组建 CSIRT 的分步指南

包括以项目计划为形式的实例和核对清单

可交付项 WP2006/5.1(CERT-D1/D2)

索引

1. 管理摘要

即将推出的本文档描述的是组建计算机网络安全应急小组 (Computer Security and Incident Response Team, CSIRT) 的全过程，涉及业务管理、流程管理和技术层面的所有相关方面。本文档实施的两个交付件在欧洲网络与信息安全局 (ENISA)《2006 年工作程序》第 5.1 章中描述：

- 本文档：*有关如何组建计算机紧急事务响应小组 (CERT) 或类似机构的分步指南书面报告，包括实例*。(**CERT-D1**)
- 第 12 章及外部文件：*分列的路线图摘录，在实践中实现轻松应用路线图。* (**CERT-D2**)

2. 法律声明

敬请注意，除非另有说明，否则本出版物仅代表作者和编辑的观点和解释。除非依据 ENISA 第 460/2004 (EC) 号条例被采纳，否则，本出版物的内容不应被视为 ENISA 或 ENISA 机构的行动。本出版物并不一定代表最新技术发展水平，可能随时更新。

会酌情引用第三方资源。ENISA 对外部资源，包括本出版物中引用的外部网站的内容不承担任何责任。

本出版物仅为培训和信息参考目的使用。ENISA 或代表其行事的任何人均对本出版物所含信息的使用不承担责任。

3. 致谢

ENISA 在此向所有为本文档做出努力的机构和个人表示衷心的感谢。在此需要对以下各方特别说声“谢谢”：

- Henk Bronk，制作第一版文档时担任顾问。
- CERT/CC，特别是 CSIRT 开发团队，为我们提供了宝贵的资料，以及附录中的课程实例资料。
- GovCERT.NL，为我们提供了 CERT-in-a-box。
- TRANSITS 团队，为我们提供了附录中的课程实例资料。
- 技术部门负责安全政策的同事，为我们提供了第 6.6 章。
- 所有审阅评述本文档的人们。

4. 简介

通信网络和信息系统已经成为经济与社会发展中必不可少的基本要素。计算机化和网络化如今已象水、电供应一样走进千家万户，成为无处不在的公用事业。

通信网络和信息系统的安全性，尤其是其可用性也因此成为社会越来越关注的问题。之所以关注是因为关键信息系统有出现故障的风险，这主要归因于系统的复杂性、偶发事故、系统错误以及实体基础设施的易受攻击性，而欧盟各国居民的安乐生活又离不开这一切提供的服务。

于是，2004 年 3 月 10 日，欧洲网络和信息安全局 (ENISA) 应运而生[1]。其目的是确保共同体内部的网络与信息安全保持在高效率、高水平，并发展成为有利于欧盟各国居民、消费者、企业和公共部门机构利益的网络和信息安全文化，为内部市场的平稳发展作出贡献。

多年来，欧洲若干安全团体，如 CERT/CSIRT、禁滥用小组 (Abuse Team) 和 WARP 等一直通力合作以求营造更加安全的互联网环境。ENISA 提供确保适当服务质量水准的措施方面的信息，其目的是为这些团体的工作提供支持。进而，ENISA 有意加强自身的能力，就如何为具体的 IT 用户组提供恰当的安全服务的问题为欧盟成员国及欧盟机构提供建议。因此，“CERT 合作与支持”这支成立于 2005 年的特设工作组将在调查研究的基础上处理有关问题，希望能够为特定（类别或组别下的）用户提供充分的安全服务（“CERT 服务”）。

ENISA 希望凭借发布此份 ENISA 《组建 CSIRT 分步指南（含补充核对清单）》报告书对组建新 CSIRT 提供必要的支持。

[1] 欧洲议会和欧盟理事会第 460/2004 (EC) 号条例：关于成立欧洲网络和信息安全局（2004 年 3 月 10 日）。由欧盟设立的“欧洲共同体代理处”，在欧盟“共同体领域”（第一层保障）内执行具体的技术、科学或管理任务。

4.1. 目标受众

本报告的主要目标群体是以保护自有或其利益相关各方所拥有的 IT 基础设施为目的，决定组建 CSIRT 的政府和其他机构。

4.2. 本文档的使用方法

本文档提供的信息涉及什么是 CSIRT、可提供的服务以及开始组建的必要步骤。本文档将使读者对组建 CSIRT 的方法、CSIRT 结构和内容有充分的、实用的综合概览。

第 4 章“简介”
介绍本报告

第 5 章“计划和组建 CSIRT 的总体策略”
第一部分描述什么是 CSIRT。同时提供有关适合 CSIRT 工作的不同环境和小组可以提供的服务的信息。

第 6 章“制定业务计划”
本章描述的是组建过程中的业务管理方法。

第 7 章“推进业务计划”
本章阐述的是业务案例和资金问题。

第 8 章“操作和技术程序实例”
本章描述的是获取信息并将其转换为安全公告的过程。本章同时提供对意外事件处理工作流程的描述。

第 9 章“CSIRT 培训”
本章汇总了一系列可用的 CSIRT 培训。图解课程实例资料在附录中提供。

第 10 章“练习：制定一份安全建议”
本章包含如何履行基本（或核心） CSIRT 服务的练习：制定安全公告（或建议）。

第 12 章“项目计划描述”
本章针对的是与本指南一起提供的补充项目计划（核对清单）。本计划旨在作为实施本指南可用的简单易用的工具。

4.3. 本文档中所用惯例

为了指导读者使用本文档，每一章在开始处都会总结在组建 CSIRT 过程中业已采取的步骤。这些总结将列在框中，如下所示：

我们已经采取第一步

每一章将以所论及步骤的实践范例结束。在本文档中，“虚构 CSIRT”指的是一家中型企业或机构的小型独立的 CSIRT。汇总在附录中提供。

虚构 CSIRT

5. 计划和组建 CSIRT 的总体策略

为保证成功开始组建 CSIRT 的过程，清楚了解团队能为客户（在 CSIRT 业内称为“用户群”）提供的服务是十分必要的。因此，要在恰当的时机、以恰当的品质提供恰当的服务，就有必要理解用户群的确切需求是什么。

5.1. 什么是 CSIRT？

CSIRT 代表的是计算机网络安全应急小组 (Computer Security Incident Response Team)。CSIRT 一词主要用在欧洲，等同于 CERT 协调中心 (CERT/CC) 在美国注册的受保护术语 CERT。
目前，此类团队有多种不同的缩写：

- CERT 或 CERT/CC（计算机紧急事务响应小组/协调中心）
- CSIRT （计算机网络安全应急小组）
- IRT（即时事件响应小组）
- CIRT（计算机即时事件响应小组）
- SERT（安全应急响应小组）

全球 IT 基础设施首次蠕虫病毒大爆发发生在二十世纪八十年代末期。该蠕虫病毒被命名为莫里斯[2]，在世界范围内迅速传播，很快感染了大量 IT 系统。

这次事件就是一个提醒信号：突然间，人们意识到在处理类似案例时系统管理员与 IT 经理间急需合作与协调。由于时间是关键因素，必须确立一种组织性、结构性更强的方式处理 IT 安全事件。因此，“莫里斯事件”过后不久，美国国防部高级研究计划署 (Defence Advanced Research Projects Agency, DARPA) 便成立了第一个 CSIRT：计算机紧急事务响应小组协调中心 (CERT/CC[3])，位于宾夕法尼亚匹兹堡市的卡内基梅隆大学。

这种模式很快传遍欧洲，1992 年，荷兰服务于高等教育和研究的国家电脑网络 SURFnet 推出了欧洲第一个 CSIRT，命名为 SURFnet-CERT[4]。随后很多类似的团队涌现出来，现在，列在 ENISA “欧洲 CERT 活动清单”[5] 中的欧洲已知的团队已然过百。

多年来，CERT 从单一的响应小组发展壮大成为完善的安全服务提供商，能够提供预防性服务，如警报、安全建议、培训和安全管理等。“CERT” 一词很快便显得不够精确了。于是，二十世纪九十年代末，“CSIRT”，即计算机网络安全应急小组一词应运而生。现在，两个术语（CERT 和 CSIRT）作为同义词使用，只不过 CSIRT 更为精确。

5.1.1. 术语“服务对象”

从现在起，（在 CSIRT 团体内）已广泛确立的术语“服务对象”将专指 CSIRT 的用户群。一个单一客户将称为“用户”，一组客户则称为“用户群”。

[2] 有关莫里斯蠕虫病毒的更多信息，请访问 http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC，http://www.cert.org

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

[5] ENISA 清单 http://www.enisa.europa.eu/ENISA%20CERT/index.htm

5.1.2. CSIRT 的定义

CSIRT 是一支由 IT 安全专家组成的团队，主要业务就是对电脑安全事件做出响应。为处理相关问题提供必要服务，并支持其用户群从破坏中恢复。

为了降低风险并将所需响应数降至最低，多数 CSIRT 还为其用户群提供预防措施和培训服务。他们针对使用中的软件和硬件中的漏洞发布建议，并将这些利用漏洞的攻击和病毒通知用户。这样，用户群可以快速安装补丁并更新系统。参见第 5.2 章“可以提供的服务项目”了解所有能够提供的服务。

5.1.3. 拥有 CSIRT 的好处

拥有一支专业的 IT 安全团队能帮助组织降低风险并预防发生重大事件，可保护组织的宝贵财产不受损失。

可获得的其他好处包括：

- 在组织内部（接触点，PoC）集中协调 IT 安全问题。
- 集中专门处理及响应 IT 事件。
- 唾手可得的专业知识可支持与辅助用户快速从安全事件中恢复。
- 在发生法律诉讼时，处理法律问题并保全证据。
- 随时跟踪安全领域中的开发成果。
- 鼓励服务对象就 IT 安全性进行合作（培养安全意识）。

虚构 CSIRT（步骤 0）
理解什么是 CSIRT： 作为实例的 CSIRT 将为一家由 200 名员工组成的中型机构服务。该机构有其自己的 IT 部门，并在同一个国家拥有另外两处分支机构。IT 在公司内扮演着绝对重要的角色，内部通讯、数据网络和全天候电子商务全都离不开 IT。该机构拥有自己的网络，通过两家不同的 ISP 配置冗余连接到互联网。

5.1.4. 不同类型的 CSIRT 环境描述

我们已经采取第一步 1. 理解什么是 CSIRT 及其能够带来的好处。 >> 下一步要回答问题：“CSIRT 将向哪些领域提供服务？”

当启动 CSIRT（就象启动其他业务一样）时，尽快明确用户群是谁、CSIRT 服务所针对的环境有哪些等问题是非常重要的。到目前为止，我们归纳出以下几类，按字母顺序排列：

- 学术领域 CSIRT
- 商业领域 CSIRT
- CIP/CIIP 领域 CSIRT
- 政府领域 CSIRT
- 内部 CSIRT
- 军事领域 CSIRT
- 国家 CSIRT
- 中小企业 (SME) CSIRT
- 供应商 CSIRT

学术领域 CSIRT
焦点
学术领域 CSIRT 为学术和教育机构，如大学或研究机构及其校园互联网环境提供 CSIRT 服务。

用户群
此类型的 CSIRT 的典型用户群是大学的教职员工及学生。

商业领域 CSIRT
焦点
商业 CSIRT 为其用户群提供商业上的 CSIRT 服务。就 ISP 而言，CSIRT 主要为终端用户的客户提供防滥用服务（拨号入网，ADSL）并为其专业客户提供 CSIRT 服务。

用户群
商业 CSIRT 通常为付费用户群提供服务。

CIP/CIIP 领域 CSIRT

焦点

该领域的 CSIRT 主要关注关键信息保护 (Critical Information Protection) 和（或）关键信息和基础设施保护 (Critical Information and Infrastructure protection)。在多数情况下，此类专项 CSIRT 会与政府 CIIP 部门紧密合作。该 CSIRT 涵盖一个国家全部关键 IT 领域并保护该国公民的 IT 使用安全。

用户群

政府、关键的 IT 企业、公民

政府领域 CSIRT

焦点

政府 CSIRT 为政府机构，在部分国家也会为其公民提供服务。

用户群

政府和政府相关机构、在部分国家还为公民（如在比利时、匈牙利、荷兰、英国或德国）提供警报服务。

内部 CSIRT

焦点

内部 CSIRT 仅为其托管组织提供服务。这里描述的更多是职能作用而不是领域。例如很多电信组织和银行都有其自己内部的 CSIRT。他们通常不为公众维护网站。

用户群

托管组织的内部员工和 IT 部门。

军事领域 CSIRT

焦点

该领域的 CSIRT 为军事组织提供服务，负责国防所需的 IT 基础设施。

用户群

军事机构或密切相关机构，如国防部的员工。

国家 CSIRT

焦点

以国家为重点的 CSIRT 一般被认为是一个国家的安全接触点。在某些情况下，政府 CSIRT 同时担任国家的接触点（如英国的 UNIRAS）。

用户群

此类 CSIRT 通常没有直接的用户群，国家 CSIRT 一般仅在整个国家起着中间媒介作用。

中小企业 (SME) CSIRT

焦点

自组 CSIRT，为企业自身的业务分支或类似用户组提供服务。

用户群

这些 CSIRT 的用户群可能是中小企业及其员工，或特殊利益团体，如一个国家的“城镇和市政协会”。

供应商 CSIRT

焦点

供应商 CSIRT 重点关注对特定于供应商的产品的支持。其目标通常是开发并提供解决方案，帮助消除漏洞以及漏洞可能造成的潜在负面影响。

用户群

产品所有者

与在上文国家 CSIRT 中描述的类似，一个团队可能服务于多个领域。这对（举例而言）服务对象及其需求的分析会产生影响。

虚构 CSIRT（步骤 1）
启动阶段 在启动阶段，新 CSIRT 计划作为内部 CSIRT，为托管公司、其在当地的 IT 部门和员工提供服务。同时还为不同办事处之间的 IT 安全相关事件的处理提供支持和协调。

5.2. CSIRT 可以提供的服务

我们已经采取前两个步骤

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？

>> 下一步将要回答问题：“将向用户群提供哪些服务。”

CSIRT 可提供多种服务，但到目前为止还没有一支现有的 CSIRT 能够提供全部服务。因此，选择适当的服务就成为至关重要的决策。以下，您将看到由 CERT/CC 发布的“CSIRT 手册”中定义的所有已知 CSIRT 服务的一个简短概述[6]。

[6] CERT/CC CSIRT 手册 http://www.cert.org/archive/pdf/csirt-handbook.pdf

响应式服务	**主动服务**	**人工因素处理**
• **警报和警告** • **事件处理** • **事件分析** • **事件响应支持** • **事件响应协调** • 事件现场响应 • 漏洞处理 • 漏洞分析 • 漏洞响应 • 漏洞响应协调	• **通告** • 技术简报 • 安全监察或评估 • 安全配置和维护 • 安全工具的开发 • 入侵检测服务 • 安全相关的信息发布	• *人工因素分析* • *人工因素响应* • *人工因素响应协调* **安全质量管理** • *风险分析* • *业务持续性和灾难恢复* • *安全咨询* • *培养安全意识* • *教育培训* • *产品评估或认证*

图表. 1 CERT/CC 的 CSIRT 服务列表[7]

核心服务（以粗体标注）：响应式服务和主动服务之间是有区别的。主动服务旨在通过安全意识的建立与培训来预防事件的发生，而响应式服务则旨在处理事件并减少事件造成的损失。

人工因素处理则包含对系统中所发现的文件或对象的分析，这些文件或对象可能涉及恶意攻击行为，如残留的病毒、蠕虫、脚本、特洛伊木马等。同时，还包括对结果信息进行处理并发布给供应商和其他相关各方，以防止恶意软件的进一步传播并降低风险。

安全和质量管理服务则是具有长期目标的服务，包括咨询服务和培训措施。

有关 CSIRT 服务的详尽解释请参见附录。

为用户群选择正确的服务是极其重要的一步，我们在第 6.1 章“定义财务模式”中会进一步谈及。

多数 CSIRT 以发布“警报和警告”为开端，为其用户群发布“通告”并提供“事件处理”。这些核心服务通常会在服务对象中树立良好形象并获得相当的关注值，一直被视为真正的“增值”。

习惯做法是以一小组用户群为“试点”，在试点期间开始为其提供核心服务，事后要求提供反馈。
感兴趣的试点用户通常会提供有建设性的反馈并帮助开发定制服务。

[7] CERT/CC 提供的 CSIRT 服务列表：http://www.cert.org/csirts/services.html

虚构 CSIRT（步骤 2）

选择正确的服务

在开始阶段已经决定新 CSIRT 将着重为员工提供一些核心服务。

已经决定的是，在试点阶段后将考虑扩展服务，可能会添加一些“安全管理服务”。具体决定将以试点用户群的反馈为基础并通过与质量保证部门紧密合作而最终得出。

5.3. 服务对象分析和目标宣言

我们已经采取前三个步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。

>> 下一步是回答问题“启动 CSIRT 可以选择哪类方法？”

下一步是更深入地考察服务对象，主要目标是选择正确的沟通渠道：

- 确定与用户群的沟通方式
- 确定目标宣言
- 制定切实可靠的实施/项目计划
- 确定 CSIRT 服务
- 确定组织结构
- 确定信息安全政策
- 雇用合适的人员
- 利用 CSIRT 办公室
- 寻求与其他 CSIRT 的合作以及可能的国家支持

这些步骤将在后文中有更详细的描述，并可用作业务和项目计划的输入项。

5.3.1. 与服务对象的沟通方式

如前所述，了解服务对象的需求非常重要，同时，掌握沟通策略，包括最有利于交换信息的沟通渠道也是必不可少的。

针对这一问题，管理理论中就有几种可能的分析目标群的方法。在本文档中我们将讨论其中两种：SWOT 分析法和 PEST 分析法。

SWOT 分析法

SWOT 分析法是一种策略规划工具，用于评估项目或企业或其他需要决策的情形下的优势 (**S**trength)、劣势 (**W**eaknesses)、机会 (**O**pportunities) 和威胁 (**T**hreats)。这一方法由 Albert Humphrey 利用财富 500 强企业的数据得出。Albert Humphrey 二十世纪六、七十年代曾在美国斯坦福大学主持研究项目。[8]

优势	**劣势**
机会	**威胁**

图表. 2 SWOT 分析法

[8] SWOT 分析法在维基百科上的解释：http://en.wikipedia.org/wiki/SWOT_analysis

PEST 分析法

PEST 分析法是另一种非常重要且应用广泛的分析服务对象的工具，目的是了解 CSIRT 运作所处环境的政治 (**P**olitical)、经济 (**E**conomic)、社会文化 (**S**ocio-cultural) 和技术 (**T**echnological) 因素。该分析法将帮助确定计划与环境是否协调，同时有助于避免依据错误的假设采取行动。

政治 • 生态/环境问题 • 当前立法国内市场 • 未来立法 • 欧洲/国际立法 • 监管机构和流程 • 政府政策 • 政府任期和变动 • 贸易政策 • 资金、拨款和奖励 • 国内市场利益集团/压力集团 • 国际压力集团	**经济** • 国内经济形势 • 国内经济趋势 • 海外经济和趋势 • 一般税收问题 • 特定于产品/服务的税收 • 季节性/天气问题 • 市场和贸易周期 • 特定的行业因素 • 市场路线和分布趋势 • 客户/终端用户推动因素 • 利息和汇率
社会 • 生活方式变革 • 人口变化 • 消费者态度和观念 • 媒体视角 • 法律修改影响社会因素 • 品牌、公司、技术形象 • 消费者购买模式 • 时尚和榜样 • 重大事件和影响 • 购买渠道和趋势 • 种族/宗教因素 • 广告和出版物	**技术** • 竞争性技术发展 • 研究基金 • 关联的/相关的技术 • 替代技术/解决方案 • 成熟的技术 • 制造方面的成熟和能力发展 • 信息和通讯 • 消费者购买机制/技术 • 科技立法 • 创新潜力 • 技术访问、许可、专利 • 知识产权问题

