

简译版

## IT 团队防止勒索软件攻击的最佳实践

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	Best practices for IT teams to prevent ransomware attacks		
原文作者	钱德拉·巴萨瓦纳 ( Chandra Basavanna )	原文发布日期	2021 年 6 月 22 日
作者简介	钱德拉·巴萨瓦纳是 SecPod Technologies 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	<a href="https://www.helpnetsecurity.com/2021/06/22/best-practices-prevent-ransomware-attacks/">https://www.helpnetsecurity.com/2021/06/22/best-practices-prevent-ransomware-attacks/</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
摘要	大多数成功的勒索软件攻击，其原因都是企业忽视了简单的安全实践。例如，在 WannaCry 攻击爆发前三个月，微软就已经发布了相关补丁，并要求企业升级他们的操作系统。实施最佳 IT 安全实践，能够帮助企业 IT 团队防止此类勒索软件攻击以及应对安全挑战。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

## IT 团队防止勒索软件攻击的最佳实践

钱德拉·巴萨瓦纳

2021 年 6 月 22 日

根据 Check Point 的研究，自今年年初以来，受勒索软件影响的组织数量以每月 9% 的速度增长。从 WannaCry、Petya 和 SamSam 到 Ryu，这些勒索软件攻击给公共和私营部门组织造成了巨大的经济和声誉损失——Colonial Pipeline 攻击事件就是最新的例子。

在防止此类网络攻击和保护多年来建立的资产方面，企业面临很大的困难。在远程办公模式下，IT 团队面临着保护远程端点的挑战，而网络攻击的增加会加重他们的负担。

大多数成功的勒索软件攻击，其原因都是企业忽视了简单的安全实践。例如，在 WannaCry 攻击爆发前三个月，微软就已经发布了相关补丁，并要求企业升级他们的操作系统。此次网络攻击是由于企业忽视漏洞修复导致的，在全球造成了超过 40 亿美元的经济损失。

### 实施最佳实践以防止勒索软件攻击

实施最佳 IT 安全实践 能够帮助企业 IT 团队防止此类勒索软件攻击以及应对安全挑战。

#### (1) 定期运行 IT 资产扫描，了解软硬件资产

了解网络中可用的硬件和软件，是 IT 团队应遵循的关键实践。持续监控 IT 资产，有助于企业识别恶意资产并将其列入黑名单。如果不清楚企业有哪些 IT 资产，不仅会给安全团队的管理带来困难，还会影响企业的网络安全状况。

#### (2) 持续进行漏洞扫描，识别安全漏洞

企业网络中存在的任何活动漏洞，都会导致严重的漏洞利用。虽说定期扫描已不再那么有效，但是企业仍应持续进行扫描以了解其漏洞情况。IT 团队可以启用自动化的漏洞扫描，以确保流程无缝运行。

#### (3) 评估漏洞的潜在风险，并确定其优先级

了解每个漏洞带来的风险，对于企业的漏洞管理流程至关重要。借助基于风险的漏洞管

理，IT 团队可以根据严重程度对漏洞进行优先级排序，并明智地规划漏洞修复工作。

#### **(4) 及时修复漏洞，不留任何死角**

IT 团队应及时识别漏洞，并及时打补丁，将企业的漏洞管理提升到一个新的水平。如果不能及时修复漏洞，就会为攻击者入侵企业网络敞开大门。在增强企业的安全状况方面，集成的漏洞和补丁管理套件可能会带来意想不到的效果。

#### **(5) 检查反病毒软件的可用性，确保定期更新**

在每个系统中，反病毒软件都充当着“安全守门人”，保护网络免受病毒侵害，并就任何潜在威胁发出告警。因此，及时更新反病毒软件以提高其有效性也很重要。

#### **(6) 密切监控端点活动**

端点是企业 IT 基础架构的主要组成部分，也是企业的支柱。端点中每天都会发生许多活动，持续监控它们有助于防止攻击。

#### **(7) 设置强大的应用程序和设备控制措施**

允许在企业网络中使用任何应用程序或设备，会导致不必要的安全漏洞。IT 团队应在企业网络中实施强大的应用程序和设备控制措施，以迅速阻止构成任何安全威胁的应用程序、USB 和外围设备。

#### **(8) 配置强口令管理策略**

对入侵者来说，简单的口令是小菜一碟。如果在端点使用容易猜到的口令，不仅会遭受外部攻击，还会为内部攻击铺平道路。IT 团队应设置严格的口令策略，要求用户定期更改口令，并在口令中使用字符和数字。

#### **(9) 强化系统配置，实现安全合规性**

HIPAA 和 PCI DSS 等各种行业法规，要求企业实施多项安全控制措施。这些控制措施能够强化系统配置并防止多种攻击。企业应遵守这些法规，或创建自己的安全策略并在企业网络中实施这些策略。

#### **(10) 检测攻击和攻陷信标 (IoA 和 IoC) 并及时进行响应**

企业网络中的一些端点可能已受到攻击，或者表现出遭受攻击的某些迹象。IT 团队必

须及时检测到 IoA 和 IoC 并迅速采取行动，以防止严重的安全事件。

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>