网络安全信息简报

安博士月刊

2014.11（Vol.25）

AhnLab ISF 2014 Review

AhnLab ISF 2014：AhnLab提示“顾客主导型安全”战略

谈论响应高级威胁的解决方案

2014年10月15日，AhnLab 综合安全博览会 2014（AhnLab Integrated Security Fair，简称为 AhnLab ISF 2014）在韩国首尔市江南区三成洞COEX隆重举行。共有2,000名的企业和公共机关的IT管理员和安全管理人士参加了本次大会。在本次大会上，AhnLab 提示了‘RE:SOLUTION, Be more advanced than threats’主题和响应最新安全威胁的‘顾客主导型安全’战略。

另外，本次大会同时进行了世界知名企业的产品和技术展示，有 Barracuda Networks、EMC Korea、 Tenable Network Security、Palo Alto Networks、Akamai Korea 和 HP Korea 等企业参加，显示了通过竞争公司之间超界限的有机协作，构筑安全生态系统的 AhnLab 的坚强意志。

AhnLab ISF 2014 的主题是‘RE:SOLUTION’，即响应安全威胁的解决方案。在本次大会上，AhnLab 通过共12个主题发表和展位进行的技术专题，强调了超越个别解决方案为主的单纯的响应，通过理解各产业群的特性、并联系技术和有实效的解决方案，走向对威胁因素的根本解决方案。

Keynote Speech 顾客主导型安全战略

AhnLab 代表权治重在会议开幕词中说道：“为了在越来越增加的高级安全威胁和多样的规范中有效实现安全，需要指定‘优先级’的基准。此时，作为基准的是情报，即顾客的经验和需要。”接着还说道：“有关安全威胁和响应的顾客经验结合于AhnLab 收集的数据和信息，提供优化于顾客特性和要求的安全，即是 AhnLab 定义的安全情报(Security Intelligence)。从这样的观点出发深入一步，对于现有安全企业提供的解决方案和技术诀窍即安全情报，AhnLab 不会单方面地转达，而是提供面向顾客的情报-‘顾客主导型安全’。”

Keynote Speech AhnLab 关键词是‘顾客经验’，安全模型是‘R.A.C.E’

AhnLab 产品企划室 Jung，JinGyo 室长在‘基于顾客经验的安全(Customer Experience Based Security)，R.A.C.E’为主题的专题演讲中提出了对于响应目前复杂多变的最新安全威胁的安全模型-R.A.C.E，该模型可以按每个顾客实现有实效的响应。他说道：“在急变的IT环境和威胁中，AhnLab 的基准点且最重要的数据是顾客经验(Customer Experience)。所谓顾客经验，不仅是顾客，即企业事业、业务流程、公司内外数据、拥有数据的影响度和危险度，还包含企业目标和价值观，文化等有形/无形数据全面的数据。”以这种顾客经验为中心响应最新的安全威胁，需要实时(Real-time)收集威胁信息并正确分析后提供。对于分析加工的信息需要以实际行动(Action)来响应，不仅联系端点解决方案，还要通过企业内部实际工作部门和网络安全部门之间的有机联系(Connected)来响应。这种响应模型便是‘R.A.C.E’。另外，随着急变的IT环境，从事于安全领域的人士的观念也需要转变。尤其是需要顾客和安全企业双向交换信息，创建定制型数据的进化(Evolution)。最后，Jung 室长还说道：“AhnLab 将通过独自研发的基础架构和多年的技术诀窍，欲成为不仅提供顾客所需的数据，还基于数据融合实际技术、服务和解决方案创造协调效应的安全伙伴。”

Re•Plan the Security　重新计划安全策略

A会场的主题是‘重新计划安全策略(Re•Plan the security)’，也是解决本次大会主题‘RE:SOLUTION, Be more advanced than threats’的第一阶段。检查从端点到网络层的现有的安全策略的实效性，提示改善方案。

