网络安全重整旗鼓:部署网络外围保护Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/571/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_571832.htm 如何在网络外围防御不够的情况下保护关键数据以及合规数据呢? 近年来，越来越多的企业开始向外部商业伙伴和移动办公的员工开放公司的网络和数据中心，而安全专家们则一再表示，网络外围防御非常薄弱，存在很多漏洞，很可能使关键数据从端点泄漏并涌出数据库和文件共享区域。 现在的安全行业仍然还没从TJX公司泄漏事故的刺痛中缓过神来，该泄漏事故发生在去年8月，11名攻击者自2004年来就隐藏在TJX公司和其他6家品牌商的网络中，总共盗取了信用卡和借记卡帐户4500万美元。 如今的网络到处都布满漏洞，企业不仅要抵御那些试图攻击漏洞盗取信用卡号码的黑客，同样也要避免那些在家里办公的员工不小心将关键资料传到外部网络。 伦比亚大学计算机科学系的教授Steven Bellovin表示，“ 通常情况下，公司经常需要透过防火墙与外部网络用户联系(包括客户、WEB服务、供应商以及外包商)，我们并没有保护好我们的关键数据，那么，我们应该怎么做呢? ”Bellovin提出了中心安全的概念，以防止外部攻击者获取数据库和文件共享区域中的关键数据。这个概念与Open Group的Jericho Forum的想法非常相似，Jericho Forum主张根据数据重要性给数据分级，重点保护存储关键数据的区域，为这些分级数据进行加密并部署不同级别的安全通信方式。 网络外围，作为过滤网络攻击的有效屏障，其实还可以发挥更多重要的作用。不管是Bellovin还是Jericho Forum，他们并没有主张让公司企业对他们的外围

边缘安全置之不理，他们也没有让公司简化信息保护的流程，他们希望开发出拥有更多过滤层、更具复杂性和多种选择的整合保护产品。“ 我们的问题在于没有从整体把握数据，结果导致大量数据泄漏事故的发生，”Jeff Boles说，他是服务器和存储咨询公司Taneja Group的验证服务主管，“ 从整体把握数据需要弄清楚被访问的资源与用户之间的关系，用户通常怎样使用数据以及数据的性质等问题。”从整体把握保护关键数据的方法为那些正试图分辨结构化数据和非结构化数据或者使用中的数据和存储中的数据的IT专业人士们提供了整合解决方案的概念，不过，数据分级、加密、监测、控制访问以及关键数据的使用等工作是很难作为整体解决的，这就使公司不得不使用各种不同的工具来保护数据不被外泄，这些工具数据丢失防护工具、访问控制和加密工具等。 如何解决数据安全威胁 首先，公司必须弄清楚哪些数据需要得到保护以及将这些数据存储在何处等基本问题，这也是Bellovin和Jericho模式的基本原理。 然而，很多公司根本不知道哪些是需要保护的数据以及数据存储的位置，Aberdeen Group的副总裁兼研究员Derek Brink表示。在Aberdeen Group五月份公布的调查显示(调查对象是120多名IT安全专业人士)，50%的受访者表示其公司已经明确了关键数据并对关键数据做了分类。“ 你肯定不会想浪费那么多钱去保护广告电子邮件，”Brink说，“ 你只需要保护真正重要的资源和数据，不过，将这些重要数据分类才是真正大的挑战。”拥有七家医院、两支医疗小组和16000名员工的Sharp HealthCare(位于圣地亚哥的夏普医疗护理中心)在数据分类方面就做得很好，该医疗护理中心使用了各种各样的手动和自动化工具来了解数据性

