企业合并安全

企业合并安全

在今天的信息安全市场上，经常发生收购和合并。虽然很难预料并购给企业带了的利益，但是并购活动通常都会对两个公司的员工产生影响。在紧张而不确定的过度阶段，公司不能简单地把不同的员工、程序和政策结合在一起，就袖手不管了。

公司的安全人员必须小心管理法规遵从、网络安全策略、Web 应用结构、恶意软件以及其他公司可能面临的外部威胁。在并购后，负担加倍。来自两个组织的员工需要一起讨论并购策略，决定安全标准以及其他的企业架构调整。

在本专题中，安全专家解释了管理两个公司完全不同的员工的最好方法、技术和策略。本文中介绍了在并购时的需要注意的问题，并为合并的每一步提供了参开的办法。

合并中的网络安全策略

企业的合并通常需要合并两个完全不同的网络策略。但是在作出最后的技术性决定前，来自两个公司的员工需要达成一致。在本文章，安全专家解释了新的安全策略的制定者必须和两方沟通后才在两家公司之间创建强大而范围广泛的关系。

- ❖ 并购：合并的网络安全策略

合并中的法规遵从

当一家公司收购另一家时，法规问题的解决似乎是 IT 安全人员面临的最困难的 问题。但是安全专家说实际上没有这么糟糕，而且提供了一些安全指南，使在法规遵从山个处于不同阶段的公司可以顺利完成并购。

- ❖ 合并过程中制定法规的最佳方式

Web 应用安全

当两家公司合并的时候，Web 应用结构也需要进行合并。如果得不到各方面的合作，保护和整合应用就会很痛苦。本文中解释可合并后的企业领导应该如何避免艰苦的斗争，以及如何对安全安排的各个方面进行无偏见的检查。

- 确保公司合并的网络应用安全

与合并相关的安全威胁

在今天的信息安全世界中，合并和收购很常见。但是这对恶意黑客和窃取数据者来说也是好消息。当公司被强制合并的时候，他们经常成为攻击的目标。本文将介绍和合并相关的顶级威胁，以及防御的方法。

- 合并和收购：并购之后 构建安全

并购：合并的网络安全策略

在技术行业内，经常会发生并购。几乎每天，商业新闻中都有一篇文章的标题是关于两个公司合并或者较大的竞争对手收购了一家小型企业的。这些交易中，每个都涵盖了一系列复杂的行为，随着重复功能、程序和资源的消失，旨在巩固业务并削减成本。

尽管，信息安全专业人士经常会接到这样的任务：调节潜在的两个不相干的网络安全策略的设置。虽然这至少可以说可能是一种尝试性的任务，但是幸运的是，有许多策略可以帮助公司在充满挑战的并购过程中获得成功。

当我们进行合并策略的进程时，重要的是要切记合并可能会影响参与者的心态。公司合并可以创造一个不确定、怀疑和恐惧的气氛，而且公司环境的突然改变会在员工之间造成一定的压力。因此，在整个网络安全策略的一体化进程中，要留意每个人所面临的困难。

下面我们来看一些可以缓解过渡转变所带来的压力的实际策略：

不要着急。记住这句格言：“罗马不是一天建成的”。安全策略的开发是一项复杂的事业，并且需要仔细的、有条不紊的方法。没有一种早期的安全策略是在短时间内完成的，因此，不要试图短时间内将其综合起来。

考虑所有的选择。在合并两个不同组织的安全策略时，可以有三个基本的公开的选择：全部采用其中的一个或者另一个安全策略；将两个策略的要素结合到一个新的策略中；或者从头开始编写一个新的策略。当一个企业开始合并进程时，重要的是对所有这些方法持开放的态度，不论合并的环境是什么情况。实际上来说，虽然政治上的考虑可能会影响到方法，但是如果整个进程不受这些问题影响的话，整个团队都会受益。比如，考虑这样一种情况：在公司网络上使用个人计算机时，合并的两个公司有不同的策略。一家公司可能完全禁止这种行为，而另一家公司可能对这种行为没有任何限制。这种情况下，可

接受的方法就是发展一项折中的策略，即如果它们已经通过了初步的安全控制测试，那么允许有限制地使用这样的系统。

囊括一个广泛的团队。某一个人闭门独立完成的策略注定要失败。应该将更广范围的人（来自并购的两个企业中）引入策略合并团队，以确保可以考虑多方面的因素。这样的安排使得更多的个人对最终结果有一种拥有的感觉，也使得合并后的企业更容易接受该小组的工作。再来看一下上面提到的例子：有关将个人所有的系统连接到公司网络方面的策略。如果该企业决定采取一个折中的策略，拥有来自有两个组织的代表就有助于为所有小组成员提供一种主人翁意识，大大增加了接受的可能性。