▲ Lee GeonYong，AhnLab 产品企划部门 课长

强化端点安全的解法：返回到基本！

尽管引进了多样的安全解决方案，端点仍然是安全的漏洞。AhnLab 产品企划部门 Lee GeonYong 课长说道：“端点用户，即组织成员认为安全解决方案将解决一切，而安全管理员则坚信用户也会遵守安全策略，因此就产生了代沟。”他强调：“为了减少对安全认知的幅度，需要确保从用户观点的‘容易理解的安全’，从安全管理员观点的‘端点的可视性’的方案。”与此相关，AhnLab 提供办公用计算机漏洞管理解决方案，其主要功能有：▲强制更新防毒软件等对漏洞项目自动采取措施 ▲通过问卷功能检查用户自定义的安全 ▲强制措施 ▲联动补丁管理解决方案

您在使用个人信息保护解决方案吗？

尽管很多企业已经引进使用个人信息保护解决方案，但是他们不确定是否满足安全合规(Compliance)。与此相关，AhnLab 软件安全部门 Park MoonHyeong 次长说道：“个人信息保护解决方案必须考虑个人信息特性，并正确履行安全合规要求。个人信息保护解决方案必须掌握通过个人信息管理员电脑等媒体流通的个人信息情况；要满足安全合规要求的加密、删除等，同时在个人信息通过多种路径泄漏的时候检测并拦截。”他还指出，仅引进个人信息保护解决方案存在局限。成功引进并使用个人信息保护解决方案，关键是应用适合企业业务环境的弹性策略，还有如何做好事后管理。

▲ Park MoonHyeong AhnLab 软件安全部门 次长

▲ Im GiCheol KFCC 电算信息部 信息安全组长

随着金融环境变化构筑主动安全战略案例

今年初，信用卡公司个人信息泄漏事件发生以后，金融圈的安全合规更是被强化 。KFCC(Korean Federation of Community Credit Cooperative)电算信息部信息安全组长 Im GiCheol 说道：“目前需要的响应方案是不仅可以预防，还可以事后监控的响应方案。KFCC在2012年已建立了中长期的信息安全总体规划，目前需要构筑综合安全。”为了构筑综合安全，KFCC 决定引进 AhnLab 综合安全托管。是根据‘安全基础构架’、‘稳定的构筑’和‘系统扩散应用技术’等三个基准检讨后选择了 AhnLab。Im 组长最后说道：“通过构筑 AhnLab 综合安全托管，期待日后事业的扩张和遵守个人信息安全合规。”

网络境界安全，超越其局限

下一代威胁变得越来越高级且复杂。而且，通过网络流入的恶意软件的感染路径也变得更加多样。AhnLab 产品企划部门 Yoo MyeongHo 次长指出，仅依靠流量处理性能和速度，作为下一代网络安全解决方案远远不足。通过当前的网络安全解决方案来响应未知的恶意软件等最新的安全威胁存在着局限。他说道：“还需要响应高级威胁的同时，最小化妨碍网络安全性能的功能。”AhnLab 下一代网络安全解决方案 TrusGuard 基于优秀的分散处理体系结构和强大的核处理功能，出色的处理性能不用说，通过应用程序控制功能封锁感染路径、配置基于用户的策略等提供主动的安全，防止内部信息的泄漏 。

▲ Yoo MyeongHo 产品企划部门 部长

Re•Do the ATP Defense　重新开始APT响应

B会场主要围绕着被称为APT(Advanced Persistent Threats)的最新高级威胁进行了发表。 提示了最近安全市场上大量出现的多样APT响应解决方案的差异和根据企业特性选择解决方案的方法。C会场引起参会者关注的是有关详细了解最近攻击技巧的专门会议。

▲ Yoon SangIn 产品企划部门 次长

为什么是“高级威胁响应”？

APT(Advanced Persistent Threat)为代表的高级威胁通过周密的预先准备工作，利用零日漏洞或未知恶意软件的新种方式持续攻击直到成功。加上，最近出现的响应高级威胁的解决方案也复杂多样，使安全管理员的业务变得更加繁重。对此，AhnLab 产品企划部门的 Yoon SangyIn 次长说道：“如安全的先天不足，要认识到APT最总也无法源泉防御。这样出发，才可以体现并运营有实效的响应体系。”还强调：“为使‘响应APT解决方案’正常运行，需要实时分析恶意软件如何生成并从哪里流入，还要在端点响应入侵的威胁。”

