数据中心的风险与对策

您的服务器固件安全吗？最好确认一下！

Microchip Technology Inc.
数据中心事业部
主管经理
Kyle Gaede

在当今的数字世界中，数据为王。通过应用数据分析来为新产品或服务提供信息，组织可以获得显著的竞争优势。此外，在 5G 和物联网等技术的加持下，设备可以比以往更轻松地连接到互联网来共享数据。这引发了新数据的爆发狂潮；研究分析公司 Statista 预计，到 2025 年，全球创造的数据将达到 180 ZB（泽字节）。这些数据中捕获到的丰富信息（信用卡号、社保号、专有 IP）使其成为对黑客有吸引力的目标，随着数据中心收集和存储的数据量的增长，针对它们的网络攻击的创新性和复杂性也日益提高。

中央处理单元（CPU）、图形处理单元（GPU）存储设备和网络卡中的固件是特别诱人的目标，因为作为电子系统的基本元素，如果它们遭到破坏，会更加难以检测。长期以来，保护这些设备中的数据免遭窃取至关重要。事实上，在最大的数据中心，这些设备现在往往会受到良好的保护。

为了寻找其他潜在的漏洞，恶意黑客在试图攻击数据中心时，越来越多地以服务器组件为目标。对于服务器中的许多常见半导体组件（例如，控制引导顺序、风扇控制和电池管理的嵌入式控制器），其固件可能会遭到破坏或被虚假固件替换，从而导致黑客可以未经授权地访问服务器上的数据或干扰正常的服务器操作。

固件攻击的隐匿性非常强，因为服务器组件固件在服务器的操作系统运行和任何反恶意软件功能生效*之前*加载。这也会使固件攻击难以被发现，即使被发现，也很难消除。

然而，许多公司对于固件安全的重视并不够。在由 Microsoft 委托对 IT 和安全决策者进行的一项调查中，受访者认为固件漏洞几乎与软件或硬件漏洞一样具有破坏性，但用于保护固件的安全预算不到三分之一。

	漏洞具有破坏性	安全预算百分比	最容易受到网络威胁
软件	78%	39%	63%
硬件	75%	32%	20%
固件	73%	29%	17%

图表来源：Microsoft Security Signals，2021 年 3 月

企业必须认真对待数据中心的固件安全，否则会自食其果。为此，在考虑固件安全时，IT 和安全团队应关注三个因素。

建立设备真实性

服务器的主板、工作负载加速器和购买后安装的附加板是由不同的供应商设计并在全球范围内制造的。这些设备的供应链容易受攻击，非法固件或硬件可以在生产和测试的各个阶段安装到电路板上，等待毫无戒心的客户在服务器中安装已遭到破坏的设备。IT 团队必须确保其添加到服务器的任何硬件都可以验证新硬件是否按规范运行。

建立代码真实性

数据盗窃并非遭到破坏的固件造成的惟一问题；IP 盗窃也可能影响组件制造商的盈利能力和声誉。如前文所述，半导体通常在一个国家/地区制造，在另一个国家/地区封装，最后在第三个国家/地区集成到系统中。

由于供应链中的接触点如此之多，缺乏道德的承包商可以轻松复制供应商的固件，将其安装在未经授权的芯片上，然后在灰色市场上销售假冒的部件。这不仅会影响原始供应商的利润，如果假冒设备的性能低下，还可能损害他们的声誉。

保护数据安全

加密是一种防止未经授权访问数据的成熟方法，但新的加密威胁正在引起网络安全领域的关注。如果应用得当，量子计算甚至可以破解最复杂的加密技术。

如今，大多数企业都在使用 128 位和 256 位加密；对于使用传统计算技术的最坚定攻击者而言，这样的措施已足以保护数据。但是，量子计算能够以呈指数级增长的速度处理数据，对于使用传统计算方法可能需要数十年才能破解的加密算法，量子计算可能只需要几天就能破解。

利用 HRoT 和稳健的加密技术保护您的固件

值得庆幸的是，2018 年，美国国家标准及技术研究所（NIST）发布了平台固件弹性的 SP 800-193 指南。据 NIST 称，这些指南提供了“保护平台免受未经授权（固件）更改、检测发生的未经授权更改，并快速安全地从攻击中恢复的安全机制。包括原始设备制造商（OEM）和组件/设备供应商在内的实施者可以使用这些指南在平台内构建更强大的安全机制。系统管理员、安全专业人员和用户可以使用这份文档来指导未来系统的采购策略和优先事项。”

NIST SP 800-193 标准推广使用“硬件信任根”或 HRoT，以确保在启动过程中，加载到服务器组件中的固件在激活之前验证为合法。当服务器启动时，HRoT 组件是第一个上电的组件，它包含了验证其自身固件和在 HRoT 激活后上电的任何组件的固件所需的加密元件。通过在服务器的嵌入式控制器中添加 HRoT 功能，企业不但可以在整个启动过程中保护服务器，甚至还可以在操作系统和反恶意软件加载并运行之前保护服务器。

NIST 也在鼓励企业采用更先进的加密算法。2016 年，NIST 在最优秀的密码学家之间举办了一场比赛，以开发能够抵御基于量子计算的攻击的算法。比赛于去年结束，NIST 宣布了四种将包含在其即将推出的后量子加密标准化项目中的新加密算法。

网络安全就像是一场军备竞赛，一方是致力于保护计算机系统的守护者，另一方是打算破坏这些系统的攻击者（包括犯罪分子和国家支持的黑客）。双方都在不停地抵抗对方的进攻。固件

已经成为这场持久斗争的最新战场，那些忽视在威胁评估和安全计划中包含固件的企业将自担风险。