Acronis安克诺斯®

让企业免受勒索病毒攻击的 **10个简单贴士**

目前最常见的恶意软件攻击是针对企业和机构的勒索软件攻击，占所有IT安全事件的39%，并且仍然在增长。到2019年，刑事勒索软件收入预计将达到115亿美元。通过一些简单的策略和步骤，加上一些先进的终端应对策略，您可以有效地保护您的企业免受勒索软件的威胁。

1

确保操作系统和应用程序保持最新状态

勒索软件攻击如在2017年爆发的臭名昭着的WannaCry会经常利用软件漏洞，这些漏洞可以通过安装最新的操作系统和应用程序补丁，更新和安全版本来关闭。企业可以通过Microsoft Windows定期查看Microsoft安全公告，以了解Windows的最新安全更新。

2

执行定期备份

定期的完整镜像备份是抵御勒索软件攻击的最简单方法。定期备份关键文件，最好是备份到公司本地和安全的云存储，可以让您逆转威胁，避免勒索软件攻击的影响。您的企业可能会丢失备份后生成的一些数据和文件，但每个人都可以快速恢复工作而无需支付赎金。

3

安装防病毒软件并保持其签名数据库最新

端点防病毒（AV）产品为各种常见的恶意软件攻击提供了有效的防御。企业应仔细选择AV产品，并对其签名数据库进行自动更新。

4

启动Acronis Backup中的Active Protection主动防御

鉴于许多新的勒索软件变种能够逃脱AV的防御，您的企业还应部署具有内置防勒索软件功能的现代数据保护软件，如带有主动防御的Acronis Backup。这项创新技术使用行为启发式和机器学习来自动检测和终止勒索软件攻击，然后自动恢复在检测到攻击之前损坏的任何文件。

5

关闭企业电子邮件系统中明显的漏洞

您的电子邮件管理员可以对所有用户进行一些简单的配置更改，这将很容易成为勒索软件攻击的潜在目标。例如，默认情况下可以显示文件扩展名（如Adobe Reader文档的.pdf）。这将使用户更容易识别潜在的威胁，可执行的JavaScript文件（文件扩展名为.js），试图伪装成无害的Microsoft Word文档（.docx）。默认情况下，可以对所有电子邮件附件进行全范围的AV扫描。

6

教用户如何避免成为勒索受害者

精心设计的网络钓鱼电子邮件通常从Facebook和LinkedIn等来源收集的个人信息，看起来很值得信赖，但这是一种常见的勒索软件攻击媒介，培训您的员工，并提醒他们注意点击电子邮件链接和打开电子邮件附件的风险，并鼓励他们如果发现任何有些可疑的电子邮件，请与发件人联系。

7

细分业务网络以减少蠕虫传播

许多勒索软件变种能够从最初受感染的机器扩散到网络上的其他服务器和PC。通过如访问控制列表（Access Control Lists,），专用VLAN和上下文感知安全分段等技术细分业务的局域网，可这种病毒传播变得艰难。

8

仅向绝对需要它们的用户和应用程序授予管理权限

授予用户帐户或应用程序的权限级别越高，如果其凭据受到损害，则可能造成的损害越大。默认情况下授予基本用户权限，并且不要通过用户帐户控制提升应用程序权限级别。

9

启用业务应用程序中的最新安全功能

像Microsoft Office这样的流行业务应用程序现在包含许多"默认拒绝"安全功能，例如，禁用Word或Excel附件中的宏执行。在公司范围内设置这些默认值以关闭勒索软件常用的一些攻击向量。

10

不允许程序从AppData和LocalAppData文件夹启动

许多勒索软件变种试图瞄准某些系统级文件夹，以伪装成标准Windows进程。在Windows安装中创建特定规则以防止文件从这些文件夹中执行。

DON’T BE A STATISTIC

大多数勒索软件受害者都会措手不及地应对威胁，即使他们支付赎金，往往也会丢失关键数据，同时也会遭受收入损失，客户的埋怨和品牌声誉受损等业务后果。通过一些简单的预防措施，加上强大的防勒索应对政策如Acronis Active Protection，您可以以最有效，最具成本效益的方式保护您宝贵的数据和业务。

Acronis安克诺斯®

有关其他信息，请访问：**www.tieten.cn**