

信息安全

认真对待 智能工厂安全问题

生产线停止运转，某水厂停产数周，高炉突然不再能够正常关闭，其后果是造成数百万美元的损失，这并非科幻，而是事实，而这一切的始作俑者就是计算机蠕虫、病毒和木马。这些数字害虫攻击工业控制系统的风险也随着联网的增加而扩大，IT 专业人士和安全专家因此一致表示，没有安保就没有工业 4.0。

文 | Jürgen Schreier

无论是木马还是其他恶意软件，事实上这样一些数字害虫今天几乎可以在所有的电子设备领域中肆掠横行，IT 专业人士 Nicolas Ehreschwendner 警告说。人们可能不愿相信，诸如硬盘、固态硬盘（SSD）和 USB 记忆棒之类的数据存

储器以及复印机、汽车、电视机和咖啡机都会受到威胁，汉堡 Attingo 数据恢复公司总经理说道。受到黑客攻击的咖啡售货机也许只会提供乏味的液体，这种事情人们或许可以接受，但如果受攻击的是工业控制，情况就完全不一样了。

1/3 的企业出现过重大安全问题

在此背景下，德国 Bitkom 协会（联邦信息技术，电信和新媒体协会）的 ITK（信息与电信协会）分会几天前所做的一份问卷调查结果令人吃惊，在过去两年中，几乎 1/3 的德国企业出现过 IT 方面的安全问题，涉事企业的比例与去年所做的相关调查结果相同。“德国企业已经成为网络犯罪以及外国情报机构关注的目标。”德国 Bitkom 协会会长 Dieter Kempf 教授说道：“确保安全防护措施处于最新状态的同时，定期投资保护自己的 IT 系统越来越重要。”

出现 IT 安全问题的中小企业的数量远远高于大型企业，这一事实特别令人担忧。ITK 协会的最新调查显示，几乎 1/3 的员工人数为 20 ~ 499 人的企业涉及工厂安全问题，而员工人数超过 500 人的企业中则几乎有 1/5 存在此类问题。“尽管大型企业往往是受攻击的目标，但鉴于其人员、财务以及技术方面的资源，他们通常能够更好地抵御攻击。”德国



图 1 趋势科技公司的安防专家 Udo Schneider 说：“新软件层出不穷，随之而来的安全漏洞也越来越多。”

Bitkom 协会会长 Dieter Kempf 谈道，这也唤醒了具有特定技术知识的创新型中小企业抵御黑客和情报犯罪的愿望。如果连咖啡售货机都能被操纵，使其吐出劣质咖啡或压根不吐咖啡，那么要是“数字害虫”进入工业控制系统，进入网络或控制室，并通过 web 攻击机器、设备或整个工厂的话，风险又是多大呢？

工业 4.0 的目标是让尽可能多的信息实现数字化，其结果是，整个企业的系统将实现相互和内外联网，这一过程从机器、传感器和生产设备的现场设备开始，经过 MES 和 ERP 系统，直至市场、销售和采购。价值链沿线的 IT 系统联网也将被大力推动。

据 BSI 估计，到 2020 年，德国在工业 4.0 领域的投资将高达 110 亿欧元左右，从长期来看，如果不希望危及自身竞争力的话，那么就没有一家企业可以置身于数字化和联网这一趋势之外，于是人们只好容忍企业的外部界限日益模糊，这便为那些心怀叵测的人开启了新的攻击区域，此外，IT 系统是可攻击的，远离互联网的所谓“内部系统”根本无法实现。随着互联的深入，IT 安全方面的风险会与日俱增，因此从逻辑上讲，由于生产或经营过程的中断或出错使企业蒙受经济损失的风险也会增加（图 2）。

这些威胁并非假设，而是真实存在的，最近由媒体报道的相关具体事例不胜枚举，在感染了由办公网络带入的所谓 Zotob 病毒（据估计）后，一家美国汽车制造商的 13 条加工生产线停止运转，造成大约 1300 万美元的损失。在一家化工厂，PE-Sality 病毒导致上级监控系统出现 8 个小时的瘫痪。特别重大的一次事件发生在 2014 年，由于下载了 Conficker 蠕虫病毒，导致一个高炉遭受攻击，无法控制关闭，造成大规模设备损坏。根据 VDMA 在 2013 年所做的一项调查，德国 29% 的机器和设备制造商都有过因安全问题导致的生产故障。

工业 4.0 安全

排名前十的威胁



图 2 敌人来自自己的企业：人为错误和破坏是大多数安全事件的原因

出现 STUXNET 后，问题防范意识有了明显改善

“恰恰在几乎所有领域的过程控制系统都不再是闭关自守，而是相互联网的工业 4.0 时代，极其复杂且动态交织的国内和国际网络信息结构需要一个能够抵御内部和外部威胁的不间断防护系统。” Ottobrunn 的网络安全公司 IABG 的 Tom Köhler 说道。一位来自 VDMA 的人士认为，没有数据和知识产权保护的跨企业生产过程对于工业 4.0 来说是无法想象的。

