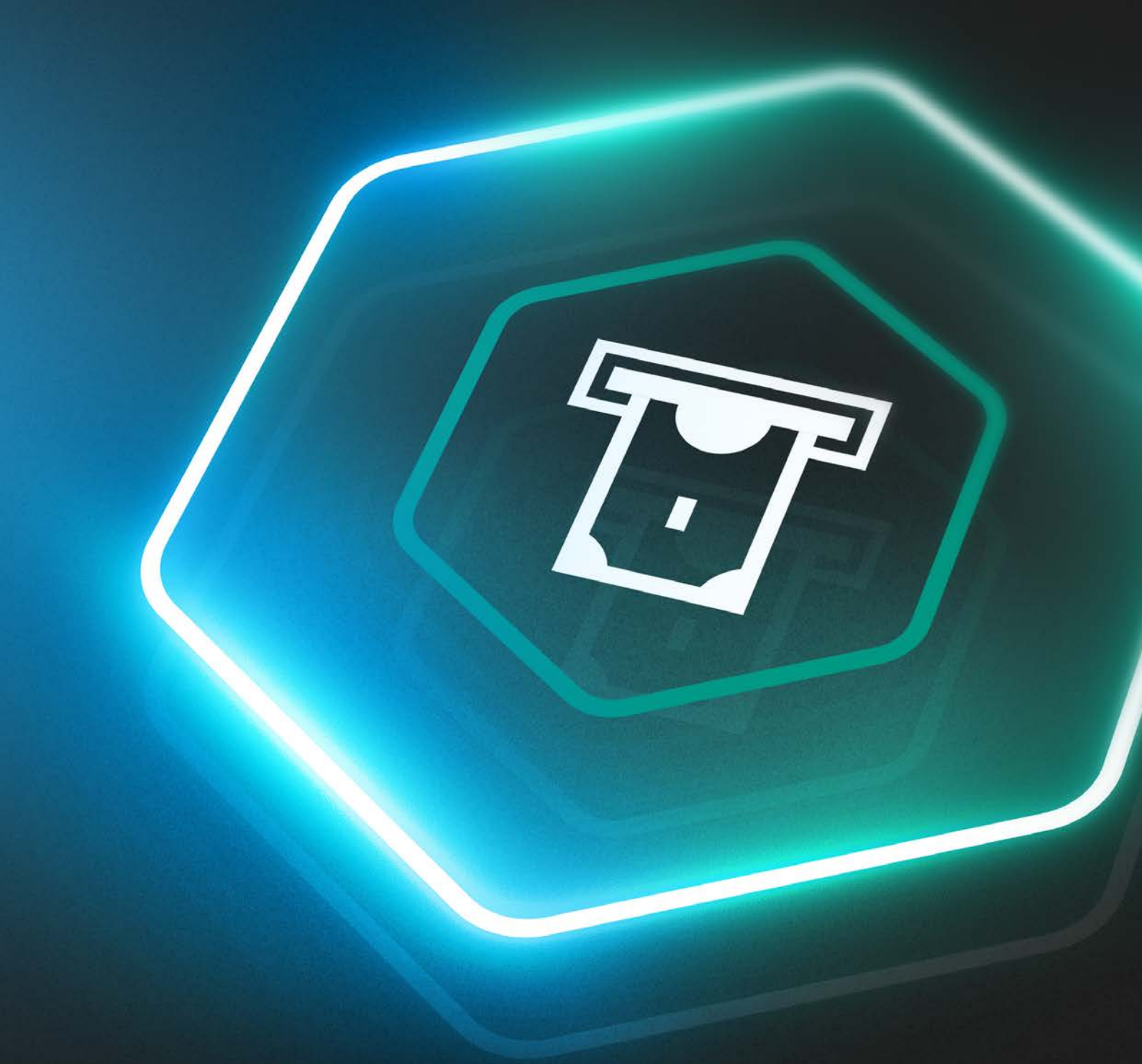

什么是嵌入式系统，
他们需要什么样的网络安全？

嵌入式系统

kaspersky 引领未来

嵌入式系统无处不在

诱人的目标

嵌入式系统处理关键的数据（财务数据、个人数据等），因此对网络犯罪分子来说是非常有吸引力的目标。

我们每天都在使用嵌入式系统。自动取款机，店内 POS 系统，自动售货机，售票亭，医疗 CT 扫描仪，甚至自动加油站，这些都是在嵌入式 Windows 或 Linux 系统上运行的专用设备。

