安天网络空间

主办：安天　2017 年 7 月 10 日（总第 94 期）试行　本期 4 版　微信搜索：antiy

安天参加第二届军民融合展并发表演讲

7 月 3 日至 5 日，第三届中国北京军民融合技术装备博览会在北京国家会议中心举行，主题为“聚焦自主创新技术装备，促进军民融合深度发展”。

展会上，安天以“赛博超脑 - 网络靶场”作为参展核心，同时展示了安天网络靶场、态势感知与监控预警系统、天擎终端甲终端防御系统、探海威胁检测系统、追影威胁分析系统、移动引擎等产品和解决方案。

安天为军工、公安、海关、水利、交通等部委行业提供安全服务与解决方案。特别是为我国重大的国防、军工科研成果提供了网络安全保障，包括载人航天、空间站对接等，安天的产品与服务不但为我国航[illegible]航，也为我国部用大飞机[illegible]客飞的网络安全提供了保障。

[illegible]7 月 3 日上午的网络空间安全论坛上，安天技术负责人发表了《网络安全领域军民融合能力流动方向》的演讲。

2016 年 5 月 28 日，习近平总书记视察了安天总部，听取了安天的汇报后，对安天人说“你们也是国家队，虽然你们是民营企业。”军民融合是当前的大势所趋，安天作为网络安全的“国家队”之一，[illegible]，[illegible]天，试看天下谁能敌！

安天获批大数据协同安全技术国家工程实验室授牌

[illegible]7 月 4 日，[illegible]安天获批大数据协同安全技术国家工程实验室并[illegible]揭牌仪式。[illegible]等多家机构共同建设国内首个[illegible]监测、预警和防御体系[illegible]。

[illegible]数据安全问题[illegible]安天[illegible]数据安全分析能力的国家实验室，[illegible]联合致力于建立大数据安全技术[illegible]测试、安全评估等大数据安全[illegible]层设计。

[illegible]随着互联网[illegible]和大数据[illegible]应用的深入，大数据正在成为网络攻击的目标，3.12“震网”（Worm.Win32.Stuxnet）[illegible]攻击事件，正是面向[illegible]发出[illegible]数据[illegible]等业务的正常运行。因此，大数[illegible]的力量。

安天参与 2017 年中央企业网络安全交流研讨大会

7 月 5 日，以“国之重器 网安筑梦”为主题的 2017 中央企业网络安全交流研讨大会在北京国际饭店会议中心成功举办。来自能源、电力、石油、海运、航空、运营商、建筑、铁路、建设、航天、核工业、电子信息、机械制造、银行、证券、保险等 200 余家中央企业和中管金融企业的 400 余位嘉宾参加会议。安天作为企业代表参加了会议，并在展览区对安天综合安全解决方案、产品部署方案、网络安全等级保护解决方案等进行了集中展示。

[illegible]本次大会旨在贯彻《网络安全法》，加强关键信息基础设施等级保护安全防护能力，落实国家网络与信息安全信息通报工作规范要求等。安天时刻不忘总书记在网信座谈会上[illegible]依托深厚的技术沉淀，在关键信息基础设施安全防护等方面贡献自己的力量，不断提高对网络安全的保障能力，助推网络强国建设部署。

安天赴约 2017 民航大数据、信息安全峰会

[illegible]2017 民航大数据、信息安全峰会于 7 月 6-8 日在成都双[illegible]安天[illegible]产品和解决方案能够有[illegible]保护关键基础设施和重要[illegible]高级持续威胁（APT）攻击的[illegible]防御态势”的主题演讲。

[illegible]届峰会围绕“智慧[illegible]区域经济”为建设具有中国特[illegible]民航、安全民航为研讨主题，着[illegible]运转的重要责任，民航业的[illegible]打造智慧交通、公安服务[illegible]安天作为国内网络安全领[illegible]域专注于民航的检测与防御技术[illegible]获得公众的[illegible]及[illegible]

保护云环境免遭勒索攻击的九个措施



Kelly Sheridan / 文　安天公益翻译小组 / 译

技术推动了更快的协作和数据传输，也使网络犯罪分子能够迅速地传播勒索软件。

1. 保护云计算层

Evidem 创始人兼首席执行官提姆·普伦德加斯特 (Tim Prendergast) 表示："最重要的事情就是保护云计算机层。自动化很容易实现，创业公司和大企业都能轻松实现。

保护计算层将确保系统和数据的可用性，并防止威胁源利用你的计算能力在整个组织中传播恶意软件。普伦德加斯特说，组织首先要做的是，向个人分配 SSH 密钥来启用安全登录。

