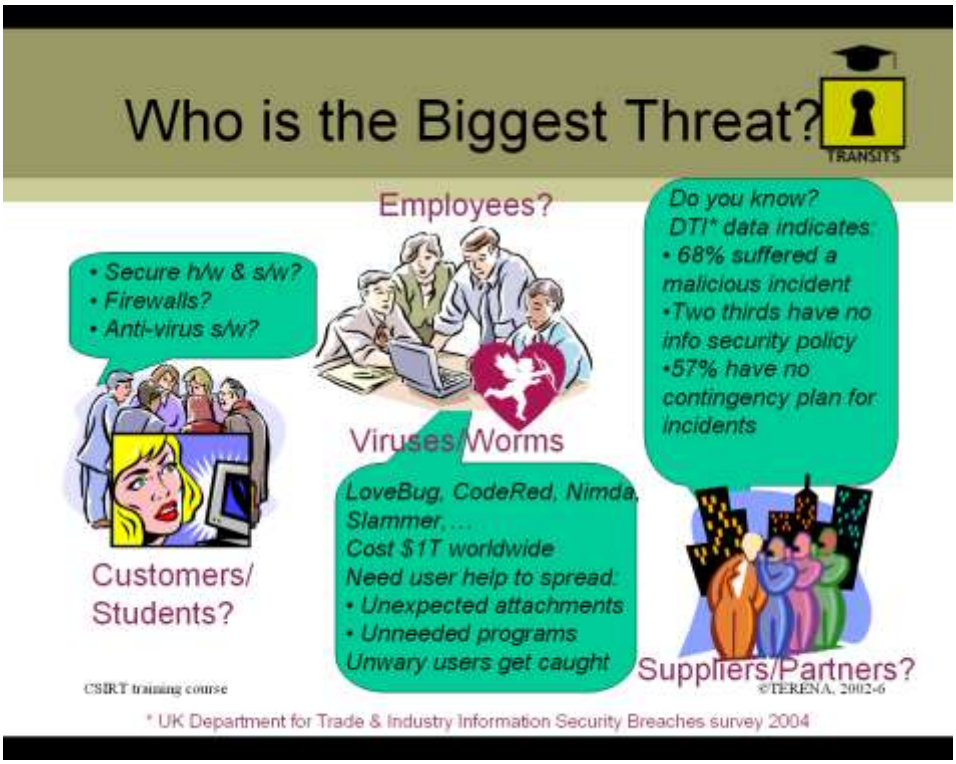
Übersicht: Die Seminarstruktur



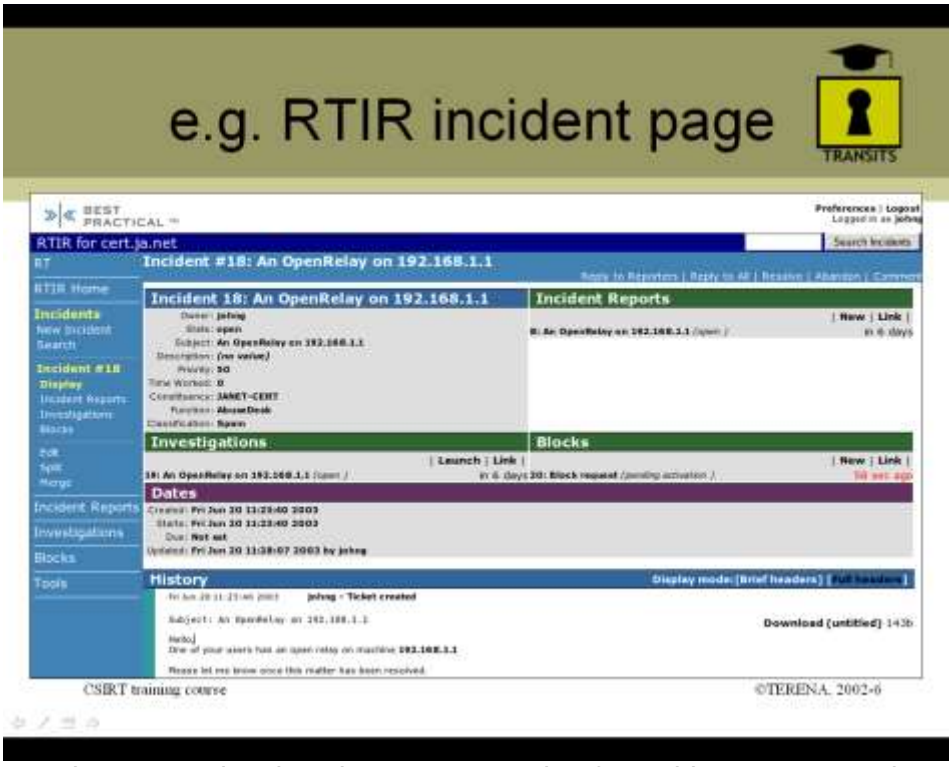
Aus dem *Technischen Modul*: Beschreibung eines Botnet



