利用 Cisco IDS 4250 传感器改善 Cisco IT IDS 的性能

思科@ IT 案例分析/安全性/Cisco IDS 4250 传感器：该案例将介绍思科 IT 部门在思科全球网络中部署内部入侵检测系统（IDS）解决方案的方法。思科全球网络是世界上规模最大、最复杂的领先企业环境之一。思科客户可以借鉴思科 IT 部门取得的经验，更好地满足类似的企业需求。

思科信息安全部门于 2001 年部署了 Cisco IDS 4230 传感器。此次部署不但证实了这种部署方案对思科的价值，还增进了思科对入侵检测的了解。但是，IDS 4230 传感器的性能和管理还有一些局限，为突破这些局限，思科移植到了 Cisco IDS 4250 和 IDS 4250-XL 传感器。

背景

IDS 对思科信息安全部门和思科 IT 部门的价值

在网络安全领域中，防火墙就好像是坚固的门锁和窗闩一样，能够阻挡他人的非法入侵。事实上，好的安全战略也应该使用入侵检测。与安全大厦内的警报器和摄像机相似，IDS 警报不但能为警卫提供很多详细信息，包括入侵者进入大厦的方法和目前所在的位置等，还能提供必要的数据，帮助警卫确定快速缉拿入侵者的最佳方式，以及将来怎样预防类似入侵的发生。在安全事故次数不断攀升，每次都花费数百万美元的环境中（参见附录 2：安全问题的严重性），为减小安全事故造成的影响，最好事先制订相应的计划，并建立起防御系统。思科内部信息安全（Infosec）部门 1 的职责就是在思科内部规划和部署防御系统，通过防火墙和 IDS 保护思科内部网络中的资源。

防火墙是思科 IT 的第一道网络防线，它能够抵御来自互联网“非军事区”（DMZ）和数据中心周围的多数入侵。但是，防火墙只是思科为企业网制订的思科电子商务安全体系结构（SAFE）的一部分 2。IDS 能够增强安全性：Infosec 已于 2001 年在全球部署了 35 个 Cisco IDS 4230 传感器，用于接收警报，在入侵者穿越防火墙后（或来自防火墙内部时）捕获相应的数据，以识别入侵者的 IP 地址，使用的端口，以及对思科某些系统的入侵模式。以便使 Infosec 能够对入侵作出快速反应，减少损失，并防止系统在将来遭受到类似的攻击。

例如，2001 年（思科部署入侵检测传感器的当年），全球服务器共遭受了两次灾难性攻击：Code Red 1 和 2（2001 年 7 月）和 NMDA（2001 年 9 月）。在这两次攻击过程中，Cisco IDS 4230 传感器都在几分钟之内就注意到了可疑流量的迅速增加，在一小时之内，Infosec 和 IT 工程师立即采取了相应的措施：

1. http://wwwin.cisoc.com/infosec/
2. http://wwwin.cisco.com/cmc/cc/so/cuso/epso/sqfr/,
   http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_package.html

- 根据大量警报识别威胁类型，按照蠕虫/病毒行动定制 IDS“签名”，并更新 IDS 传感器签名文件。
- 暂时断开与大型重点目标节点的网络连接，尤其是集中了大量微软互联网信息服务器（IIS）的思科实验室。思科在全球共有 1200 多个实验室。
- 临时禁止可疑蠕虫/病毒流量（端口 80/tcp）流向重要的远程接入用户（全球 35,000 多位用户）。
- 利用网关路由器上的 Cisco IOS Software 特性——基于网络的应用识别（NBAR）阻挡与蠕虫或病毒相关的流量（思科现在使用 Cisco CSS 11500 系列内容服务交换机执行此项任务，同时避免增加网关路由器的负担）。
- 对外出流量（流向互联网）实施新的高速缓存引擎规则，以避免蠕虫/病毒流量向外传播；添加新的 Cisco 500 系列高速缓存引擎，处理其它负载（但不阻挡向外的端口 80/tcp 访问，因而业务可正常运行）。
- 向思科员工通报网络已发生问题，并已采取了临时的防御措施。
- 从 IDS 及其它地方收集受感染的服务器 ID，临时对主机和网络分区，隔离受感染的服务器。
- 开发相应的工具，清除受感染的服务器。
- 鼓励其它思科网络部门动脑筋想办法（例如，用代理服务器提供远程接入，开放已清除病毒的、安全的关键业务系统）。
- 开发各种工具，查找已受感染或易受感染的主机，并自动对比较薄弱的代码进行升级或提供补丁。

