



## 防御勒索软件攻击七步走

哈尔滨安天科技集团股份有限公司



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，



# 中国网络安全产业联盟

## China Cybersecurity Industry Alliance

---

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。

