执行摘要

亚太是快速发展的地区，在数字化转型领域正在突飞猛进。该地区分布着非常多样化的经济体，在发展未来的互连城市 - 智能城市方面引领风气之先。许多经济体见证了这些方面快速发展所带来的好处，物联网(IoT)在一些组织中已很常见，工作人员继续灵活地远程工作，更多的设备也连接到互联网。

在开启快速发展大道的同时，也带来了严重的网络安全威胁以及公司和个人的风险。攻击者正在变得越来越复杂高端，并采用最先进的技术来攻击组织。

2017 年经历了一波前所未有的网络攻击高潮，而各种网络安全措施也疲于应付，但仍然没有一个过硬的数字基础设施基石。从这个角度来看，亚太的公司每分钟收到 6 个威胁，但只有 50% 的警报被调查。

由独立第三方研究机构进行的思科2018亚太地区国家安全能力基准研究报告提供了对于 11 个国家/地区 2000 个受访者安全实践的深入分析研究。其中包括北亚的中国、韩国、日本，东南亚的新加坡、泰国、马来西亚、越南、菲律宾和印度尼西亚，南部的澳大利亚以及印度。*

在此报告中，我们重点介绍了网络安全事故造成的亚太地区的潜在经济损失，防御者有大量工作要做的情况，以及面临的挑战。我们的研究和洞察旨在帮助各组织有效地应对当今快速演变、复杂高端的威胁。

此报告的主要研究结果为:

1. 安全漏洞

   攻击者正在变得越来越复杂高端和好斗。在亚太，公司一天最多收到 10,000 个威胁。即一分钟收到 6 个威胁。近 69% 被调查的公司一天收到 5,000 多个威胁。

   但是，在警报总数的情况下，也只有 50% 的警报被调查。

2. 缺乏安全应对措施

   针对数字安全基础设施部署问题，我们的研究对 2000 名受访者进行了调查。其中， 9% 的受访者称其组织内部没有配备专门的网络安全专家，而 13% 的受访者称其组织内部没有直接负责网络安全的主管。

   在受访者中，仅 42% 的称其高管人员认为网络安全非常重要，而仅 44% 的人强烈认为应当明确安全管理人员的职责并建立相应的管理制度。

3. 经济和声誉受损

   网络攻击会造成深远的影响和后果，包括公司的财务和声誉损失。在东南亚，51% 的网络攻击造成的损失超过 1 百万美元。近 10% 的受访者称，攻击让他们损失超过 5 百万美元。研究中 33% 的受访者称，攻击会使他们损失 1 到 5 百万美元。

4. 多管齐下的攻击

   网络攻击的形式也在变化。攻击者现在不仅针对 IT 基本设施，同时也针对影响企业日常运营和运作的运营技术 (OT)。

   30% 的组织已经经历了这些类型的网络攻击，而 50% 的称，他们预计也会遇到这种情况。此外，41% 的亚太受访者称，如果其运营基本设施受到攻击，他们的业务会受到影响。

5. 来自利益相关者的更大关切

   除财务损失外，网络安全事故也在逐渐削弱亚太组织赢得其客户和利益相关者信心的能力，72% 的组织称，来自其客户的更大隐私关切延长了其销售周期。近一半的组织称，其销售周期延长了一个月以上。

   在接下来的年份，专责们也认为，来自如投资人、保险公司、监管者、商业合作伙伴、行政领导、监控/利益组、媒体和员工等利益相关者的关切也会开始上升。

给防御者的建议

当黑客不可避免地攻击其组织时，防御者是否做好了准备？他们如何能够快速恢复？Cisco 2018 亚太安全功能基准研究的结果提供了对于 11 个国家/地区 2000 个受访者安全实践的深入分析研究，显示防御者会面临大量的挑战。

即使如此，防御者会发现，提升战略安全和遵守常见最佳实践可以降低暴露于新出现风险的机会，延缓攻击者的进程，并提供对于威胁情势的更深洞察力。他们应考虑:

- 部署可以调整升级的一线防御工具，如云安全平台。
- 确认他们遵守针对应用程序、系统和设备补丁的公司策略和实践。
- 实施网络分段以帮助降低网络大面积崩塌。
- 采用下一代端点流程监控工具。
- 及时访问准确的威胁情报数据和流程，让这些数据可以纳入到安全监控和事件处理。
- 执行更深和更先进的分析流程。
- 审查和实施安全响应程序。

*在 2017 年对日本、中国、印度、澳大利亚受访者进行了调查。2018年6月在研究的后面阶段对新加坡、印度尼西亚、泰国进行了调查。

- 经常备份数据和测试恢复流程 – 在瞬息万变、充斥着网络勒索病毒和破坏性网络武器的世界里至关重要的那些程序。
- 审查第三方的安全技术效力测试以帮助减少供应链攻击风险。
- 执行微服务、云服务和应用管理系统安全扫描。
- 审查安全系统和探索使用 SSL 分析，如果可能，也使用 SSL 解密。

防御者也应考虑采用先进的安全技术，包括机器学习和人工智能。恶意软件在加密的网络流量中隐藏其通讯，不怀好意的内鬼通过公司云系统发送敏感数据，安全团队需要有效的工具来防止或检测隐匿恶意行为的加密的使用。

关于报告

思科2018亚太地区国家安全能力基准研究报告介绍了我们最新的安全行业发展动态，旨在帮助组织和用户防御攻击。我们也审视黑客用来突破这些防御和规避检测的技术和战略。本报告还重点介绍了 Cisco 2018 安全功能基准研究的重要研究结果，检查企业的安全态度及其对于防御攻击之准备工作的认识。