防御攻击的七个安全实践

简译版

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	7 Security Practices to Protect Against Attacks, Ransomware		
原文作者	玛丽·E·沙克利特（Mary E. Shacklett）	**原文发布日期**	2021 年 9 月 7 日
作者简介	玛丽·E·沙克利特是 Transworld Data 公司的总裁。		
原文发布单位	Information Week		
原文出处	https://www.informationweek.com/security-and-risk-strategy/7-security-practices-to-protect-against-attacks-ransomware		
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 bbs.antiy.cn 安天公益翻译板块		
摘要	企业的 IT 团队应关注下述七个安全领域：（1）培养合格的安全人员；（2）认真应对社会工程攻击；（3）跟上安全技术和软件更新的步伐；（4）更主动、更频繁地使用审计员；（5）审查供应商的安全实践；（6）与 HR 一起审查员工离职实践；（7）通知董事会和其他高管。		
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。		

防御攻击的七个安全实践

玛丽·E·沙克利特

2021 年 9 月 7 日

2021 年全球信息安全和风险管理支出预计将超过 1500 亿美元。很明显，企业已经知道安全的重要性。但是，有多少企业能跟上最新的安全实践和技术呢？

企业的 IT 团队应关注下述七个安全领域。

1. 培养合格的安全人员

通常，企业依靠其网络专家来确保和监控其网站的安全性。这是一种很好的实践；但是，聘请在安全方面具有特定专业知识的专家，或在安全实践和技术方面培训和认证一部分员工也是很有意义的。企业的目标应该是创建端到端的安全防御和策略，而非逐个网络或逐个系统解决安全问题。此安全策略应着眼于企业可能遭受的所有攻击，而非攻击发生后的反应性措施。企业还应定义自己的安全需求，以主动地获取所有权。

2. 认真应对社会工程攻击

“社会工程”是一个包罗万象的术语，企业应确保所有员工都了解日常安全实践，并加以实施。在边缘计算环境中（在这种环境中，没有 IT 背景的用户需要控制工厂和远程办公室的技术），这一点尤为重要。考虑到物联网（IoT）和网络入口点的数量不断增加，恶意软件、勒索软件和病毒最有可能从边缘入侵。零信任策略是解决边缘安全问题的一种好方法，该策略可以检测网络上所有未授权访问或已安装的设备，然后自动将其关闭。IT 和 HR 之间的合作也很重要，以确保每年对新老员工进行安全实践培训。

3. 跟上安全技术和软件更新的步伐

安全软件不断发展，以监控和减轻不断出现的新威胁。系统、网络和设备制造商也在不断升级安全措施。之前，很多企业会推迟软件更新；但是现在，安全问题日益严重，这种做法就很不可取了。企业的首席信息官（CIO）应向董事会和其他高管介绍保持当前安全最佳实践的重要性，并为关键任务安全软件安排预算。最后，IT 团队应通过网络“推送”，自动、同步地部署设备安全更新。

4. 更主动、更频繁地使用审计员

我从未见过喜欢 IT 审计的 CIO，我也不喜欢。尽管如此，IT 安全审计员可以发挥重要的作用。他们能够审计企业系统的安全性，并识别安全漏洞。他们还会为企业推荐安全最佳实践和策略。至少，企业应使用外部审计员执行年度 IT 安全审计，最好每季度进行一次小型审计，重点关注 IT 安全方面，例如社会工程攻击或 IT 安全策略审查等。

5. 审查供应商的安全实践

许多企业已将关键应用程序和系统迁移到云中，或者在供应商维护和保护的云中使用基于 SaaS 的应用程序。一旦供应商的系统遭到攻击且数据遭窃，这些公司也会成为受害者。因此，那些考虑使用新供应商的公司，其 RFP 应包含对供应商安全实践的全面审查。他们应向供应商询问其最新的 IT 安全审计。如果该供应商无法提供最近的审计报告，则公司应另寻供应商。最后，即使已经与供应商签订了合同，公司也应持续对供应商进行安全策略和实践审查，可每年进行一次。至少，供应商的策略和实践应符合公司的策略和实践。如果 SaaS 供应商使用其他供应商的数据中心来托管其系统，则公司还应审查托管供应商的安全实践和策略。如果供应商使用的托管数据中心遭到攻击，公司应清楚责任所在。

6. 与 HR 一起审查员工离职实践

当员工离职时，企业就出现了安全漏洞。如果离职是非自愿的，则被解雇的员工试图破坏系统的风险会更大。IT 和 HR 团队应每年开会审查员工离职流程。员工是否立即被送出门？员工的所有 IT 设备是否都已经上交，所有系统访问权限是否都已注销，谁负责进行检查？如果员工出自 IT 部门，是否有程序能够确保关闭任何可能的系统“后门”？

7. 通知董事会和其他高管

CIO 应向董事会和其他高管介绍当前安全环境，以及正在采取哪些措施来保护企业环境。他们越了解这些信息，就会越明白安全的重要性以及对其进行规划和资助的必要性。CIO 应计划向董事会和其他高管提交年度安全报告，并每季度向他们通报所有正在进行的安全活动和审计。

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