通过案例来分析‘响应高级威胁’，从引进到运营

AhnLab Global TAC 部门 Lee JongHyun 课长说道：“通常人们认为APT是利用高级技术的攻击，但是从结果来看，这也是通过人才可以实现的攻击。这就需要从攻击者的观点来理解。”攻击者为了入侵到企业内部，首先分析目标企业的系统和安全解决方案，然后研究如何避开安全解决方案的检测。与此相比，企业谋求响应方案的行动看起来很消极。另外，最近很多安全解决方案都主张可以响应APT，但是实际上很多解决方案的功能的大部分与APT响应无关。最后 Lee 课长提示了选择‘响应APT解决方案’的基准：▲分析通过网络流入的所有文件； ▲ 可以检测最近攻击趋势的技术； ▲管理效率； ▲费用效率，还指点了先要考虑实际运营方案。

▲ Lee JongHyun　AhnLab Global TAC 课长

▲ Lim ChaSeng AhnLab 网络开发室 课长

通过基于Exploit的APT攻击事例来分析基于行为的技术局限

AhnLab 网络开发室的 Lim ChaSeong 课长演示了一些恶意软件的入侵过程。如实际利用攻击企业的文件Exploit攻击、根据用户特定行为才出现的恶意软件攻击行为、还有根据安装在特定操作系统的特定应用程序的行为出现的恶意软件等。Lim 课长首先警告：“比起其他安全威胁，APT攻击发生频率虽然不高，但是问题是这是真正的攻击。”他还指出：“实际上无法体现所有IT环境的情况下，仅依靠目前的基于行为的技术很难检测到这种威胁的流入。”AhnLab 通过独自研发的动态内容分析技术(Dynamic Intelligent Content Analysis, DICA)，在这些文件型恶意软件在执行恶意行为之前迅速检测。

APT攻击最后的防线‘端点’安全的进化

最近的安全入侵事故，可以发现即使追踪攻击痕迹并在端点提取可疑文件，但是大部分的情况无法找到文件流入的路径或嵌入到文件的寄主文件的痕迹。这就是1%的未知威胁。AhnLab 产品企划部门 Kim ChangHee 次长说道：“只有确认威胁流入的路径和寄主文件等相关的所有的过程，才可以确认正确的损害，并响应附加威胁。”他还强调：“确保对威胁的可视性、及时性和正确性，才可以掌握并响应端点的未知威胁。”AhnLab 提供的端点威胁监控及分析/响应解决方案-AhnLab MDSE 可以实时检测和分析端点的所有文件、行为和流入的路径，提供相关的详细的信息。安全管理员根据提供的可视性信息和威胁水准，可以迅速做出决策。

▲ Kim ChangHee　AhnLab 产品企划部门 次长

Re•See the Intelligence 重新审视安全情报

C会场以“重新审视安全情报”为主题进行，公开了以需求者中心重新改编的‘AhnLab 安全构架2014’，而目前主要是以提供者中心的报价模型。还介绍了下一代综合威胁检测/分析模型和基于云计算的安全战略及服务。另外，还共享了 AhnLab 安全托管服务和通过EMC/RSA、Akamai 等合作伙伴的服务联系检测和响应最新高级安全威胁的实际案例研究。

▲Choi KwangHo AhnLab SI 事业部门 组长

下一代安全构架的协同战略

尽管企业大量投资于响应安全威胁，但是网络安全事故不断发生。这是为什么呢？AhnLab SI 事业部门 Choi，kwangHo 组长指出：“从防御情景侧面来看，当发生事故时需要从被动响应为主变化为主动的预先响应；从合规侧面来看，从基于检查表变化为基于业务影响度分析；从运营侧面来看，从劳动集中型观点变化为情报观点。”还强调：“在实际环境中应用时需要针对强化用户方便和接近性，而不是对事故的责任。”与此相关，AhnLab 公开了以需求者中心重新改编的‘AhnLab 安全构架2014’，共提供4种报价模型，如‘强化APT响应及事后追踪’、‘内部控制高级化’、‘强化个人信息吴用/乱用的监控’、‘安全托管的高级化’。