如果没有 IDS 在前几小时向思科提供的警报，思科许多受感染的服务器都将崩溃，业务受影响的程度也会严重得多。另外，思科还极有可能成为感染其它互联网企业和用户的感染源。

2003 年 1 月，业界接收到 SQL Slammer 警报之后，Infosec 果断地切断了防火墙上极少使用的端口，有效地阻挡了 SQL Slammer 的传播。我们的 IDS 系统告诉我们，这种反应获得了极大的成功，思科没有遭受到任何攻击。

思科 IT 部门内部的 IDS

为保护互联网接入点和数据中心 3，思科 Infosec 与思科 IT 网络组协作，共同建立了基于防火墙的安全体系结构。2001 年，Infosec 共部署了 35 个 Cisco IDS 4230 传感器（IDS 4235 传感器的前身 4），以便监控越过防火墙防线的入侵。这些 IDS 网络传感器属于独立设施，放置在被保护数据流的附近（但不在数据流之上），由 Infosec 团队所有并提供管理，支持服务则由 IT 部门和全球网络团队提供。

Infosec 将这些 IDS 网络传感器安放在全球的内部互联网接入位置，即互联网与思科网络连接的地方。主要的互联网站点包括加利福尼亚州圣何塞（620Mbps 互联网接入）、北卡罗莱那州研究三角园区（465Mbps 互联网接入）、荷兰阿姆斯特丹（180Mbps 互联网接入）、日本东京（20Mbps 互联网接入）和澳大利亚悉尼（10Mbps 互联网接入）。新增加的小互联网接入地点包括得克萨斯州里查得森、马萨诸塞州查姆夫德、以色列、香港、新加坡和印度班加罗尔。另外，思科还在五个思科生产数据中心各安放了一个 IDS 网络传感器：圣何塞第 12 大厦和第 K 大厦、研究三角园区、阿姆斯特丹和悉尼。Infosec 将这些 Cisco IDS 4230 传感器部署在互联网接入网络内，即将传感器安放在防火墙的两边，同时检测进入思科的流量和通过防火墙的流量（见图 1）。例如，来自圣何塞互联网的流量将通过一对网关路由器，通过时将接受一对 Cisco IDS 4230 传感器的检查。流量首先由一对防火墙过滤，然后接受一对 IDS 4230 传感器的检查，看哪些内容正在通过防火墙。为提高性能，IDS 4230 传感器成对部署在较大的互联网接入站点上（参见下面的“挑战”）。对于较小的互联网接入站点，每个站点只需要一个 IDS 传感器，因为交换机可以覆盖传送到传感器的所有流量。

