简译版

如何从网络风险中消除人为错误

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	How to remove human error from the cyber risk equation		
原文作者	Henry Harrison	原文发布日期	2019 年 10 月 23 日
作者简介	Henry Harrison 是 Garrison 公司的首席技术官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/10/23/mitigate-human-error/		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

如何从网络风险中消除人为错误

Henry Harrison

2019 年 10 月 23 日

为了保护企业的网络资产，企业开始关注人为错误。毕竟，绝大多数攻击者利用企业员工来突破公司的防御，期望这些员工无法“看到”隐藏在看似无害的 web 链接、电子邮件或消息中的威胁。

鉴于这一点，企业领导开始意识到、并且越来越关注人为错误。根据 Shred-it 的研究，在遭受攻击的公司中，将近一半的高管认为员工或内部人员的错误或意外失误是发生攻击的主要原因。

为了解决这一问题，一些企业试图提高其员工的技能，希望他们能够具备“高度网络安全意识”。但是，这种举措被证明是徒劳的。企业当然可以对员工进行基本的“常识”安全实践培训。但是，超出此范围的任何培训可能都无法达到目标。另外，要求最终用户对攻击负责是一种“甩锅”的行为。

Gartner 预测，由于 IT 安全团队无法有效应对数字风险，到 2020 年，将有 60%的数字业务遭受重大服务故障。Gartner 提出了一个相当明显但又令人困扰的问题：如果企业的安全团队都无法应付日益复杂的网络威胁，企业又怎能期望普通员工能够应付呢？

那么，企业是接受残酷的现实——重大网络攻击是“何时会发生而非是否会发生”的问题，还是探索其他途径来增强企业保护？

我建议企业选择后者。企业可以采用一些行之有效的技术/实践和工具来保护其运行环境，同时显著降低（即使不能彻底消除）人为错误的风险。接下来，我们将介绍其中的两项技术。

Web 隔离

Web 隔离也称为远程浏览，可以将用户设置在一个隔离的环境中，让用户在其中浏览潜在风险网站。如果恶意软件感染了环境，则这种隔离可以确保恶意软件无法访问敏感的系统或数据，确保用户实际端点的安全，从而将损害降到最低。从概念上讲，web 隔离建立在用户浏览器已经提供的沙箱功能之上，如果执行得当，可以创建更高级别的安全性。

安全团队可以采用以下两种方法之一，通过 web 隔离应对基于恶意软件的网络钓鱼攻击。

（1）入站邮件网关

邮件网关通常提供链接重写功能，以确定应如何处理链接。使用某些 web 隔离解决方案，可以重写入站邮件中的链接；这样一来，在用户点击链接时，就可以通过 web 隔离的方式打开链接了。如果存在应该使用本机端点浏览器打开的已知和可信链接，则许多邮件网关允许将链接的发件人或域列入白名单。

（2）代理或安全 web 网关

当然，邮件网关只重写电子邮件中的链接。而攻击者可以利用其他渠道，例如聊天或文件传输，将钓鱼链接发送给用户。为了应对该风险，企业可以考虑部署基于代理（或其他安全 web 网关）的解决方案。在这种情况下，安全团队会在代理中构建一个 URL 白名单，通过 web 隔离严格限制对非白名单域的访问。

定义白名单的方法可能会有所不同。许多企业执行非常严格的白名单，仅限于能够提供安全文档和审计报告的已知和受信云服务。

另一种更灵活的方法是：记录用户最近一两个月访问过的所有域，并使用这些域创建白名单。即使是最大的企业，此白名单也很有可能覆盖不了所有网站的 1%。但它很可能覆盖用户下个月要浏览的域的 99%以上。

用户几乎不会注意到任何差异——超过 99%的浏览将完全像以前一样进行。但是这种方法几乎可以保证，任何网络钓鱼链接都不会出现在白名单中。因此，如果网络钓鱼链接被打开，最终将以 web 隔离的形式进行。

硬件安全

Web 隔离的想法非常好，但是如果 web 隔离解决方案本身可以被破坏，那么它就没有用处了。为了避免这种风险，企业可以使用基于硬件安全（hardsec）的方法。

数十年来，我们受益于在 CPU 上运行的软件的惊人灵活性。但是，这种灵活性也是当今 IT 环境的致命弱点——如今的 IT 环境非常复杂，简单的漏洞就可能产生无法预料的影响。软件可以提供强大的能力——通过提供正确的指令，企业就能开发出能够想象到的任何功

能。但是同样地，攻击者也能够利用这种强大的能力；他们可以替换指令，从而破坏计算平台的所有功能。

这也是所有安全软件的弱点。其结果是，精心设计的保护工具可能使企业暴露在更大的风险中。的确，许多端点安全产品都有非常严重的漏洞。因此，使用这些产品反而不“安全”。

硬件安全已经成为一种可行的替代架构。硬件安全大约 10 年前起源于英国政府安全社区，并在此后不断发展。它使用硬件方法（而非通常的软件和基于监控的方法）来应对日益增长的网络安全挑战，部署“现场可编程门阵列”（FPGA）集成电路，而非 CPU。FPGA 只能使用特定的物理 FPGA 引脚进行编程，这使安全团队可以通过物理硬件设计和实施来限制可以重新编程 FPGA 的人员——只有能够访问受保护特权管理环境的人员才能重新编程 FPGA。攻击者无法将数据传输到引脚，因此无法进行编程。

与复杂、灵活、为攻击者提供了大量漏洞利用机会的软件工具相比，硬件安全控制相对简单且狭窄。它们“太笨拙而无法被攻破”。

借助硬件安全措施，我们可以将硬件和软件的优势结合起来：（1）硬件安全的优势——硬件安全不同于传统的图灵计算机逻辑，不会遭受软件漏洞的侵害；（2）软件的灵活性，允许通用硬件平台根据其编程方式发挥多种作用。

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，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿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