根据《IT安全法》，生产急救用止痛药的企业可能会成为关键性保护基础框架内的一员

图片来源：©chagpg,©peterschreiber.media - stock.adobe.com

您对网络安全了解吗？

PROCESS-Tip

* 更多信息请登录：pharm.vogel.com.cn
* **反馈编码：201224**

《IT安全法》对药品生产意味着什么？——黑客攻击对于每一家药品生产企业而言都是噩梦般的存在：不仅破坏了企业形象，而且还会对药品供应链的安全造成威胁。因此，有关保护关键性产品的法律法规就要求了药品生产企业在特定条件下需要承担更多的责任和义务。

文 / Anke Geipel-Kern

黑客攻击是制药企业所深恶痛绝的。美国知名制药企业Merck公司在2017年6月就遇到了巨大的药品供应难题——受到了计算机勒索病毒“Not Petya”的攻击，致使生产瘫痪。

勒索软件给这家企业造成的经济损失估值为6.7亿美元，这还不包括给企业形象带来的污点。这家制药巨头受到的巨额损失绝不是孤立的个案，Deloitte公司的一项调查研究指出：制药企业是黑客和恶意软件首选的攻击目标。因此，一般情况下存储在海量数据中的“知识产权”对制药企业来讲有着至关重要的意义。任何窃取了竞争对手药物有效成分的人都是一颗潜在的重磅炸弹，如果他能利用窃取到的知识产权将药品顺利投放到市场，就可以轻松地赚到一大笔钱。专家预估，全球的药品市场规模约为一万亿美元。因此，这里蕴藏着丰厚的收获。

针对物联网的黑客

随着工业4.0时代的到来，IT系统和生产系统更加趋向于自动化和网络化，黑客攻击制药企业的趋势也会延续下去。总部位于Wuppertal-Elberfeld市的拜耳公司的API活性药物成分生产基地IT

本文作者系本刊德文版杂志副主编。

技术领导人 Dirk Spingat 博士表达了自己的看法，“在制药行业领域中，我们看到了两种完全相反的发展趋势。数字化技术要求在各个自动化层次之间有着更大的开放性，一方面使得整个系统更易被入侵，另一方面也提高了 IT 安全保护的要求。”

AV 测试研究所对不同恶意软件发展状况的研究结果也证实了这一点。犯罪分子在很早以前就开始关注物联网，并且在 2018 年第一季度就开发出比以往任何时候都多的、专门攻击网络系统的恶意软件。据 AV 测试研究所的专家介绍，经典病毒“特洛伊木马”的数量正在下降。据悉，AV 测试研究所掌握着全球最大的恶意软件数据库。

在网络安全方面，德国制药业仍然处于相对比较宽松的法律法规框架内运作。但立法机构正在逐步完善相关的法律法规。自 2017 年 6 月开始，德国的《IT 安全法》第二条中新增加了这样一条规定：如果生产厂家进口到德国市场的处方药以及血液和血浆制品的数量超过 465 万件时，则被视为“关键性的基础医药制品”。

主管部门的协调

这一限制性规定是为避免所有德国企业生产的药品不会受到关键性产品保障法规的制约而制定的。即便是联邦政府的联邦信息安全办公室（BSI）前来问询，为保护相关企业的隐私也会拒绝为其提供数据和名称。

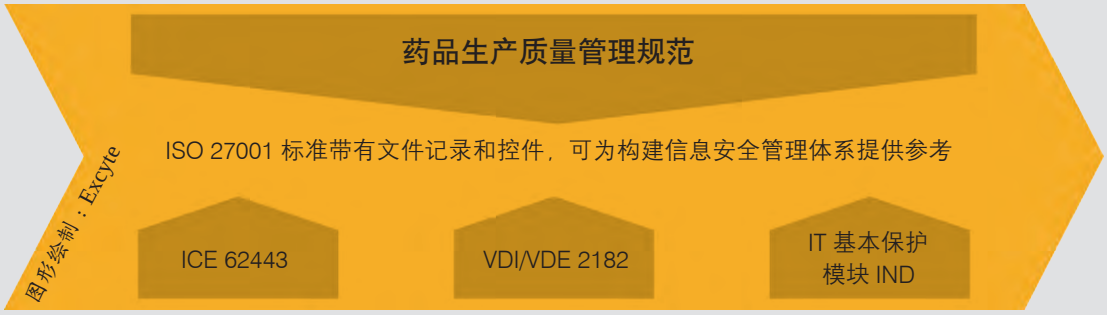
受关键性产品保障法规监管的制药企业应立即开始行动。时间在点点滴滴地流逝：2018 年仅要求相关企业进行自查，确定自己是否属

广告

过程模型

如何避免重复工作

在 2018 年的智能制造工艺流程大会上，Excyte 公司的安全技术专家 Robert Geiger 提出了规划设计和实施信息安全管理系统（ISMS）的过程模型。构建这一模型的出发点是专门针对自动化的生产系统创建一套满足企业自动化生产网络要求的网络安全保护策略。利用这一过程模型可以帮助企业规避遇到的风险，保护自己关键性的工业控制系统（ICS）。在此基础上，企业可以通过查询在制药行业中通常已经使用了一段时间的所有与 IT 系统安全措施、指南、标准操作程序（SOPs）和组织措施等有关的信息和资料，丰富其使用的信息安全保护系统，以满足现代化的、符合法律法规的信息安全管理系统的要求。过程模型满足了生产领域的技术要求和企业组织工作方面的安全保护措施的要求，例如，ISO27001 标准中有关制药企业典型的质量保证要求、法律法规方面电子记录 / 电子签名技术标准 Part 11、计算机系统验证和 ISPE GAMP 5 以及企业组织管理方面 IEC 62443 标准对基础设施进行认证的要求。这一过程模型显示了制药企业药品质量保证体系的协同保障作用，并将自动化的药品生产纳入到了信息安全管理之中，集成了更多的技术标准。