图表. 3 Pest 分析模型

有关 PEST 分析法的详细描述可访问维基百科[9]。

这两种分析法对服务对象的需求给出了全面的、结构性的概述。所得结果将很好地成为业务提案的补充，从而也有助于获得组建 CSIRT 所需的资助。

沟通渠道

分析中包括的一个重要话题便是可能的沟通和信息发送方法（“如何与服务对象沟通？”）

在可能时，应该考虑定期亲自拜访用户群。事实证明，面对面的交谈更便于合作。如果双方都希望在一起工作，这些会面的结果便是形成更加开放式的关系。

通常 CSIRT 掌握着一系列沟通渠道。以下各项经实践证明是有用的，值得考虑

[9] PEST 分析法在维基百科上的解释：http://en.wikipedia.org/wiki/PEST_analysis

- 公共网站
- 网站的封闭式会员区
- 报告事件的网页表单
- 邮件列表
- 个性化电子邮件
- 电话/传真
- 短消息服务 (SMS)
- “老式”纸质信函
- 月度或年度报告

除了使用电子邮件、网页表单、电话或传真推动事件的处理（从服务对象处接收事件报告、与其他团队协调或给受害者提供反馈和支持）之外，多数 CSIRT 还在公共可访问的网站上以及通过邮件列表发布其安全建议。

! 如果可能，信息应该以安全的方式发送。例如电子邮件可以使用 PGP 数字签名，敏感的事件数据应该总是加密发送。

如需更多信息，请参见第 8.5 章“可用的 CSIRT 工具”。同时可参见第 2.3 章“RFC2350”[10]。

虚构 CSIRT（步骤 3a）

对服务对象和适当的沟通渠道进行分析

与管理层和服务对象的关键人物举行会议，集思广议，为 SWOT 分析法准备足够的内容。所得结论是有需要核心服务的需求：

- 警报和警告
- 事件处理（分析、响应支持和响应协调）
- 通告

必须确保信息在组织严密的前提下发送，并且能够收到信息的服务对象越多越好。因而在此决定，以安全建议为形式的警报、警告和通告将在专用网站上发布，并通过邮件列表发送。CSIRT 则通过电子邮件、电话和传真接收事件报告。下一步计划用统一的网页表单。

参见下页的 SWOT 分析法实例。

优势	劣势
• 在公司内部有一定的经验。 • 他们满意该计划并希望合作。 • 得到管理层的支持和资助	• 不同部门之间、不同分支机构之间缺乏沟通。 • 遇 IT 事件无协调 • 太多的“小部门”

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

机会 • 大量非结构性的漏洞信息 • 迫切需要协调 • 减少事件造成的损失 • 在 IT 安全性问题上有很多可以做的 • 为员工提供 IT 安全性教育	**威胁** • 可用资金不足 • 人员配备不足 • 高期望值 • 文化

图表. 4 SWOT 分析法实例

5.3.2. 目标宣言

在分析了服务对象针对 CSIRT 服务的需求和期望之后，下一步则是起草目标宣言。

目标宣言描述的是依据组织为用户群提供的产品和服务所划分出的组织在社会中的基本职能。宣言允许就新 CSIRT 的存在和职能进行清晰交流。

习惯做法是使目标宣言紧凑但不过于严苛，因为通常宣言需要保持几年不变。

以下是部分 CSIRT 经营中的目标宣言实例：

“<CSIRT 名称> 为其<用户群（定义用户群）>提供信息并辅助其采取主动方法降低计算机安全事件带来的风险并在事件发生时做出响应。”

“为<用户群>提供支持，帮助预防 IT 相关的安全事件的发生并做出必要响应”[11]
目标宣言很重要，是启动的必要步骤。请参见第 2.1 章 “RFC2350”[12] 获取更多有关 CSIRT 应该发布信息的详细描述。

虚构 CSIRT（步骤 3b）

虚构 CSIRT 的管理层制定了以下目标宣言：
“虚构 CSIRT 为其托管公司的员工提供信息和帮助，降低计算机安全事件造成的风险并在此类事件发生时做出响应。”

据此，CSIRT 明确表明其是内部 CSIRT，其核心业务是处理 IT 安全相关的问题。

[11] Govcert.nl 的目标宣言：http://www.govcert.nl

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

6. 制定业务计划

我们已经采取以下各步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。
4. 环境和用户群分析
5. 确定目标宣言

>> 下一步是确定业务计划

分析得出的结果良好概括了服务对象的需求和（假定）劣势，可以作为下一步骤的输入项。

6.1. 确定财务模式

分析之后便精选数个核心服务作为开端。下一步则是考虑财务模式：服务提供具备哪些参数既恰当，又经济划算。

在理想情况下，资金应该用于满足服务对象的需求，但在现实中必须依据特定的预算提供服务组合。因此从计划资金问题入手是很现实的做法。

6.1.1. 成本模式

会影响成本的两大主要因素是服务时间和将雇用的员工数（和员工素质）。是否有提供全天候事件响应和技术支持的需要，还是仅需要在办公时间内提供这些服务？

根据所期望的可用性和办公室设备（例如是否能够在家工作？），按随叫随到值班表或排定的值班表工作可能比较有利。

一个可行方案是在办公时间内同时提供主动服务和响应式服务。在办公时间之外则仅提供有限度的服务，例如，仅在出现重大灾难和事件的情况下提供服务，由一名员工在非办公时间值班。

另一个选择是寻求国际间其他 CSIRT 团队的合作。已经有“全天候”合作的实例。例如，欧洲和美洲的团队间的合作经验就是互惠互利的，提供了一种共享双方工作时间的有益方式。以太阳微系统公司 (Sun Microsystems) 的 CSIRT 为例，在世界不同时区有多家分支机构（但都是同一 CSIRT 的成员），通过在全世界的团队间轮班值守实现全天候服务。这样做控制了成本，因为团队员工都在正常办公时间内工作，而且能兼顾那些夜间休息的地方。

习惯做法是与服务对象深入分析对全天候服务的切实需求。夜间出现的警报和警告在接收方第二天早晨才会读到时显然已失去意义。“需要服务”和“想要服务”之间还是有细微

区别的，但工作时间确实能够带来员工数量和所需设施上的巨大差异，从而在很大程度上影响成本模式。

6.1.2. 收入模式

在了解了成本之后，下一步就该考虑可能的收入模式：如何为计划的服务提供资金。可供审定的部分方案如下：

使用现有资源

对公司其他部分现有的资源进行评估总是有益的。是否有已就职员工（例如在现有的 IT 部门）具备所需背景和专业知识？多数情况下，可以与管理层安排在启动阶段将该员工临时调派到 CSIRT，或由其临时为 CSIRT 提供支持。

会员费

另一种可能性便是将服务通过年缴或季缴会员费的形式售与服务对象。附加服务可以按使用付费，例如服务对象服务或安全监察。

其他可行方案：为（内部）服务对象提供免费服务，为外部客户提供付费服务。另一种做法是在公共网站上发布建议和信息公告，而特殊的、更详尽的或定制的信息则是“仅限会员”访问。

经实践证明，“按 CSIRT 服务订购”在提供足够资金方面，尤其是在启动阶段其作用有限。例如，团队和设备的固定基本费用必须事先预付。通过销售 CSIRT 服务为这些费用提供资金很难，而且要求对财务进行详尽地分析并找出“收支平衡点”。

补助

另一个值得考虑的可能性是，可以向政府或政府机构申请项目补助，现今多数国家都针对 IT 安全项目备有可用资金。联系内政部可能是一个好的开端。

同时开发其他收入模式当然是可行的。

6.2. 确定组织结构

CSIRT 的适当组织结构很大程度上取决于托管组织和服务对象的现有结构。同时还取决于永久或临时聘用的技术专家的工作能力。

一支典型的 CSIRT 这样定义团队内的角色：

管理层

- 总经理

员工

- 办公室经理
- 会计师
- 沟通顾问
- 法律顾问

业务技术团队

- 技术团队负责人
- 技术性 CSIRT 技师，提供 CSIRT 服务
- 研究员

外部顾问

- 需要时聘用

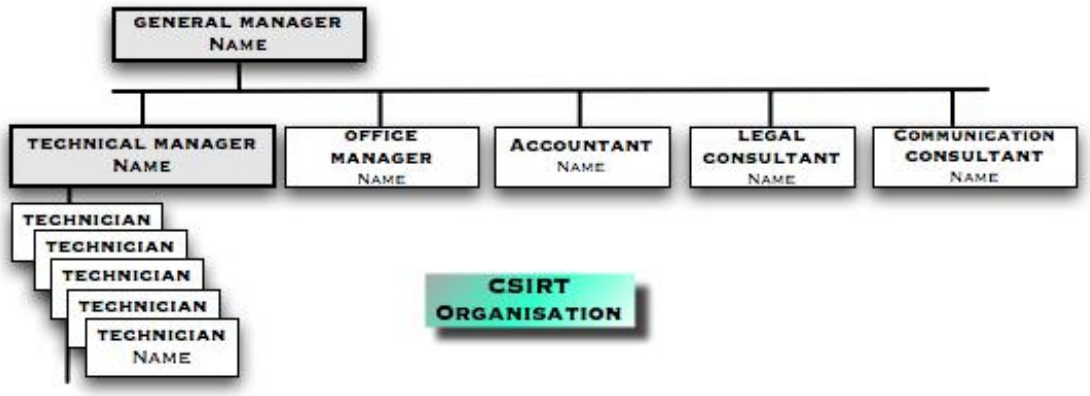
聘用法律专家是极有帮助的，尤其是在 CSIRT 的启动阶段。这样做会增加成本，但最后将节省时间并避免出现法律上的麻烦。

服务对象内部所具备的专业知识各不相同，且在 CSIRT 拥有良好的媒体形象时，聘请一位沟通专家加入团队是很有必要的。这些专家的工作重点可以是将艰深的技术问题转化为用户群或媒体合作伙伴更易理解的消息。沟通专家还会将服务对象的反馈提供给技术专家，从而成为服务对象和技术专家之间的“译员”和“服务商”。

以下是运行 CSIRT 所使用的部分组织模式实例。

6.2.1. 独立的业务模式

所展示的 CSIRT 是作为独立的组织存在，拥有自己的管理层和员工。

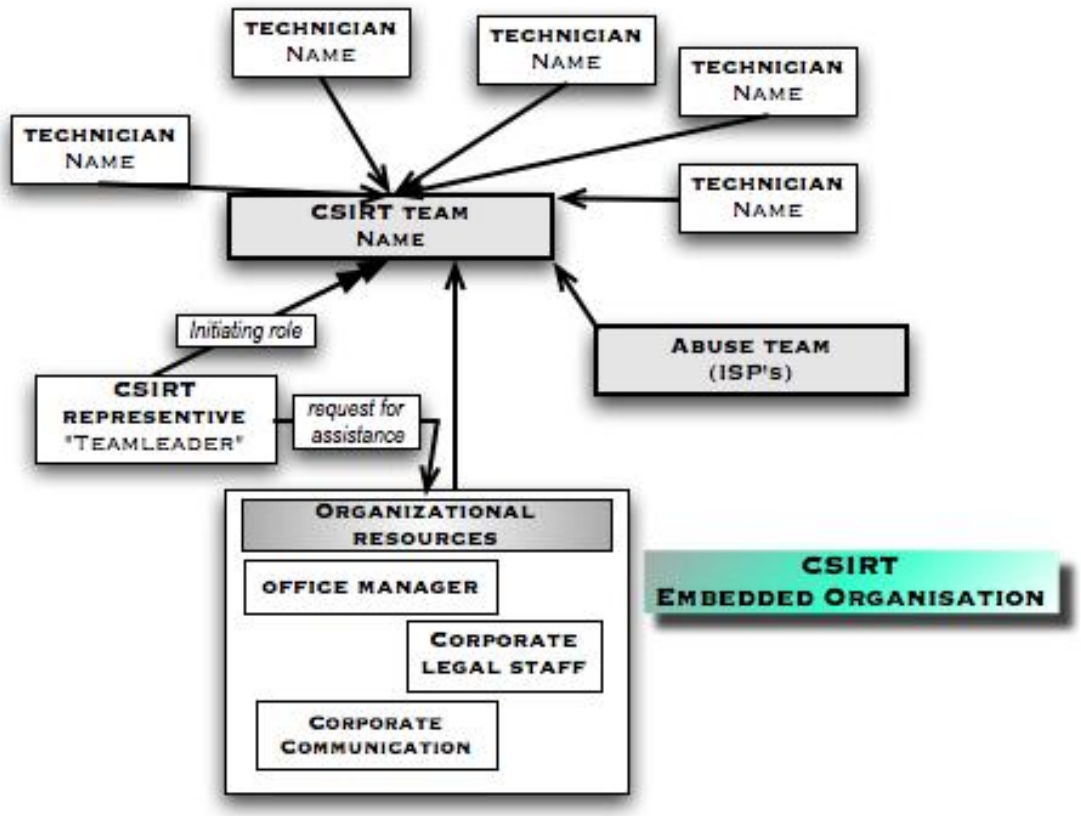


图表. 5 独立的业务模式

6.2.2. 嵌入模式

如果 CSIRT 将在现有组织内部组建，例如使用现有 IT 部门组建，则可使用此种模式。CSIRT 由团队负责人领导，团队负责人对 CSIRT 的活动负责。团队负责人在解决事件或开展 CSIRT 活动时会召集必要的技术人员。团队负责人可以在现有组织内部请求帮助，提供专家支持。

此种模式还可针对出现的特定情形进行调整。在此情况下，团队可配备固定名额或等效全职员工 (Full Time Equivalent, FTE)。例如，在 ISP 处的禁滥用举报处 (abuse desk) 对于一个或（多数情况下）一个以上等效全职员工而言当然是全职工作。

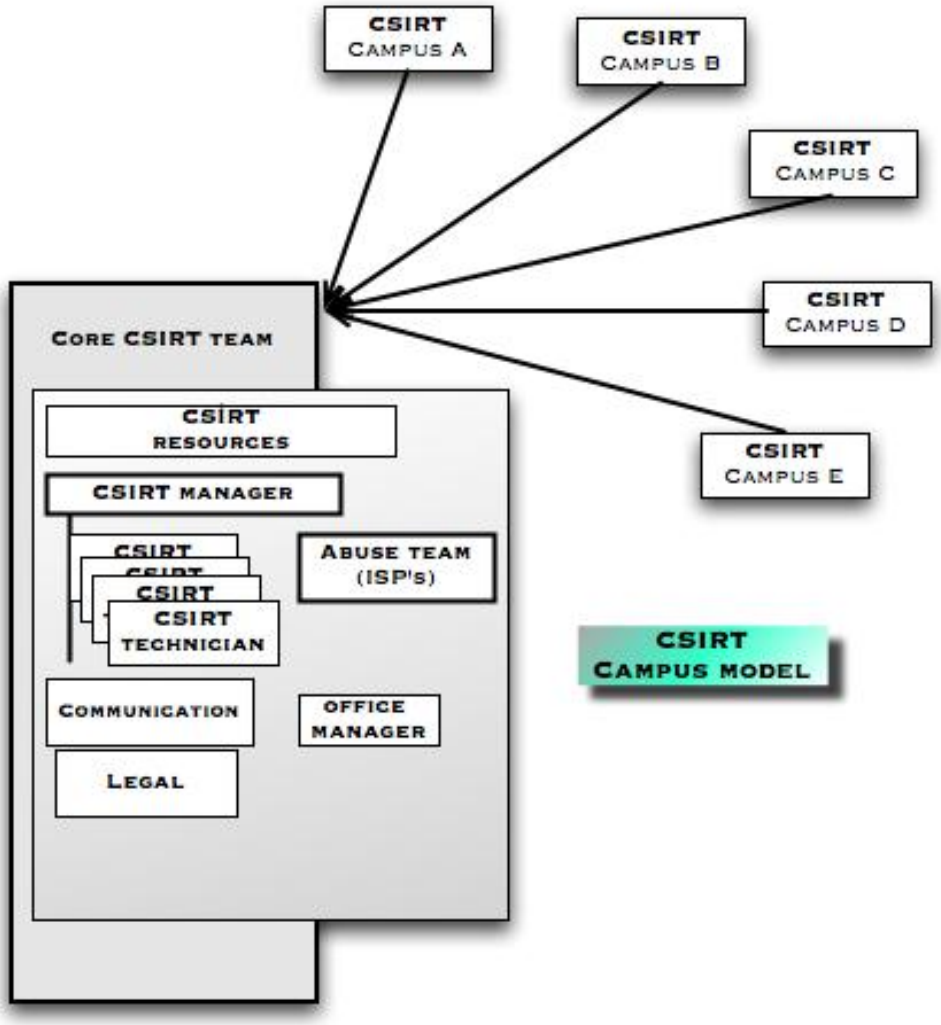


图表. 6 组织嵌入模式

6.2.3. 校园模式

校园模式，不言而喻，多由学院和研究 CSIRT 所采用。多数学术和研究组织由不同地区的各大学和校园组成，分布于一地或整个国家（如国家学术研究网络）。通常这些组织相互独立，常常经营着自己的 CSIRT。这些 CSIRT 通常在“母” CSIRT 或核心 CSIRT 的保护伞下组织活动。核心 CSIRT 负责对外协调并且是对外的单一接触点。在多数情况下，核心 CSIRT 将向适当的校园 CSIRT 提供核心 CSIRT 服务并发布事件信息。

一些 CSIRT 将其 CSIRT 核心服务传播给其他校园 CSIRT，从而降低核心 CSIRT 的管理费用。



图表. 7 校园模式

6.2.4. 志愿模式

此种组织模式描述的是一群人（专家）携手合作，在自愿的基础上互相（也为其他人）提供建议和支持。这是一种结构松散的团体，高度依靠参与者推动。

此种模式通常由（举例来说） WARP 社区采用[13]。

6.3. 雇用合适的人员

确定了将交付的服务和支持级别并选择了组织模式之后，下一步即是为工作网罗人数适当的技术人才。

从这方面而言，究竟需要多少技术员工很难给出过硬的数字，但以下关键值已经证明是比较好的做法：

- 为了交付两项核心服务，即建议公告的发布和事件处理：至少需要 4 名 FTE。
- 针对办公时间内提供全套服务的 CSIRT 并维护系统：至少需要 **6 到 8** 名 FTE。
- 针对提供全员全天候值班（在非办公时间两人轮班），至少需要 **12** 名 FTE。

这些数字还包括后备力量以应对生病和节假日等。同时还有必要检查一下地方集体劳动合同。如果人员在办公时间之外工作可能会因必须支付的额外津贴而造成额外的费用支出。

[13] WARP 机构 http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_02.htm#12

以下是对一支 CSIRT 技术专家的关键能力的简要概述

一般技术员工职务描述项目：

个人能力

- 灵活、有创造性并具备良好的团队精神
- 强大的分析能力
- 以简单的措词解释艰深的技术问题的能力
- 能够严守保密性并按照程序工作
- 良好的组织能力
- 能够承受持续的压力
- 强大的沟通和写作能力
- 思维开放，愿意学习

技术能力

- 对互联网技术和协议有全面的认知
- 熟悉 Linux 和 Unix 系统（取决于服务对象的设备）
- 熟悉 Windows 系统（取决于服务对象的设备）
- 熟悉网络基础设施设备（路由器、交换器、域名服务器、代理服务器、邮件等)
- 熟悉互联网应用程序（SMTP、HTTP、FTP、telnet、SSH 等）
- 熟悉安全威胁（DDoS、网络钓鱼、恶意破坏、数据盗窃等）
- 熟悉风险评估和实际实施

其他能力

- 愿意全天候工作或值班（依服务模式而定）
- 适应长距离出差（遇到紧急情况时可在办公室，适应长期出差）
- 教育水平
- 具备在 IT 安全领域工作的相关工作经验