3. http://wwwin.cisco.com/infosec/tech references/#architecture

4. http://wwwin.cisco.com/cmc/cc/pd/sqsw/sqidsz/prodlit/ids4f_ds.html

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/index.html

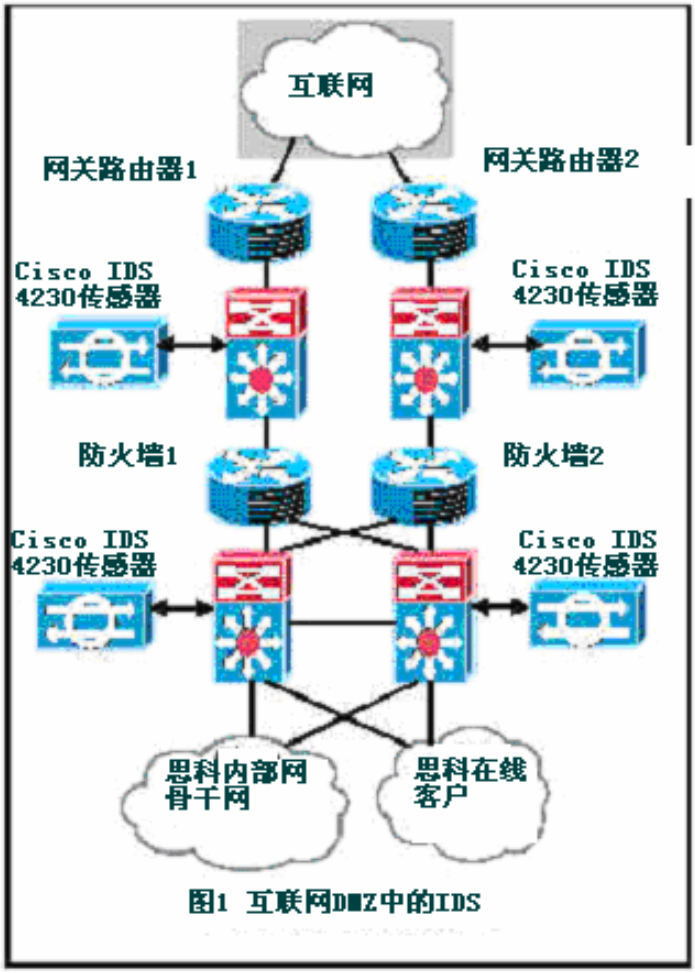


图1 互联网DMZ中的IDS

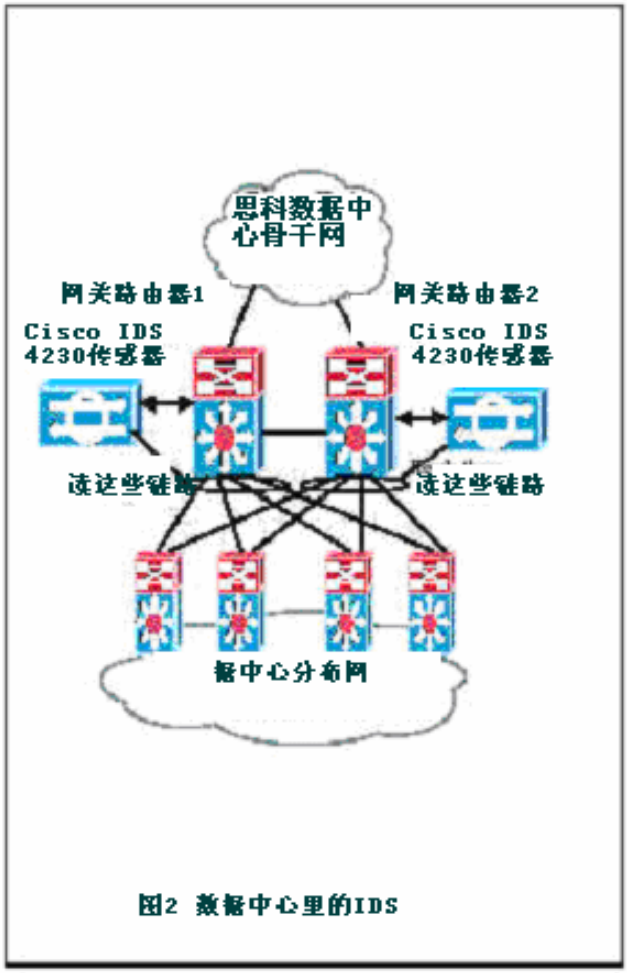


图2 数据中心里的IDS

另外，Infosec 还在数据中心周围安放了 Cisco IDS 4230 传感器，即在全球的每个思科生产数据中心外面安装了一个或多个传感器（见图 2）。由于 IDS 4230 的性能较低，因此，每个传感器（需要成对部署）只扫描离它最近的网关路由器上的流量（参见下面的“挑战”）。需要重申的是，小数据中心只需要一个 IDS 4230，因为交换机可以覆盖传送到传感器的所有流量。

