防范和打击勒索软件攻击的最终检查表

© 2016 思科和/或其附属公司。保留所有权利。

据关键基础设施技术学院（一个行业智囊团）最近发布的一份报告称，2016 年是勒索软件爆发年。就抗击勒索软件而论，最好的进攻就是最好的防御。您的组织是否已准备好抵御攻击？不用耗费大量时间考虑防御策略，而是使用此检查表来保护您的企业，以免受到精心策划的攻击。

☐ 1. 备份所有数据

定期计划备份是您战胜勒索软件的最强大武器。在发生攻击时，关闭终端的电源，然后重新映像终端并重新安装最新备份，防止勒索软件扩散到网络中的其他系统。

清除勒索软件将需要擦除系统，因此为了在受到攻击后快速恢复，系统状态备份或快照是必不可少的。备份越频繁，丢失的数据越少。备份频率应依据数据的战略重要性以及组织可承受的数据丢失量来确定。由于所有连接的设备都将进行加密，所以存储必须采用外置型存储且在备份完成后不会映射或连接到相应设备。

☐ 2. 频繁打补丁

有些用户运行的过时软件存在已知漏洞，勒索软件攻击者经常以此为跳板，利用漏洞悄悄潜入这些用户的网络。不一致的补丁版本和过时的软件使组织易受攻击。养成定期更新软件的好习惯。毫无疑问，为经常遭到利用的 Java 和 Flash 等第三方软件打补丁可成功防范众多攻击。

☐ 3. 对用户进行攻击源方面的培训

安全链中的最薄弱环节通常是人。如果员工落入网络钓鱼邮件或其他社会工程圈套，就会让您的组织易受攻击。就识别各种社会工程威胁场景对用户进行培训。犯罪分子之所以会采用这些手段，是因为比起发现侵入软件的方法，利用人们天生轻信的倾向常常更容易一些。

安全就是要知道谁以及什么内容可以相信。培训您的用户，要求他们在阅读邮件时向自身询问以下问题：

1. 我是否认识发件人？
2. 我是否确实需要打开该文件或访问该链接？
3. 我是否确实从该公司订购了产品？

© 2016 思科和/或其附属公司。保留所有权利。

☐ 4. 保护您的网络

通过部署分层方法来保护您的网络。使用下一代防火墙 (NGFW) 和入侵防御系统 (IPS) 等技术。分层防御可为您提供多种方法以在网络内的多个区域执行安全措施。通过消除单点故障，可有效保护网络和数据。

☐ 5. 分段网络访问

网络分段可限制攻击者可以访问的资源量。它在逻辑上将网络资产、资源和应用分组到独立的区域。通过始终动态控制访问，可帮助确保在单次攻击时不会危及整个网络。

企业大部分的网络是“一马平川”的，在业务部门之间、用户和数据之间、特定数据和业务部门之间等，几乎很少甚或没有分段。分段可用于终止或减缓恶意软件的逐步渗透，并控制所产生的威胁。

☐ 6. 密切关注网络活动

您无法保护自己看不到的东西。获得深入的网络可视性听起来可能是一项艰巨的任务，但它至关重要。能够看到网络和数据中心发生的所有事情，即可帮助您发现已经绕过您的外围防御而渗透到您的内部环境的攻击活动。

通过部署和强化所谓的隔离区 (DMZ) 来保护周边。DMZ 是包含您组织中面向外部的服务并使之与一个通常更大和不受信任网络（例如，互联网）接触的物理或逻辑子网。隔离区为您的局域网 (LAN) 增加另一层保护。它让外部网络节点仅能直接访问 DMZ 中的服务器，而不能访问您的内部网络的任何其他部分。

☐ 7. 防止初始渗入

有时，您的用户可能无意识地访问包含恶意广告的受感染网站或邮件，从而使您的网络接触到恶意软件。初始勒索软件感染通常通过邮件附件或恶意下载发生。通过努力阻止攻击者在其勒索软件活动中发送的恶意网站、邮件和附件，即可保护您的网络。

考虑建立一个公司管制的文件共享程序，组织的用户和公司合作伙伴之间可以通过该程序交换文件。使用文件共享解决方案，并指示用户不得共享或接受邮件中的文件，这样做几乎就可以完全缓解包括附件的网络钓鱼攻击。

© 2016 思科和/或其附属公司。保留所有权利。

☐ 8. 防护您的终端

在终端上部署防病毒解决方案并不足以防御勒索软件。自带设备 (BYOD) 工作场所日益普及，您必须找到能够完全控制进入网络的笔记本电脑、移动设备和平板电脑的解决方案。关键是，您的解决方案应能够做到以下两点：让您可看到网络中连接了哪些设备，以及帮助您执行可阻止用户访问受感染网站或下载可疑文件的策略。

考虑实行“最低权限”概念。即，任何给定帐户应具有执行适当任务所需的最低权限。此概念可应用于常见场所，但通常不包括终端上的用户权限和网络共享中的用户权限。此概念的关键是恶意软件很多时候都是使用当前登录用户的权限级别来运行。如果该用户是管理员，则攻击者也是管理员。请始终使用双因素身份验证。黑客可能会窃取密码，但几乎不可能同时窃取密码和智能手机或令牌。

☐ 9. 获取实时威胁情报

要主动与威胁对抗，重要的是了解您的网络攻击者。威胁情报为安全从业人员提供针对其区域、行业乃至特定公司的网络犯罪分子的事先警告，以便您有时间采取行动。那么，您如何获得实时威胁情报？及时了解最新信息和向 Talos 等威胁情报组织学习。

Talos 团队由 250 多名全职威胁研究人员组成，他们的工作是防范已知威胁和新出现的网络安全威胁。该团队通过博客文章、时事通讯、社交媒体、社区论坛和教育视频公开分享安全信息，为使互联网对每个人而言都变得更安全提供帮助。该团队负责密切关注其内容发布并在威胁临近时通知您的组织，从而让您受益。

☐ 10. 对勒索赎金说不

虽然许多企业都忍不住支付赎金以重新获得其系统的控制权，但这应该是您最后考虑的选择。请与当局联系，克制住不要向这些网络犯罪分子支付赎金。

更多相关信息

有关网络可视性和思科勒索软件的更多详情，请访问 http://www.cisco.com/go/ransomware。

© 2016 思科和/或其附属公司。保留所有权利。思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。本文提及的第三方商标均归属其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)