虚构 CSIRT（步骤 4）

制定业务计划

财务模式

由于公司拥有全天候电子商务业务以及全天候服务的 IT 部门，因而决定在办公时间内提供全套服务，办公时间之外提供值班服务。为服务对象提供的服务将是免费的，但是在试点和评估阶段可能会对外部客户提供的服务进行评估。

收入模式

在启动和试点阶段，CSIRT 将由托管公司资助。在试点和评估阶段将讨论更多的资助，包括向外部客户销售服务的可能性。

组织模式

托管组织是小型公司，因而选择了嵌入模式。

在办公时间内，三名员工之一将提供核心服务（发布安全建议和事件处理/协调）。

公司的 IT 部门已经聘用到具备适当技能的员工。与该部门达成协议，新 CSIRT 可在需要时临时请求支持。同时也可以使用二线值班技术人员。
将有一个核心 CSIRT 团队，包含四名全职成员和五名 CSIRT 团队成员。这些人中有一名可以循环轮班。

员工
CSIRT 团队负责人具备安全相关的以及第一、二级支持的专业背景，并具备危机应变管理工作相关工作经验。其他三名团队成员是安全方面的专家。来自 IT 部门的兼职 CSIRT 团队成员在公司基础设施各自负责领域也都是专家级人物。

6.4. 办公室的利用和办公设施

办公设施和办公空间的利用、以及物理安全措施是一个很宽泛的话题，因此，在本文档中恕不赘述。本章意在简短描述此话题。

有关物理安全措施的更多信息，可参见以下网址：
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

“强化建设”
由于 CSIRT 经常需要处理极其敏感的信息，习惯做法是让团队负责办公室的物理安全措施。这将极大程度上依靠托管公司的现有设备和基础设施以及现有信息安全政策。

例如，政府在处理分类表时对保密信息的处理要求极为严格。与所在公司或机构核查当地法规和政策。

通常一支新的 CSIRT 必须通过与其托管组织合作了解当地法规、政策和其他法律问题。

对需要的所有设备和安全措施的详尽描述已然超出本文档的范围。但是，以下您将看到为您的 CSIRT 列出的基础设施精选：

构建的一般规则

- 使用访问控制
- 起码将 CSIRT 办公室设置为仅供 CSIRT 员工访问。
- 利用摄像机监控办公室和办公室入口。
- 将保密信息归档存入带锁抽屉或保险箱。
- 使用安全的 IT 系统。

IT 设备的一般规则

- 使用员工可以支持的设备
- 加固所有系统
- 所有系统在连接到互联网之前必须安装补丁并更新。
- 使用安全软件（防火墙、多个反病毒扫描软件、反间谍软件等）

维护沟通渠道

- 公共网站
- 网站的封闭式会员区
- 报告事件的网页表单
- 电子邮件（PGP / GPG / S/MIME 支持）
- 邮件列表软件
- 配备专门针对服务对象的电话专线：
    - 电话
    - 传真
    - 短消息服务 (SMS)

记录跟踪系统

- 联系人数据库，包含团队成员、其他团队等详细信息。
- 客户关系管理工具
- 事件处理通报管理系统

自一开始便在以下各项中使用“企业风格”：

- 标准电子邮件和公告格式
- “老式”纸质信函
- 月度或年度报告
- 事件报表格式

其他问题

- 预知带外通讯以备遭到攻击
- 预知互联网连接性的冗余度

如需更多有关特定 CSIRT 工具的信息，请参见第 8.5 章“可用的 CSIRT 工具”。

6.5. 制定信息安全政策

根据不同类型的 CSIRT，需要有专用的信息安全政策。除了描述所需操作和管理流程及程序之外，此类政策必须符合法规和标准，对于 CSIRT 的责任而言这点尤为重要。CSIRT 通常受国家法律法规的约束，一般在欧洲立法（通常为法规）和其他国际协议背景下实施。标准一般不直接起约束作用，但可以是法律法规强制或建议执行的。

以下是一系列可能的法律和政策：

国家的
- 关于信息技术、电信、媒体的各种法律
- 数据保护和隐私权法律
- 数据保持法律法规
- 财务、会计和企业管理法规
- 公司治理和 IT 治理的行为准则

欧洲
- 电子签名指令 (1993/93/EC)
- 数据保护指令 (1995/46/EC) 和电子通信隐私权 (2002/58/EC)
- 电子通信网络和服务指令 (2002/19/EC – 2002/22/EC)
- 公司法指令（如第八号公司法指令）

国际
- 新巴塞尔协议（尤其针对经营风险的管理）
- 欧洲理事会的《关于网络犯罪的公约》
- 欧洲理事会的《人权公约》（第 8 条关于隐私权）
- 国际会计标准（IAS；在某种程度上强制 IT 控制）

标准
- 英国 BS 7799 标准（信息安全）
- 国际 ISO2700x 标准（信息安全管理系统）
- 德国 IT-Grundschutzbuch、法国的 EBIOS 及其他国家合约

要确定您的 CSIRT 是否依据本国和国际法规行事，请向法律顾问咨询。

在信息处理策略中有待解决的最基本问题是：

- 如何给收到的信息“加标签”或“分类”？
- 如何处理信息，尤其是独占性信息？
- 披露信息应该考虑哪些因素，尤其是如果将事件相关信息传递给其他团队或站点时应该考虑哪些事项？
- 就信息处理而言是否需要考虑法律因素？
- 是否具备加密技术使用政策以保护归档和（或）数据通信，特别是电子邮件的独占性和完整性？
- 该政策是否包括可能的法律边界条件，如发生诉讼时的密钥证书或强制性解密。

虚构 CSIRT（步骤 5）

办公室设备和地点

由于托管公司已经拥有足够的物理安全措施，新 CSIRT 在此方面已得到良好补充。一间被称之为“作战室”的房间用作紧急情况协调室。购买了保险箱用于存放加密资料和敏感文档。设立了独立的电话线，包括电话交换台，以便在办公时间接听热线，同时在非办公时间可用号码相同的手机值班。

现有的设备和企业网站也可用于公布 CSIRT 相关的信息。安装并维护邮件列表，其中一部分仅限于团队成员与其他团队间的沟通。所有员工的详细联系信息都存储在一个数据库中，一份打印稿保存在保险箱中。

法规

由于 CSIRT 是利用现有信息安全政策嵌入公司的，针对 CSIRT 的对应政策已在公司法律顾问的帮助下确立。

6.6. 寻求与其他 CSIRT 的合作以及可能的国家支持

在本文档中，已多次提及有其他 CSIRT 机构存在，并且这些机构迫切地需要彼此间合作。最好的做法是尽早联系其他 CSIRT 以便与 CSIRT 团体取得必要联系。通常其他 CSIRT 都非常愿意帮助新组建的团队完成启动。

搜索一国内的其他 CSIRT 或全国 CSIRT 合作活动，可以从 ENISA 的“欧洲 CERT 活动清单”[14] 开始。

在查找适当的 CSIRT 信息源时如需帮助请联系 ENISA 的 CSIRT 专家：

cert-relations@enisa.europa.eu

[14] ENISA 清单：http://www.enisa.europa.eu/ENISA%20CERT

以下是对 CSIRT 团体活动的概述。请参见“清单”以获取更全面的描述和更多信息。

欧洲 CSIRT 机构

TF-CSIRT[15]

TF-CSIRT 特别工作组推动了欧洲计算机网络安全应急小组 (CSIRT) 间的协作。本特别工作组的主要目标是为经验和专业知识的交流提供论坛、为欧洲 CSIRT 团体设立试点服务并辅助组建新的 CSIRT。

特别工作组的主要目标是：

- 为交流经验和专业知识提供论坛
- 为欧洲 CSIRT 社区设立试点服务
- 为响应安全事件推行通用标准和程序
- 辅助组建新 CSIRT 并培训 CSIRT 员工。
- TF-CSIRT 的活动重点着眼于欧洲及邻近国家，符合 2004 年 9 月 15 日欧洲计算机网络研究教育协会 (TERENA) 技术委员分检批通过的工作范围。

全球 CSIRT 机构

FIRST[16]

FIRST 是首家事件响应组织，而且是公认的全球领导者。FIRST 的会员制使事件响应小组能够更有效地对安全事件提供服务，包括响应式服务和主动服务。

FIRST 将政府、商业和教育培训组织的各种计算机网络安全应急小组维系在一起。FIRST 旨在鼓励事件预防中的合作与协作、激发对事件的快速响应并加强成员和团体间最大程度地共享信息。

除了 FIRST 在全球事件响应团体构建的信任网络之外，FIRST 同时还提供增值服务。

虚构 CSIRT（步骤 6）

寻求合作

通过使用 ENISA 的清单可快速查找到一个国家的一些 CSIRT 并与之取得联系。为新近聘用的团队负责人安排对其中一支 CSIRT 的实地拜访。他了解到国家 CSIRT 活动并出席一次会议。

会议的收获不仅仅是有助于收集工作方法的实例，还获得了其他团队的支持。

7. 推进定业务计划

我们到目前为止已经采取以下各步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。

[15] TF-CSIRT:http://www.enisa.europa.eu/ENISA%20CERT/pages/04_01_02.htm#06

[16] FIRST:http://www.enisa.europa.eu/ENISA%20CERT/pages/05_02.htm

4. 环境和用户群分析
5. 确定目标宣言
6. 制定业务计划
    a. 确定财务模式
    b. 确定组织结构
    c. 开始聘用员工
    d. 利用并装备办公室
    e. 制定信息安全政策
    f. 寻求合作伙伴

>> 下一步便是将上述各项融入项目计划并启动！

最好提出一个业务案例作为确定项目的开端。此业务案例将作为项目计划的基础，将作为申请管理层支持和获取预算或其他资源的基础。

事实证明，坚持向管理层报告有助于保持对 IT 安全问题的高度警觉性，并据此可获得对自己的 CSIRT 的持续支持。

开始业务案例应从分析问题和机会入手，为此可以使用第 5.3 章“服务对象的分析”中所描述的分析模型，同时寻求与潜在服务对象的紧密联系。

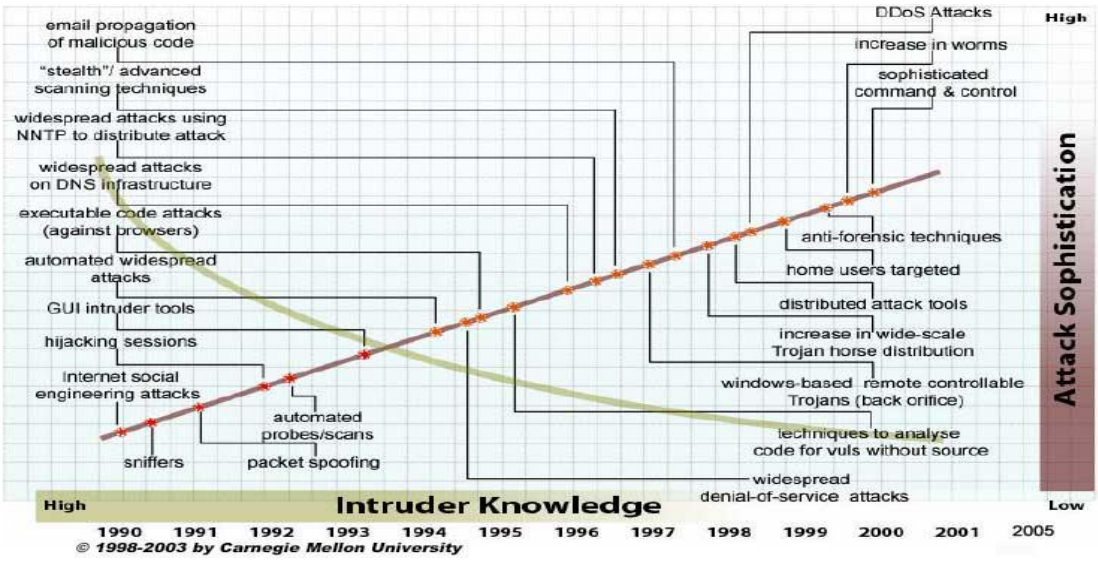
如早先所述，在启动 CSIRT 时有很多需要考虑的事情。最好根据 CSIRT 在发展中的需求调整上述资料。

习惯的做法是，在向管理层报告自己的情况时尽可能地切合实际，可以利用报纸、互联网中的最新文章，解释 CSIRT 服务和内部事件协调为什么对企业资产的安全如此重要。同时有必要指出的是，由于公司或机构的经营离不开 IT，只有坚持给予 IT 安全事项足够的支持，才能保障公司或机构的经营稳定性

（Bruce Schneier 的一席话切中要害：*“安全性不是产品，其本身是一个过程[17]！”*）

用于说明安全性问题的一个著名工具是以下由 CERT/CC 提供的图表：

[17] Bruce Schneier:http://www.schneier.com/



图表. 8 入侵者知识和攻击手法趋势（来源：CERT-CC[18]）

该工具形象地呈现了 IT 安全性趋势，尤其是面对不断增加的攻击手法，相应的必备技能却在减少的趋势体现无余。

另一点需要指出的是，针对漏洞的软件更新可用性和对抗这些更新的攻击开始之间的时间窗不断缩短：

补丁 -> 攻击程序		**扩张速率**	
尼姆达病毒：	11 个月	红色代码：	以天计
Slammer 蠕虫：	6 个月	尼姆达病毒：	以小时计
Nachi 病毒：	5 个月	Slammer 蠕虫：	以分钟计
冲击波病毒：	3 周		
Witty：	1 天 (!)		

演示中还可以展示收集的事件数据、潜在的改进以及经验和教训。

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

7.1. 业务计划和管理触发因素描述

为管理层的演示，包括对 CSIRT 的宣传不足以独自构成业务案例，但如果执行恰当，在多数情况下均会赢得管理层对 CSIRT 的支持。另一方面，业务案例不应仅仅作为对管理层的试探，而应该用于与团队和服务对象的沟通。业务案例听上去非常商业化，远远脱离 CSIRT 的实际情况，但可以为 CSIRT 的组建提供良好的关注焦点和方向。

以下问题的答案可用于制定优秀的业务案例（给出的实例是假设性的，仅用于说明。“真实的”答案完全有赖于“真实的”情形）。

- 问题是什么?
- 您希望与用户群一起实现什么？
- 如果什么都不做会发生什么？
- 如果采取行动会发生什么？
- 会有哪些费用支出？
- 会获得什么？
- 应该什么时候开始，什么时候结束？

问题是什么?

在多数情况下，当 IT 安全性成为公司或机构核心业务不可分割的一部分时、当 IT 安全事件会给业务带来风险，使安全减灾成为日常业务运作时，便会产生组建 CSIRT 的想法。

大多数公司或机构都拥有专门的支持部门或支持人员，但多数情况下对安全事件的处理并不充分，并缺乏其应有的结构性。多数情况下，安全事件的工作领域要求有特殊的技能和关注。寻求一种结构性更强的方法是有好处的，可以降低业务风险，减少给公司造成的损害。

多数情况下的问题是缺乏协调，现有知识并未用于处理事件，而这些知识本可以阻止今后事件的发生、防止财务损失并（或）可避免给机构声望带来损害。

希望与服务对象一起实现哪些目标？

如早先所述，您的 CSIRT 将为其用户群服务，辅助他们解决 IT 安全事件和问题。其他目标还包括提高 IT 安全性知识水平并培养安全意识。

在这种文化背景下，一开始便努力采取积极主动的、预防性的措施，从而削减经营成本。

将这种合作与援助文化引入公司或机构多数情况下可促进整体效率。

如果什么都不做会发生什么？

处理 IT 安全性问题的非结构化方式会导致进一步的损害，绝不仅仅是有损机构名望这么简单。还有可能造成财务上的损失和卷入法律问题。

如果采取行动会发生什么？

对安全性问题的发生有了预防意识。这将有利于更有效地解决问题并防止未来遭受损失。

会有哪些费用支出？

根据组织模式的不同，费用包括 CSIRT 团队成员的工资和机构、设备、工具和软件的许可费用。

会获得什么？

根据业务和过去的损失，可获得对程序和安全实践的更高透明度，从而保护企业的宝贵资产。

具体时间表是什么？

参见第 12 章“项目计划描述”，获取对项目计划实例的描述。

现有业务案例和方法的实例

以下是一些值得研究的 CSIRT 业务案例实例：

- http://www.cert.org/csirts/AFI_case-study.html
  组建金融机构 CSIRT：实例研究

  本文档的目的是将一家金融机构（本文档下文中简称为 AFI）在制定和实施安全问题处理计划及计算机网络安全应急小组 (CSIRT) 中的经验和教训与大家分享。

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  CERT POLSKA 业务案例汇总（PDF 格式的幻灯片）。

- http://www.auscert.org.au/render.html?it=2252
  在二十世纪九十年代要组建一支即时事件响应小组 (IRT) 可是项艰巨的任务。很多组建 IRT 的人都不具备相关经验。本文件检视了一支 IRT 在团体中可能承担的角色，以及在组建过程中和开始运作之后应该处理的问题。这样做有利于加强对之前未解决之问题的认识，因而现有 IRT 可从中受益。

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  信息安全实例研究，保护企业，作者：Roger Benton

  本练习是保险公司向企业范围安全系统迁移的实例研究。本文的意图是提供在创建安全系统或向安全系统迁移时可遵循的途径。最初，一个简单的在线安全系统是用于控制对公司数据访问的唯一机制。泄露风险严重：在线环境之外再无完整控制。任何人只要具备基本编程技能便可添加、更改和（或）删除生产数据。

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriott 的电子商务安全策略：商务与 IT 协作

  根据万豪国际酒店集团 (Marriott International, Inc.) 的 Chris Zoladz 的经验，电子商务安全是一个过程，不是一个项目。这是 Zoladz 在最近由综艺社群 (Intermedia Group) 主办，在波士顿举办的电子商务安全会议和博览会上的发言。作为负责万豪酒店信息保护的副总裁，Zoladz 虽然不是律师，但他代表法律部门进行报告。他的职责便是掌握万豪酒店最有价值的业务信息的存储位置以及在公司内外的移动方式。万豪酒店为技术基础设施制定有独立的职责，即由 IT 安全架构师负责支持安全性。

虚构 CSIRT（步骤 7）

推进定业务计划

现决定从公司历史记录中收集确实的消息。这对于 IT 安全形势的统计概览非常有用。当 CSIRT 组建并开始运作时，应该继续此类收集，以确保掌握最新的统计数字。

联系其他国内 CSIRT 并采访了解其业务计划。他们将有关 IT 安全事件的最新发展及事件所耗成本等信息编译成幻灯片，以期能够提供必要支持。

在此虚构 CSIRT 的实例中，说服管理层，使其了解 IT 业务的重要性的需求并不迫切，而且要开始第一步骤并不困难。准备业务案例和项目计划，包括对组建成本和运作成本的预估。

8. 操作和技术流程（工作流程）实例

我们到目前为止已经采取以下各步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。
4. 环境和用户群分析。
5. 确定目标宣言。
6. 制定业务计划。
   a. 确定财务模式。
   b. 确定组织结构。
   c. 开始聘用员工。
   d. 利用并装备办公室。
   e. 制定信息安全政策
   f. 寻求合作伙伴。
7. 推进业务计划
   a. 使业务案例得到批准。
   b. 使一切与项目计划相符。

>> 下一步是：使 CSIRT 具备可操作性

拥有一个定义恰当的工作流程有助于改进每次发生事件或漏洞时的处理质量和所需时间。

正如实例框中所述，虚构 CSIRT 将提供基本的 CSIRT 核心服务：

- 警报和警告
- 事件处理
- 通告

本章提供的工作流程实例描述的是一支 CSIRT 的核心服务。本章同时还包含从不同来源收集信息、检查其相关性和可靠性并重新发送给服务对象的有关信息。最后，本章包括最基本的程序和特定 CSIRT 工具的实例。