Aus dem *Technischen Modul*: Basislayout eines Rootkits



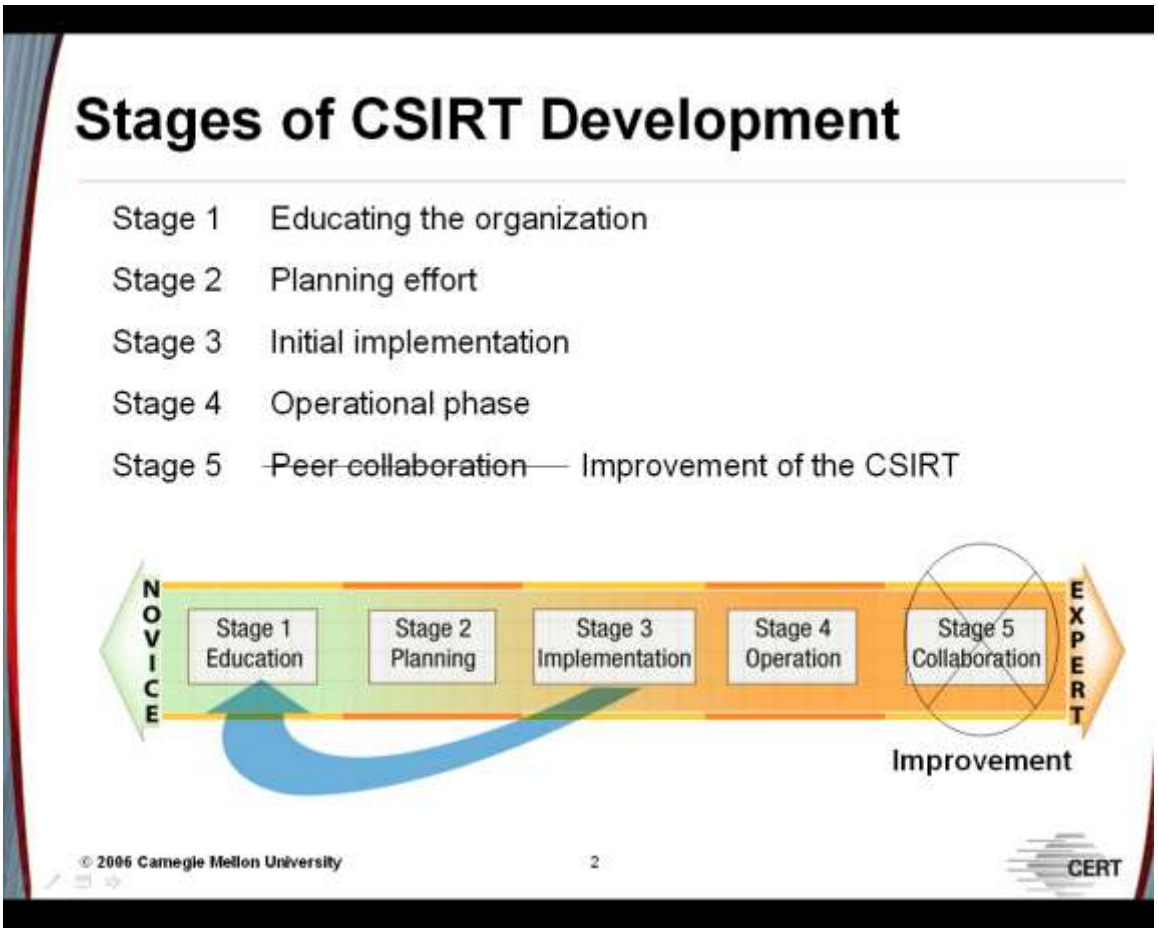
Aus dem *Organisatorischen Modul*: Insider oder Outsider – worin besteht die größte Gefahr?



