数据泄露成企业重大威胁　亡羊补牢不如未雨绸缪

[趋势科技中国]– [2014 年 7 月 23 日]美国最大的无线通信提供商 Verizon 近期发布了“2013 年数据泄露事故调查报告（DBIR）”，报告显示：几乎 70%的数据泄露事故都是由第三方检测出的，而这恰恰反映了许多企业长期疏忽数据泄露检测的真实现象。“后知后觉”的企业只能采取更多的危机公关手段、花费更多的修复成本，来减少因数据泄露事件造成的致命伤害。但这只能是数据安全管理的唯一答案吗？

“亡羊补牢”不一定能挽救企业

如今，利用各种软件、终端秘密获取用户各类信息早已不是秘密，现有的数据分析技术，让黑客很容易就能把零碎的信息聚合成完整的“待售商品”。另外，高级持续性威胁（Advanced Persistent Threat，APT）和“鱼叉式”攻击的广泛出现，不但让互联网阴云密布，更让机密业务数据泄露的可能性大幅增加。

2013 年，知名企业或是互联网公司的数据泄露事件愈演愈烈，致使很多创新的产品信息、业务计划、客户资料、涉密数据信息都暴露在外。但 Verizon 的报告说明了更严重的问题，很多泄密事件都不是“受害者”自己发现的，社交网络、安全检测公司或者第三方媒体成为了数据泄露事件的“爆料人”。

针对数据泄露的特殊性及其可能为企业带来的长久影响，趋势科技(中国区)首席技术总监蔡

昇钦认为：“亡羊补牢，为时已晚。受害者往往没有将精力和资金放在数据泄露监测上，极其糟糕的情况不断发生，在这些外泄数据可以从互联网上‘随意下载’的时候，IT 部门才开始组织修补动作，但法律惩罚和信任危机有可能会让他们无法翻身。所以，与其在数据泄露事件发生后进行封堵，不如提前采取措施修补漏洞。”

主动消除威胁方可封堵“泄密暗道”

那么，漏洞出现在哪里？威胁出现在哪里？哪个病毒开始在网络中泛滥？入侵者从哪条路径进入到数据中心？我们有什么样的措施避免威胁的扩大化？这一系列的疑问其实归纳起来，就是威胁的主动发现和智能阻断。

对此，蔡昇钦表示：“企业不希望关乎核心知识产权的文档、客户私密资料、商业计划离开内部网络环境，更加不允许在网络外部传递与交流。可是，现代组织不能拒绝互联网的交互，不能将机构封闭在一个信息孤岛，而 BYOD 网络和传统 PC 终端在外界通讯时都可能成为数据泄露的‘暗道’。因此，一旦攻击者伺机把恶意代码投放到公司网络内部，受攻击的目标必须要能尽快的加以侦测和控制，利用可视化的追踪工具来看看攻击者去过哪些地方、造成了哪些损害，这才是应对预防数据泄露最有效的操作。”

为了帮助企业用户远离数据泄露风险，在全网范围内主动寻找并封堵“泄密暗道”，趋势科技推出了 TDA 威胁发现设备和 TDS 整套威胁管理解决方案，可实现传统安全设备无法涉及的多重协议关联分析领域，以及最重要的根源分析功能。另外， 由于 TDA 集成了趋势科技独有的云安全技术，具备了启发式检测功能与沙盒模拟技术，因此可以对最新威胁第一时间发现，并进行检测和彻底的取证分析。一旦 TDA 检测引擎发现了可能造成数据泄露的攻击

活动，以及被恶意软件感染的端点，实时威胁预警机制和行动指导方案便能够帮助用户立即启动，在数据外泄之前剿灭攻击。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn 。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。