

简译版

## 防御勒索软件攻击七步走

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	When Ransomware Strikes: 7 Steps You Can Take Now to Prepare		
原文作者	Patrick Hill	原文发布日期	2017 年 11 月 6 日
作者简介	Patrick Hill 是 Atlassian 的 SRE 解决方案负责人。 <a href="https://www.darkreading.com/author-bio.asp?author_id=4842">https://www.darkreading.com/author-bio.asp?author_id=4842</a>		
原文发布单位	Dark Reading		
原文出处	<a href="https://www.darkreading.com/endpoint/when-ransomware-strikes-7-steps-you-can-take-now-to-prepare-/a/d-id/1330313?">https://www.darkreading.com/endpoint/when-ransomware-strikes-7-steps-you-can-take-now-to-prepare-/a/d-id/1330313?</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		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

# 防御勒索软件攻击七步走

Patrick Hill

2017 年 11 月 6 日

如果你明天上班时发现公司遭到了勒索软件攻击,你知道该怎么办吗?你会打给谁求助?如果你的电脑被锁定,你将如何找到他们的电话号码?你将如何通知客户?

防御勒索软件攻击需要做好多方面的准备,包括技术方面,例如对数据进行离线备份。本文不讨论这些技术措施,主要谈谈可以采取的实际操作措施,以便在事件发生之后进行有效地应对。你的应急计划是什么?你希望你的团队囊括哪些人才?你将如何沟通?

很少有人能够未卜先知,但是提前规划能够帮助人们更加轻松地应对灾难。当涉及勒索软件时,提前规划也是很重要的。今年 5 月,WannaCry 勒索攻击爆发,在头几天就感染了大约 30 万台计算机。之后,联邦调查局网络司司长称勒索软件是一种“普遍的、日益增长的威胁”,并指出未来很可能会出现更多的勒索软件攻击。其他一些报告也预测勒索软件攻击会增加。

为了应对勒索攻击,我们可以采取以下 7 个措施。其中一些措施可以广泛应用于其他重大事件,而另一些则专门针对勒索软件攻击。

**1. 制定响应预案。**你的团队成员可能不习惯处理紧急情况,所以要确保他们知道该怎么做。这包括他们将会聚集在哪里讨论问题,媒体问询应该在哪里举行,以及该告诉客户和员工什么内容。大多数时候,这意味着规划“谁、什么、何时、如何做”的问题。一旦制定了计划,请提前与你的团队分享。

**2. 将响应计划存储在多个位置。**如果您的事件响应计划存储在 PC 上但 PC 被锁定了,那么您将无法开始恢复过程。勒索软件可能会影响你的台式机或服务器,或两者都影响。将计划副本存储在多个位置,包括至少三个独立的云服务,并设置日历提醒以便定期更新。

**3. 选择团队成员。**事件发生后,你想要谁参加讨论?除了首席执行官和首席信息官之外,您可能想要公关、法律、人力资源和其他部门负责人参加响应讨论。现在您需要制定一个清单,并确保清单上的每个人都知道这回事。此外,获得他们下班后的联系方式,并与其他团队成员分享。

**4. 制定沟通计划。**您可能会发现首选的沟通方式被锁定了，因此您需要了解还有哪些沟通渠道可供使用。电子邮件可能已经无法使用，所以请准备其他沟通手段。如果你的智能手机正常运行，那么可以在团队内部使用通信应用程序——只要确保每个人都安装了这个应用程序就行。但是勒索软件也可能会攻击移动设备，所以请准备好备用方案。将电话号码和个人电子邮件地址存储在多个地点是个不错的办法。

**5. 确定负责人。**攻击发生后还有很多事情要做，包括指挥员工，联系执法部门、客户和合作伙伴。需要有人监督和管理恢复工作，准备好随时回答问题。负责人可能是首席信息官、首席运营官、安全主管等，但是最好明确这个人的权限。提前确定这个负责人，避免出现措手不及的情况。

**6. 讨论一下你将如何进行响应。**你决定支付赎金与否取决于事件的严重程度和性质，但是提前讨论这个话题比临时抱佛脚要强。联邦调查局表示，它不鼓励支付赎金，因为这会激励未来的攻击，但也指出每个企业都需要自己做决定。您应该提早讨论这个问题，至少要让你的团队熟悉这种权衡。

**7. 了解你的风承受能力。**你无法计划所有的事情，所以要弄清楚你可以承受多大的风险，以及你可以应付的潜在伤害，然后做一个权衡。例如，有些公司每个月都会做一次灾难恢复演习，以确保他们随时做好准备，这算是比较频繁的，有的公司则每季度做一次。这完全取决于你想要在系统中建立多少“保险”。这是些艰难的决定，需要事先确定。

如果幸运的话，你永远不会遭遇勒索软件攻击，但是运营一个公司不能靠运气。您的技术团队将会投入大量的工作来防范攻击并减轻损害。但是响应、告知客户并保持公司的运营是需要进行管理的。通常很难想象从来没有遇到过的情况，但是试着想象一下，一天早上你的手机响了，得知公司遭到了勒索攻击。那个时候，你会希望做了哪些准备呢，现在就着手做这些准备吧。