挑战

思科网络和数据中心骨干网由超高速连接组成，多数为千兆位以太网。互联网接入的速度也很高。为处理圣何塞的互联网接入，思科 IT 建立了四条 155Mbps 的 OC-3。数据中心和互联网接入点都需要吞吐量达 150-250Mbps 的入侵检测网络传感器，但是，在 2001 年，由于高速入侵检测设备尚未推出，因此，Infosec 团队选用了性能受 100Mbps 快速以太网接口限制的 Cisco IDS 4230 传感器。

由于性能受限，Infosec 最初的方案是将发送到每个 Cisco IDS 4230 传感器的流量分成多个组，只将部分流量发送至交换机，并为每个流量组分配一个 IDS 4230。但是，这种方法也有严重的弱点，其中最大的弱点是，尽管每个网关只提供两个接收端口，但实际使用的只有一个。最后，Infosec 团队接受了用不同方式划分流量的缺点，在每个网关上安放了一个 IDS 4230，并且只让传感器扫描通过网关对的一半流量。虽然这种方法使每个 IDS 的平均吞吐量下降到了 100Mbps 以下，但经常会遇到 IDS 无法读的流量“钉”。如果流量“钉”超过 100Mbps，那么，IDS 将无法读到超过 100Mbps 的所有信息，也就无法捕获与这些流量相关的潜在警报。

另外，这种方法还有其它的局限：使用两个传感器使 IDS 体系结构变得更加复杂，不但降低了数据中心网关体系结构的灵活性，还增加了部署和管理成本。更不利的是，这种方法还降低了 IDS 解决方案的有效性。由于将流量分成了多个部分，并且只允许部分通过（尤其是在流量高峰期，有时与网络入侵相关），因而使 IDS 无法看到流量的全貌。这种局限不但提高了虚警率（和误警率），还使 Infosec 团队无法部署需要使用全双工流量格式信息的某些入侵签名。

另一个问题是，IDS 4230 提供了很少的管理工具。为自动执行所需的许多管理功能，Infosec 花费了几个月来开发工具，包括更新配置和签名文件、重新启动传感器等（参见附录 1：吸取的教训）。

解决方案和成效

思科 Infosec 已经开始用 IDS 4250 取代 IDS 4230，以便在更大的互联网 DMZ 内支持 500Mbps 的流量。此项工作从圣何塞开始。第一个 IDS 4250 传感器（那时正处于β测试阶段）于 2002 年 11 月安装在圣何塞的 DMZ，替换了两个 IDS 4230。替换之后，Infosec 取消了小型 IRSD 传感器不得不实行的流量分割和交换机跨区，简化了体系结构，使 IDS 传感器能够首次“读”所有的网络流量，从而能够更加全面地抵御各种威胁。我们不但能为 IDS 添加双工警报签名，还能为 IDS 4250 传感器部署 Cisco IDS Sensor Software 4.1，这样，思科 IT 不但能享受到这些好处，还能将一台设备配置为多个“虚拟传感器”，更换掉数据中心里的大量 IDS 4230 传感器。这种方法不仅释放了数据中心的空间，还降低了管理成本。

下一步计划

思科 Infosec 计划通过三个步骤升级到最新的 IDS。第一步是将互联网接入点中的 35 个 Cisco IDS 4230 传感器升级为 IDS 4250 传感器，此项工作在圣何塞升级成功之后进行。第二步是将数据中心里的 IDS 4230 升级到 IDS 4250-XL，以便利用其千兆位性能处理通往数据中心的千兆位以太网网关接口。当这些升级都完成时，Infosec 将能够完全取消 IDS 内的流量分割和交换机跨区。第三步是将这些 IDS 4250 传感器移植到最新的 IDS Sensor Software 4.1，以便改善管理，降低虚警率，这些因素是 Infosec 当前 IDS 部署的最大问题（参见附录 1：吸取教训）。目前，Infosec 正在为计划的内升级进行评估 IDS Sensor Software 4.1，具体时间表将由人力资源部和预算审核部确定。