8.1. 评估服务对象的安装基础

第一步是了解服务对象安装的 IT 系统的概况。据此，CSIRT 可评估所得信息的相关性，并在重新发送前进行筛选；这样用户群便不会因收到基本无用的信息而不堪重负。

习惯做法是从简单开始，例如，使用以下的 excel 表单：

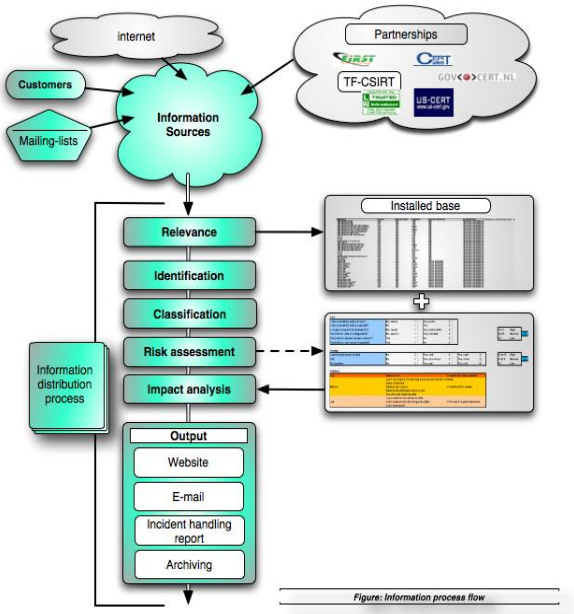
类别	应用程序	软件产品	版本	操作系统	操作系统版本	用户
台式机	Office	Excel	x-x-x	Microsoft	XP-prof	A
台式机	浏览器	IE	x-x-	Microsoft	XP-prof	A
网络	路由器	CISCO	x-x-x	CISCO	x-x-x-	B
服务器	服务器	Linux	x-x-x	L-distro	x-x-x	B
服务	网络服务器	Apache		Unix	x-x-x	B

利用 excel 的过滤功能，能够轻松选择适当的软件并查看哪位用户使用的是何类软件。

8.2. *生成警报、警告和通告*

警报、警告和通告的生成全部遵循以下相同的工作流程：

- 收集信息
- 评估信息的相关性和来源可靠性
- 以收集的信息为基础评估风险
- 发送信息



图表. 9 ：信息流程

在以下段落中将对本工作流程进行更为详尽的描述。

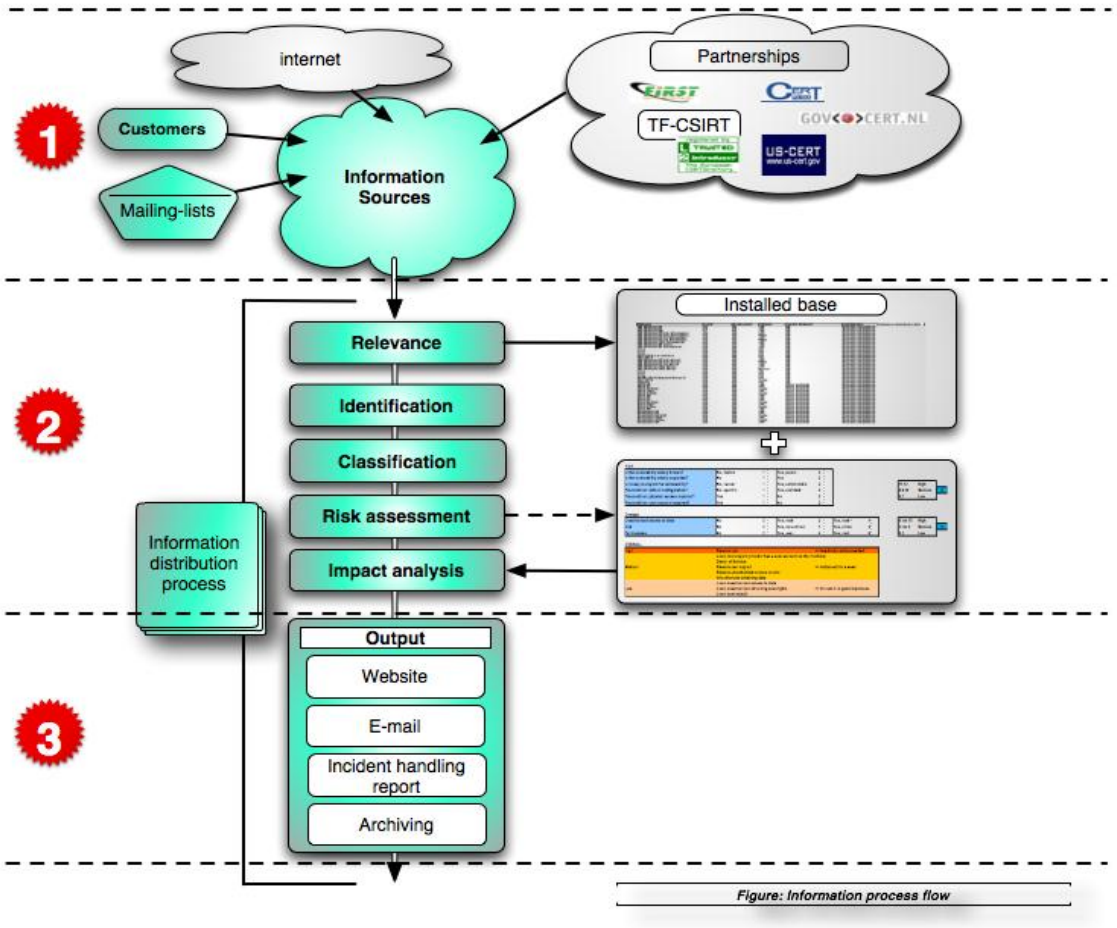


Figure: Information process flow

步骤 1：收集漏洞信息。

通常有两种主要类型的信息来源可为服务提供有用信息：

- 有关（您的） IT 系统的漏洞信息
- 事件报告

根据不同的业务种类和 IT 基础设施，有很多公开的和不公开的信息源能够提供漏洞信息：

- 公开和密闭式邮件列表
- 供应商漏洞产品信息
- 网站
- 互联网上的信息（Google 等……）
- 提供漏洞信息的公共和私有合作伙伴（FIRST、TF-CSIRT、CERT-CC、US-CERT……）

所有这些信息都有利于提高对 IT 系统中特定漏洞的深入了解。

如前所述，在互联网上有大量有益的、易于访问的安全信息来源。ENISA 特别工作小组 2006 年“CERT 服务”大概于 2006 年年底制作了一份更为全面的清单[19]。

步骤 2：鉴定信息并评估风险

这一步将形成对服务对象 IT 基础设施的特定漏洞造成影响的分析。

识别

在将收集的漏洞信息发送给服务对象之前，必须对其来源进行鉴别以确定来源的可靠性。否则，人们有收到错误警报的可能，进而会导致业务流程不必要的混乱，最终将损害 CSIRT 的声望。

[19] 特别工作小组“CERT 服务”：http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

以下过程展示的是识别消息可靠性的实例：

识别消息及其来源可靠性的过程

通用核对清单

1. 来源是否已知并依其资质正确注册？
2. 信息是否通过正常渠道获得？
3. 是否包含有“奇怪”信息，让人“感觉”是错误的？
4. 根据您的感觉，对信息有疑问，请勿采取行动，并请再次核查！

电子邮件来源

1. 来源地址是否为组织所熟识并且在来源清单上是否为已知？
2. PGP 签名是否正确？
3. 如果有疑问可检查消息的完整标题。
4. 如有疑问，使用 “nslookup” 或 ”dig” 校验发送者的域名[20]。

WWW – 来源

1. 当连接到安全网站 (https ://) 时检查浏览器证书。
2. 检查内容来源和有效性（技术上的）。
3. 有疑问时，请勿点击任何链接或下载任何软件。
4. 有疑问时，执行 “lookup” 和 “dig” 校验域名并执行 “traceroute”。

电话

1. 仔细听清姓名。
2. 你熟悉电话里的声音吗？
3. 如有疑问，请询问电话号码并请求回呼致电者。

图表. 10 信息识别过程实例

相关性

对早先开发安装的硬件和软件的概述可用于筛选所接收漏洞信息的相关性，以期找到下述问题的答案：“服务对象是否使用此部分软件？”；“信息与其是否相关？”

分类

部分收到的信息可以分类或标记为受限制的（例如来自其他团队的事件报告）。所有信息必须根据发送者的需求及自己的信息安全政策进行处理。一个习惯的基本规则是“如果信息不象预计中的清晰则不要发送信息；如有疑问，请询问发送者，获得许可后发送。”

[20] CHIHT 中检查身份的工具：http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

风险评估和影响分析

确定（潜在）漏洞的风险和影响有多种方法。

现确定风险是漏洞有被利用的潜在机会。在此有多个重要因素（特别是）：

- 漏洞是否是众所周知的？
- 漏洞是否广泛传播？
- 漏洞是否容易被利用？
- 漏洞是否远程可利用？

所有这些问题均有利于正确判断漏洞的严重性。
计算风险的一个极其简单的方法就是遵循以下公式：

影响 = 风险 X 潜在损害

潜在损害可能是

- 对数据的未授权访问
- 拒绝服务 (DOS)
- 获得或扩大权限

（如需更详尽的分类表，请参见本章最后）。

在这些问题解答完毕之后，便可在建议中添加整体评级，告知潜在风险和损害。经常使用的简单表述是低、中和高。

其他更为全面的风险评估方案是：

GOVCERT.NL 评级方案[21]

荷兰政府 CSIRT GOVCERT.NL 研发出一种风险评估矩阵，矩阵在 Govcert.nl 启动阶段开发，并仍在根据最新趋势进行更新。

RISK

Is the vulnarability widely known?	No, limited	1	Yes, public	2	
Is the vulnarability widely exploited?	No	1	Yes	2	
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2	
Precondition: default configuration?	No. specific	1	Yes, standard	2	
Precondition: physical access required?	Yes	1	No	2	
Precondition: user account required?	Yes	1	No	2	

11,12	High	0
8,9,10	Medium	
6,7	Low	

Damage

Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4	
DoS	No	0	Yes, non-critical	1	Yes, critical	5	
Permissions	No	0	Yes, user	4	Yes, root	6	

6 t/m 15	High	0
2 t/m 5	Medium	
0,1	Low	

OVERALL

High	Remote root	>> Imediately action needed!
	Local root exploit (attacker has a user account on the machine)	
	Denial of Service	
Medium	Remote user exploit	>> Action within a week
	Remote unauthorized access to data	
	Unauthorized obtaining data	
	Local unauthorized access to data	
Low	Local unauthorized obtaining user-rights	>> Include it in general process
	Local user exploit	

图表. 11 GOVCERT.NL 评级方案

EISPP 公用建议格式描述[22]

欧洲信息安全推广计划 (European Information Security Promotion Programme, EISPP) 是由欧洲共同体（欧盟）依据第五个框架计划联合资助的项目。EISPP 项目旨在开发一个欧洲框架，不仅为了共享安全知识，更为了确定向中小企业传播安全信息的内容和方式。通过向欧洲中小型企业提供必要的 IT 安全服务，鼓励这些企业开发并使用值得信任的电子商务，从而增加新业务并带来更好的机遇。EISPP 在欧洲委员会看来是在欧盟内部构建欧洲专家网络的先锋。

德国建议格式（DAF）[23]

DAF 是德国 CERT-Verbund 的一家机构，是不同团队之间生成并交换安全建议的基础设施的核心组成部分。DAF 专门针对德国 CERT 的需求量身定制；标准由 CERT-Bund、DFN-CERT 、 PRESECURE 和 Siemens-CERT 制 定 和 维 护 。

[21] 漏洞矩阵：http://www.govcert.nl/download.html?f=33

[22] EISSP:http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#03

[23] DAF:http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#02

步骤 3：发送信息

CSIRT 可从多个发送方法中选择，具体要取决于用户群的希望和您的沟通策略。

- 网站
- 电子邮件
- 报表
- 归档和研究

由 CSIRT 发送的安全建议应始终保持相同的结构。这将增强可读性，读者可以快速查找到所有相关信息。

建议至少应该包含以下信息：

建议的标题 ……
参考编号 …… **受影响的系统** - …… - …… **相关的操作系统和版本** …… **风险** （高、中或低） …… **影响/潜在损害** （高、中或低） …… **外部 ID 是：** （CVE，漏洞公告 ID） ……
漏洞概述 …… **影响** …… **解决方案** …… **描述（细节）** …… **附录** ……

图表. 12 建议方案实例

有关安全建议的完整实例请参见第 10 章“练习”。

8.3. 进行事件处理

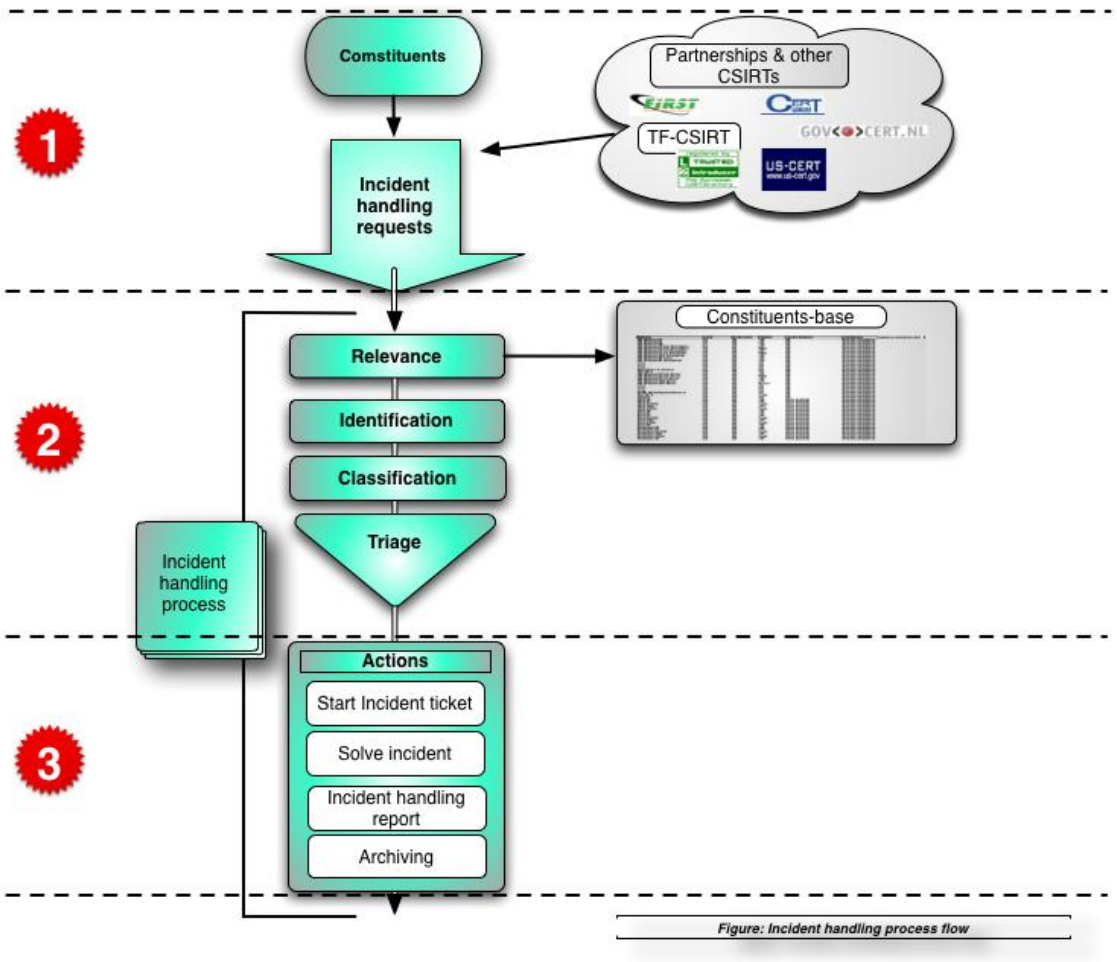
如在本章介绍部分所述，事件处理过程中的信息处理过程与警报、警告和通告编译过程中使用的信息处理过程极为相似。但是信息收集这一部分却略有不同，获得事件相关数据的常见方式是从服务对象或其他团队处接收事件报告，或从事件处理过程中所涉各方收集反馈。信息通常通过（加密的）电子邮件传送，有时也在必要时使用电话或传真。

当通过电话接收信息时，习惯做法是接听电话的同时将每一个细节都记录下来，使用事件处理/报告工具或制作备忘录均可。必须立即（在电话结束前）生成一个事件编号（如果目前为止尚无此事件编号）并签发给电话中的报告方（或事后通过总结性的电子邮件发送）作为日后沟通的参考。

本章其余部分描述的是事件处理的基本过程。对有关事件管理完整流程及所有相关工作流程和子流程的深入分析可在 CERT/CC 文档“确定 CSIRT 的事件管理流程”中找到[24]。

[24] 确定事件管理流程：http://www.cert.org/archive/pdf/04tr015.pdf

从根本上说，事件处理都遵循以下工作流程：



图表. 13 事件处理流程

步骤 1：接收事件报告

如前所述，事件报告有多种渠道能够送抵 CSIRT 处，主要是通过电子邮件，但也可通过电话或传真。

如前所述，习惯做法是在收到事件报告时以固定格式记录下所有细节。这样做可确保不遗漏重要信息。以下可看到的是方案实例：

事件报告表单
请填写此表并传真或发送电子邮件至：…….. *标记有 * 号的行是必填项。* *姓名和组织* 1. 姓名*： 2. 组织名称*： 3. 行业类型： 4. 国家*： 5. 城市： 6. 电子邮件地址*： 7. 电话号码*： 8. 其他： *受影响的主机* 9. 主机数： 10. 主机名和 IP*： 11. 主机功能*： 12. 时区： 13. 硬件： 14. 操作系统： 15. 受影响的软件： 16. 受影响文件： 17. 安全： 18. 主机名和 IP： 19. 协议/端口： *事件* 20. 参考编号 (ref #)： 21. 事件类型： 22. 事件开始： 23. 这是进行中的事件：是 否 24. 恢复时间和方法： 25. 已知漏洞： 26. 可疑文件： 27. 对策： 28. 详细描述*：

图表. 14 事件报告的内容

步骤 2：事件评估

在此步骤，将检查报告事件的可靠性和相关性，并对事件进行分类。

识别

欲避免不必要的行动，习惯做法是检查最初报告事件的人是否值得信任，此人是否是自己的用户之一或同行 CSIRT 的用户之一。应用的规则与第 *8.2* 章“生成警报”中所述规则相似。

相关性

利用此步骤，可检查事件处理请求是否来自 CSIRT 服务对象，或所报告的事件是否涉及服务对象的 IT 系统。如果不符合上述来源，报告通常会纠正发送到正确的 CSIRT[25]。

分类

利用此步骤通过对事件严重性进行分类准备分检。详细描述事件分类细节已超出本文档的范围。最好从利用 CSIRT 案例分类方案（针对企业 CSIRT 的实例）为开端：

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.		

