

精译版

保护云环境免遭勒索攻击的九个措施

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	9 Ways to Protect Your Cloud Environment from Ransomware		
原文作者	Kelly Sheridan	原文发布日期	2017 年 6 月 27 日
作者简介	Kelly Sheridan 是 Dark Reading 的副编辑。 https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/9-ways-to-protect-your-cloud-environment-from-ransomware/d/d-id/1329221?image_number=1		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。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态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

保护云环境免遭勒索攻击的九个措施

Kelly Sheridan

2017 年 6 月 27 日

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

业内专业人士表示：“您能做的最重要的事情就是保护云计算层。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。他还认为，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

相关专家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。

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，该专家建议使用廉价的云存储来存储截图、文件、文件夹以及重建您的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。

“这是灾难恢复的问题，而不仅仅是 PII（个人身份信息）被盗、网络和数据不受破坏的入侵事件。”

有人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。

“我们都在使用实时云存储，这是很棒的，”他说，“但是快速自动同步意味着所有的副本都被感染，所以我们需要采取额外的措施进行定期备份。”

3. 网络分段

业内专业人士表示,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。

他以 Target 泄露事件为例进行解释:“如果我生活在一个非分段网络中,我的整个网络都会在本地上网。”攻击者只需要感染 HVAC 系统就能执行灾难性的攻击。

在云中,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区可以保护它们。

4. 身份管理

有关专家认为身份管理是继保护云计算层之后第二大重要措施。

他说:“如果没有强大的身份管理,您就不了解谁在关键安全层之外做什么。一旦你设置了核心安全层,就能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。”

越来越多的人随时随地使用云处理工作,因此身份管理变得越来越重要。分散的劳动力使得监控活动和寻找异常行为“非常重要”。“身份管理也延伸到企业的围墙外了。”

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。员工只能访问他们工作所需的账户和系统。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)策略和访问控制列表可以帮助企业组织和控制云存储的权限。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。

业内专家还强调了监控用户活动和账户权限的重要性。勒索软件攻击者的目标是获取目标账户的更高访问权限。如果他们获得了权限,就可以在系统上创建不应该存在的账户。

在管理方面,保护特权账户是相对简单的。“我可能无法覆盖数千个用户账户,但我可以覆盖200个管理账户。”他说。

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。有人

认为，“从管理的角度来看，这是一种一站式入站访问方法，”并指出它已经存在了一段时间了，但还没有被广泛采用。

该主机是单一的管理入口点。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，所以它简化了保护服务器和维护严格访问控制的流程。如果这个服务器被跳过，我们很容易创建一个新的服务器。

“跳转主机也不能免疫攻击，但是能够将攻击面减小到一个非常小的接入点。”保护一台服务器的安全比保护数千台更容易，特别是在新兴的攻击中。

7. 基于云的安全即服务

业内专家指出最重要的问题之一是 我们越来越难确定哪些端点容易受到勒索软件攻击，更别提安装安全软件来保护它们了。

他建议企业实施基于云的安全即服务（security-as-a-service）解决方案，该方案共享一个共同的威胁情报库，可以阻止勒索软件下载。虽然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 类型的功能。

8. 设置（系统）管理程序防火墙规则

在（系统）管理程序级别管理防火墙，使安全领导者能够制定关于谁可以发送、接收和访问入站和出站数据，哪些数据可以发送，以及发送多少的明确规则。

许多专家在设置出站规则方面颇为犹豫，但这是很重要的，因为勒索软件会导致知识产权的暴露。如果您可以在防火墙上编写实时监控和执行操作，您就能够更好地在整个环境中保持一致性。

还有专家补充说，领导者应该执行入口和出口过滤。“监控 C&C 活动，只允许符合规定的流量出站。”

9. 不要让服务与 SaaS 系统通信

相关专家警告，不要让服务与诸如 Github 这样的 SaaS 服务通信。一旦威胁源访问了您的 Git 库，当服务与 Github 通信时，他们就能感染和访问更多的公司系统。

他建议企业将 Git 或代码库存储在自己的云环境中，但是指出这种做法可能需要时间来适应。

“人们很难采用这一方法，”他承认，“随着服务越来越好，还有更多的自主托管选项，公司可以更好地控制离开其环境的数据。”