畅通的交流。任何合并中都必然会存在混乱，因此重要的是在信息安全责任方面与员工进行管理交流。在合并策略的时候，应当采取过渡阶段的措施，以确保全体员工了解对他们的期望是什么。在这个问题上，从组织中的其它员工那里获得一些提示。在一段时间内，两个组织是否需要采用不同的管理结构来运行呢？如果是的话，就可能需要告知员工，在接到指示之前，他们只需要遵守与过去相同的安全策略和程序。无论如何，要重点突出、言简意赅，并与整个组织的员工进行沟通交流。

采取分阶段的方法来改变。如果合并策略会导致一方或者两方在开展业务时发生急剧的变化，那么有可能的话，试着分阶段实施这些策略。这就使员工有时间按步骤地适应这些新要求，并且可以有机会评估员工接受策略的进度，以确保整个进程有条不紊的进行。比如，在某个组织中，外界可以不受约束地访问是以前的规范，如果某个员工想要强制在此实施内容过滤，那么最好考虑分阶段实施：最初的阶段先阻止最异常的站点访问；接下来的阶段中，警告用户新的策略可能会阻止他们所访问的内容。这就使得用户有机会测试，确定在哪些区域新的策略可能会干扰业务的需求。

公司合并带来了众多技术和业务方面的挑战。然而，合并网络策略并非总是关于技术方面的。成功的并购决议一方面需要与两个不同的组织进行有效地沟通另一方面需要审慎的决定，同时考虑到双方的策略和员工。

（作者： Mike Chapple 译者：李娜娜 来源：TechTarget 中国）

合并过程中制定法规的最佳方式

即使是在最佳的环境中，对于所涉及的双方而言，并购也是痛苦的。对于合并企业而言，它们可能是合乎逻辑的，但是对于 IT 员工而言，试图将两个不相干的系统结合在一起就可以是一场噩梦。特别是对于那些专门负责任何法规制定问题的 IT 安全小组。

如果组合两个 IT 安全的基础设施看起来是项艰巨的任务的话，可想而知，将两家公司不同阶段的制定法规程序合在一起是一项多么艰难的任务。让我们感到欣慰的是，它可能并不像所看起来的那么坏。将法规制定结合起来的两个关键的决定性因素是合作伙伴所从事的行业，以及他们所必需面对的合并特殊法规所规定的具体细节。创建一个统一标准的遵守团队，包括两家公司从事制定法规的员工，这是减缓进程的一种有效方式。

行业内部

通常情况下，一个组织的法规要求是由其所从事的行业决定的。金融公司要求能够满足《萨班斯-奥克斯莱法案》（SOX）和《格雷姆-里奇-比利雷法案》（GLBA）的规定。那些从事健康中心和医疗领域的公司必须得满足《健康保险便利及责任法案》（HIPAA）的标准，发行或者使用信用卡的公司必须满足《支付卡行业数据安全标准》。

显而易见，暂且不谈合并的企业，即使是单个企业也经常会有重叠的现象发生。发行信用卡的银行必须要满足《萨班斯-奥克斯莱法案》（SOX）、《格雷姆-里奇-比利雷法案》（GLBA）和支付卡行业（PCI）数据安全标准的规定。大型的卫生保健公司，如果是公开交易或者是金融组织的一部分，除了需要满足通常的 HIPPAA 要求以外，可能要求满足《萨班斯-奥克斯莱法案》（SOX）标准。

法规的具体问题

关于上面所提到的每一种普遍适用的法规，最关键的问题是考虑访问管理、信息安全策略、客户数据的保护、以及监测与测试。

SOX 的第 404 条是关于影响 IT 安全的规定。这一条要求控制那些可以访问敏感客户和金融数据的 IT 系统。虽然它对于如何实施这些控制是模糊的名单是它基本上查找涵盖访问控制管理、加密、防火墙和恶意保护的文件。此外，适当的位置必须有一个可靠的信息安全策略，以概述这些条款的实施要求。

从合并的角度而言，SOX 审计员和管理者会寻找关于访问管理控制方面的报告。然而，在审计员到达之前，安全专业人士需要询问一些关键问题，以确保两家公司在同一级别的环境中：两家公司使用什么类型的访问管理系统呢？他们是否都使用 Active Directory，还是其中一个使用 LDPA，而另一个使用别的协议？现在，两家公司帐目审计的情况如何？

虽然，GLBA（Gramm-Leach-Bliley 法案）与 SOX 的规定类似，但是它更侧重于保护客户的数据，而非访问控制管理。GLBA 要求对机密数据加密；访问系统时，使用强密码；限制员工访问客户的数据，以及为客户记录的物理安全。在合并的情况下，有了 SOX，安全小组可以对比每家公司的加密方法、客户数据处理程序、以及全面坚持其各自的信息安全策略。策略和程序需要调整为两家公司都适用的共同标准。此外，有了 SOX，所有这些都需要为管理者提供文件证明。