如需了解其它关于各种业务解决方案的思科 IT 案例分析，

请访问 Cisco IT@Work：www.cisco.com/go/ciscoitatwork

注：

该出版物介绍了思科从部署自己开发的产品之中的收益。文本描述的结果和收益是由多种因素促成。思科并不能保证在其它地方也能获得类似的结果和收益。

思科按事实撰写本文，不提供任何明确或隐含的保证，包括隐含的可销售性，或者适合某种目的。某些国家的法律不允许否认明确或隐含的保证，因此，该否认声明可能并不适用于您。

附录

附录1：吸取的教训

在建立和使用入侵检测系统（IDS）的过程中吸取的主要教训是，如果没有精通网络技术的专门人员管理系统、调试签名集、每日监控攻击警报、在检测到攻击时及时通报并快速采取相应措施，IDS 就无法发挥其应有的作用。遭受到攻击时，如果不能及时正确地作出反应，警报系统将形同虚设。

警报收集系统

安装 IDS 传感器只是部署过程的一小部分。Infosec 还在每个地区安装了几台地区 Unix（Solaris）本地导向器，以及与 IDS 相连的服务器。这些本地导向器与加利福尼亚州圣何塞思科总部站点的一对全球导向器相连，它们从 IDS 传感器接收和存储警报（警报分为 6 级，从 0 级到 5 级），然后通过 Cisco PIX® VPN 链路将紧急警报（3 级到 5 级）发送到全球导向器。我们平均为 2-3 个传感器安装了一台本地服务器，部分原因是我们采用了特别的地区安全体系结构（香港或得克萨斯州里查德森等某些远程站点有一条互联网链路，没有数据中心），另一部分原因是在发生病毒复制或拒绝服务等危机时，来自一个传感器的大量警报可能会淹没一台本地导向器服务器。基于此种原因，圣何塞采用了一对全球导向器。其中一台导向器用于处理多数流量，另一台用于在遭遇到大规模攻击时处理紧急负载。另外，Infosec 还使用这些服务器复制对签名集的更改。

调整签名集

在传感器和警报收集系统到位之后， IDS 传感器提供了 800 多个默认“签名”。这些签名是对入侵或攻击前期可疑行为的定义，例如大量开放端口、多次试图进入受限主机或者试图呼叫和获取网络 IP 地址等。但是，每个网络和用户群都是唯一的，而且许多合法业务行为都将触发这些默认签名。例如，思科 IT 的内部企业管理（EMAN）系统（http://eman）每隔 15 秒钟就呼叫一次网络设备，与攻击行为颇为类似。为有效区分正常业务流程和签名集，Infosec 花费了三周时间扫描早期警报和提炼签名集（排除与特定地址相关的警报，例如 EMAN 服务器）。按照这种调整，他们关闭了特定源 IP 地址和目标 IP 地址的 50 个默认签名。

Infosec 团队在不断地调整这个签名集，因为网络处在不断的变化和扩展之中，新服务器和 LAN 不断加入，Infosec 必须保证传感器的流量分析中包含新设备。有时，Infosec 团队应该每个季度彻底停止一次调整程序，分析 IDS 收集到的最大的警报集，然后重新调整系统，保证没有遗漏上季度调整之后发生变化的签名。这项任务的执行时间应该

长达或超过一个月（第一周调整某个站点的 IDS 签名，第二周调整另一个站点，以此类推）。另外，Infosec 团队还根据思科曾经遭遇过的攻击添加签名。根据经验，Infosec 为 VSEC 业务部提供了 30 多个新签名，这些新签名已列入产品的默认签名集中。

降低虚警率

即使在初始调整完成之后，全球 IDS 系统仍将产生大量警报——只有业务熟练的专业人员才能处理这么多的警报。Cisco IDS 系统产生的警报数量为每日 1000～3000 条（平均每小时 100 多个事件）。对于业界其它公司而言，这已经是很低的数字了。（在 NIMDA 病毒攻击高峰期，每小时产生的事件多达 100 万个。）警报表一般会列出源 IP 地址、目标 IP 地址和可疑行为。如果想理解警报的含义，不但要非常熟悉相关网络实体的 IP 地址，还要熟悉网络上开展的常规业务。

