如何制定全面的网络安全计划？ PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E5_88_B6_E5_c101_461739.htm 我正在公司修订的网络安全计划，我应该使用什么样的工具来制定时下最新的策略呢？是否存在能够使之更简单的工具呢？ 安全是一个不断发展的目标，需要持续的管理和细化，从而能够保障服务和系统在一定程度上的机密性、完整性和有效性，而这对你的业务以及颇有价值的信息来讲是至关重要的，这些高值信息一般是处于我们防护架构中的核心。 不断涌现的以客户信息以及私密数据丢失为极端的事件，促使我们中的许多人回过头来大范围对基础设施及其使用的安全工具进行重新评估。 在种种情况下，你会困惑如何能够使用网络工具来帮助制定最新的安全策略。 一种轻率的，同时我怀疑为很流行的答案是，工具不是用来制定策略的，而是用来强化策略的，依我来看，这种观点是不恰当的，因为工具对安全流程最大的贡献就是强化策略，工具对侵入回环系统的行为记录下日志，这种行为就能够说明发生了策略变更。换而言之，知道了工具所未覆盖的东西，能够使我们将这些东西纳入(或者更新)到我们的安全策略当中。 虽然你问的是细节问题，但我仅提供我所能建议的。 众所周知，生计工具并不被认为是策略工具。但是，如果使用另外的方法，其中的许多工具都能够对你策略的整合发挥一定作用。 漏洞扫描器-这些扫描器有助于你确定补丁策略，一旦你知道了暴露的漏洞，你就会决定是否该继续采用当前的环境、时帧和补丁SLA，以及防火墙的规则。 应用安全扫描器-这些扫描器能使你决定安全编码标

准，以及是否应该投资编码扫描技术来自动实施和增强你所植入的标准。 流数据和基于网络的异常检测-知道了典型的网络行为，你能够更好关注到希望通过策略或者其它工具来阻止的一般行为，所有的这些技术都实现网络流量的可视化。 IDS-优秀的IDS系统能够向你提示攻击入侵的消息，并提示你决定应在架构上采用什么样的技术。IDS能够提示你特定操作系统上遭受到攻击，需要部署另外一个操作系统来作为防御策略的一部分，或者你没有发现蠕虫正试图从一个网络扩散到另外一个网络，IDS会提示你生成一个部分或者全部分离网络的安全策略。 以上并非为安全领域仅有的成熟技术，当然还有很多例子 新兴工具 除了成熟工具之外，一些新的技术也正在出现，其中一些成功了，一起并没成功，其中有很多的技术，尽管还在发展过程中，也是非常只得关注的。其中典型的例子就是网络风险映射应用和数据丢失防护。 网络风险映射产品将过滤出漏洞数据和网络设备配置，并帮助你排序区分出哪些是需要首先解决的。这些数据是基于定义节点的危险程度、直接漏洞主机、网络设备的非安全配置以及易受越级攻击危害影响的主机等得出。 数据丢失防护工具(常被称为DLP)能够更好的帮助用户如何规范操作行为，帮助你如何教育用户，帮助你得知普遍业务风险之所在。DLP是一系列的解决方案集，能够为信息和概念保障安全，这些方案通过三种方法直接实现，即打散活动数据线、休眠数据线和使用数据线。 活动数据DLP是通过部署在网络最外侧点或者网络汇聚点的传感器设备来实现的。这些传感器对传送的数据进行检测，检测其是否触发了繁殖防护规则或者是否包含了敏感数据，例如，任何试图将知识产权发送到网络之外的行为

，都会依据设置的规则生成日志记录，与此类似，当个人身份信息、用户列表或者价格信息被发送时，也会按照规则生成日志记录。这些传感器能够同其它的安全系统，例如代理服务器或者邮件发送代理等，实现集成来阻止这些数据的传送。 休眠数据DLP通过部署在网络节点中的附加设备来实现的，这些设备检测敏感数据的繁殖，或者其它违背规则的数据，例如使用活动数据传感器系统的数据等，一般情况下，网络附加设备也能够为管理者提供一些“ 注册识别 ”或者“ 指纹识别 ”传感文件的工具，例如输入传感数据、检测这些文件的端节点等。休眠数据DLP系统还能够向相邻的DLP系统(例如活动数据DLP)发送指纹信息，或者“ 文件签名 ”，从而加强对检测或防护数据离开网络行为的控制。 使用数据DLP是通过部署在用户桌面上的软件终端来实现的，这是对例如软件防火墙、HIDS/HIPS和防病毒等其它安全方案的补充。这些代理可以确保管理者能够防止敏感数据通过非认可的IO通道离开公司，例如非加密的USB设备，或者用户的Web邮箱。 DLP的概念使信息安全的系列技术能够得以规范化协作。 还是那句话，包括我所提到的之外，还有很多能够引起你兴趣的新兴技术，当你最终评估你的网络安全工具包的下步发展时，你可以考虑是DLP、网络风险映射，还是其它的新兴技术能够发挥一定的作用，从而帮助你加强当前不能或者不足以控制的防护和检测。 最后一条建议：网络安全不是所有事情的中心，评估服务器技术以及他们对安全目标的贡献。如可能，采取一些减少差距的措施，加强现有防御控制的深度，或者采用其它对你的安全目标有贡献的其它方法。 100Test 下载频道开通，各类考试题目直接下载。详细