HIPAA 规定了医疗行业公司对患者信息的保护。这里的重点是，与 GLBA 一样，HIPAA 是在保护客户的——在这种情况下，是在保护患者的——信息。在并购中，两家公司不得不对其控制客户信息的记录进行比较，然后为管理者提交一份共同的文件。

SOX、GLB 和 HIPAA 都是由法律支持的政府法规。另一方面，PCI 是由五家最大的信用卡公司组成的联盟支持的行业标准：Visa、MasterCard、Discover、American Express 和 JCB。PCI 是一项综合的标准，有 12 条要求，囊括了客户数据的保护、加密、网络安全和防火墙、访问管理控制、信息安全策略、以及网络安全的监测和测试。它涵盖了多个领域，这些领域的安全方式各有不同，这就使合并公司成了件令人头疼的事情。

所有有关的数据和访问

即使所有的法规都是针对相同的基本项目——访问控制、客户数据的保护、以及网络安全的监测——确保遵守每一项这些特殊要求。与规定类似的法规并不意味着该法规可以转化为另一条法规。

为了使整个过程更加容易，新收购的公司必须为合并后的组织任命一个人负责法规制定的平衡点。这个人应当来自两个并购伙伴之一，并且能够直接与两家公司制定法规的员工合作，进而实现法规制定的和谐。

(作者：Joel Dubin 译者：李娜娜 来源：TechTarget 中国)

确保公司合并的网络应用安全

合并和收购为 IT 部门创造了一个具有挑战性的环境。尽管交易可能会很快完成，但是接下来的系统整合却需要花费几个月的工夫——如果不是几年的话——来完成。

新近合并的组织试图通过组合其网络应用基础设施提高效率，这种行为是很常见的。而这样的努力可以带来大量与安全相关的挑战，通往成功的最佳途径需要一个公正的安全机制考核，以及英明的决策，以确定哪些运行效果最好，哪些需要添加或者替换。

网络应用合并风险分析

当两个企业合并的时候，它们肯定会有不同的安全理念、策略、技术、以及网络应用安全的相关要求。比如，允许客户追踪订货进度的电子商务网站就必须比在订货完成后仅发送电子邮件的网站允许对后端系统进行更深入的访问。如果一个组织已经使用博客和 wiki 技术来与雇员和客户进行交流，那么变更控制就可能成为另一个冲突。

由于每家公司有不同的方法和需求，来自两家企业的人员共同组成的团队必须承担对新公司所暴露风险的评价工作，并为合并的网络安全操作设定目标。在被收购公司进行正当审查时，应当实行风险分析，包括确定关键业务的驱动装置、工作流程的需要、预算、时间和性能标准，进而理解现有安全基础设施背后的安全策略和业务逻辑。

但是，在两个合并的企业整合网络应用程序前，应该使用综合的渗透测试对其边界防御的强度、远程访问的安全性和第三方连接进行评估。这期间，两个企业应当继续分开运作。只要这些任务完成，两个企业的安全情况就会变得明朗。渗透测试可以帮助确定是否可以实现基本的安全目标，并且标记出可能对网络应用的合并产生任何影响的不足之处。

安全往往是与具体的应用程序直接挂钩的，尤其是基于 Web 的应用。在安全防御和程序中实施任何变更之前，需要对其影响进行评估。如果客户的信息数据库合并了，最受关

注的领域可能就会出现。应该重新评估应用和用户访问权限，而且所有应用中的数据有效性都要进行重新评估，以确保它们可以正确处理数据领域内的任何变更。应用程序处理信息的方式的任何变更都应当进行审查，确保该应用程序不会突然受到逻辑攻击的威胁。下一步，应当在物理安全和事故响应程序过程中，对业务连续性和灾难恢复计划进行更新和测试。随着企业开始合并，可能会出现网络容量问题。在任何过渡期，都需要对系统和应用的稳定性进行监测，以使业务流程的中断最低。

结论

尽管在合并中保持应用程序的安全性是一个挑战，但是这样的事件为降低成本、实行一套安全技术标准、以及研究新的理念和安全管理模式提供了机会。许多组织发现使用负责所有的安全进程的中央安全概况很有用。通常人们认为这是一种更有效的模式，因为它可以确保安全性更加协调，更有效地利用资源。毕竟，资源利用是促使公司合并的第一要素。

(作者：Michael Cobb 译者：李娜娜 来源：TechTarget 中国)

