如何改善网络安全事件响应

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	Why are current cybersecurity incident response efforts failing?		
原文作者	萨迪克·阿卜杜拉（Sadik Al-Abdulla）	**原文发布日期**	2022 年 5 月 26 日
作者简介	萨迪克·阿卜杜拉是 Onapsis 的首席产品官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/05/26/incident-response-approach/		
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	关键业务应用程序，例如 SAP 和 Oracle 提供的企业资源规划（ERP）系统，被认为是企业“皇冠上的珠宝”。虽然这些应用程序具有很高的价值，但却因存在关键漏洞而不断面临风险。本文将探讨当前网络安全事件响应工作失败的原因，以及主动、基于风险的方法如何帮助企业最有效地降低风险，并最大限度地利用有限的资源获得回报。		
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。		

如何改善网络安全事件响应

萨迪克·阿卜杜拉

2022 年 5 月 26 日

关键业务应用程序，例如 SAP 和 Oracle 提供的企业资源规划（ERP）系统，被认为是企业“皇冠上的珠宝”（高价值资产）。这些资产包含企业最有价值的数据，包括机密财务信息、客户信息和合作伙伴信息等等。一旦攻击者能够访问这些应用程序，就能劫持企业的工资系统、关闭其制造设施或将大笔资金转移到自己的银行账户，给企业造成严重的破坏。

虽然这些应用程序具有很高的价值，但却因存在关键漏洞而不断面临风险。与此同时，安全团队也一直面临着有限带宽/资源的挑战。

本文将探讨当前网络安全事件响应失败的原因，以及主动、基于风险的方法如何帮助企业最有效地降低风险，并最大限度地利用有限的资源获得回报。

了解当前事件响应流程中的差距

许多公司在多层技术上投入巨资，以确保其关键业务的安全。为了控制每一个攻击向量，他们购买端点安全工具、网络防御、身份验证和身份解决方案，以及应用程序交付服务等。当然，这些功能非常重要。与之相比，企业对包含最重要资产的关键业务应用程序投入的预算或时间却非常有限。多起攻击事件显示，网络犯罪分子能够直接进入关键业务应用程序，并且保持在数月甚至数年内都不被发现，期间秘密窃取高达数百万美元的资金。

在网络安全领域，收益递减规律也普遍存在：任何资产（或任何攻击向量）的第一层防御都能够最显著地降低风险。既然关键应用程序会被直接攻击，那它们也必须直接受到保护。

企业通常会创建事件响应手册，其中概述了基于攻击类型（例如勒索软件或零日漏洞利用）的策略。但是，企业应更深入地了解关键应用程序环境，并创建关注最重要的资产、系统和流程的手册，这样才能更有效地降低企业的风险。

采用基于风险的事件响应方法

通过基于风险的事件响应方法，企业能够根据漏洞和事件的风险级别来确定其优先级。要想确定漏洞和事件的风险，最简单的方法是计算其发生频率和严重程度。恶意软件不断地

入侵端点，而进行响应和清理可能会花费数千美元（直接成本和生产力损失）。此外，全世界的安全团队都认同，企业必须优先考虑和修复面向互联网的系统中的漏洞。因为这些系统不断遭受攻击，面临的风险也在不断增加。

同样，许多威胁组织会导致企业的运营和 ERP 系统停机，给企业造成数百万甚至数千万美元的损失。大型企业通常以千万美元为单位来衡量 ERP 系统的简单维护成本；而关键业务应用程序的漏洞会带来多大的损失，就更加难以想象了。随着漏洞的严重程度不断增加，应用程序的风险也在不断增加。

面向互联网的系统遭受攻击的比例最高，而关键业务应用程序攻击造成的影响最大。通过基于风险的方法，IT 团队可以正确分配时间和预算，从而最大程度地降低风险。

结合现代漏洞管理工具

借助现代漏洞管理工具，安全团队可以全面了解 IT 环境中的所有资产，包括本地、云中或两者兼有的资产。这样一来，他们就能对系统内的所有资产进行清点，识别任何隐藏的或先前已知的漏洞，并将它们记录下来。

这些工具还可以自动评估威胁、威胁对业务的影响及相关风险，对每个威胁进行详尽的描述并提供解决方案。通过这些工具的漏洞管理功能，安全团队可以全面了解企业的威胁环境和攻击面，从而将时间、资金和资源分配给高优先级的任务。

这听起来很理想，而且能够直接推动基于风险的事件响应流程。但是现实情况是，企业的事件响应存在关键差距。举例来说，诸如防火墙和漏洞扫描程序等传统工具是必要的，它们可能涵盖关键业务应用程序中的系统级问题。但是，它们不支持应用程序。因此，它们可能会检测到底层操作系统漏洞，但无法检测到 SAP 自定义代码问题或 E-Business Suite（EBS）应用程序层漏洞。

保护企业的高价值资产

如今，攻击者拥有直接攻击关键应用程序的知识和能力。只有那些准备充分的企业，才能保护其高价值资产并防止攻击造成长期影响。

安全官和事件响应团队需要做好准备，将 IT 环境中其他地方存在的标准和安全运营成熟度模型引入关键业务应用程序。攻击者已经在这样做了；防御者也该这么做了。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护（EPP）、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应（NDR）和网络流量分析（NTA）的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁（APT）的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在多地设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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*