图表. 15 事件分类方案（来源：FIRST）[26]

[25] CHIHT 中检查身份的工具：http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

[26] CSIRT 案例分类 http://www.first.org/resources/guides/csirt_case_classification.html

分检

分检是一种医疗人员或处理突发事件人员使用的体系，在需要护理的伤员数超出现有资源能力时，可用于对有限的医疗资源进行定量分配以便尽最大可能处理最多的病患[27]。

CERT/CC 给出的描述如下：

分检是任何事件管理能力的最基本要素，针对任何现有 CSIRT 更是如此。分检是整个组织了解报告内容至关重要的途径。所有信息均以此为媒介流向一个单一接触点，使企业能够了解进行中的活动和所有报告数据的全面相关性。分检允许对收到的报告进行初始评估并排队等候进一步处理。如果报告或请求的初始文档和数据输入在检测过程未完成，则可在此处开始。

分检功能提供了所有已报告活动当前状态的即时印象：哪些报告是未完成的或已结束的、哪些行动待决、以及每类报告各收到多少。这一过程可帮助识别潜在安全问题并优化工作量。分检过程中收集的信息可用于生成漏洞及事件趋势和统计数据，供上级管理层参考[28]。

由于分检要求深刻理解事件对服务对象特定部分的潜在影响，并具备确定处理事件的最适合人选的能力，因而进行分检的团队成员必须是最富经验的人员。

[27] 分检在维基百科中的解释：http://en.wikipedia.org/wiki/Triage

[28] 确定事件管理流程：http://www.cert.org/archive/pdf/04tr015.pdf

步骤 3：操作

通常，经过分检的事件会进入由一个或多个事件处理者使用的事件处理工具中的请求队列，这些处理者需遵循这些步骤。

启动事件单

事件单编号可能已在上一步骤中生成（例如当事件通过电话报告时）。如果尚未生成，第一步则是创建此类编号，以用于进一步的事件沟通。

事件的生命周期

处理事件遵循的步骤并非一条直线直至最终产生解决方案，而是遵循一圈循环步骤直至事件最终解决，所有相关各方均获得了所有必要信息。这一循环即是通常所指的“事件生命周期”，包含以下过程：

分析：	对所有报告事件的细节进行分析。
获取联系信息：	以便向所有相关各方，如其他 CSIRT、受害者和被攻击滥用的系统所有者进一步报告事件相关信息。
提供技术援助：	帮助受害者快速从事件结果中恢复并收集更多有关攻击的信息。
协调：	通知其他相关各方，如负责攻击所用 IT 系统的 CSIRT 或其他受害者。

这一结构被称之为“生命周期”，这是因为一个步骤会引出另一个步骤，直至最后一步，随即协调部分可再次引出新的分析，整个周期再次开始。所有各方收到并报告了所有必要信息后，过程结束。

有关事件生命周期的更为详尽的描述，请参见 CERT/CC CSIRT 手册[29]。

事件处理报告

编译报告以备管理层就事件提问。同时习惯做法是编写一份关于“经验与教训”的文档（仅供内部使用）以指导员工在未来事件处理过程中避免出错。

归档

参见早先在第 6.6 章“制定信息安全政策”中描述的归档规则。

有关事件管理和事件生命周期的综合指南，请参见附录第 A.1 节“更多材料”。

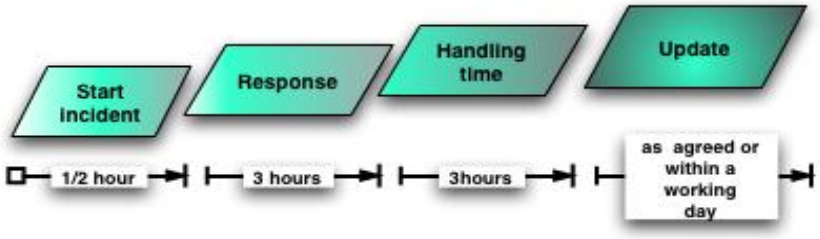
8.4. 响应时间表实例

响应时间的确定经常被忽略，但却是 CSIRT 与其服务对象之间构建良好服务级别协议 (SLA) 不可或缺的一部分。在事件处理过程中为用户群提供及时反馈对于用户群自身的职责和团队的声望都是至关重要的。

[29] CSIRT 手册：http://www.cert.org/archive/pdf/csirt-handbook.pdf

必须与服务对象明确响应时间，以避免错误的期望。以下最为基本的时间表可作为与 CSIRT 服务对象间制定更详细服务级别协议的开始。

以下是实际响应时间表实例，从收到援助请求开始：



图表. 16 响应时间表实例

习惯做法是引导服务对象接受响应时间，特别是在出现紧急事件与 CSIRT 联系时的响应时间。在多数情况下，最好在初期即联系 CSIRT，并鼓励服务对象在有疑问时联系 CSIRT。

8.5. 可用的 CSIRT 工具

本章提供 CSIRT 常用工具的部分指标。在此仅提供实例，更多指标可在“事件处理工具交换所”[30] (CHIHT) 找到。

电子邮件和消息加密软件

- GNUPG http://www.gnupg.org/
  GnuPG（开源“公钥加密”软件）是 RFC2440 OpenPGP 标准的开源实现，完整且免费。GnuPG 允许您对数据和通讯加密和数字签名。

- PGP http://www.pgp.com/
  商业实现

事件处理工具

管理事件及其进度，对操作保持跟踪。

- RTIR http://www.bestpractical.com/rtir/
  RTIR 是免费开源事件处理系统，针对 CERT 团队及其他事件响应团队需求而设计。

客户关系管理工具

当拥有大量不同用户群并需要跟踪所有预约和细节时，客户关系管理数据库便可大显身手。有大量不同的变化，以下是部分实例：

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

- Sugarforce（免费开源版本） http://www.sugarforge.org/

信息检查

- Website watcher（网站监察员） http://www.aignes.com/index.htm
  此程序监控网站的更新和变化。

- 监视网页 http://www.watchthatpage.com/
  该服务通过邮件发送有关网站变化的信息（免费和商业）。

[30] CHIHT:http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

查找联系信息

查找报告事件所需的正确联系信息绝不是项简单的任务。可以使用的信息源有以下几个：

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

此外，CHIHT 还列出了部分可用于查找联系信息的工具[34]。

虚构 CSIRT（步骤 8）

建立工作流程和操作及技术程序

虚构 CSIRT 重点关注交付核心 CSIRT 服务：

- 警报和警告
- 通告
- 事件处理

团队开发的程序运行良好，每个团队成员都能够轻松理解。虚构 CSIRT 同时聘用法律专家处理法律责任和信息安全政策。团队采用一些有用工具并通过与其他 CSIRT 讨论找到有关操作问题的相关信息。

生成安全建议和事件报告的固定模板。团队使用 RTIR 进行事件处理。

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

[32] RIPE 数据库中的 IRT-object：http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_01.htm#08

[33] Trusted Introducer:http://www.enisa.europa.eu/ENISA%20CERT/pages/04_01_03.htm#07

[34] CHIHT 中检查身份的工具：http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

9. CSIRT 培训

我们到目前为止已经采取以下各步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。
4. 环境和用户群分析。
5. 确定目标宣言。
6. 制定业务计划。
   a. 确定财务模式。
   b. 确定组织结构。
   c. 开始聘用员工。
   d. 利用并装备办公室。
   e. 制定信息安全政策
   f. 寻求合作伙伴。
7. 推进业务计划
   a. 使业务案例得到批准。
   b. 使一切与项目计划相符。
8. 使 CSIRT 具备可操作性。
   a. 创建工作流程
   b. 实施 CSIRT 工具

>> 下一步是：培训员工

本章列出两个主要 CSIRT 专用培训来源：TRANSITS 和 CERT/CC 课程。

9.1. TRANSITS

TRANSITS 是欧洲项目，目的在于通过解决经验丰富的 CSIRT 员工短缺的问题，促进计算机网络安全应急小组 (CSIRT) 的组建和现有 CSIRT 的加强。通过向（新） CSIRT 的员工提供专家培训课程，针对提供 CSIRT 服务中涉及的组织、经营、技术、市场和法律等问题对员工进行培训，使该目标得以实现。

尤其是，TRANSITS 具备

- 发展成熟、保持更新、定期修订的单元式培训课程资料
- 有组织的培训班，提供课程资料
- 允许（新）CSIRT 员工参加这些培训班，尤其强调欧盟成员国的参与
- 传播培训课程资料并确保宣传的结果[35]

ENISA 为 TRANSITS 课程提供便利与支持。如果需要了解申请课程的方法、要求和费用，请联系 ENISA 的 CSIRT 专家：

[35] TRANSITS：http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_02.htm#11

cert-relation@enisa.europa.eu

请在本文档的附录部分查找课程实例资料！

9.2. CERT/CC

计算机和网络基础设施的复杂性以及管理方面的挑战使恰当管理网络安全极其困难。网络和系统管理员在面对攻击方面，可用人员不足，同时缺乏安全实践，难以将损害降至最低。由此引起的是计算机安全事件频发。
当发生计算机安全事件时，组织必须快速有效地响应。组织对事件的识别、分析和响应越快，就越能限制损害，降低恢复成本。组建计算机网络安全应急小组 (CSIRT) 是提供快速响应能力的最佳途径，并有助于阻止未来事件的发生。

CERT-CC 为经理和技术人员提供的课程所涉及领域包括如创建并管理计算机网络安全应急小组 (CSIRT)、响应并分析安全事件、以及改善网络安全性。除非另有说明，否则所有课程均在宾夕法尼亚的匹兹堡市开设，我们的成员还会在卡耐基梅隆大学教授安全课程。

CSIRT 专用的 CERT/CC 课程[36]

创建计算机网络安全应急小组 (CSIRT)
管理计算机网络安全应急小组 (CSIRT)
事件处理的基础
技术员工的高级事件处理

请在本文档的附录部分查找课程实例资料！

虚构 CSIRT（步骤 9）
培训员工 虚构 CSIRT 决定派遣其所有技术员工参加下一次 TRANSITS 课程。团队负责人需额外参加 CERT/CC 的“管理 CSIRT”课程。

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

10. 练习：制定一份安全建议

我们到目前为止已经采取以下各步骤：

1. 理解什么是 CSIRT 及其能够带来的好处。
2. 新团队将向哪个领域提供服务？
3. CSIRT 可为其服务对象提供哪些类型的服务。
4. 环境和用户群分析。
5. 确定目标宣言。
6. 制定业务计划。
   a.确定财务模式。
   b. 确定组织结构。
   c. 开始聘用员工。
   d. 利用并装备办公室。
   e. 制定信息安全政策
   f. 寻求合作伙伴。
7. 推进业务计划
   a. 使业务案例得到批准。
   b. 使一切与项目计划相符。
8. 使 CSIRT 具备可操作性。
   a. 创建工作流程
   b. 实施 CSIRT 工具
9. 培训员工

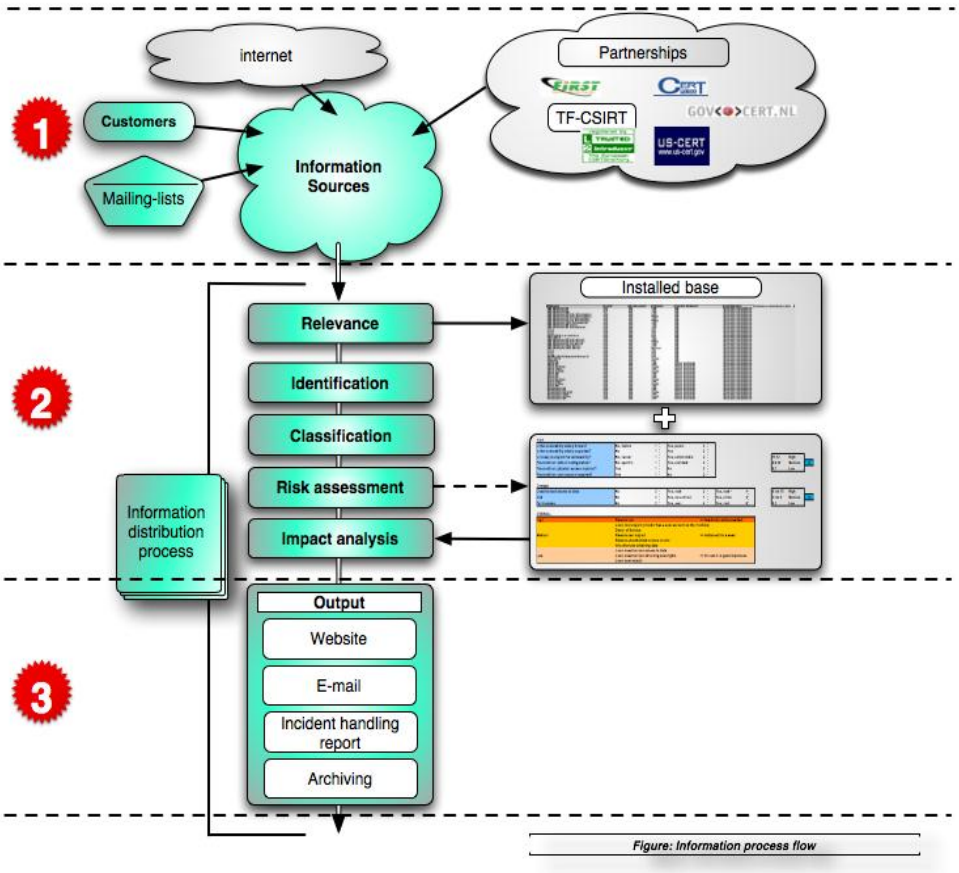
>> 下一步是练习并为实际投入工作做好准备！

作为说明，本章描述的是日常 CSIRT 任务的练习实例：创建安全建议。

起点便是以下由微软 (Microsoft) 发出的原始安全建议：

公告标识符	微软安全公告 **MS06-042**
公告标题	**Internet Explorer 累积性安全更新 (918899)**
摘要报告	本更新能够解决 Internet Explorer 中存在的多个允许远程代码执行的漏洞。
最高严重性评级	危急
漏洞的影响	远程代码执行
受影响的软件	**Windows、Internet Explorer。**如需更多信息，请参见受影响软件和下载位置一节。

本供应商公告处理的是近期发现的 Internet Explorer 中的漏洞。供应商针对多个版本的 Microsoft Windows 发布了多个软件修复。



虚构 CSIRT 在通过邮件列表收到此漏洞信息后，开始进入第 8.2 章“生成警报、警告和通告”中所述的工作流程。

步骤 1：收集漏洞信息。

第一步是浏览供应商网站。在网站上虚构 CSIRT 校验信息的可靠性并收集有关漏洞和受影响 IT 系统的更多细节。

步骤 2：鉴定信息并评估风险

识别

通过将电子邮件收到的漏洞信息与供应商网站上的文字相互验证，已完成对信息的校验。

相关性

虚构 CSIRT 将网站上找到的受影响系统清单与服务对象所使用的系统清单进行比对。经此发现至少有一个用户在使用 Internet Explorer，所以，漏洞信息确实是相关的。

类别	应用程序	软件产品	版本	操作系统	操作系统版本	用户
台式机	浏览器	IE	x-x-	Microsoft	XP-prof	A

分类

信息是公开的，因此可以使用并重新发送。

风险评估和影响分析

对问题的回答显示风险和影响水平为“高”（Microsoft 评级为危急）。

风险

漏洞是否是众所周知的？	是
漏洞是否广泛传播？	是
漏洞是否容易被利用？	是
漏洞是否远程可利用？	是

损害

可能的影响是远程可访问性及潜在的远程代码执行。本漏洞包含多个问题，使损害风险为“高”。

步骤 3：发送

虚构 CSIRT 是内部 CSIRT。其沟通渠道包括电子邮件、电话和内部网站。CSIRT 按第 8.2 章“生成警报、警告和通告”中的模板制作本建议。

建议标题
Internet explorer 中发现多个漏洞

参考编号
082006-1
受影响的系统
- 所有运行 Microsoft 的台式机系统

相关的操作系统和版本
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 和 Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 和 Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems 和 Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

风险 （高、中或低）
高
影响/潜在损害 （高、中或低）
高
外部 ID 是：（CVE，漏洞公告 ID）
MS-06-42

漏洞概述
Microsoft 发现 Internet Explorer 中存在多个危急漏洞可导致远程代码执行。

影响
攻击者可完全控制系统，安装程序、添加用户和争夺、更改或删除数据。缓解因素是，只有用户以管理员权限登录时会发生上述问题。使用权限较少的身份登录便可几乎不受影响。

解决方案
立即为 IE 安装补丁

描述（细节）
参见更多信息 ms06-042.mspx

附录
参见更多信息 ms06-042.mspx

本建议现已准备就绪，可以发送。由于是危急公告，建议在可能时致电用户群。

虚构 CSIRT（步骤 10）
练习 在运作的最初几周内，虚构 CSIRT 使用多个虚构案例（从其他 CSIRT 处获得作为实例使用）进行练习。而且，他们以硬件和软件供应商发布的实际漏洞信息为基础发布了一系列安全建议，并针对服务对象的需求进行调整。

11. 结论

本指南至此结束。本文档旨在简明概述组建 CSIRT 所需的各种流程。文档并未声明是完整的也不会涉及过多特定细节。相关推荐文献，请参见附录中第 A.1 节的“更多材料”。

虚构 CSIRT 接下来的重要步骤是：

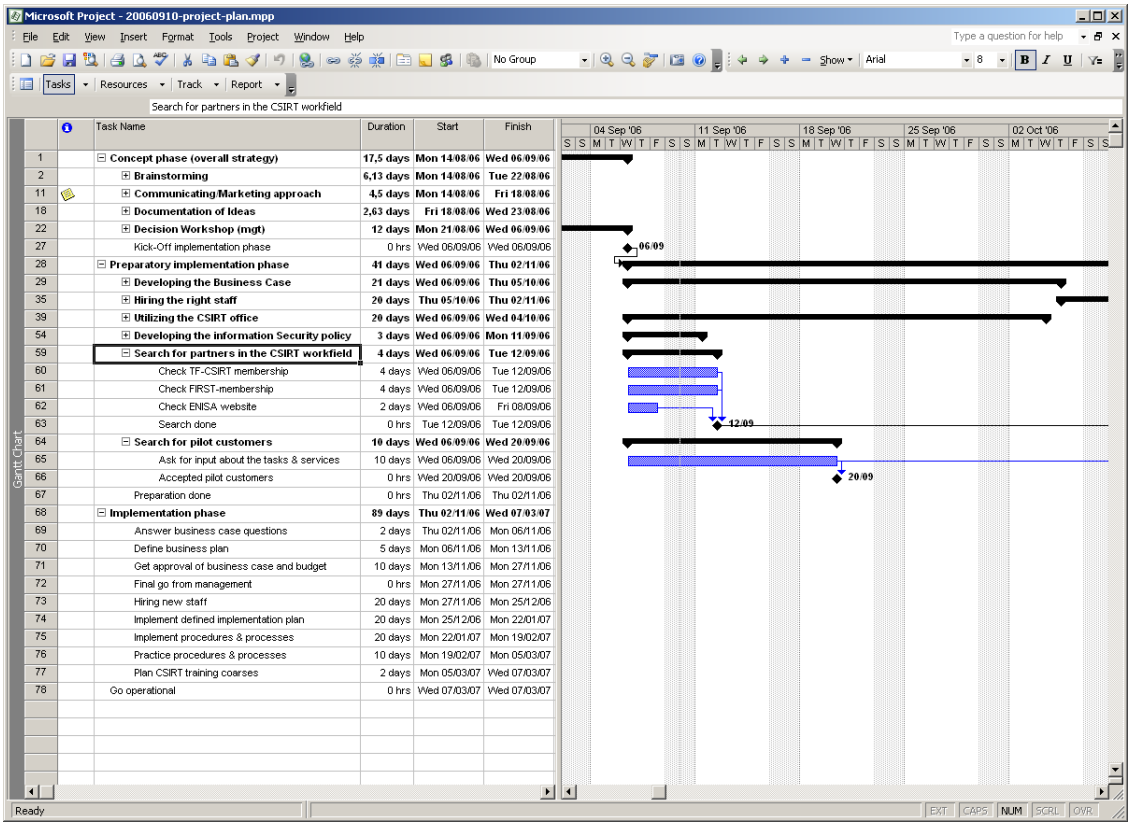
- 接收服务对象的反馈以便对提供的服务进行调整。
- 进入常规的日常工作
- 练习紧急情况
- 与各种 CSIRT 团体保持紧密联系，其目标应该是有朝一日能够投身志愿工作

