改善应用程序和权限管理：关键安全控制更新

作者 John Pescatore

2016 年 4 月

Ivanti AppSense

赞助

©2016 SANS™ Institute

企业所面临的威胁不断变化，但几乎所有成功的攻击都是利用了一组核心的安全漏洞。互联网安全中心 (CIS) 定期更新“关键安全控制措施”，[1] 一张列出了 20 种安全控制措施的优先列表。如果运用得当，表中的措施都能有效屏蔽最先进的定向威胁，并支持以更快的速度检测和解决那些通过了初级防护措施的威胁。

CIS 最高优先级控制列表中的一部分提供的是“立竿见影”的措施，能够立即降低高级目标威胁带来的风险。例如，几乎所有形式的攻击在安装需要管理员权限的恶意软件时，都需进行权限提升。钓鱼是破坏性攻击最常见的前端形式，其作用是获取用户认证，以便开始权限提升。钓鱼之所以能够成功，是因为应用程序和权限管理。

最新的控制列表更新，也就是 6.0 版，认识到了这种普遍弱点，并提高了这些领域的优先级。例如“控制管理权限的使用”从控制措施中的第 12 名上升到了第 5 名，而“基于须知原则的受控访问”则从第 15 名小幅上升到第 14 名。“清点授权软件和未授权软件”仍然是最关键的控制措施，而“安全配置硬件和软件”的排名还是第三位。

安全中心最高优先级控制列表中的一部分提供的是“立竿见影”的措施，能够立即降低高级目标威胁带来的风险。

其他对安全控制的定义中同样也强调了应用程序和权限管理。例如“控制管理员权限”在国家安全局的“IA 十大迁移策略”中排第二位，[2] 而应用程序白名单控制，以及操作系统补丁、应用程序补丁和管理权限限制均名列澳大利亚国防通讯局的 4 大网络入侵应对策略中[3]（见图 1）。

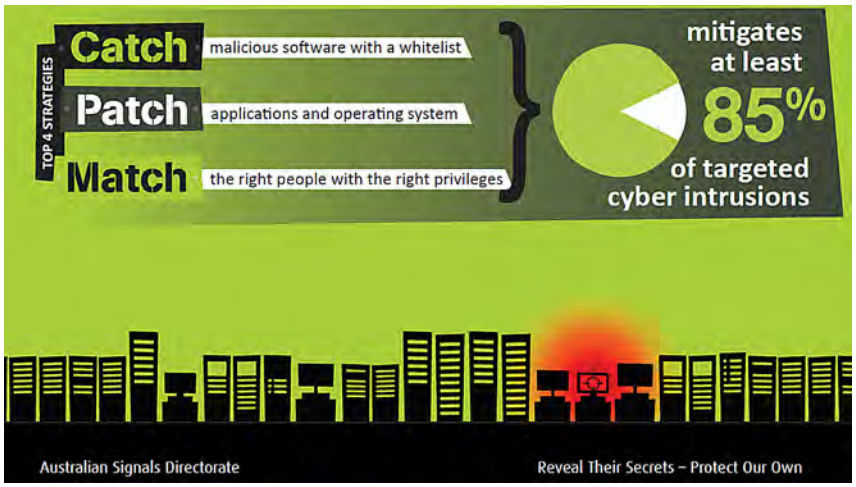

图 1 澳大利亚国防通讯局 4 大网络入侵应对策略[4]

[1] CIS 高效网络防护控制 6.0 版，www.cisecurity.org/critical-controls.cfm
[2] 国家安全局，信息安全指南，www.nsa.gov/ia/mitigation_guidance/
[3] 澳大利亚国防部，定向网络入侵应对策略，www.asd.gov.au/infosec/mitigationstrategies.htm
[4] 澳大利亚国防部，定向网络入侵应对策略，www.asd.gov.au/infosec/mitigationstrategies.htm

应用程序控制和权限管理在安全方面的优势是众所周知的，这些通常被认为是安全入门常识。然而，大部分入侵报告表明，入侵成功的原因依然是在这些领域控制和流程缺失或低效。

实施应用程序控制和权限管理最大的障碍是害怕对自身造成损失，例如导致业务中断或是由于合规软件和关键业务访问被屏蔽，导致帮助台接到的请求大幅增加。但是在过去几年中，产品和技术都有了进步，如今在很多成功的案例中，使用应用程序控制和权限管理对业务运营造成的影响非常小，甚至根本没有。

