企业面临的三个网络安全挑战

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	Three ways to keep your organization safe from cyberattacks		
原文作者	乔什·布雷瑟斯（Josh Bressers）	**原文发布日期**	2021年9月14日
作者简介	乔什·布雷瑟斯是Elastic公司的产品安全总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/09/14/organization-safe-cyberattacks/		
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	本文介绍了企业面临的三大网络安全挑战：（1）企业必须了解其技术堆栈；（2）企业应实现告警响应的自动化；（3）企业需要营造一种跟进问题的文化，以确保问题得到解决。企业应重新审视其安全方法，使其适应“新常态”。实现透明可以为企业扫清障碍，帮助企业、企业客户和企业合作伙伴创建和维护安全的环境。		
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。		

企业面临的三个网络安全挑战

乔什·布雷瑟斯

2021 年 9 月 14 日

如今，诸如勒索软件等网络攻击不断登上新闻头条，越来越多的公司沦为受害者。在过去的一年里，我们看到了迄今为止最为严重的数据泄露事件和现实世界攻击。

自新冠疫情爆发以来，企业不得不重组其工作场所，迅速转向远程办公。如今，员工已逐渐适应了远程办公模式。我们的办公网络已经发展到包括家中客厅、地下室和城市公园等等。但是，这种变化给企业开发人员和安全团队带来了更严峻的挑战。

下面，我们将介绍企业面临的三个网络安全挑战。这三个挑战看似无关，实际上却彼此紧密关联。通过改进沟通策略，企业可以更好地应对这些挑战。

首先，企业必须了解其技术堆栈。技术堆栈是指企业 IT 基础架构的集合，包括从操作系统和编程语言到服务器、数据存储、应用程序监控工具、商业智能解决方案等的所有内容。对于企业的首席信息安全官（CISO）而言，要想应对庞大的技术堆栈和攻击手段日益高明的攻击者，需要一种新的安全方法来确保系统、数据和设备的安全。

其次，企业应实现告警响应的自动化。有道是："如果一切都是紧急情况，那么就没有一件事情是紧急的。"企业的安全团队不断从开发平台、持续集成系统、安全监控工具，甚至手表收到大量告警。矛盾的是，这种不断涌来的通知恰恰会让他们逐渐麻木，从而忽略某些告警。这个问题似乎很容易解决——即，优先考虑重要的告警。但是，企业每天都会收到大量告警及相关误报，他们无法及时处理所有告警。因此，有成千上万的告警没有得到处理，因此很多企业并不像他们想象地那样安全。为解决这一问题，企业应部署自动化的告警响应系统。

第三，企业需要营造一种跟进问题的文化，以确保问题得到解决。今年的重大数据泄露事件说明，一些看似无害的告警有可能会引发一系列事件，从而导致大规模的网络攻击。举例来说，Sunburst 恶意软件在被发现之前，就已经在目标企业的网络中呆了一年多。因此，企业应部署主动的网络安全计划，并重视合作。

（1）了解技术堆栈

实际上，技术挑战就是沟通方面的挑战。例如，是否有合适的人员帮助理解问题？是否有合适的工具用于通信和交流？

换句话说，“孤岛”是无法解决问题的。一个人用一台电脑完成任务的日子已经一去不复返了。现在，企业拥有大量管理着几乎所有内容（数千个应用程序、数百个容器和数十个云）的工具，人工审计等做法已经无法应对这些工具了。

要想保护企业的 IT 基础架构，企业的软件开发人员首先要评估和了解该基础架构。他们应了解企业正在使用哪些工具，以及这些工具是如何相互影响的。这有助于精简后续的软件更新，及时修复漏洞代码和系统，以保护企业数据。

（2）实现告警响应的自动化

企业 IT 团队每天都会收到数千条安全告警，一些 IT 专家每天甚至会收到超过 100 万条告警。及时区分关键告警与噪音，是企业 IT 团队的重中之重。

为此，企业应实现告警响应的自动化，以节省 IT 团队的时间和精力。自动化工具可以有效、高效地剔除噪音，筛选出有意义的告警。这样一来，IT 团队可以更快地确定需要立即处理的告警。

（3）跟进问题

企业全体员工都应意识到，安全是所有人的共同责任。但是，不断增加的数据事件表明，这一点常被置若罔闻。为了增强企业的安全性，全体员工应更好地彼此合作和沟通。

面对这样的问题，企业可以从开源社区中汲取灵感。例如，Debian 社区认为，在整个企业中实现彻底透明，是维持“企业契约”的核心。

企业应重新审视其安全方法，使其适应“新常态”。实现透明可以为企业扫清障碍，帮助企业、企业客户和企业合作伙伴创建和维护安全的环境。

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