12. 项目计划的描述

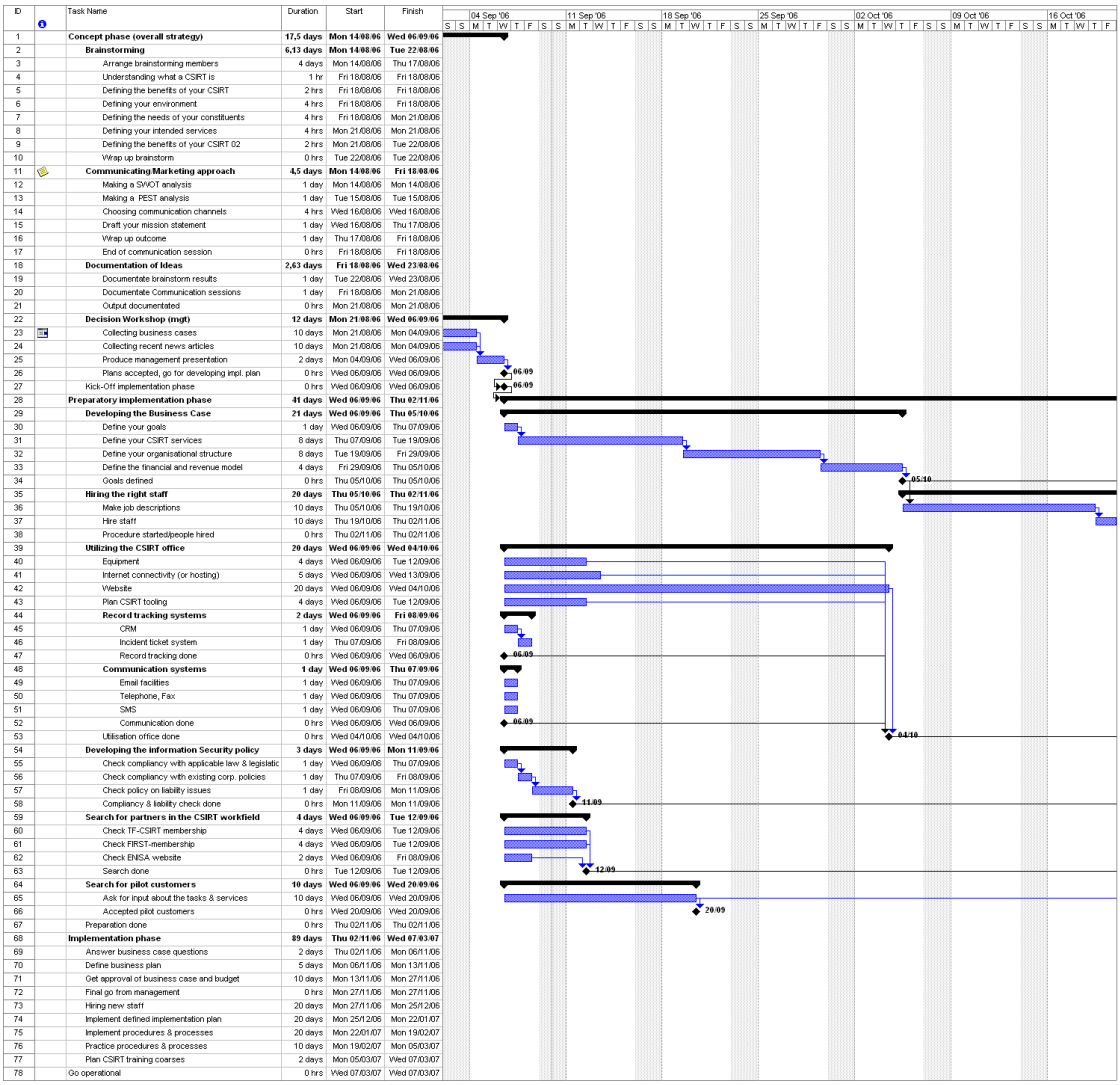
注：项目计划是对所需时间的首次预估。根据可用资源，项目的实际持续时间会有异。

可获得 CD 版的项目计划，也可从 ENISA 网站上获得项目计划。其完全涵盖本文档中描述的全部流程。

主格式是 Microsoft Project，因此可直接用于此项目管理工具。



图表. 17 项目计划



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the Information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

图表. 18 项目计划，包含所有任务和一部分甘特图

项目计划可用的格式还有 CVS 和 XML。需要更多可向 ENISA CSIRT 专家请求：cert-relations@enisa.europa.eu!

附录

A.1 更多材料

CSIRT 手册 (CERT/CC)
非常全面的参考手册，涉及所有与 CSIRT 工作相关的话题
来源：http://www.cert.org/archive/pdf/csirt-handbook.pdf

确定 CSIRT 事件管理流程：初稿
对事件管理的深入分析
来源：http://www.cert.org/archive/pdf/04tr015.pdf

计算机网络安全应急小组 (CSIRT) 实践现状
对有关世界各地 CSIRT 状况（包括历史、统计数字等）的实际情形的全面分析
来源：http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
对组建 GOVCERT.NL 和荷兰国家警报服务 'De Waarschuwingsdienst' 过程中的经验和教训的全面描述。
来源：http://www.govcert.nl/render.html?it=69

RFC 2350：对计算机网络安全应急响应的期望
来源：http://www.ietf.org/rfc/rfc2350.txt

NIST[37] 计算机安全事件处理指南
来源：http://www.securityunit.com/publications/sp800-61.pdf

ENISA 欧洲 CERT 活动清单
参考文献，列出了欧洲 CSIRT 及其各种活动的信息
来源：http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] NIST：美国国家标准和技术研究所

A.2 CSIRT 服务

特别感谢提供此列表的 CERT/CC

响应式服务	*主动服务*	*人工因素处理*
• 警报和警告 • 事件处理 • 事件分析 • 事件现场响应 • 事件响应支持 • 事件响应协调 • 漏洞处理 • 漏洞分析 • 漏洞响应 • 漏洞响应协调	• 通告 • 技术简报 • 安全监察或评估 • 安全配置和维护 • 安全工具的开发 • 入侵检测服务 • 安全相关的信息发布	• 人工因素分析 • 人工因素响应 • 人工因素响应协调 *安全质量管理* • 风险分析 • 业务持续性和灾难恢复 • 安全咨询 • 培养安全意识 • 教育培训 • 产品评估或认证

图表. 19CERT/CC 提供的 CSIRT 服务列表

服务描述

响应式服务

响应式服务旨在针对援助请求、CSIRT 服务对象发来的事件报告以及对 CSIRT 系统的威胁或攻击作出响应。部分服务可能由第三方通知或观察监控或 IDS 日志和警报发起。

警报和警告

本服务包括宣传描述入侵者攻击、安全漏洞、入侵警报、计算机病毒或欺骗的信息，并针对处理所产生问题，就应该采取的短期行动过程提供建议。作为对当前问题的响应发送警报、警告或建议，通知用户群相关活动并为保护用户群的系统或恢复受影响的系统提供指导。信息可以由 CSIRT 创建，也可自供应商、其他 CSIRT 或安全专家或其他部分的服务对象处获取并重新发布。

事件处理

事件处理涉及对请求和报告的接收、分检、和响应，以及对事件的分析。特别的响应活动可以包括

- 采取行动，保护受入侵者活动影响或威胁的系统和网络
- 通过相关建议和警报提供解决方案和减灾策略
- 寻找网络其他部分的入侵者活动
- 过滤网络信息流通量
- 重建系统
- 修补或修复系统
- 制定其他响应或临时策略

由于事件处理活动是由不同类型的 CSIRT 以不同的方式实施，根据采取的活动类型以及援助类型对本服务进一步分类如下：

事件分析

在此有多个层面的事件分析和多个子服务。实质上，事件分析是对所有可用信息和证据或与事件相关的人工因素的检验。分析的目的是识别事件范围、事件导致的损害程度、事件性质以及可用的响应策略或应急措施。CSIRT 可利用漏洞和人工因素分析（描述见下文）的结果了解特定系统发生的一切，并提供最完整的全新分析。CSIRT 将事件的活动关联起来以确定相互关系、趋势、模式或入侵者签名。根据 CSIRT 的使命、目标和流程，可作为事件分析的一部分提供的两项子服务是

法庭证据收集

收集、保留、记录和分析发生泄密的计算机系统的证据，确定系统遭受的更改并辅助重现导致泄密的事件。信息和证据的收集必须能够提供可查验并且是法院依据举证程序法规可采纳的监管链。涉及法庭证据收集的任务包括（但不限于）制作受影响系统硬盘的位图复本；检查系统的更改，如新程序、文件、服务和用户；查看运行的程序和开放端口；以及检查特洛伊木马程序和工具包。履行此职责的 CSIRT 员工应准备好担任审判程序的专家证人。

跟踪

跟踪入侵者的来源或识别入侵者访问的系统。此活动包括跟踪了解入侵者侵入受影响系统和相关网络的方式、完成访问所使用的系统、攻击的源头、以及还有哪些系统和网络曾作为攻击的一部分。还包括尝试确定入侵者身份。此项工作可独立完成，但通常会涉及与执法人员、互联网服务提供商、或其他相关机构一起合作。

事件现场响应

CSIRT 提供直接的现场援助，以帮助用户群从事件中恢复。CSIRT 亲自对受影响系统进行物理分析并执行系统修复和恢复，而不仅仅是通过电话或电子邮件提供应急响应支持（见下）。此服务包含遇可疑事件或发生事件时所需当地采取的全部行动。如果 CSIRT 不在受影响现场，团队成员可出差到现场并执行响应。在其他情况下，当地团队可能已经在现场，按日常工作提供事件响应。在事件处理作为系统、网络或安全管理员日常工作职责的一部分提供，取代组建 CSIRT 时尤为如此。

事件响应支持

CSIRT 通过电话、电子邮件、传真或文档辅助并指导攻击受害者从事件中恢复。所涉及的技术援助包括对收集的信息进行整理分析、提供联系信息、或转达对减缓和恢复策略的指导。该种形式并不涉及上述直接现场应急响应行动。CSIRT 可远程提供指导，现场人员可自行执行恢复。

事件响应协调

CSIRT 在事件所涉各方间协调响应工作。各方通常包括攻击的受害者、攻击涉及的其他站点和在攻击分析中请求援助的任何站点。还可包括为受害者提供 IT 支持的各方，如互联网服务提供商、其他 CSIRT 以及网站的系统和网络管理员。协调工作包括收集联系信息、通知网站其潜在的受牵连性（作为受害者或攻击源）、收集有关牵涉网站数的统计数字并促进信息的交换与分析。部分协调工作可能包括通知组织的法律顾问、人力资源或公共关系部门并与之协作。还包括与执法机构的协调。此服务不提供直接的现场事件响应。

漏洞处理

漏洞处理包括接收有关硬件和软件漏洞的信息和报告；分析漏洞的性质、机制和影响、并为检查和修复漏洞制定响应策略。由于漏洞处理活动是由不同类型的 CSIRT 以不同的方式实施，此服务根据采取的活动类型以及援助类型进一步分类如下：

漏洞分析

CSIRT 对硬件或软件中的漏洞执行技术分析和检查。这包括可疑漏洞的校验和硬件或软件漏洞的技术检测以确定漏洞位置及被利用方式。分析可包括检查源代码、使用调试程序确定漏洞发生位置、或尝试在测试系统上再现问题。

漏洞响应

此服务包括确定适当响应以减缓或修复漏洞。可包括开发或研究补丁、修补和应急措施。还包括通过创建并发送建议或警报，将缓解策略通知其他人。服务包括通过安装补丁、修补或应急措施执行响应。

漏洞响应协调

CSIRT 就漏洞事宜通知企业或服务对象的相关各方并共享有关漏洞修补或减缓的信息。CSIRT 查明漏洞响应策略已成功实施。此服务可涉及与供应商、其他 CSIRT、技术专家、用户成员、以及最初发现并报告漏洞的个人或团体的沟通。活动包括推动对漏洞或漏洞报告的分析、协调相应文档、补丁或应急措施的发布时间安排、以及将不同各方完成的技术分析进行合成。此服务还可包括对公共或私人的漏洞信息或相应响应策略的归档或知识库的维护。

人工因素处理

人工因素是系统上查找到的文件或对象，可能是探测或攻击系统和网络的文件或对象、也可能是用于对抗安全措施的文件或对象。人工因素包括但不限于计算机病毒、木马程序、蠕虫、脚本病毒和工具包。

人工因素处理涉及收集有关信息以及入侵者攻击、勘测和其他未授权或破坏活动中所用的人工因素复本。一旦收到，即对人工因素展开检查。检查包括分析人工因素的性质、机制、版本和使用、制定（或建议）响应策略以检查、移除和防御这些人工因素。由于人工因素处理活动是由不同类型的 CSIRT 以不同的方式实施，此服务根据采取的活动类型以及援助类型进一步分类如下：

人工因素分析

CSIRT 对系统中找到的任何人工因素进行技术检测和分析。完成的分析可包括识别人工因素的文件类型和结构、比较新的和现有的人工因素或同一人工因素的不同版本，以了解其相似性和差异、或反向设计或汇编代码以确定人工因素的目的和功能。

人工因素响应

为检测和移除系统中的人工因素应采取的行动，以及为阻止人工因素的安装应采取的行动均会通过本服务得以确定。还涉及创建签名，签名可添加到反病毒软件或 IDS。

人工因素响应协调

此服务涉及将与人工因素有关的分析结果和响应策略与其他研究人员、CSIRT、供应商和安全专家共享及合成。活动包括通知他人并将不同来源的技术分析加以合成。活动还包括对有关已知人工因素及其影响以及相应响应策略的公开或用户所拥有的归档进行维护。

主动服务

主动服务旨在事件发生前或检测到事件前，改善服务对象的基础设施和安全流程。主要目标是避免事件并在事件发生时降低其影响并缩小其范围。

通告

通告包括但不限于入侵警报、漏洞警告和安全建议。这些通告会通知用户群有中长期影响力的最新发展，如新发现的漏洞或入侵工具。通告使用户群能够在最新发现的问题被利用之前保护其系统和网络。

技术简报

CSIRT 会监控并观察新技术研发、入侵者活动、及相关趋势以帮助识别未来威胁。所评论的话题可扩大到包括法律法规上的规则、社会或政治上的威胁以及新兴技术。此服务涉及阅读安全邮件列表、安全网站、以及科学、技术、政治及政府领域的最新新闻和期刊文章，提取与用户系统和网络安全性相关的信息。服务可包括与这些领域的权威各方的沟通，以确保获得最好、最精准的信息和解释。此服务最终会形成一些着眼于中长期安全问题的通告、指南、或建议。

安全监察或评估

此服务依据组织制定的或其他适用的行业标准制定的要求，对一个组织的安全基础设施进行详细审核和分析。还包括对组织安全实践的评审。可提供的监察或评估有多种不同类型，包括

基础设施检查

手动检查硬件和软件配置、路由器、防火墙、服务器和台式设备以确保其符合组织或行业最佳实践的安全政策和标准配置。

最佳实践检查

询问员工及系统和网络管理员，以确定其安全实践是否与制定的组织安全政策或部分特定的行业标准相匹配

扫描

使用漏洞或病毒扫描以确定易受攻击的系统和网络。

渗透测试

通过有目的的攻击系统和网络以测试网站的安全性

在执行此类监察或评估之前需取得高级管理层的批准。部分方法可能会是组织政策所禁止的。提供此类服务可包括制定一套执行测试或评估可用的通用实践方法，同时针对负责执行测试、评估、监察或审核的员工，制定一套所需技能或认证要求。此服务还可向具备执行监察和评估专业知识的第三方承包商或托管的安全服务提供商寻求外包。

安全工具、应用程序、基础设施和服务的配置和维护

此服务可识别对 CSIRT 服务对象或 CSIRT 自身所用工具、应用程序和整体计算机基础设施进行安全配置与维护的方法并提供适当的指导。除了提供指导之外，CSIRT 还可执行配置更新并可维护安全工具和服务，如 IDS、网络扫描或监控系统、过滤器、包装器、防火墙、虚拟专用网络 (virtual private networks, VPN)或验证机制。CSIRT 甚至可以将其作为主要职能提供这些服务。CSIRT 还可根据安全指南配置并维护服务器、台式机、笔记本、个人数字助理 (PDAs) 以及其他无线设备。服务包括在 CSIRT 认为会使系统易受攻击时，对配置中的问题或工具和应用程序的使用进行管理升级。

安全工具的开发

此服务包括服务对象或 CSIRT 自己要求或期望的新的、用户特定的工具开发。服务包括（举例来说）为服务对象所用的定制软件开发安全补丁或为重建受感染主机开发安全软件套装。还包括开发能够扩展现有安全工具功能性的工具和脚本，如针对漏洞的新插件或网络扫描、能够推动加密技术使用的脚本或自动补丁分发机制。

入侵检测服务

履行此服务的 CSIRT 检查现有的 IDS 日志、对任何达到其限定极限值的事件进行分析并做出响应、或根据预先确定的服务级别协议或升级策略转发警报。入侵检测和关联安全日志的分析是一项艰巨的任务，不仅要确定传感器在环境中的放置位置，还要收集并分析捕获的大量数据。在多数情况下，合成并解释信息需要具备专业工具或专业知识才可以识别错误的警告、攻击、或网络事件并采取措施消除或减少此类事件。部分组织选择将此类活动外包给其他拥有更多专业知识的人，如托管安全服务提供商。

安全相关的信息发布

此服务为用户群提供全面的、易于查找并旨在改进安全性的有用信息集合。此类信息可包括

- 针对 CSIRT 的报告指南和联系信息
- 警报、警告和其他通告的归档
- 有关当前最佳实践的文档
- 一般计算机安全指南
- 政策、程序和核对清单
- 补丁开发和发送信息
- 供应商链接
- 当前事件报告中的统计数字和趋势
- 其他可以改善整体安全实践的信息

这些信息可以由 CSIRT 或组织的其他部门（IT、人力资源、或媒体关系）开发并发送，可以包括来自外部资源，如其他 CSIRT、供应商和安全专家的信息。

安全质量管理服务

凡属此类别的服务并非唯一针对事件处理或特别针对 CSIRT。这些是已广泛普及、已得到认可的服务，旨在改善组织整体的安全性。通过利用在上述响应式和主动服务中获得的经验，CSIRT 可为这些原本无法利用的质量管理服务带来独特的视角。这些服务的目的是，以在对事件、漏洞和攻击的响应中获得的知识为基础，融入反馈和经验及教训。将这样的经验融入已确立其地位的传统服务（见下述）作为安全质量管理过程的一部分，可以改进组织内的长期安全工作。根据不同的组织结构和责任，CSIRT 可以提供这些服务，或作为更大组织团队的一部分参与其中。
以下描述解释了 CSIRT 的专业知识如何使每项此类安全质量管理服务受益。

风险分析

CSIRT 可以为风险分析和评估带去增值效应。这将改进组织评估实际威胁的能力，对信息资产中的风险提供实际可行的品质化和量化评估，并对保护和响应策略进行评审。履行服务的 CSIRT 可以指导或辅助针对新系统和业务流程的信息安全风险分析活动，评估对用户资产和系统的威胁与攻击。

业务持续性和灾后恢复计划

参考过去发生的事件和对新浮现事件或安全趋势的未来预测，越来越多的事件有给业务运营带去灭顶之灾的潜在可能性。因此，计划工作在确定如何对此类事件做出最佳响应以确保业务运营持续性时，必须考虑到 CSIRT 的经验和建议。履行此服务的 CSIRT 在应对与计算机安全威胁和攻击有关事件时就涉及业务持续性和灾后恢复计划。