本白皮书将讲解 CIS 关键控制 6.0 版中的更新，关注应用程序控制和权限管理在运用得当时，带来的高回报、立竿见影的效果。

定向攻击为什么会成功

每年，ID 防窃资源中心 (ITRC) 都会就所有公开宣布的数据入侵情况发布统计和分析。2015 年，据 ITRC 宣称，共披露了 781 次入侵，平均每次入侵都造成 216,000 条记录泄露（见图 2）。

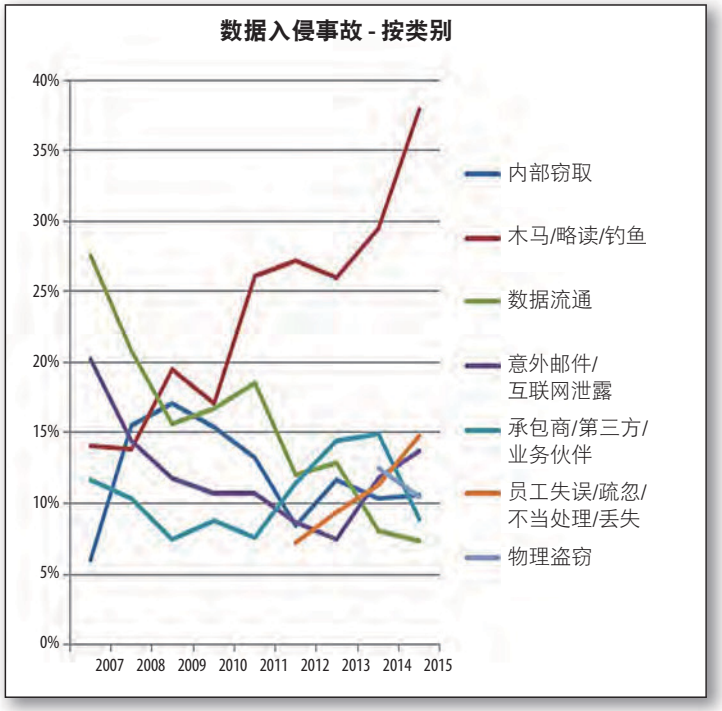

图 2 钓鱼相关活动呈上升趋势[5]

[5] ID 防窃资源中心，2016 年数据入侵报告，www.idtheftcenter.org/2016databreaches.html

报告发现，规模最大、增长最快的进攻手段是木马 / 略读 / 钓鱼，其中钓鱼技术占了绝对多数。Verizon 数据入侵调查报告 (DBIR) 得到了相似的结论（参见图 3）。

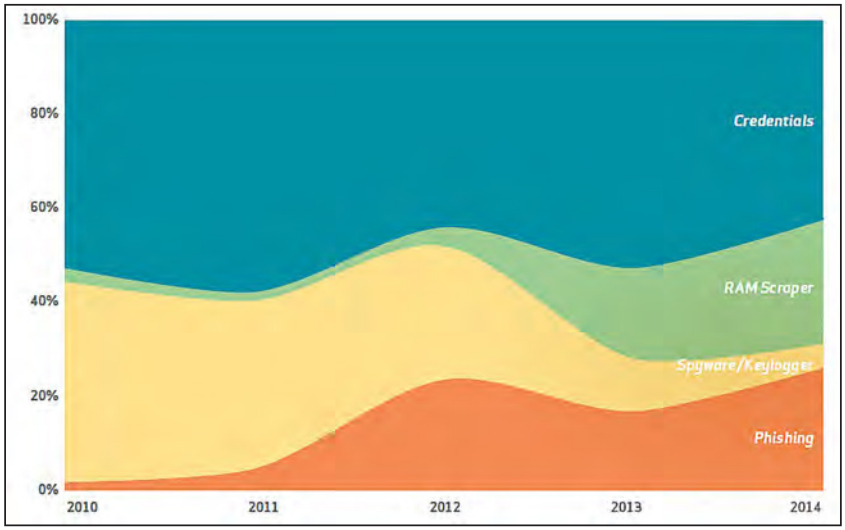

图 3 成功的身份窃取和钓鱼 [6]

钓鱼成功有以下原因：

- 重复使用的密码一直被广泛使用。
- 邮件和网络浏览未能做到强有力的身份验证，区分合法链接和欺骗性链接。
- 用户不断被狡猾的定向钓鱼攻击欺骗，泄露自己的认证信息。
- 企业继续过多地使用用户权限，用来安装软件和获取数据。

所有这些因素共同造成了成功实施钓鱼攻击。所有领域都需要提升安全控制，但删除密码、保护邮件和网络应用程序，以及改变用户行为都需要长期努力。安全项目可以通过改进安装、执行应用程序及分配用户访问级别等安全控制措施，打乱常见攻击形式，实现短期效果。