Infosec 已经开发出了相应的程序，可以将这些警报传输到 Oracle 数据库，查找网络上正常行为的基线，然后将警报值与基线进行比较。任何时候警报值高得不正常，这些警报被做记号以便操作员审查。这种方法减轻了 Infosec 的负担，每天只审核和解决五个问题即可。每个问题的检查和解决时间为几分钟到一小时。Infosec 派三名员工负责执行此项任务，与此同时，这三名员工还全职参加其它安全项目。

对攻击作出反应

IDS 曾经为 Infosec 团队预报过真正的攻击。Infosec 可以在事后调查攻击者进入网络的方式（或者内部攻击来自何方），并关闭进入网络的入口。IDS 传感器确实能够断开和重新建立触发警报的连接，从而阻挡攻击者的入侵。但 Infosec 团队指出，由于几乎所有连接都属于合法的商业事件，因而他们还没有使用过这种自动切换/重设特性（即使确定攻击是合法的，Infosec 团队仍要切断连接，关闭端口，并向防火墙块添加新的 IP 地址， 以此类推）。通过分析攻击性质得到的信息不但有助于寻找最佳防御途径，还能提供未来防御方式。

另外，尽管攻击者通常使用 DHCP 或 NAT 地址，因此难以与攻击者使用的服务器联系起来，但现场分析有时也能暴露攻击者的 IP 地址。

管理 IDS 解决方案

Infosec 共花了 6 个月的时间研究 IDS 4230 管理界面，为帮助管理员管理和监控传感器，还编写了 20 多种定制程序。多数客户都使用 Cisco Secure Policy Manager，这种产品可支持 IDS 和 PIX 产品，需要为不同的设备提供不同的界面，但在当时仍旧无法满足需求。IDS Sensor Software 4.1 支持 SSL 和 XML 界面，不但能简化安全管理和界面定制，还能促使第三方厂商提供很好的管理工具。

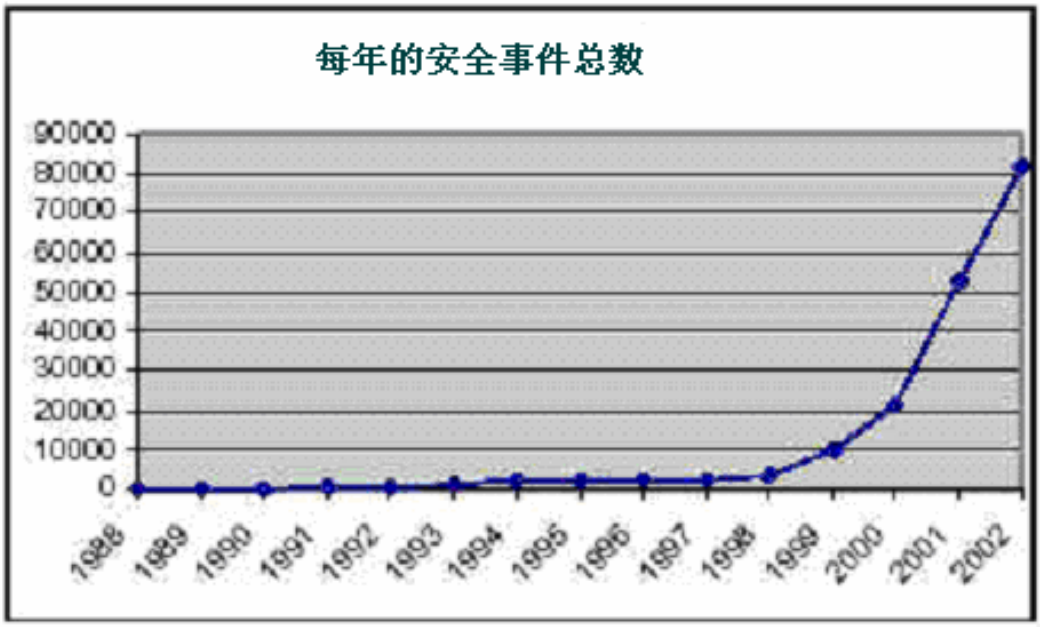
某些 Infosec 程序使用可信的 SSH 密钥先将签名文件更新内容从全球导向器发送到地区性本地导向器，然后再发送到远程传感器。其它程序能够自动执行升级任务和其它管理功能。