安全咨询

可利用 CSIRT 为用户业务运营实施最佳安全实践提供建议和指导。针对购买、安装或保卫新系统、网络设备、软件应用程序或企业范围的业务流程事宜，提供此服务的 CSIRT 均参与准备建议与识别需求。服务包括在组织或服务对象安全政策开发过程中提供指导和援助。还涉及为立法机构或其他政府机关提供证据或建议。

培养安全意识

CSIRT 能够识别用户群需要更多信息的地方，并指导用户更好地遵守公认的安全实践和组织安全政策。用户群体安全意识的普及不仅能改善其对安全问题的理解，也能帮助他们以更安全的方式履行其日常职责。这样做可减少攻击成功几率，增加用户成功检测和报告攻击的机会，从而减少恢复所需时间并消除或降低损失。
履行服务的 CSIRT 通过制作文章、海报、时事通讯、网站或其他信息资源，解释安全最佳实践并对应采取的预防措施提供建议，以期增强安全意识。活动还包括进度安排会议和研讨会，以使用户群掌握安全程序和对组织系统的潜在威胁的最新动态。

培训/教育

服务包括通过研讨会、培训班、课程和自学教程向用户群提供有关计算机安全问题的信息。话题包括事件报告指导、适当的响应方法、事件/响应工具、事件预防方法和其他保护、检测、报告和响应计算机安全事件的必要信息。

产品评估或认证

就履行此服务而言，CSIRT 可对工具、应用程序或其他服务进行产品评估以确保产品的安全性及其对公认的 CSIRT 或组织安全实践的遵从性。检查的工具和应用程序可以是开源

的或商业产品。此服务可作为评估提供，也可通过认证程序提供，具体要取决于组织或 CSIRT 所应用的标准而定。

A.3 实例

虚构 CSIRT

步骤 0 — 理解什么是 CSIRT：

作为实例的 CSIRT 将为一家由 200 名员工组成的中型机构服务。该机构有其自己的 IT 部门，并在同一个国家拥有另外两处分支机构。IT 在公司内扮演着绝对重要的角色，内部通讯、数据网络和全天候电子商务全都离不开 IT。该机构拥有自己的网络，通过两家不同的 ISP 配置冗余连接到互联网。

步骤 1：启动阶段

在启动阶段，新 CSIRT 计划作为内部 CSIRT，为托管公司、其在当地的 IT 部门和员工提供服务。同时还为不同办事处之间的 IT 安全相关事件的处理提供支持和协调。

步骤 2：选择正确的服务

在开始阶段已经决定新 CSIRT 将着重为员工提供核心服务。

已经决定的是，在试点阶段后将考虑扩展服务，可能会添加“安全管理服务”。具体决定将以试点用户群的反馈为基础并通过与质量保证部门紧密合作而最终得出。

步骤 3：对服务对象和适当的沟通渠道进行分析

与管理层和服务对象的关键人物举行会议，集思广议，为 SWOT 分析法准备足够的内容。所得结论是有需要核心服务的需求：

- 警报和警告
- 事件处理（分析、响应支持和响应协调）
- 通告

必须确保信息在组织严密的前提下发送，并且能够收到信息的服务对象越多越好。因而在此决定，以安全建议为形式的警报、警告和通告将在专用网站上发布，并通过邮件列表发送。CSIRT 则通过电子邮件、电话和传真接收事件报告。下一步计划用统一的网页表单。

步骤 4：目标宣言

虚构 CSIRT 的管理层制定了以下目标宣言：
“虚构 CSIRT 为其托管公司的员工提供信息和帮助，降低计算机安全事件造成的风险并在此类事件发生时做出响应。”

据此，CSIRT 明确表明其是内部 CSIRT，其核心业务是处理 IT 安全相关的问题。

步骤 5：制定业务计划

财务模式
由于公司拥有全天候电子商务业务以及全天候服务的 IT 部门，因而决定在办公时间内提供全套服务，办公时间之外提供值班服务。为服务对象提供的服务将是免费的，但是在试点和评估阶段可能会对外部客户提供的服务进行评估。

收入模式
在启动和试点阶段，CSIRT 将由托管公司资助。在试点和评估阶段将讨论更多的资助，包括向外部客户销售服务的可能性。

组织模式
托管组织是小型公司，因而选择了嵌入模式。
在办公时间内，三名员工之一将提供核心服务（发布安全建议和事件处理/协调）。

公司的 IT 部门已经聘用到具备适当技能的员工。与该部门达成协议，新 CSIRT 可在需要时临时请求支持。同时也可以使用二线值班技术人员。
将有一个核心 CSIRT 团队，包含四名全职成员和五名 CSIRT 团队成员。这些人中有一名可以循环轮班。

员工
CSIRT 团队负责人具备安全相关的以及第一、二级支持的专业背景，并具备危机应变管理工作相关工作经验。其他三名团队成员是安全方面的专家。来自 IT 部门的兼职 CSIRT 团队成员在公司基础设施各自负责领域也都是专家级人物。

步骤 6 利用办公室和信息安全政策
办公室设备和地点
由于托管公司已经拥有足够的物理安全措施，新 CSIRT 在此方面已得到良好补充。一间被称之为“作战室”的房间用作紧急情况协调室。购买了保险箱用于存放加密资料和敏感文档。设立了独立的电话线，包括电话交换台，以便在办公时间接听热线，同时在非办公时间可用号码相同的手机值班。

现有的设备和企业网站也可用于公布 CSIRT 相关的信息。安装并维护邮件列表软件，其中一部分仅限于团队成员与其他团队间的沟通。所有员工的详细联系信息都存储在一个数据库中，一份打印稿保存在保险箱中。

法规
由于 CSIRT 是利用现有信息安全政策嵌入公司的，针对 CSIRT 的对应政策已在公司法律顾问的帮助下确立。

步骤 7 寻求合作

通过使用 ENISA 的清单可快速查找到一个国家的一些 CSIRT 并与之取得联系。为新近聘用的团队负责人安排对其中一支 CSIRT 的实地拜访。他了解到国家 CSIRT 活动并出席了一次会议。

会议的收获不仅仅是有助于收集工作方法的实例，还获得了其他团队的支持。- -

步骤 8 推进业务计划

现决定从公司历史记录中收集确实的消息。这对于 IT 安全形势的统计概览非常有用。当 CSIRT 组建并开始运作时，应该继续此类收集，以确保掌握最新的统计数字。

联系其他国内 CSIRT 并采访了解其业务计划。他们将有关 IT 安全事件的最新发展及事件所耗成本等信息编译成幻灯片，以期能够提供必要支持。

在此虚构 CSIRT 的示例中，说服管理层，使其了解 IT 业务的重要性的需求并不迫切，而且要开始第一步骤并不困难。准备业务案例和项目计划，包括对组建成本和运作成本的预估。

- -

步骤 9 建立工作流程和操作及技术程序

虚构 CSIRT 重点关注交付核心 CSIRT 服务：

- 警报和警告
- 通告
- 事件处理

团队开发的程序运行良好，每个团队成员都能够轻松理解。虚构 CSIRT 同时聘用法律专家处理法律责任和信息安全政策。团队采用一些有用工具并通过与其他 CSIRT 讨论找到有关操作问题的相关信息。

生成安全建议和事件报告的固定模板。团队使用 RTIR 进行事件处理。

- -

步骤 10 培训员工

虚构 CSIRT 决定派遣其所有技术员工参加下一次 TRANSITS 课程。团队负责人需额外参加 CERT/CC 的“管理 CSIRT”课程。

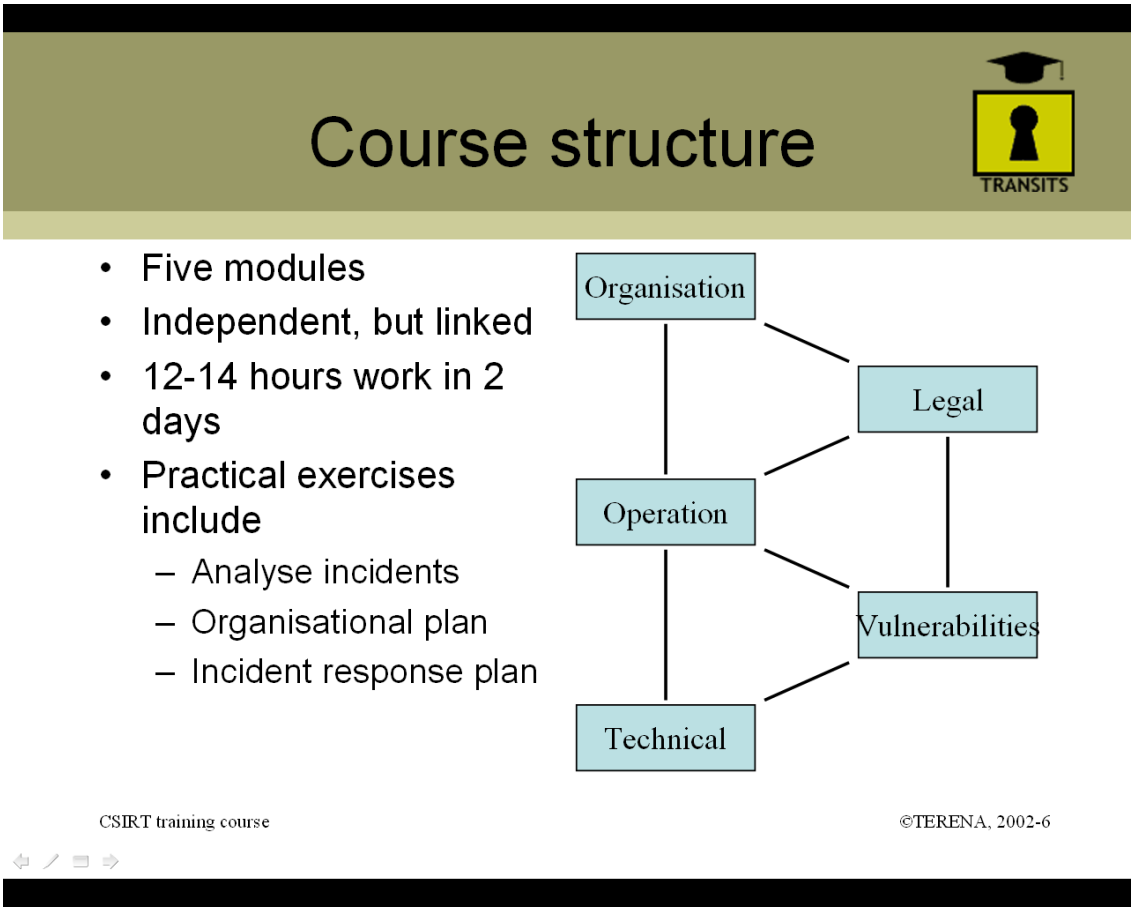
- -

步骤 11：练习

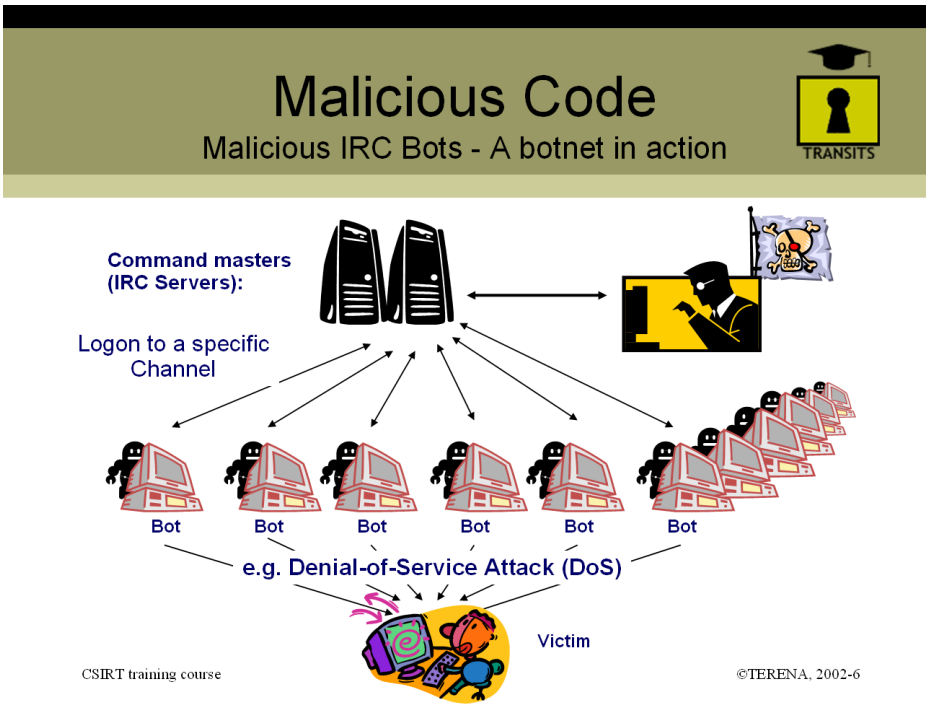
在运作的最初几周内，虚构 CSIRT 使用多个虚构案例（从其他 CSIRT 处获得作为实例使用）进行练习。而且，他们以硬件和软件供应商发布的实际漏洞信息为基础发布了一系列安全建议，并针对服务对象进行调整。

A.4 CSIRT 课程中的实例资料

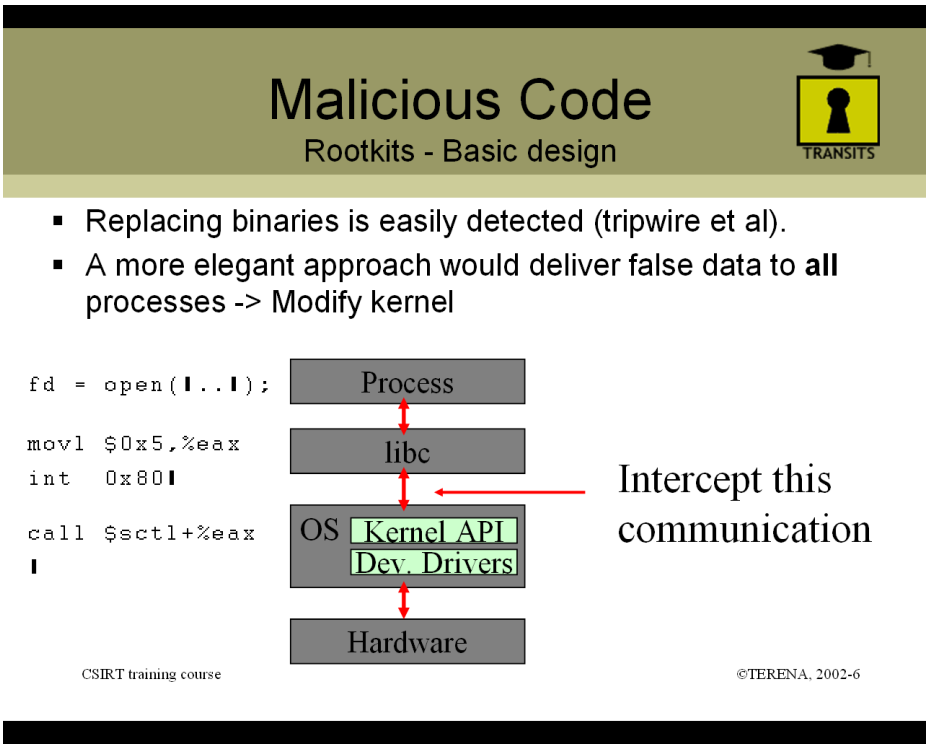
TRANSITS（经 Terena 特许，http://www.terena.nl）