质并管理好关键数据，技术安全架构师Starla Rivers表示。 夏普医疗护理中心使用了赛门铁克公司的Vontu数据丢失防护产品套件来发现关键非结构化数据，例如医保卡号码和社保卡号码等。Vontu首先会是通过识别几个关键数据库中的数据，这些关键数据库是存储HIPAA法案(健康保险流通与责任法案)、金融法规与其他法规审计数据的区域。接着 Vontu会检查这些数据在数据库外面的文件共享区域和端点处的行径来最终确定关键数据。 根据Bellovin和Jericho的理论，DLP供应商们认为，DLP工具最好用于监控少量的重要的数据类型。因此，Vontu在执行初次扫描时并不需要标记关键数据库中的每种类型的数据，人们通常会标记前五种或者前六种需要保护的数据类型。Aberdeen调查结果显示，像夏普医疗护理中心一样，大多数公司会最先对合规数据进行分类并予以保护。 Vontu首先会发现网络文件共享区域的关键数据，然后会跟踪这些数据在端点处的行径并在数据周围执行组策略。另外，夏普医疗中心还利用了另一种产品：Varonis系统公司的Varonis DatAdvantage来管理数据以及审计工作。“ 假设某公司有120名员工，我希望根据部门数据的性质来确定适合访问包含关键数据的文件夹的人员，这意味着必须确定哪些人能够访问文件夹、多久能进行一次访问以及他是否应该有访问特权等问题，”Rivers指出，“ 我们现在面临的挑战就是如何限制访问权，目前我们正在使用Varonis来实现这一目的。”当Vontu确定了包含关键数据的文件夹后，Rivers会将文件列表交给负责管理这些关键数据的管理人员们，然后管理人员们要再次核实这些文件是否包含影响商业运作的信息，从记录、区域、操作人和时间等角度来核实。 Rivers还使

用Varonis和Vontu工具来分析数据保留和其他进程(很难写入单个政策)的监管规则，“我们需要遵守很多法律法规，却没有一条数据保留规则可以让我写一条政策，”Rivers指出，“有些部门根本不需要存储关键数据，而有些部门可能需要将数据保留10年时间。”IT技术组和业务部门的管理人员可以从Vontu和Varonis工具的分析结果中获取很多有效信息，同时可以通过电子邮件对用户进行简单培训，并且当用户违反某些政策Vontu还会弹出警告，这样因员工操作过程中造成的违规率就能够大大降低。Taneja集团的分析师Boles谈到数据保护模式的时候说，很多公司仍然处于对数据分类的阶段，要想进入下一阶段(通过判断数据使用方式和监控站点数据流量来控制数据访问)还需要下功夫。网络和端点 基于网络的DLP设备很符合Bellovin提出的模式，即更近距离地保护数据库安全，数据库应用防火墙也是如此，例如Guardium和Imperva公司的防火墙能够用于数据硬化、发现、分类、监控和审计。“Bellovin有理由担心保护数据库的问题，特别是当考虑数据库与网络服务器关系的时候，”Richard Rees表示，他是国际最大的灾难恢复提供商SunGard Availiability Services公司的安全解决方案主管，“当我们对客户的网络服务器做渗透测试时，我们只是将该服务器作为向数据库返回数据的渠道，而我们却发现其中存在着各种各样需要修复的漏洞，SQL注入攻击、跨网站脚本攻击等。”Bellovin想到一些办法。他提出一种网络SQL语言，在这种被成为“NewSpeak”的语言中，任何动词都不能用于不安全的命令，“没有命令可以指示说，‘给我信用卡号码’，这不是网络服务器能够做的事情，相反，命令应该是这样：‘这是总额，发送此次