基于可视性的下一代安全管理模型构筑战略

AhnLab 服务产品企划部门的 Lee，SangGu 部长说道：“未来的安全战略需要转换观点，即通过持续的监控和分析入侵事故的征兆并及时检测，还有强化对发现的问题的改善。”由此，AhnLab 推出了下一代安全管理模型的核心因素：▲基于大数据的收集和分析 ▲收集和处理多样的数据，确保可视性 ▲通过不同设备之间的相关分析，检测异常征兆 ▲ 基于情景的内容分析 ▲通过数据视觉化，确保安全洞察力 ▲合作和自动化。基于这些核心因素的 AhnLab 下一代安全托管服务(NG-MSS)应用了优化于下一代远程托管的基础构架、双SIEM、基于数据视觉化的用户仪表板，提供与他服务差别的威胁检测和安全可视性。

▲Lee SangGu AhnLab 服务产品企划部门 部长

▲Cho NamYong EMC RSA 安全事业部门 部长

响应最新安全威胁的下一代安全托管战略， Beyond SIEM

目前的安全威胁趋势如下：攻击者的攻击能力越来越强大，发现攻击所需的时间越来越长。EMC RSA 安全事业本部 Cho NamYong 部长说道：“如果以前是基于特征码的预防为主的安全战略，当前需要基于情报主导型(Intelligence-driven)检测方式的新的接近。”EMC的情报主导型安全(Intelligence-driven Security)有如下：▲收集事件的数据并可视化(Visibility) ▲检测嵌入安全威胁的异常行为(Analysis) ▲将事业损失降到最低的措施(Action)等。Cho，NamYong 部长提示了联系数据包(Packet)、日志(Log)、端点(Endpoint)和网络流(NetFlow)的 Beyond SIEM 模型 。

基于云计算的安全服务战略及顾客案例

随着多样的黑客工具的登场，高级的攻击也随着增加，这就需要在攻击发生的发源地检测异常征兆并拦截的方案。Akamai Jung TaekJin 理事说道：“通过基于云计算的多境界安全，不仅可以有效防御分布式拒绝服务攻击，还可以防御SQL资料隐码攻击、跨站脚本攻击等多样的Web应用程序攻击。”接着介绍了典型的韩国制造企业的被攻击事例，该公司通过 AhnLab 托管服务和Akamai Web防火墙，即RUS(Rule Update Service)拦截了互联网领域的有害攻击。Akamai 通过与 AhnLab 的合作伙伴关系提供▲AhnLab 安全专家建立优化的网络安全策略 ▲365日/24小时全天候监控及响应 ▲管理员和运营解决方案等强大的云计算安全。

▲Jung TeakJin Akamai 理事

在历届展会成功举办的基础上，AhnLab ISF 2014 通过技术交流和产品演示等活动，为用户、企业、研究机构提供了一个广阔的交流平台。访客借此不仅用心听发表，还积极访问展位留心看最新技术的演示，并收集符合企业实际情况的解决方案的信息。

在技术展示区，访客的步伐也是来往不断。AhnLab 事业伙伴参与了技术展示，不仅介绍了多样的最新技术，还介绍了联系当前安全解决方案强化安全水准的方案。本届展会参与的 AhnLab 的事业伙伴有，Barracuda Networks、Tenable Network Security、Paloalto Networks 和 HP korea 等。

随着高级安全入侵事故的增加，AhnLab 取证分析组的技术展示区聚集了很多访客。AhnLab 取证分析专门组织 A-FIRST(AhnLab Forensic & Incident Response Service Team)不仅提供入侵事故的事后响应，而且还提供包括事前响应的取证分析服务。

本次活动根据 AhnLab 强调的主题 - ‘与合作伙伴共生’ 和 ‘生态系统’ ，合作伙伴区布局弄得更加多彩多样。Barracuda Networks、EMC Korea、 Tenable Network Security、Palo Alto Networks、Akamai Korea 和 HP Korea 等屈指可数的网络安全提供商和 Markwin、Soft 2000、韩国信息系统、Ellysys 和 Unipoint 等 AhnLab 的合作伙伴的参与使本次大会更是热闹。

http://www.ahn.com.cn

http://global.ahnlab.com

http://www.ahnlab.com

关于安博士（AhnLab,Inc.）

安博士的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

安博士已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号院望京SOHO220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932 / +86 21 6095 6780 | v3site@ahn.com.cn

© 2014 AhnLab, Inc. All rights reserved.