[6] Verizon，2015 年数据入侵调查报告，www.verizonenterprise.com/DBIR

作为关键安全控制的应用程序控制和权限管理

多年以来，实践经验及 Verizon DBIR 这样的研究不断发现，大部分攻击成功的原因是基本安全保护不到位：企业和政府机构对阻挡真实攻击最有效的安全基础关注不足。早在 2008 年，国家安全局负责评估关键基础设施系统安全性的渗透测试人员就持续遇到这个问题，并发布了如今关键安全控制的早期版本。[7]

这些控制措施现在由非盈利组织 CIS 继续维护，是一项由社区推动的工作，致力于通过简单而经过验证的方法找出最有效的降低真实世界威胁风险的投入和行动。关键步骤有：

CIS 关键控制是一项由社区推动的工作，致力于找到一种简单而经过验证方法，能够对优化列出最有效的降低真实世界威胁风险的投入和行动。

- **让入侵为防守提供信息：**继续监控入侵，判断根本原因，着重寻找能够截断入侵途径、降低检测时间、最小化进攻冲击和/或降低恢复时间及成本的安全控制措施。

- **用“什么有效”的运营数据验证控制措施：**中断业务运营的安全控制无法获得成功，即使其对防御真实世界攻击卓有成效。CIS 关键控制列出了经过考验的、能大大降低风险，同时将业务中断降到最低的有效应用方法。

- **集成与自动化：**单纯叠加更多安全流程及控制很少能提高安全级别，通常，需要高层级人员配置和较难技能要求的新“解决方案”都会被闲置。多项 SANS 调查表明，雇用并留住有经验的安全人员对 CISO 来说一直是项挑战。[8] 控制列表中所推荐的安全控制措施，能通过可靠的工具和流程支持安全相关数据在多个安全流程中的集成，让有经验的安全分析员如虎添翼。

大约每隔 18 个月，CIS 都会考虑威胁、企业技术需求和解决方案成熟度的变化，通过公开的、社区推动的方式重新审视上述因素，并更新关键控制措施。控制措施按照效果和效率排名，随后记录并发布新的控制措施排名版本（和验证指南）。

[7] 系统网络安全协会，“CIS 关键安全控制：简史，” www.sans.org/critical-security-controls/history

[8] 系统网络安全协会，“SANS 2013 年关键安全控制调查：从觉察到行动，” 2013 年 6 月，www.sans.org/media/critical-security-controls/CSC_Survey_2013.pdf

CIS 关键安全控制措施 6.0 版概览

最近一次更新是 2015 年第三季度，发布了 CIS 关键控制 6.0 版。

在更新后的 6.0 版中，威胁数据和解决方案效果评估发生了一些变化。最重要的包括:

- “控制管理权限的使用”、“维护、监控和分析审核日志”、“数据保护”和“基于须知原则的受控访问”的优先级排名都显著提高。
- “防范恶意软件”、“无线访问控制”、“安全技能评估和充分培训”及“应用程序软件安全”的优先级排名都有所**下降**。
- “网络工程安全”被**移除**出了独立安全控制措施名单，其概念融入了其他领域中。
- “电子邮件和 Web 浏览器保护”作为新的控制措施**加入**了列表。

这些改变很大程度上是因为认识到了在 2015 年，绝大多数造成损失的成功攻击都使用了钓鱼或基于邮件或 Web 的技术获取认证信息，并利用合法用户权限，躲过了检测，安装定向可执行文件。在措辞和子控制措施优先级上的改变也反映了这一趋势。新控制措施排名参见图 4。

图 4 CIS 关键安全控制措施 6.0 版更新控制排序

6.0 版的最终结果是，需要对一些能够立即有效防御真实世界攻击的控制领域提升重视度。其他一些机构也验证了这些回报率最高的安全控制措施的效果。例如，SANS 列出五项控制措施，即 SANS“五大优先”，能够以最快速度提升效率，有效减少来自先进定向攻击的风险：1) 软件白名单，2) 安全标准配置，3) 应用程序安全补丁，4) 系统安全补丁和，以及 5) 管理权限最小化。

本文后续部分将集中阐述应用程序控制/白名单及权限管理。

应用程序控制/白名单（控制 2）

优先级排第二的控制措施是“清点授权软件和未授权软件。”控制措施 2 中推荐的措施包括：

> “积极管理（清点、追踪和纠正）网络中的所有软件，只有授权软件能够进行安装和运行，发现未授权和未受管理的软件，阻止其安装或执行。”

主动管理和控制能够在 PC 或服务器上运行的可执行文件，建立对恶意软件的有效防护。

CIS 关键安全控制 6.0 版认为，积极控制应用程序很重要，因为

> “控制不足的机器更有可能运行与业务目标无关的软件（带来潜在安全隐患）或在系统被突破后，运行攻击者带来的恶意软件。对所有软件的管理控制在规划和执行系统备份和恢复时，也扮演着关键角色。”

积极管理哪些可执行文件能够在 PC 或服务器上运行，建立对恶意软件的有效防护，因为只有授权软件可以不受阻碍地运行，而未授权软件要么无法运行，要么只能在满足安全规则的条件下运行，这也是保证端点安全的有效方法。

注意“积极管理”不仅仅指简单的锁定。锁定意味着 IT 决定用户可以使用哪些应用程序，且用户无法安装可执行文件。尽管锁定听上去是最安全的方法，如今现实的企业环境意味着锁定必可避免会导致业务中断，迫使用户通过违规或影子 IT 手段绕过锁定，或是导致公司管理层发布各种锁定的例外情况，最终失去锁定的意义。

比锁定更进一步的方法是“白名单”，IT 审核通过一组用户可以运营的应用程序，这些程序与授权限制保持一致。白名单成功与否取决于白名单中包含的业务所需应用程序的比例，以及 IT 评估应用程序加入请求并将其加入批准列表的速度。保持批准列表的准确性和响应性可能需要大量 IT 人力。

为了处理白名单带来的运营问题，一种替代方案是基于文件性质决定允许/屏蔽，而不是基于可执行文件的哈希表或签名。通过这种技术，维护一个被审核的发布方和文件所有者名单，所有来自这些地方的文件都会受到信任。文件所有权通过操作系统管理，因此用户和其他非受信来源引入系统的可执行文件将无法运行，带有受信任发布方签名的可执行文件除外。由于受信任的发布方也有可能制造受感染的可执行文件，因此受信任发布方的名单应当尽可能小，并且仅限于高度可信的机构。

应用程序控制的衡量标准

“CIS 关键安全控制（6.0 版）评测指南”为每种控制措施定义了衡量成功的标准。标准包括统计网络中未授权应用程序的数量，需要花多长时间将其移除，以及检测到新软件的时长。[9]

应用程序控制加强了支持“灰名单”的能力，名单中的软件会自动应用安全政策，从而可以运行（如防病毒软件等）。这些政策可以限制连接、权限级别、使用时间等，在满足业务需求的同时降低风险。这样在增加灵活性的同时也有助于维护安全、业务需求和人员级别之间的平衡。

权限管理（控制 5 和 14）

在 6.0 版更新中，两个控制领域的优先级有所提升，原因是其在减少真实世界攻击风险时卓有成效：

控制措施 5：控制管理权限的使用 “用于追踪/控制/避免/纠正对计算机、网络和应用程序管理权限的使用、分配和配置的流程和工具。”

控制措施 14：基于须知原则的受控访问 “依照经过审批的分级，正式判定哪些人员、计算机和应用程序需要并有权获取对关键资产（例如信息、资源、系统）的安全访问，并对这些安全访问进行追踪/控制/避免/纠正的流程和工具。”

[9] 互联网安全中心，高效网络防护控制措施 6.0 版，下载，www.cisecurity.org/critical-controls/download.cfm（需要令牌）

权限访问控制衡量标准

“CIS 关键安全控制（6.0 版）评测指南”为控制措施 5（控制管理权限的使用）定义了衡量成功的标准，包括配置了多少未授权的升级操作系统帐户，哪些应用程序不需要双重认证，权限变更等。控制措施 14（基于须知原则的受控访问）的衡量标准包括不需要登录的数据集比例和未使用数据丢失防护的业务系统比例。[10]

安装/执行软件和读取/修改敏感数据。攻击者通常会利用帐户权限过高或是管理员权限泛滥的情况，引起重大业务损失。

与应用程序控制相似，低质量的权限管理也经常引起严重的业务中断。“按需共享”经常违背“须知”原则或群组访问控制。当限制过于静态或复杂时，IT 部门就需要配置大量人力，以在合理的时间内响应获取访问或管理权限的请求。需要采取机制，允许在认证过程中提供受限制的例外情况，同时支持用户在低风险情况下进行自助服务。

最佳实践部署指南

对于关键控制措施或其他对控制的概念，一种常见的反应是认为控制已经是一种被熟知的安全实践，并不新鲜。尽管这可能是对的，但一个又一个调查，一次又一次渗透测试和一份又一份入侵报告表明，这些基本控制措施要么没有得到应用，要么缺少维护。

相反地，企业或政府机构成功避开入侵或将先进的定向攻击造成的损失减到最小时，都无一例外地应用了例如“应用程序控制”和“权限管理”等控制措施，并且流程足够成熟，能在响应威胁的变化的同时，满足业务对灵活性和可扩展性需求。这些机构采取的实践包含以下方面：

- **在开始前获得来自管理层和平级的支持。**改变对谁都很难，但提高安全性需要我们做出改变。获得高层管理和核心平级部门（例如 IT、法务和业务部门）的支持是推动改变的关键。以下有三种可靠方法能赢得他们对安全措施改革的认可与支持，按照实施效果排序分别是：

    1. **审计/入侵后报告。**不幸的是，人们总是在灾难发生后才想起做出改变。最好的情况是，业内另一家公司遭到了入侵，为您提供了问题根源信息分析，帮助您赢得了相关变更措施的审批。最差的情况（由第三方对您公司或机构遭遇的入侵提供事后报告）是一味更有效也更严重的催化剂，例如负面审计报告。

[10] 互联网安全中心，高效网络防护控制措施 6.0 版，下载，www.cisecurity.org/critical-controls/download.cfm（需要令牌）

2. **重大业务或变更。**M并购通常会带来业务和 IT 运营的改变。重大 IT 变更（例如迁移到 Windows 10 或软件服务化）也会带动改变。“应用程序控制”和“权限管理”往往可以融入这些变更计划，作为流程改进的一部分。

3. **合规性或竞争驱动。**联邦信息安全管理法案 (FISMA)、HIPAA、北美电力安全公司 (NERC)、PCI 和所有其他规定体系对“应用程序控制”和“权限管理”均有要求。案例研究，如 SANS 的“成功案例”记录了从这些领域安全改革中获得了实际回报的公司。

- **从一开始就要明智。**“应用程序控制”和“权限管理”如果应用不得当，都可能中断业务进行。在部署这些控制措施前，应当清点关键业务应用程序和访问需求，并加以记录和了解。部署的第一阶段应当“仅限观察”：让所有运营部门在没有强制实施的情况下运营至少一周，分析针对潜在中断可能需要采取的措施。

  下一步是小规模原型测试，需要引入强制措施，但仅针对安全和 IT 人员，以及自愿的外部志愿者。等到所有流程问题都解决后，可以将一些问题用户，例如开发人员、经理和超级管理员加入测试中。

- **做好准备后执行。**测试完成并实现改进后，管理层应当宣布这些功能将在特定日期实行，**但您不应在宣布那天开始执行。**等待至少一周，看看有哪些抱怨。这样您就可以向管理层指出这些机构性问题，因为他们在真正实施之前，就开始抱怨了。只有解决这些问题后，才能开始执行。

- **将业务中断降到最低。**总会出现需要承担风险的情况，例如必须安装一个未知的可执行文件，或必须将访问权限授予一位新用户或业务合伙人。应当选出一些流程和产品，用于支持临时例外、用户自助服务报警、增强例外监控等。

- **保持防御威胁的效果。**所有安全控制措施，尤其是“应用程序控制和权限管理”，只有在能够提高防御威胁和泄露的力度，降低企业风险时，才有价值。随着威胁和 IT/业务实践的进化，控制策略也需要进行调整。应当对涉及存在漏洞的内部 PC 的入侵报告进行分析，判断您的流程和战略中是否有漏洞。

- **持续监控。**“应用程序控制”和“权限管理”控制提供有价值的数据，既可以用于调整控制，最小化业务中断，也可以用于探测新的威胁规律或识别已知的漏洞标记。所有安全控制都应当与安全信息和事件管理 (SIEM) 或安全运营使用的其他分析工具集成。

在部署“应用程序控制”和“权限管理”时采取渐进式的方法与成功的规律相一致。首先专注于了解哪些应用程序会访问关键业务数据的工作，然后收紧用户层面的访问权限和服务器层面的应用程序控制。使用从这里学到的知识，确保更广泛地应用能够降低风险的方案，同时避免引起过多业务中断。

关于作者

John Pescatore 于 2013 年 1 月加入 SANS 担任新兴技术总监。此前他在 Gartner 担任了 13 年首席安全分析师，在 GTE 任职 11 年，并曾为国家安全管理局服务，设计了安全语音系统，也曾效力于美国特勤局，研发了安全交流和语音系统，“偶尔还要负责安装弹道护甲”。John 曾在国会作为网络安全事宜的证人，被提名为 2008 年 15 位安全领域最具影响力的人物，并是国家安全局认证的密码逻辑工程师。

赞助方

SANS 鸣谢赞助方：