合并和收购：并购之后 构建安全

你是否已经留意到了最近商业新闻的标题？合并和收购一直在频繁发生，而且常常出乎意料——尤其是在信息安全市场——并且许多信息安全专家在将两个完全不同的公司合并方面面临着艰巨的任务。但是，如果不能恰当地处理整合进程的话，会严重影响企业的安全状态，甚至使得合并后的公司与过去相比更不安全。

当企业发现自己出现在新闻头条中——以任何理由，包括合并或者收购——它通常会成为漏洞扫描、网络钓鱼企图、以及其它恶意活动的攻击目标。并购活动也会带来内部威胁，因为紧张的业内人士可能担心合并会如何影响他们工作的稳定。因此，一些人可能开始从网上收集一些有价值的信息。所有这些都增加了安全小组所面临的挑战，因为它指出了合并策略，以及如何最好地保护公司。

正在进行合并的公司应该谨记下面的安全问题，并相应地做出规划：

统一信息安全策略——合并的企业几乎总是在其信息安全策略方面存在严重的差距。在规划合并过程中，必须检查并合并这些策略。如果每一方都遵循自己的方针，那么这个过程就需要谨慎对待。与高层管理合作，挑选一个可以最终决定难处理的政策问题的领导人。很有可能其中一个企业的策略比另一个更全面，因此，当需要做出艰难的决定时，重要的是做出可以提高安全性的选择。

一旦策略得到了统一，就进行差距分析，在两个企业中评估新策略。制定一份指南，规定两家公司需要遵守哪些程序和技术方面的变更。

调整策略和技术需要一些时间。重要的是，要尽可能早地开始策略统一和评估工作，也许甚至是在合并公告发布前。但是大多信息安全专家都是通过阅读新闻消息，才得知自己公司被并购，所以在公告前预先规划通常是不可能的。

在策略整合的过程中，一些技术领域必须立即加以处理，支持组织预防攻击，因为只要合并过程一开始，这个组织就很容易受到攻击。

了解网络结构——开始的时候要获得两家公司的因特网和商业伙伴之间的连接的体系结构图。确保两家公司有能力监控它们的 DMZ 和重要的内部网络，尤其是带有入侵检测系统（IDS）传感器的网络。当合并发生时，在两家公司另外配置传感器，寻找威胁的证据。调节它们寻找最有可能的攻击，重点是 Windows 问题、Web 应用攻击、或者某个特定环境中常见的其它类型的攻击。指派两家公司的信息安全工作人员和系统管理员分析 IDS 警报，进而确定系统是否已经受到了攻击。

决定无线局域网的配置——如果其中一家企业在很大程度上都依靠 Wi-Fi，而另一家不是，那么它们的脆弱程度就存在很大的差异。如果其中一家企业可能已经逐渐习惯了使用无线网，我们要做的不是禁止这家企业使用无线网，而是要检查它们无线基础架构的安全设置。如果它缺乏加密技术或者认证技术不够强大，那么就要考虑采用改进的技术加强它，比如 WPA2。

决定 USB——为了减少内部数据安全泄露和其它内部威胁，公司可以选择在笔记本电脑上禁用 USB 设备。在做出这个选择之前，必须要考虑这种行为的行政影响和功能影响。

控制恶意软件——确保两家公司都配置了最新的杀毒和反间谍软件特征库。此外，为了将系统受到威胁的机率降到最低，确保两家企业的系统都配置了最新的重要补丁。

教育员工——在这个关键时刻，考虑员工的信息安全意识。在信息安全策略得到合并以后，应该制订全面的安全意识项目。即使是在策略完成之前，合并的公司应该考虑推出一个短期的、集中的于有针对性的网络钓鱼攻击的危险的安全意识项目。在公司餐厅中，按桌逐个发放传单、信息表，以及一些有指示作用的电子邮件都可以用来有效地警告员工，他们不应该相信所有的链接，而且应该经常核实电子邮件地址的来源。还需要告知工作人员永远都不应该运行可执行的电子邮件附件，即使它包含在 ZIP 文件中。

检测防火墙和入侵检测系统工具——一旦合并完成以后，安全小组的成员应该留意从互联网向外传输的大量数据。依照员工“正常”的因特网使用模式，公司可能会希望对FTP 或者 HTTP 所传输的任何大于一定量的文件进行扫描，可以是 100MB 或者 1GB。任何违反行为都可能是重要数据泄露的征兆。同时监控 Web 代理器的日志，并确定是否下载了攻击工具并且在任何一家公司内部使用。

因此，最后，为了防止合并过程中发生信息安全威胁，合并的公司应当有两个主要目标：

1. 对策略、程序和技术的长期调整
2. 由一系列快速攻击技术防御所支持的加强政策

成功地执行这个双管齐下的策略可以帮助正在合并的公司显著地降低风险。

（作者：Ed Skoudis 译者：李娜娜 来源：TechTarget 中国）