附录2：安全问题的严重程度

CERT

CERT 协调中心（CERT/CC）由美国政府资助，2002 年共发现和报告了 82,000 多个安全事件。安全事件总数几乎每年翻一番。

http://www.cert.org/stats/cert_stats.html



CSI/FBI“2002 年计算机犯罪和安全调查”

以下内容摘自 CSI/FBI“2002 年计算机犯罪和安全调查” （ URL 如下）：

- 过去一年中，90%的被访者（主要是大公司和政府机构）遭遇到计算机安全问题
- 80%的被访者承认计算机安全问题造成了财务损失
- 44%（223 位被访者）希望/能够将财务损失量化
- 223 位被访者遭受的财务损失总额为$455,848,000（注意：每次事件平均损失达$2,000,000）
- 与前几年相同，最大的财务损失来自专有信息被盗（26 位被访者的财务损失总额为$170,827,000）和财务欺诈（25 位被访者的财务损失总额为$115,753,000）
- 认为互联网连接更容易引发安全问题的被访者（74%）连续第五年超过了认为安全问题更多地来自内部系统的被访者（33%）
- 34%的被访者将入侵报了案（1996 年，只有 16%的被访者报案）
- 被访者发现了很多攻击和滥用，这些攻击和滥用包括：
- 40%的被访者发现了来自外部的系统侵入
- 40%的被访者发现了拒绝服务攻击
- 78%的被访者发现了员工滥用互联网接入权限（例如，下载色情文字或盗版软件，或者不正确地使用电子邮件系统）

- 85%的被访者发现了计算机病毒

我们连续第四年向被访者询问了互联网电子商务问题，某些结果如下：

- 98%的被访者拥有 WWW 站点
- 52%的被访者在站点上开展电子商务
- 38%的被访者的 Web 站点在前两年中遭遇过非法访问或误用，21%的被访者称他们不知道是否遭遇过非常访问或误用
- 25%的被访者称遭遇过 2～5 次攻击
- 39%的被访者称遭遇过 10 次以上的攻击
- 70%的被访者遭遇过故意破坏攻击（2000 年只有 64%）
- 55%的被访者称遭遇过拒绝服务攻击（2000 年为 60%）
- 12%的被访者称事务处理信息曾经被盗
- 6%的被访者称遭遇过财务欺诈（2000 年只有 3%）

摘自 CSI/FBI“计算机犯罪和安全调查”。

http://www.gocsi.com/press/20020407.html

2002年KPMG安全调查

以下内容摘自 2002 年 KPMG 安全调查（URL 如下）：

87%的被访公司今年（2002 年）曾经遇到过某种形式的安全问题，包括：

- a）61%的被访者遇到过病毒
- b）28%的被访者遇到过意外电子邮件入侵
- c）15%的被访者遇到过拒绝服务攻击
- d）13%的被访者丢失过软件
- e）12%的被访者遇到过 Web 站点入侵/攻击

其它内容包括：

- 清除 NIMDA 病毒的成本高达 120 亿美元
- IT 安全的总花费超过 41 亿美元
- 内部/外部攻击比例从 80/20 发展到现在的 50/50
- 法律风险包括：合同法、私密性法（NPP4）、贸易实践法（s52）和事故涉及的第三方法
- 预期成本=风险×资产值×反应时间
- 95%的 Web 服务器或电子邮件服务器都被入侵过

2002 年 KPMG 安全调查的网址为：

http://www.principles.com/au/mod/fileman/files/Security_Review_2002.ppt

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19～21层
邮编：100738
电话：(8610)85155000
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32～33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)85193000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86961000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn