彻底保证安全性的方法

IBM® 红皮书 ® 观点出版物，来自 IBM 技术研究院

作者：**Chung-Sheng Li**，博士，IBM 研究总监，**Katsumi Ohnishi**，IBM 高级架构师和 **Josuyla R. Rao** IBM 研究总监

要点

采用功能广泛的安全方法来预测和阻止攻击者渗透您的系统：

- 将您的安全范式从传统外围防御更改为细颗粒度的微外围安全连续体。
- 采用微外围防御和安全智能，是应对移动、社交和云计算趋势模型中新兴威胁的关键。
- 将您的解决方案从产品转变为集成的综合式安全智能的模式。
- 实施安全智能以减轻来自不断增长的数据量、云和移动用户扩散及网页技术的风险。

安全性现状

您计算机上有关安全性的桌面图标通常显示为一面盾牌，它代表着个人防火墙。它可以提供保护，抵御种种威胁和攻击，并搜索您的系统，寻找破坏防火墙的入侵者。虽然这种保护是细颗粒度安全性的有效例证，但是组织不会在其企业范围内始终建立类似的保护。因此，许多对业务至关重要的服务器继续依赖粗颗粒度的企业防火墙保护措施以及入侵检测和保护机制。

如今的企业和政府均须采取更广泛的方法来保护信息免遭恶意攻击者或渗透者入侵。当用户需要快速便捷地访问信息，同时期待这些信息受到保护时，这一任务则并不简单。结果，企业对于实施更智慧的方法来对访问权限进行细颗粒度的控制并对潜在看似不相关的威胁进行远距离检测的需求变得日益强烈。此类方法还必须依赖于多层包含式方法来隔离入侵并将损失最小化。

企业面临的困境在于必须允许对其系统进行访问以支持开展任务与提供服务，同时保护其信息资产。然而，风险仍在持续增长。例如，数据量正不断增长。云、移动和远程办公用户正在使用各种设备从多个位置访问网络。各种应用程序越来越多地使用因特网来进行协作和通信。通过使用 Web 2.0 技术，来自企业外部的用户也可以访问数据和控件。所有这些风险表明一个安全漏洞会在任何地方发生，并且可能级联到全球反响。

应对此类风险是通过构建大型防火墙以保护整个企业。然而，现今的趋势是保护网络内的每个资源。此类资源包括服务器、中间件、存储器、面向服务的体系结构、应用程序和信息，而每个资源可能具有不同的战略价值。

对安全漏洞做出回应不足以保护企业的信息、网络与业务。您必须预测并防止恶意攻击的发生。要做好准备，您需要将安全性视为一个将物理和虚拟事件、看似无害的和可疑事件以及本地和全球活动关联在一起的连续统一体。您必须采用情报和执法机构中所使用的安全知识。在这些机构中，有人会煞费苦心地收集并分析即将发生事件的线索 （例如，网络恐怖份子在攻击前的闲聊）。

威胁始终存在于不同级别上

企业面临着内部和外部安全威胁的风险，如 图 1 中所示。

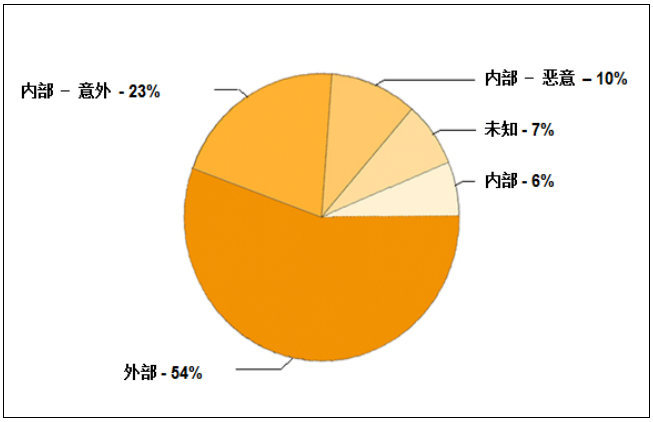

图 1　攻击事件百分比

内部威胁包括内部人员恶意尝试和无意尝试以突破安全，通过恶意代码、数据泄露，或者窃取有价值的数据，击破系统中的弱点。外部威胁包括拒绝服务（DoS）、网络蓄意破坏和宣传、僵尸网络（运行攻击软件的遭控制的计算机组）和设备破坏。还包括对关键基础架构的破坏，例如电网和燃料、通信及运输系统。

避免威胁的安全措施包括用户背景调查、限制访问、物理监控、平台完整性监控、桌面控制和对用户交互进行概要分析及审核。此类措施还包括检测并预防将敏感数据传输至未经授权的外部站点。

其他威胁包括 SQL 资料隐码攻击、网络钓鱼和高级持续威胁（APT），许多知名公司已体验过这些威胁。 APT 是对业务资产最严重的攻击，因为它是随着时间分阶段进行的。

APT 通过以下途径发展：

1. 攻击者利用社交媒体发送看似无害的电子邮件消息。此技术被称为*网络钓鱼*。这些电子邮件消息包含附件或者隐藏的应用程序，可突破安全保护。此类应用程序被称为*恶意软件*。
2. 恶意软件会安装工具以允许攻击者远程访问并控制防火墙保护下的服务器与计算机。
3. 恶意软件会获取用户凭证。然后，它会转移到特权用户，最终转移到高价值目标。
4. 恶意软件会在关键点建立对登台服务器的访问权。
5. 攻击者会将敏感数据传输至外部受控制机器上的外部登台服务器上。

通常情况下，企业通过增强组织边界的外围防御来响应此类威胁。由于需要跨界开展业务，所以该方法已日渐失效。同时，它也无法应对内部违规的威胁。

2008 年，内部违规数量首次超越了外部违规，这给网络安全中基于外围的传统防御模式带来了挑战。

您如何准备与管理极度影响您利润底线的风险，例如，就成本、业务成功和有效性而言。考虑到安全方法和产品的扩散，如何为您的数据资产选择最佳保护则令人感到困惑。

对影响深远的解决方案的需求

数十年来，企业信任 IBM 为其提供的网络、数据和系统，期望获得高品质、高性能和领先的技术。现在，这些企业对其资产安全有同等期待。为满足这种安全市场需求， IBM 从产品式的方法转向集成的企业方法，以提供安全智能。此方法基于各项关键的基本元素，这些元素将主动管理、实时信息、分析关联和预测威胁管理纳入考虑范围之中。

IBM 安全智能模型涵盖从合规性到基础架构的全部安全问题。该模型框架有助于识别、预测与补救 IT 威胁及企业风险，并实现合规性。该框架的安全功能使用 “ 计划 – 执行 – 检查 – 行动（PDCA）” 的循环模式。这些循环基于*纵深防御（defense-in-depth）*的原则，是一种分层的、结构化的安全培训、预防、检测和补救的方法。IBM 的此项解决方案是由数千名安全计划研究人员、开发人员、咨询人员和论题专家共同构建的。此外， IBM 已经为数千个安全性项目提供过咨询和实施服务，因此掌握了最佳实践和流程的实践专业知识。

安全框架

安全智能是在风险发生之前进行预测、监控和分析的艺术与科学，它是当前市场的宠儿。安全智能可以提供从安全与网络设备到服务器操作系统、应用程序、端点和基础架构资源的统一可视性与实时分析。安全智能涉及以下几个关键方面，每个方面都会从基本级别到最优级别或者从被动立场到主动立场转变：

- *人员*，从一个集中目录移至具有强大身份认证的用户、进行基于角色的分析、身份管控和特权用户控制。
- *数据*，从加密、访问控制、访问监控和数据丢失预防升级至数据流分析和数据管控。社交计算在拦截数据泄露和穿透性的钓鱼攻击中变得日益重要。
- *应用程序*，从应用程序扫描、防火墙和源代码扫描移至安全应用程序工程流程与欺诈检测。
- *基础架构*，从粗颗粒度的反病毒外围防御升级至资产管理和端点与网络安全性管理 （入侵检测和预防以及深度包检测），至高级网络监控、侦查与数据挖掘。

安全智能的关键解决方案点

IBM 专注于交付安全智能中的四个主要领域：高级威胁、云计算、移动计算和法规与合规性。

高级威胁（APT）是复杂的、针对性的攻击，旨在获取对关键信息的连续访问。这些威胁变得越来越严重，越来越频繁。解决方案是一个强大的网络层，该网络层集成安全、分析与威胁智能，此外还包含人员与社会因素，因为高级威胁通常始于钓鱼攻击。

通过整合大量数据，安全智能解决方案可提供针对各种威胁 （包括 APT）的防御措施的更为深入的洞察。 IBM 安全信息与事件管理（SIEM）解决方案可帮助您区分实际的威胁与假象。它还通过更多上下文的数据与智慧的分析，助其减少警报误报。

大部分企业意识到他们需要利用云计算，但是仍对潜在风险感到担忧。作为服务与安全供应商， IBM 具备良好的条件在云与平台中提供安全的基础架构，从而在安全的数据中心和云中隔离信息。

根据 Gartner, Inc. 的报告，截至 2014 年， 90% 的企业将支持在移动设备上使用企业应用程序。[1] 为跟上这一不断扩展的工作环境，大多数 CIO 的首要顾虑是为员工提供广泛的访问，同时保护其移动设备的安全。 IBM 专注于对企业数据的安全访问，同时支持隐私性，并为端点、网关和应用程序开发提供广泛的安全功能。 IBM 还提供各种产品以集成并交付移动设备管理功能，并为用户应用程序和系统提供访问控制和联合身份。

我们需要一个更全面的方法，在风险发生之前对其进行预测、监控和分析。

企业将大量人力和物力投资于遵守政府与行业法规需求，通常其成本也在不断增加。借助 IBM，企业能够将法规映射至其 IT 和业务基础架构，由此减少成本、精简系统复杂性、自动执行配置并简化监控、审计与报告。 IBM 提供的产品可以提供受信的日志记录和关联，并执行编排、分析和仪表板功能。

有关安全智能的更多信息

仅仅构建外围防御无法保护您的业务安全。通过使用 IBM 安全性框架中的产品和服务 （如 图 2 中所示），IBM 能够帮助您预测、识别并补救威胁，同时实现合规性。为了实现这些目标， IBM 为人员、数据、应用程序和基础架构构成的 IT 基础架构域提供各种产品和服务，以及合规性和安全服务。

[1] Gartner Newsroom
http://www.gartner.com/it/page.jsp?id=1480514

图 2　IBM 安全框架

IBM 提供端到端的安全智能，包括针对各主要业务领域的全面服务和产品：

- 人员。 IBM 通过使用以下产品来提供身份评估、基于角色的分析、用户控制、部署和托管服务：
  - IBM Tivoli Identity and Access
  - IBM Tivoli Federated ID
  - IBM Tivoli Single Sign-on
- 数据。 IBM 通过使用以下产品来提供评估、加密、数据丢失预防（DLP）部署、流分析和管控服务：
  - IBM InfoSphere® Guardium®
  - IBM InfoSphere Optim™ Data Masking
  - Tape and disk encryption
  - IBM Tivoli® Key Manager
- 应用程序。 IBM 通过使用以下产品来提供评估、安全工程流程与欺诈检测服务：
  - IBM Rational® AppScan® Source Edition
  - IBM Rational AppScan Standard Edition
  - IBM Tivoli Security Policy Manager
- 基础架构。 IBM 通过使用以下产品来提供网络安全（入侵检测和预防以及深度包检测）、侦查、数据挖掘、穿透测试、防火墙、入侵预防系统、漏洞管理器服务以及受管移动保护的服务：
  - IBM Tivoli Network Intrusion Prevention
  - IBM WebSphere® DataPower® XML Gateway
  - IBM Tivoli Endpoint Manager (antivirus by using Trend Micro)
  - IBM Security zSecure™ mainframe security

接下来：IBM 如何提供帮助

为帮助您实施安全智能， IBM 提供 IBM X-Force® 研发团队的服务，该团队是世界上最著名的商业安全研究与开发团队之一。该团队研究并监控最新的威胁趋势（包括安全漏洞、攻击和主动攻击）、病毒和其他恶意软件、垃圾邮件、网络钓鱼及恶意网页内容。除了为客户及公众提供如何应对新兴与致命威胁的建议， X-Force 团队还交付安全内容以保护 IBM 客户免受这些威胁。

X-Force 团队每两年发布一次 IBM X-Force 趋势与风险报告，以帮助客户、研究人员与公众了解最新的安全风险并保持领先于新兴威胁。该报告深入探索了当今安全专家所面临的最重要的挑战。欲查阅 IBM X-Force 趋势与风险报告，请访问：

ibm.com/security/xforce/download.html

除了 IBM X-Force 团队， IBM 服务和产品还提供全方位的解决方案，帮助保护您的数据、应用程序和基础架构免受攻击；保护您的信息资产；并允许您的用户进行安全访问。

查阅参考资料，获取更多信息

欲知本文标注的概念详情，请参阅以下资源：

- 有关安全的 IBM 红皮书出版物

  http://www.redbooks.ibm.com/Redbooks.nsf/portals/Security?Open&count=20

- IBM X-Force 趋势与风险报告

  http://ibm.com/security/xforce/downloads.html

- IBM 高级安全研究院

  http://instituteforadvancedsecurity.com/default.aspx

- 安全发展：IBM 安全工程框架（REDP-4641）

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区：
INTERNATIONAL BUSINESS MACHINES CORPORATION “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和 / 或程序进行改进和 / 或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有所不同。本文档的用户应当验证其特定环境的适用数据。

版权许可：

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。

本文档“REDP-4944-00”创建或更新于 2013 年 4 月 04 日。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corporation 在美国和 / 或其他国家或地区的商标或注册商标。这些术语和其他 IBM 已注册商标的术语在本信息中首次出现时都使用适当的符号（或）加以标记，以表示在本信息发布时由 IBM 在美国注册或拥有的普通法商标。这些商标也可能是其他国家或地区的注册商标或普通法商标。在 Web 地址 ibm.com/legal/copytrade.shtml 中包含了 IBM 商标的最新列表

以下术语是 International Business Machines Corporation 在美国和 / 或其他国家或地区的商标：

AppScan®
DataPower®
Guardium®
IBM®
InfoSphere®
Optium™
Rational®
Redbooks®
Redbooks（徽标）
Tivoli®
WebSphere®
X-Force®
zSecure™

以下术语是其他公司的商标：

其他公司、产品或服务名称可能是其他公司的商标或服务标记。