于关键性企业。到 2019 年年中，信息安全系统审核的过渡期就已经结束。从那之后，立法机构对每家企业进行了仔细的审查，并有罚款的趋向，但是罚款的金额不高。

Spingat 博士对 BSI 的工作方式给予了高度赞誉，毕竟这是在处理一个复杂程度很高的技术问题。他说道，“IT 安全是一个非常现实的话题，而且是与法律规定无关的话题。但每一家企业都应在保障自身利益的前提下保护好自己的 IT 资产。如果您对法规的适用尚不明晰，可以前往主管当局以获得支持和建议。”那些本身没有 IT 安全保护部门的中小型企业对主管当局的政策非常认可。Spingat 博士继续说道，“即使您的生产基地不属于关键性保护的类别，但关键性检查的风险分析能够更好地说明其安全可靠性，并不会带来任何损失。”

许多受到关键性保护的企业已经做足了功课，至少在 2018 年 12 月 GAMP 5 良好自动化生产实践指南（第五版）的技术论坛中获得了自己所需的咨询结果——Spingat 博士的专家团队针对关键性保护法规的实施情况进行了专业的讨论。

如这项法规一样，这项工作仅仅是建立起了一个总体框架。BPI、BAH、Vfa 和 Pro Generika 等医药协会与药品批发商协会 Phagro 共同制定了针对医药产品的实施细则，正在等待 BSI 的审批。拜耳公司的专家就是这些细则的制定者之一。

基于风险控制的分析

履行立法者规定的义务似乎并不难：

- 明确一个联络点；
- 报告 IT 安全方面的事故；
- 采用符合当代技术水平的保护措施；
- 每 2 年进行 1 次验证。

借助于药品生产质量管理规范（GMP）、计算机系统验证、ISPE GAMP 5 和电子记录 / 电子签名技术标准 Part 11 等法规，制药行业在风险管理方面更加得心应手了。“但法律法规的制定者在

此基础之上又增加了一点：IT 安全由系统各部分的完整性、可用性和保密性组成。GMP 规范要求进行的风险分析的着眼点是数据的完整性。到目前为止，可用性还一直处于一种‘幕后’的状态。相信在关键性保证规范问世之后，可用性会变得更加重要。”Spingat 博士强调道。

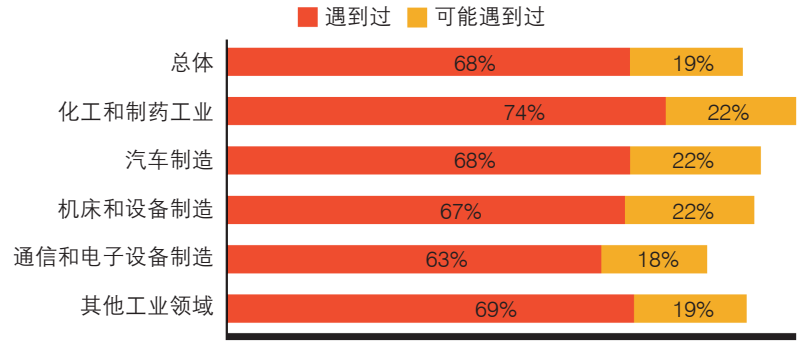
那么，药品生产企业需要做哪些准备呢？专家指出，制药企业需要注重下列两个问题：

- 仅仅按照 GMP 规范落实工作的企业也可以使用这一管理系统来贯彻关键性保护的有关措施，但必须有进一步的扩展（利用其风险管理中的可用性），以满足关键性保护法规的有关要求。
- 已经通过了 ISO 27001 标准认证的企业当然可以继续使用这些认证证书，但要审查所有的认证检查因素是否满足关键性保护法规的要求。

因此，未来将会继续保留风险管理系统。GMP 专家却在担心将来不得不建立多个平行的相邻系统。

黑客关注的制药和化工行业

在过去的两年中，“贵公司的数据是否受到了或可能受到过黑客进攻，以致资料被窃？”“是否遭遇过工业间谍的影响？”等问题的调查问卷报表。



相关信息：2018 年 5 月对职工人数超过 10 人的德国工业企业的调查问卷。(n=503)

资料来源：Bitkom©Statista 2018；图片来源：PROCESS

洁净公用工程系统的理想选择

无论您的生产需要什么：我们都为您提供完美的系统 - 基于膜法或者蒸馏法的制备设备、正确的预处理和配套的储存和分配系统

20多年来BWT一直是纯水/超纯水和现在的冷注射水制备系统的标杆。OSMOTRON PRO - 它预安装在一个不锈钢模块上，采用先进工艺并且在全球几百个药品生产工厂都运行良好，并且让业主的投资极小化。

BWT MULTISTILL蒸馏水机为您提供无与伦比的可靠性、长寿命和稳定性。我们的降膜技术生产出的产品水质远超相关行业标准，如欧洲、美国和中国药典 - 而且性价比极高。

BWT OSMOTRON® PRO

BWT MULTISTILL

bwt-pharma.com

广告