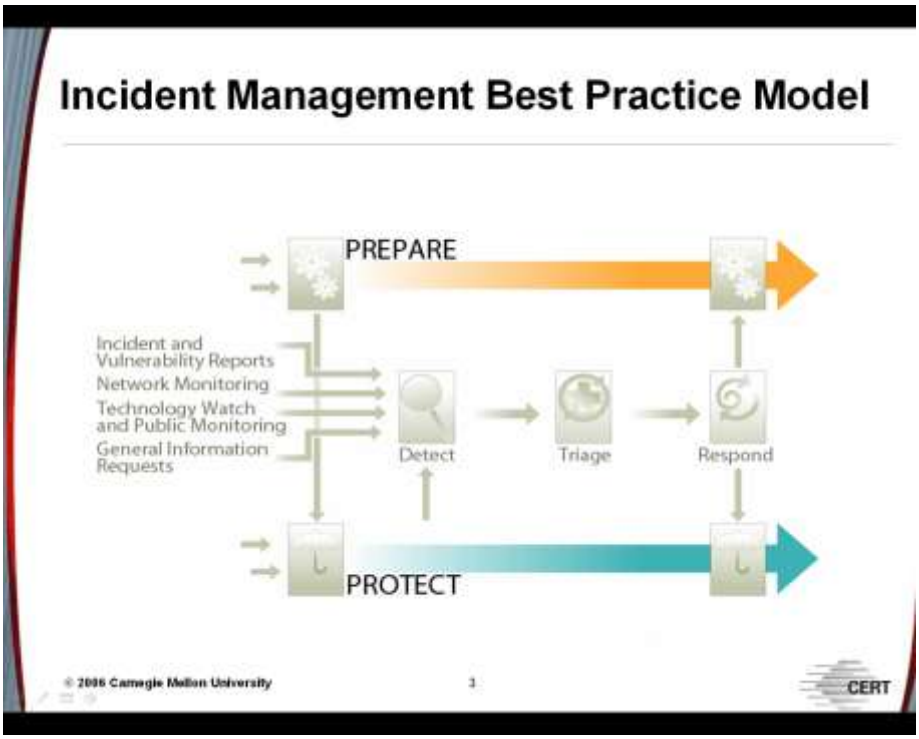
Aus dem *Operational track*: Request Tracker for Incident Response (RTIR)

„Einrichtung von CSIRT-Teams“ (mit freundlicher Genehmigung vom CERT/CC, http://www.cert.org)

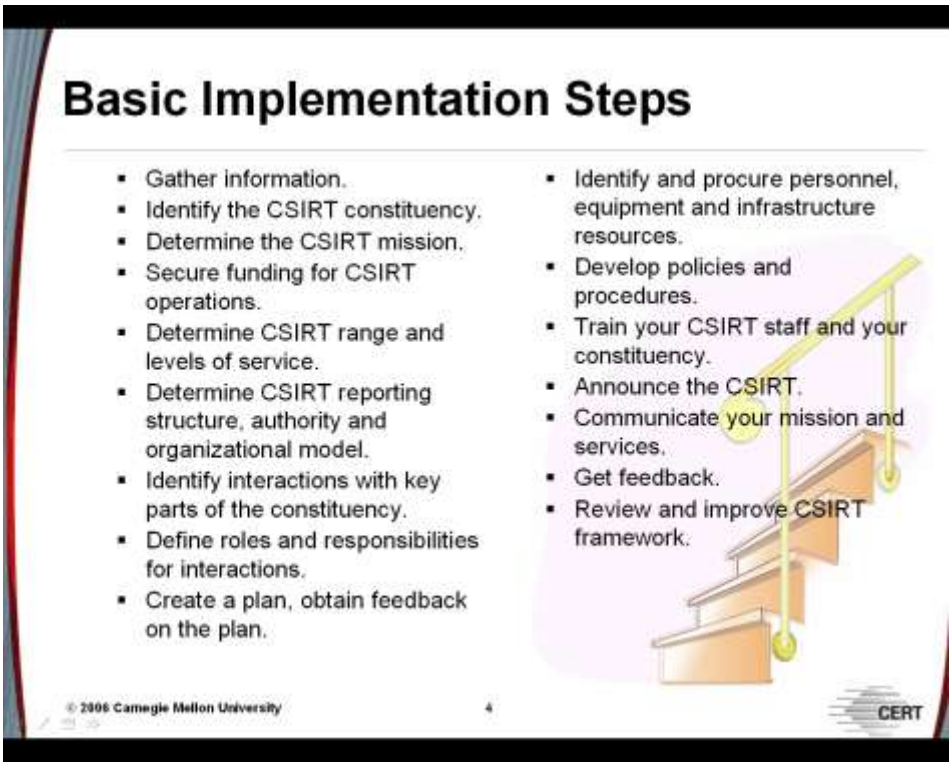
Die ENISA dankt dem CSIRT Development Team beim CERT-Programm für die freundliche Genehmigung, den Inhalt ihrer Schulungskurse verwenden zu dürfen!



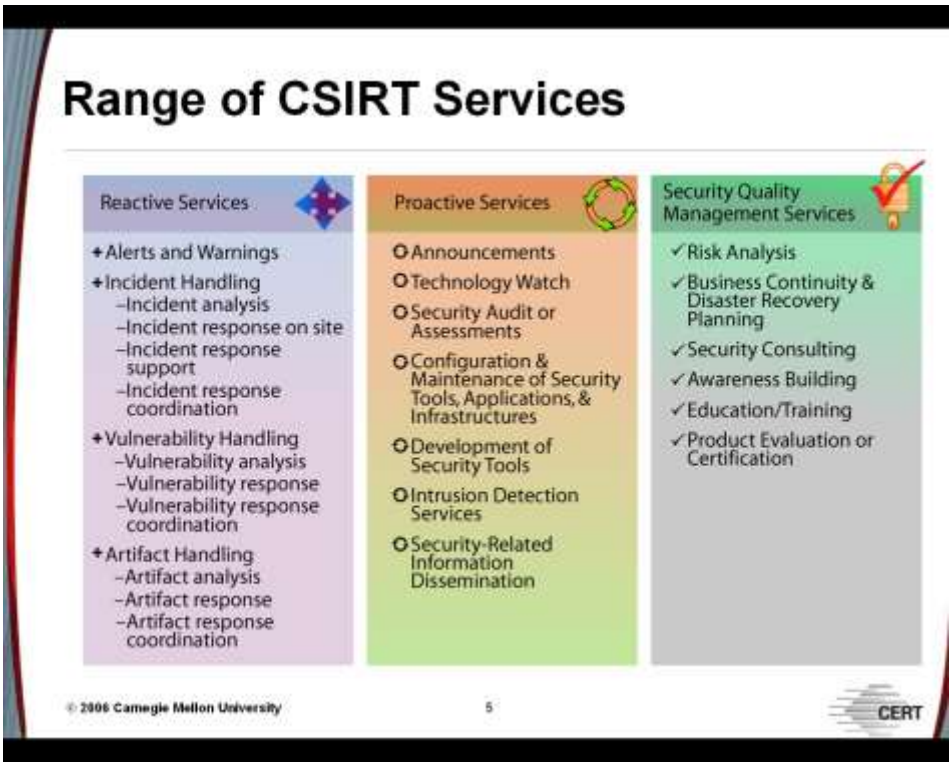
Aus dem *CERT/CC-Schulungsseminar:* Phasen bei der Einrichtung eines CSIRT



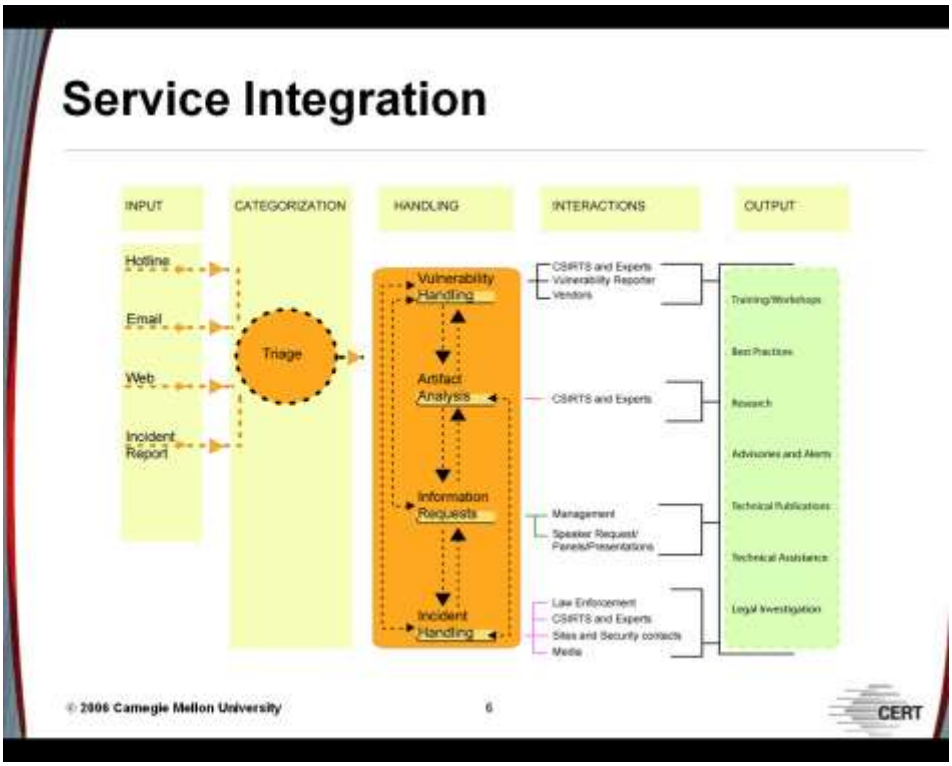
Aus dem *CERT/CC-Schulungsseminar*: Bewährte Verfahren bei der Behandlung von Sicherheitsvorfällen



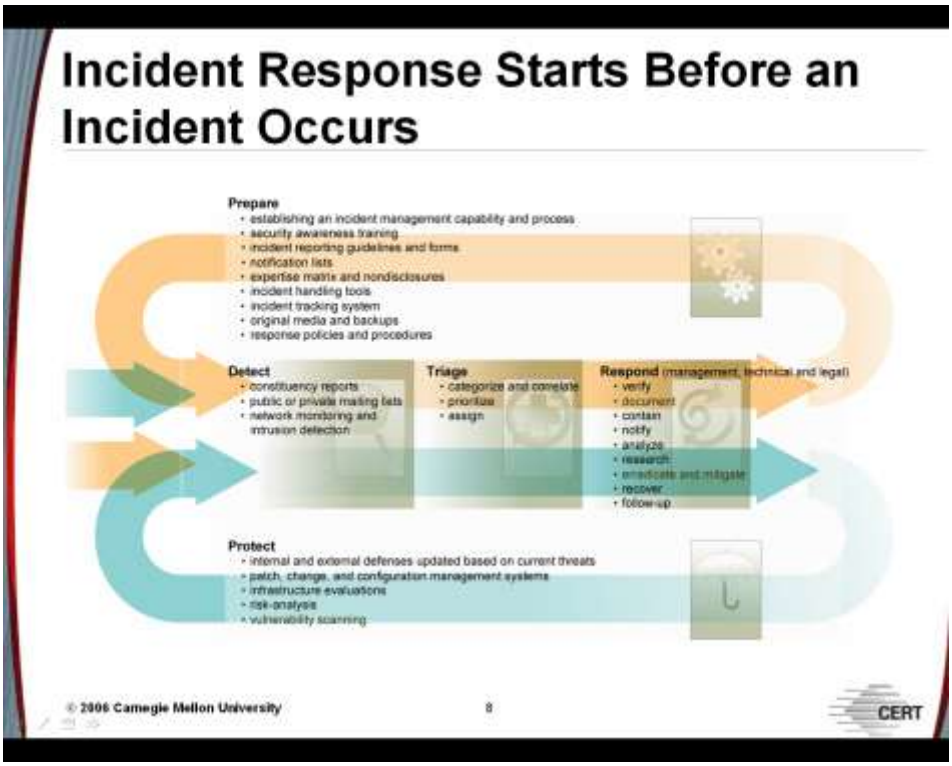
Aus dem *CERT/CC-Schulungsseminar*: Bei der Einrichtung eines CSIRT zu beachtende Schritte