2. 分离数据存储

Shpantzer 建议了解正式和非正式资产所在的位置，这是规划勒索攻击应对方案时非常重要的一步，但是经常被忽视。他解释说，例如，许多开发人员正在云端的服务器上进行快速测试，但是并不完全了解这样做的安全性和合规性。有时他们会暴露生产数据库的完整副本，这种错误会在勒索软件和可用性问题之外增加保密性问题。至于存储，Shpantzer 建议使用廉价的云存储来存储截图、文件、文件夹以及重建操作所需的任何东西。将它们冷存储在一个单独的 MFA（多因素身份验证）保护的账户中。

雷维斯 (Reavis) 还建议分离数据存储，特别是脱机备份，以便在发生攻击时保护备份。

3. 网络分段

皮伦蒂 (Pironti) 表示，既然现在的架构已经合适，企业应该利用这个机会对网络进行分段。这样可以限制和遏制勒索攻击的传播。

在云中，皮伦蒂继续说，安全团队可以使用架构在关键活动之间设置"门"，如果发生攻击事件，组件周围的墙壁和隔离将保护它们。

4. 身份管理

普伦德加斯特认为身份管理是继保护云计算层之后第二个重要措施。

能够了解人们的特性和正常的行为模式，这可以帮助你做出更明智的业务决策。

5. 数据访问管理

除了采用复杂、安全的密码和多因素身份验证外，企业还应限制员工对敏感信息的访问。这会限制攻击者访问账户时能够执行的攻击规模。

身份和访问管理 (IAM) 策略和高级控制列表可以帮助企业细致地控制云存储的权限。桶策略可以帮助企业根据账户、用户或条件（如 IP 地址或日期）设置或拒绝权限。

6. 使用跳转主机

跳转主机位于不同的安全区域，提供了访问系统中其他服务器或主机的唯一方法。普伦德加斯特表示，"从管理的角度来看，这是一种一站式入站访问方法。

设置为堡垒主机信息进入点。它配置了标准的 DNS 名和 IP 地址，并且只允许企业 IP 登录，然后才会授予更广泛的访问权限。

因为跳转主机是单一入口点，所以简化了保护服务器和维护严格访问控制的流程。如果该台服务器被黑，我们很容易创建一个新的服务器。

普伦德加斯特 (Prendergast) 说："勒索主机也不能免疫攻击，但是能够将攻击面减少到一个非常小的接入点。"例如一台服务器的安全性保护就不会那么容易，特别是在新型的攻击中。

7. 基于云的安全即服务

富勒建议组织检查其现有的安全即服务解决方案，该方案能够一致地保护云和本地。他没有具体介绍该解决方案，但是指出需要安全 Web 网关和 CASB 来帮助保护。

8. 设置（系统）管理程序防火墙规则

许多专家在设置中都忽略了这一步骤。但这是很重要的，因为勒索软件会导致知识产权的暴露。如果可以在防火墙上将写入时监控和执行操作，就能够更好地在数据泄露之前阻止攻击。

麦伦蒂补充说，领导者应该执行入口和出口过滤。"监控 C&C 活动，只允许签名、已知的流量。

9. 不要让服务与 SaaS 系统通信

普伦德加斯特警告说不要让服务与诸如 GitHub 这样的 SaaS 服务通信。一旦威胁源访问了你的 [illegible]，他建议企业将 Git 或代码存储在自己的云环境中。但是指出这种做法可能需要 [illegible]。

"随着服务越来越好，还有更多的日志和数据。"

原文名称	9 Ways to Protect Your Cloud Environment from Ransomware
作者简介	Kelly Sheridan，Dark Reading 的资深编辑。
原文信息	2017 年 6 月 27 日发布于 Dark Reading。 原文地址：https://www.darkreading.com/cloud/9-ways-to-protect-your-cloud-environment-from-ransomware/d/d-id/729222?image_number=4

免责声明

本译文译者为安天实验室工程师，出于个人兴趣在业余时间所译，未获原文作者授权，译者与安天实验室均无法对本译文的准确性做出保证，亦未获得相关的版权授权，鉴于译者及安天实验室分别为多项国际翻译奖项的获得者，因此导致的版权问题承担责任。译者力图忠于所获得原文完整准确地翻译，但译者保证译文为安天实验室工程师翻译，同时对所获得原文完整存在性、或者安天实验室翻译质量及准确性、或者译文是否侵犯第三方权利不做保证，译者与安天实验室不承担翻译责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和意见。

本译文亦不得用于任何商业目的，未经原作者、译者和安天实验室书面授权，基于上述问题产生的法律责任，译者与安天实验室有权追究。