这样的警告完全为人们所接受，因为自从 2010 年遭到 Stuxnet 攻击后，行业的安全意识有了明显提升。2 月 10 日在法兰克福美因河畔举办的深受好评的 VDMA 产业安防资讯日就是一个证明，人们分别从各种技术和法律角度对安全问题进行了探讨，因为像工业 4.0 设备生成的大量数据归谁所有这样的法律问题也需要澄清。

必须实事求是地对待工业 4.0 范畴内的安全问题

不过也没有理由恐慌，这应该是 VDMA 活动所传递的最重要的信息。趋势科技公司的安防专家 Udo Schneider 在其报告中认为，德国工程师可能会做很多事情，但绝不喜欢冒险，从设备安全角度来看这是好事，但从 IT 安防角度出发则是坏事，毕竟一种没有理由的感觉（因为有风险，所以最好不碰它）可能会阻碍人们实事求是地对待工业 4.0 范畴内的安全问题。“人们可以让一个生产过程更加安全，但却无法确保绝对安全。” 安防专家称，因为“新软件层出不穷，随之而来的安全漏洞也越来越多（图 1）。” 追求安全的机器制造商（机器准则）和受过安全训练的“IT Fuzzi”（Schneider）之间的“文化冲突”必须克服。“安全和安防专家必须坐在一起共同寻找解决方案。” 毕竟他们有一个共同点：“他们都熟悉评估和降低风险的过程。” Schneider 表示。如同安全问题一样，安防领域同

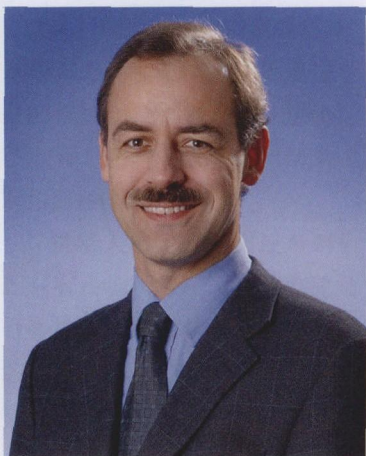


图3 英飞凌科技公司 (Infineon) 的 Detlef Houdeau 博士主张“德国制造”，他表示：“对于国外购买的设备，人们虽然了解其基本功能，但却根本不知道它们还有哪些作用。”

样也有各种框架，其中包括 ISO 27XXX (ISMS 建设 / 运营)、ITIL (信息技术基础设施库) 或 COBIT (测试基础，IT 控制，合规)。

工业安保需要办公室方案和匹配方案的组合

如趋势科技公司的安防专家 Udo Schneider 在 VDMA 安防资讯日上所介绍的那样，当然有一些技术解决方案，通过办公领域的标准 IT 方案、杀毒软件、防火墙以及加密技术，在工业安防方面已经取得了一些成效。然而越接近操作层面，就越需要匹配的解决方案。

英飞凌科技公司 (Infineon) 业务经理 Detlef Houdeau 博士在法兰克福对曾在国内 IT 峰会上介绍过的工业 4.0 设备的安全远程控制进行了一次示范，使用这种安全架构可以避免 5 种不同的威胁：

- 通过加密和带密码的平板电脑提供社交工程 (内部窥探) 方面的保护；
- 通过硬盘加密防止平板电脑中的企业数据丢失；
- 通过使用经过完整性测试的网络组件保护分布式企业网络的完整性；

- 通过加密通信渠道确保端对端通信；
- 通过源代码的加密存储保护知识产权。

该方案由一个使用安全元件的加密狗以及一个使用来自弗劳恩霍夫安全信息研究所 (Fraunhofer-SIT) 的 Raspberry-Pi (树莓派：一款基于 Linux 系统，仅为一张信用卡大小的个人电脑) 和安全元件 (英飞凌科技公司的 TPM 芯片) 的赫斯曼路由器组成。所有“安全锚”均为德国制造，只有这样

才能保证数字主权，Houdeau 表示：“对于国外购买的设备，人们虽然了解其基本功能，但却根本不知道它们还有哪些作用 (图 3)。” 系统在今年应该可以投入使用，作为集成商的德国电信除了接管后面的一体化进程 (基础设施服务、旧设备封装以及企业权限管理) 外，还将负责网络监管，用户是那些没有庞大的 IT 部门、更喜欢使用完整包的中小企业。MM

系统可以如此优雅夺目!



reddot design award
winner 2015

菲尼克斯电气工控机不仅注重提升系统形象，而且从品质上保证！臻选系列 Designline 工控机，整机 IP65 防护等级，圆角设计，支持多点触控，VESA 100 安装方式，无需控制柜，荣获 2015 工业界 iF 设计奖 (iF Design Award)。

优选 2 代 VL2 工控机，窄边框设计，宽屏显示，具有 15.6"、18.5"、21.5" 三种尺寸供选择，支持多点触控，具有不同性能等级 CPU 选择，荣获 2015 红点奖 (Red Dot Award)。

* Red Dot 与 iF 奖是工业界非常著名的设计大奖，是对产品出色、高品质设计的认可。

菲尼克斯电气

Tel: 025-52121888
www.phoenixcontact.com.cn

PHOENIX CONTACT
INSPIRING INNOVATIONS

CIS 02-15.002.L1

© PHOENIX CONTACT 2015

▲ 反馈服务编码 M2143