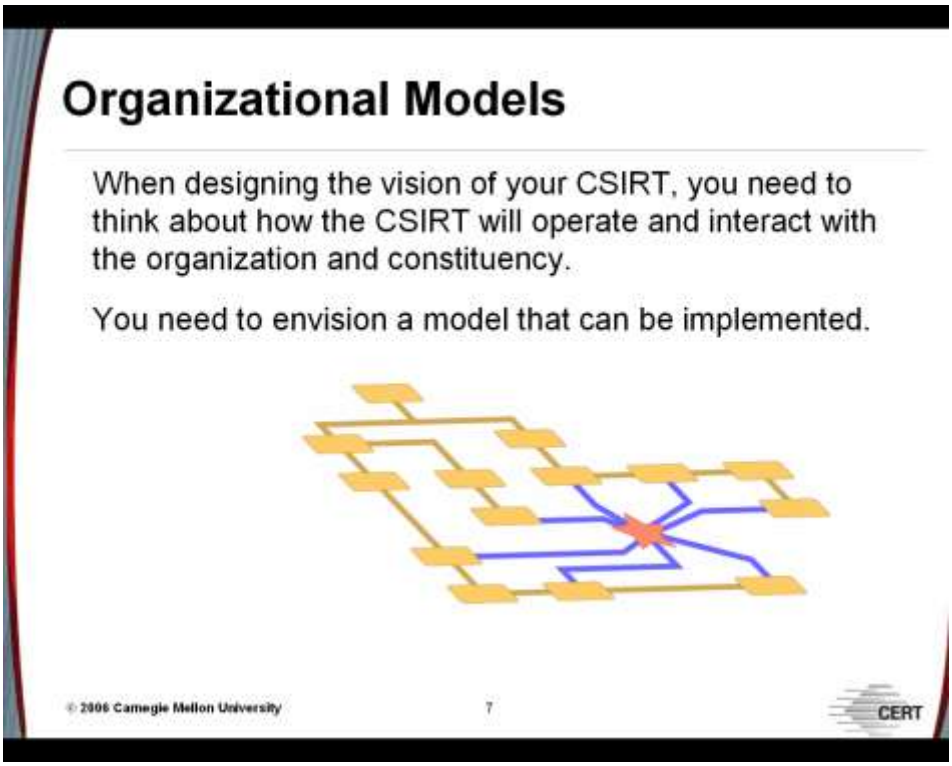
Aus dem *CERT/CC-Schulungsseminar:* Die von einem CSIRT angebotenen Dienstleistungen



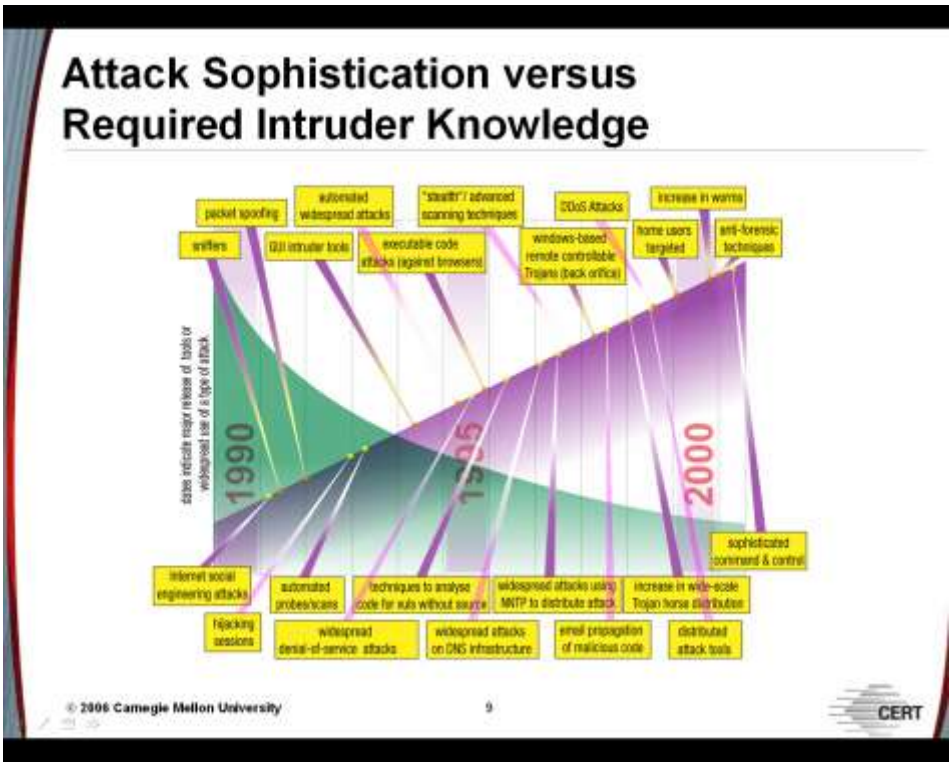
Aus dem *CERT/CC-Schulungsseminar:* Arbeitsablauf bei der Vorfallbehandlung



Aus dem *CERT/CC-Schulungsseminar:* Reaktion auf Sicherheitsvorfälle



Aus dem *CERT/CC-Schulungsseminar:* Organisation des CSIRT



Aus dem *CERT/CC-Schulungsseminar:* Geringeres Wissen, größerer Schaden