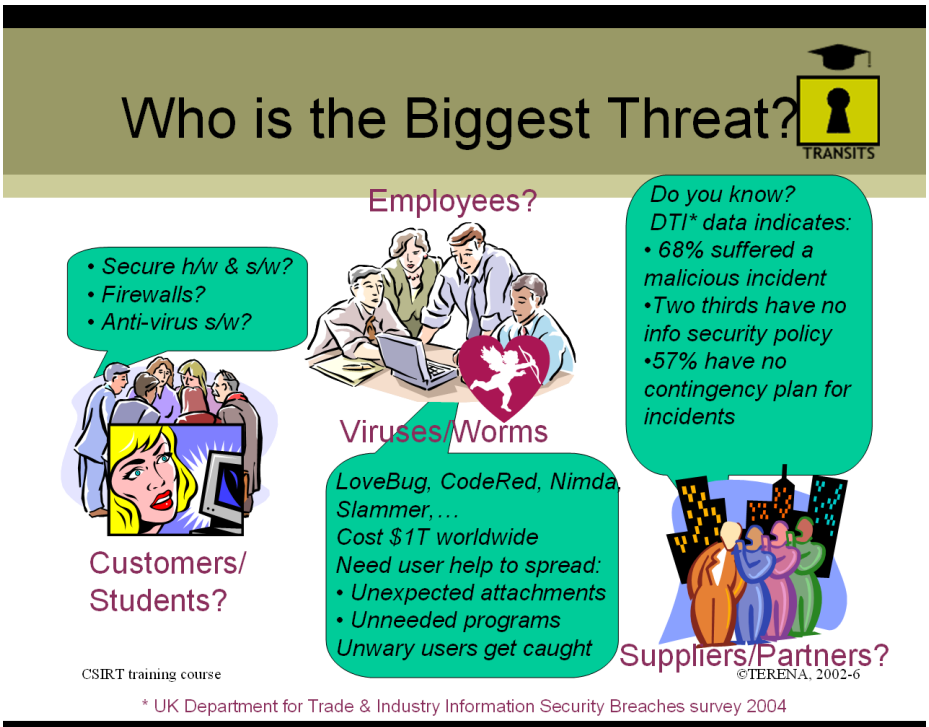
概览：课程结构



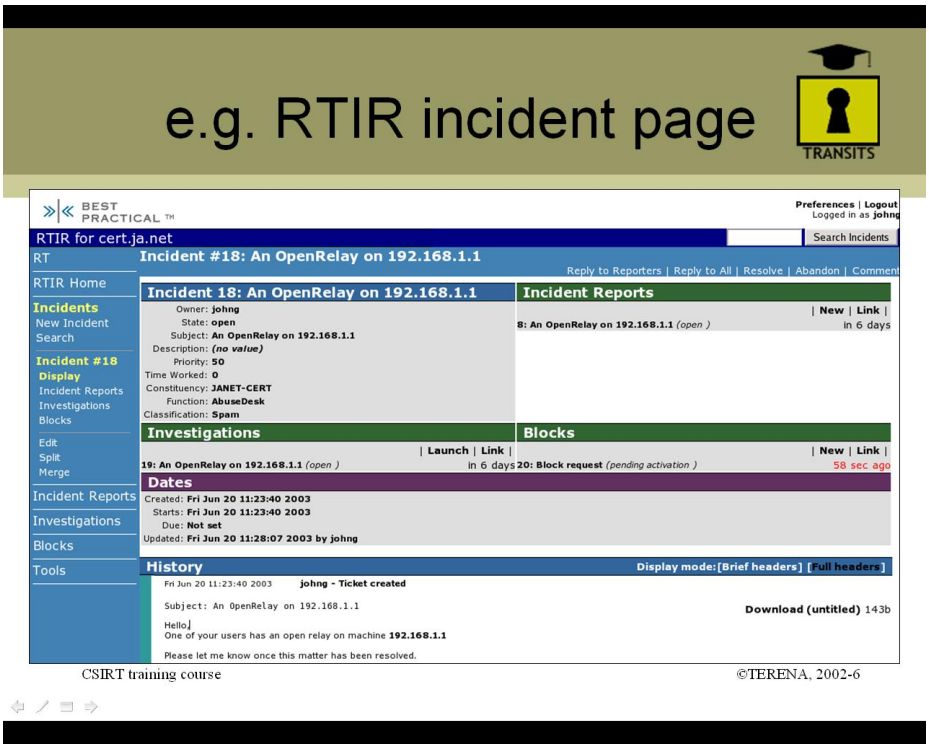
来自*技术模块*：僵尸网络 (Botnet) 的描述



来自*技术模块*：Rootkit 的基本设计



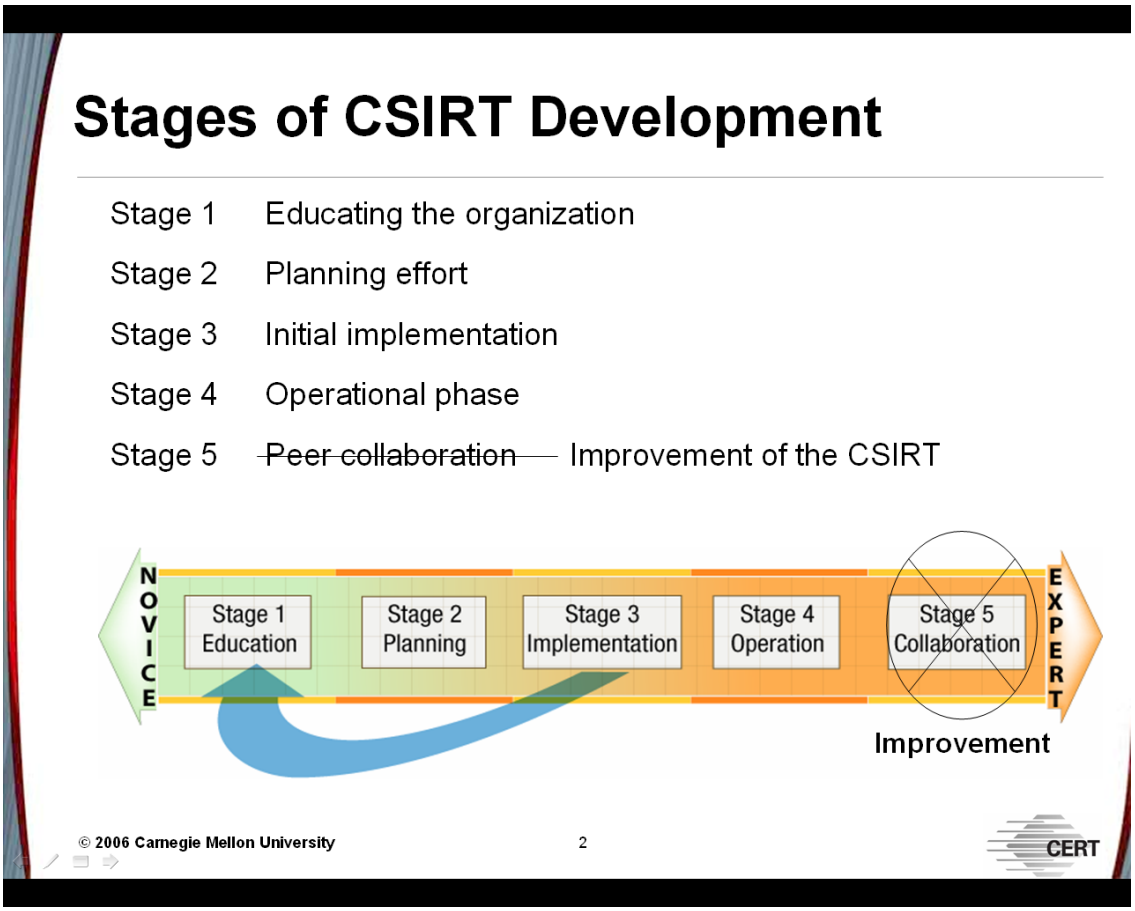
来自*组织模块*：圈内人或圈外人 — 谁受威胁更大？



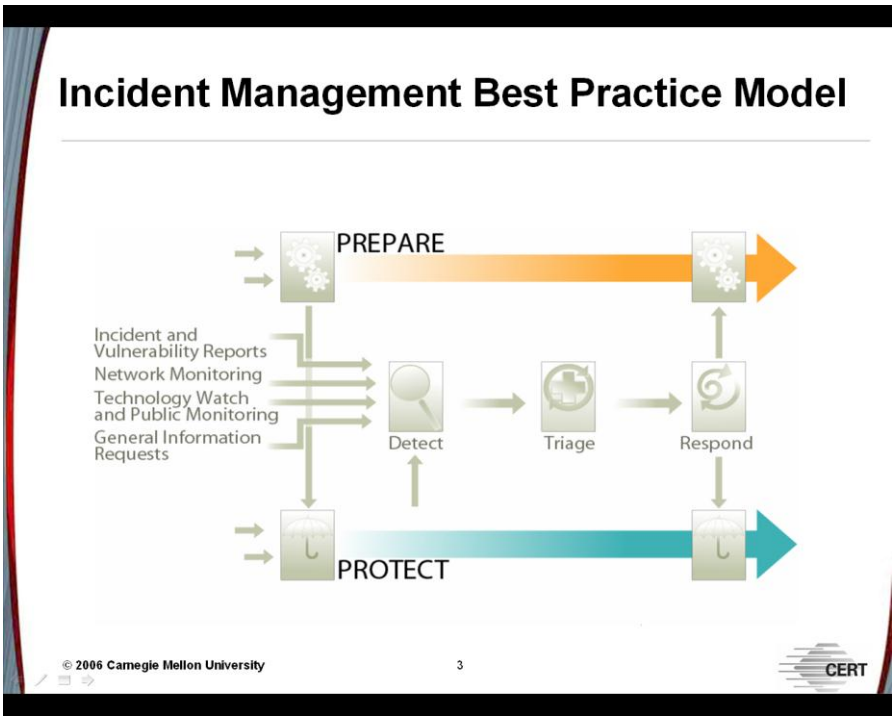
来自*操作跟踪*：针对事件响应的问题跟踪系统 (RTIR)

“组建 CSIRT”（经 CERT/CC 特许，http://www.cert.org）

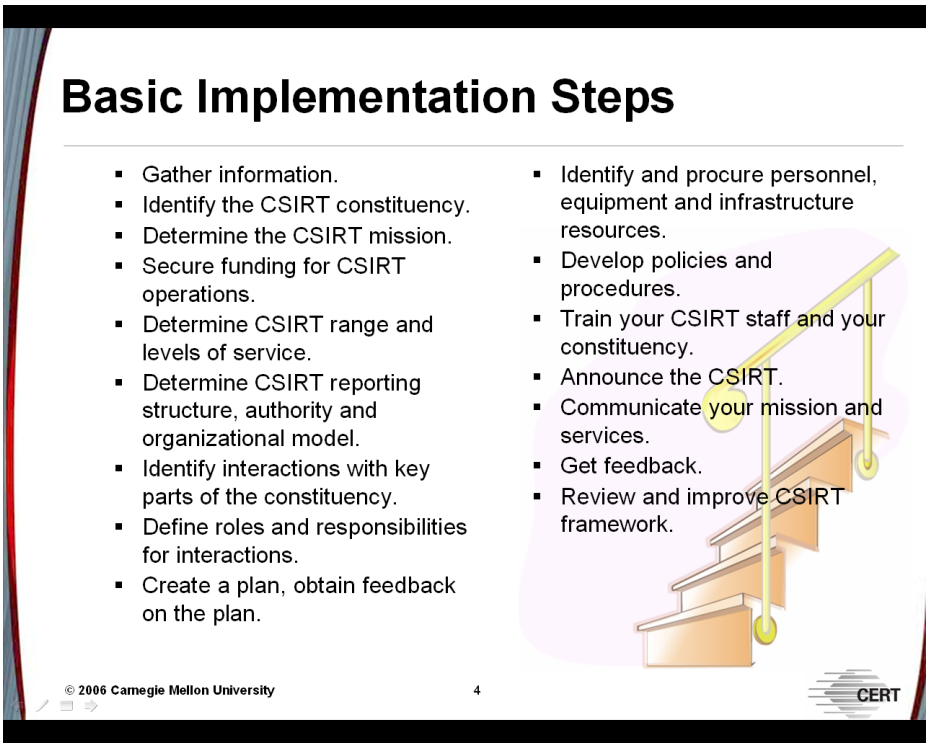
ENISA 对 CERT 计划的 CSIRT 开发团队允许我们使用其培训课程的内容表示衷心的感谢！



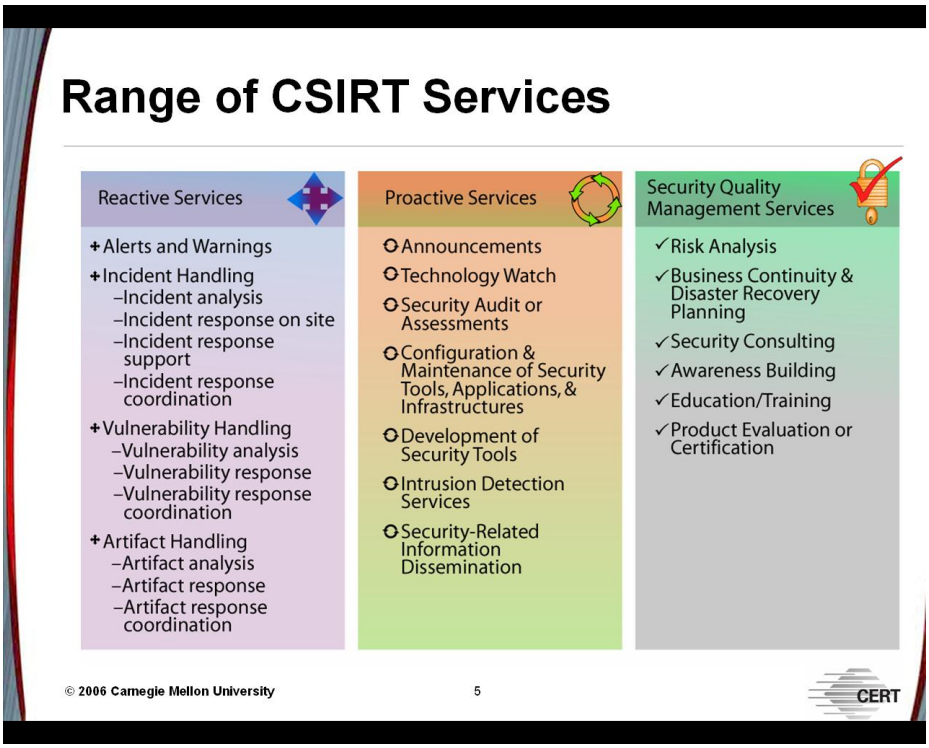
来自 *CERT/CC 培训课程*：CSIRT 的开发阶段



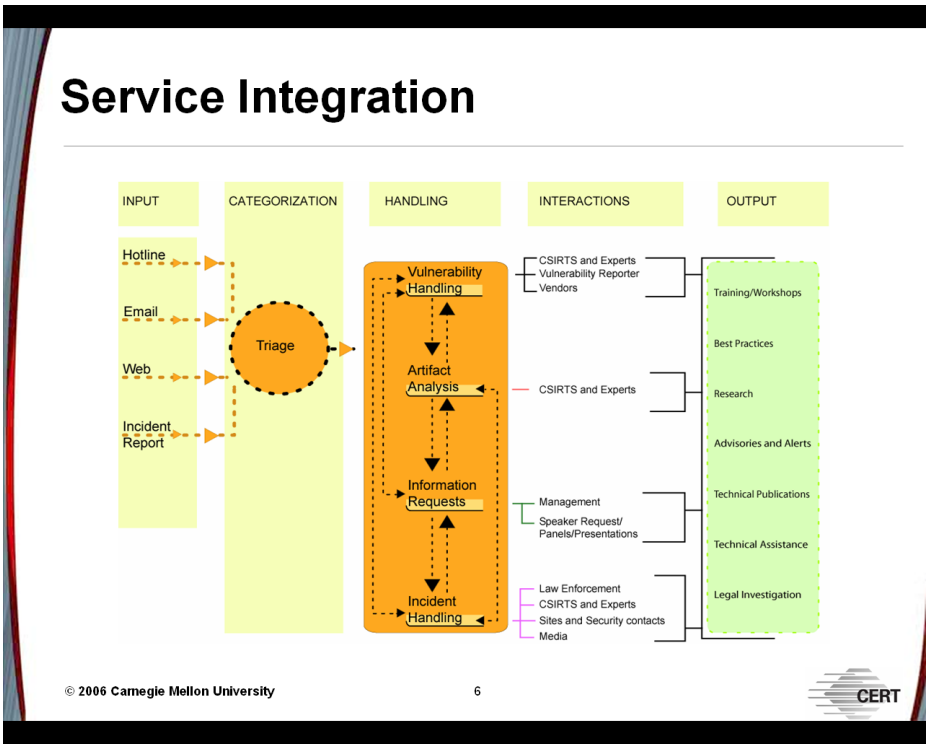
来自 *CERT/CC 培训课程*：事件管理中的最佳实践



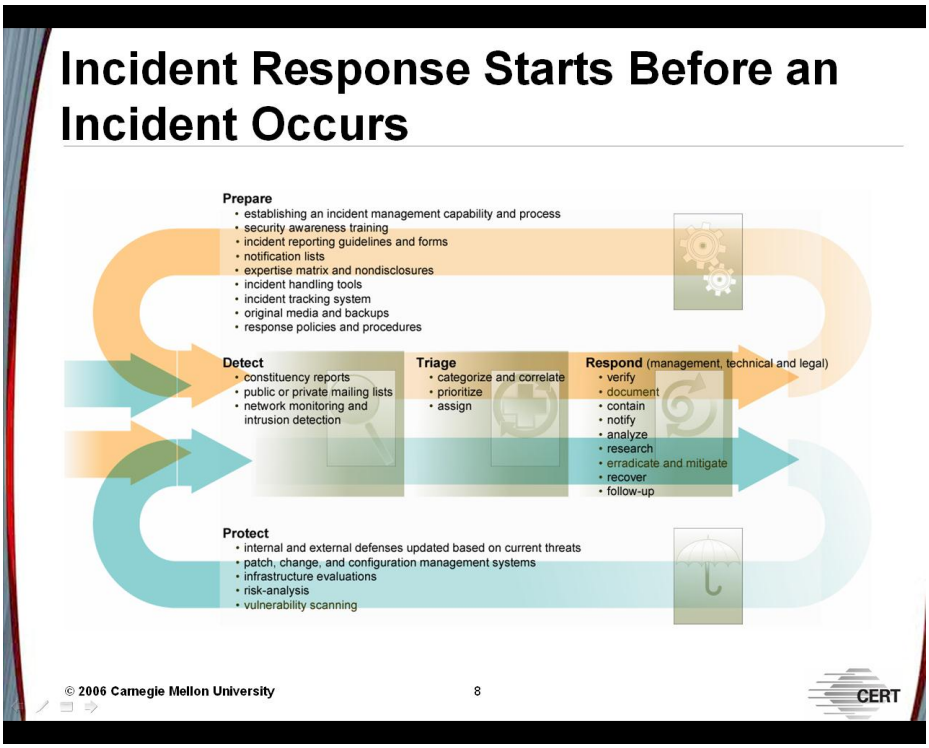
来自 *CERT/CC 培训课程*：组建 CSIRT 应遵循的步骤



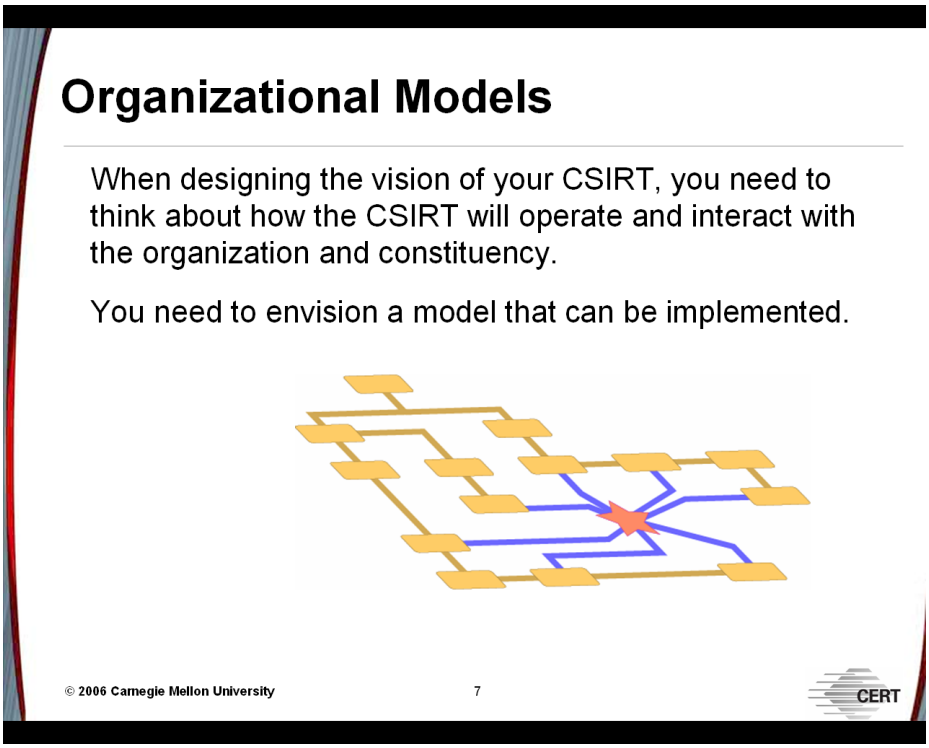
来自 *CERT/CC 培训课程*：CSIRT 可提供的服务



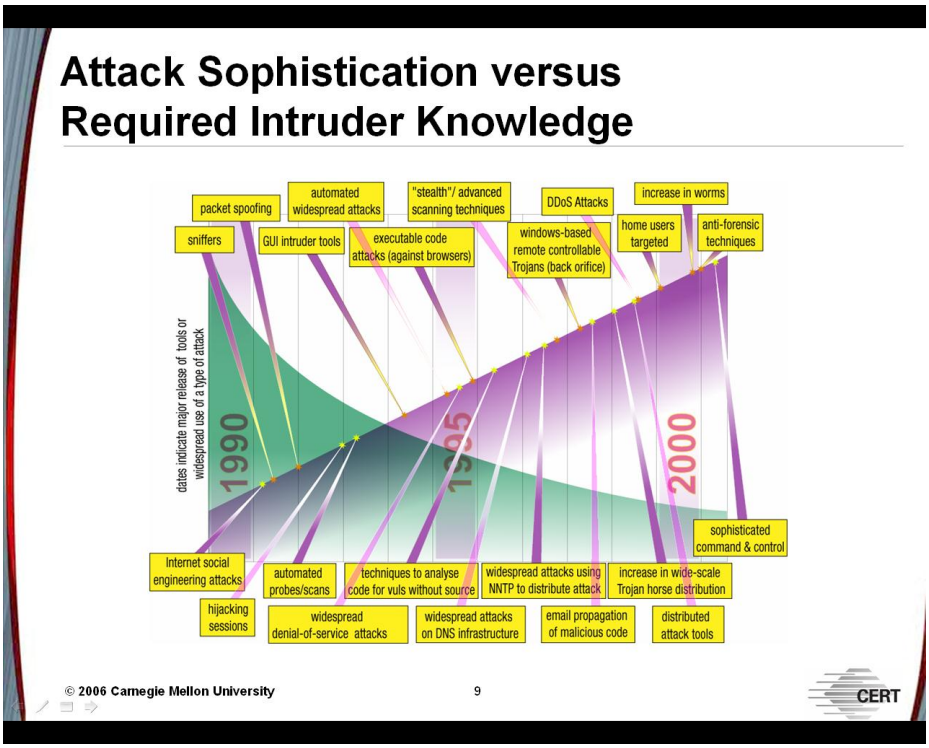
来自 *CERT/CC 培训课程*：事件管理工作流程



来自 *CERT/CC 培训课程*：事件响应



来自 *CERT/CC 培训课程*：应该如何组织 CSIRT？



来自 *CERT/CC 培训课程*：了解的越少，损害越多