交易进行结算’，”Bellovin 解释说，“不应该存在泄漏数据库信息或者读取信用卡号码的动词命令。”通过重写命令，开发者可以将Web应用程序进行硬化。不过，这不仅需要教会开发者使用不会被欺骗的命令语言，而且要让数据库明确理解语言含义，分析家认为这不可能短期内能够实现。Bellovin还建议取消Web服务器的验证功能，并且取消数据库的每个帐户证书。他推荐使用用户级的验证方式，这可能要通过联合身份验证模式来实现，例如TriCipher公司使用的模式，能够为电子商务应用提供网络验证。与此同时，Jericho论坛认为访问权应该根据数据本身的安全属性来决定，这样就可以简便地通过加密来实现访问控制，因为访问权可以临时设置。“我认为验证应该是伴随每一条SQL命令的，即每次用户从web服务器向数据库发出SQL命令时都需要进行验证，”Bellovin解释说，“如果用户提出请求查看某些用户记录，而该请求不包含的时候，数据库服务器将不会作出回复。即使黑客攻击网络服务器也无法登陆帐户，因为他无法找到密码，密码只有用户本人和数据库知道。”Imperva和其他数据库保护产品只要能够将几种保护机制(包括启发式机制、相关联机制以及签名机制等)整合在一起就能支持这样一个体系，同时，还必须利用一种简单的“有效/无效-请求-回复-传输/交换(valid/invalid request-response-transmission/transaction)”系统，能够对传输的每个站点进行检查。“Bellovin所说的是真正意义上的同心层，”SunGard公司的Rees说，“在网络外围不能没有防火墙和入侵监测系统，因为它们确实能够保护网络，虽然它们不一定能保护应用程序。”除了为分类数据监测数据库和网络外，公司还必须防止数据在端点处泄漏出

去。 为此，很多端点保护公司一直在努力试图将DLP系统整合入他们的产品套件中(通常是通过收购来实现)。自赛门铁克公司去年12月完成对 Vontu的收购以来，很多公司也开始收购DLP厂商，包括2007年Trend Micro公司对Provilla的收购以及McAfee最近对Reconnex的收购等。现在这些公司的DLP组合就更加完善了，不仅包括网管监测装置，而且还包括能将数据导入报表控制台的端点代理。 DLP公司还将加密技术添加到产品组合中，加密技术也是新安全模式的另一层必要的数据保护层。例如，Sophos最近收购了一家德国数据安全公司Utimaco，而McAfee去年秋天买下SafeBoot公司，从而使产品组合的数据加密功能更加完善。使用这些工具时，公司就能在端点制定自己的政策，例如“ 当下载数据到USB设备时需要加密 ”。“ 端点最终必须发展成为灵活的、有弹性而强硬的网络外围，或者说是网络的皮肤， ”来自南卡罗莱纳洲的O ’ Berry说，他正在评估McAfee 公司的Reconnix iGuard同时他还部署了McAfee公司的端点DLP代理，并使用Safeboot进行端点加密。“ 端点是犯罪分子首要攻击的地方，他们能够利用端点远程控制电脑，对终端用户实施keylogger和钓鱼攻击，以获取大量资金。 ” Signal Financial Credit Union公司表示他们公司因使用网关和端点DLP产品而阻止了98%的数据泄漏问题，该公司在网络端点处部署了Code Green Networks公司的Content Inspection检测设备来检查输出电子邮件流量并予以保护，以及创建电子票和管理规则和角色等工作。 为增强网络的数据丢失防护能力，该公司还使用了Blue Coat系统公司的ProxySG产品设备来代理其他输出信息流量，包括SSL流量(需要使用可选SSL解密卡进行解密)等，对外数据传输通

常隐藏于常用的SSL协议下。“ DLP设备能够监测所有输出的数据，尤其是对关键信息的监护，包括帐户信息、信用卡号码和其他重要数据类型等， ”Kensington公司的首席技术官Steven Jones表示，他们公司在端点处部署了Code Green 代理来避免通过USB端口和无线网络的数据泄漏。 O ’ Berry认为， 关键数据的泄漏可能发生在输出流或者公司网络的端点处，这意味着我们需要在数据库、端点处、网络和Web中增加额外的保护层。 用Bellovin的话来做结语：“ 我们需要以不同的方式来思考这个问题，因为目前所做的网络外围保护根本不够。我们需要在重要数据周围部署具有更强安全性的数据中心架构，因为网络外围处的安全漏洞是不可避免的。 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com