这些设备处理关键的数据（财务数据、个人数据等），因此对网络犯罪分子来说是非常有吸引力的目标。这就是为什么对这些设备进行可靠保护对于任何使用它们的公司都至关重要。

然而，企业并不总是像对待标准办公系统那样考虑嵌入式系统的安全性，他们的安全性常常被搁置一旁。但保护它们非常重要，这些系统的独特细节不能被忽视。

嵌入式系统：行业和设备类型

行业

- 金融服务
- 交通和旅游（票务）
- 零售
- 餐厅和酒店
- 医疗
- 政府和非商业
- 娱乐业

设备

- 自动取款机
- 售票机
- 加油机
- 结帐
- 销售点
- 医疗设备
- 传统端点
- 投币式自动售货机和游戏机

嵌入式系统的特点

虽然嵌入式系统可能看起来与传统工作站没有什么不同，但事实并非如此。
它们有几个显著差异，在制定保护战略时必须得到考虑。

使用模型

典型的嵌入式系统从根本上不同于普通台式计算机，后者被单个用户用于各种任务。另一方面，嵌入式系统通常被几乎无限数量的用户使用，并且执行的任务范围很窄。

还有其他一些差异。例如，与嵌入式系统的交互经常使用特定的输入设备（具有高度专业化用户界面的数字小键盘和/或触摸屏）进行，使得不可能输入任意的数据和命令。

允许外部外围设备连接的交换端口通常只供技术专业人员使用。与"外部世界"的通信通过互联网、本地网络或使用功能有限的信息存储设备（如银行卡）进行。

自动取款机显然不用于读取电子邮件或访问网站，因此这些渠道不能被用作攻击向量。与此同时，网络连接变得越来越重要。这是用于攻击嵌入式系统的主要渠道之一，因为几乎所有类型的嵌入式系统都连接到公司的本地网络。这意味着，在破解它之后，攻击者可以尝试通过网络危害这些专门设备。至于端口，恶意行为者甚至可能从嵌入式系统的特定物理位置中获利。

物理位置

根据使用模式，大多数基于嵌入式系统的计算机设备位于公共空间。一个耐用的钢铁外壳和与设备进行交互的手段有限，这样设计是为了防止意外访问系统的硬件和软件元素。但是，由于没有任何设备可以完全免维护，因此即使是最耐用的外壳也可以用钥匙打开，这意味着入侵者也可以打开它。获得对计算机设备硬件的访问权限后，他们然后可以附加标准鼠标和键盘，插入带有恶意软件的笔式驱动器或者甚至是可外部启动的操作系统，这些将允许他们绕过计算机设备自己的操作系统打开计算机设备。

在某些情况下，这甚至可以是单板计算机，其可用于侵入系统或（例如）分析使取款机向用户发出钞票的命令。从那时起就轻而易举了，攻击者所要做的就是将选择的工具嵌入到系统中，用它们使内置计算机做任何他们想做的事情，从转移资金或执行影子交易到窃取用户数据。除非嵌入式系统得到适当保护……

安全挑战：

直接篡改内建软件（包括操作系统、专用软件和安全解决方案本身）的高风险。

使用寿命长和有限的系统资源

嵌入式系统在构建时考虑到特定任务，通常只有"必要和足够"级别的的处理器性能。而且由于使用嵌入式计算机系统的计算机设备往往具有较长的使用寿命，因此遇到（例如）硬件薄弱且过时的自动取款机并不寻常。

安全挑战：

过时和薄弱的硬件构成了重大问题，不足以满足许多现代安全解决方案。

过时和易受攻击的软件

基于嵌入式系统的昂贵计算机设备使用久后的另一个缺点是软件过时。他们简朴的系统配置通常不允许使用较新的操作系统，较新版本的专用应用程序软件通常不能与旧操作系统一起使用（或者相反，可能没有较新版本的中间件可用，而较旧的版本不能与新操作系统一起使用）。结果，有些系统正在积极使用中却不再有安全更新为其发布，这意味着任何漏洞都可以在缺乏特殊保护的情况下被恶意行为者利用。

安全挑战：

由于软件漏洞而增加的攻击风险和极其有限的安全解决方案选择结合；很难找到与 Windows XP 等旧操作系统兼容的现代安全产品。绝大多数制造商不再支持它们。

弱互联网连接

一些设备，如自动取款机、票务终端和自动加油站，位于没有有线互联网或无线互联网缓慢或不可靠的偏远位置。应用程序软件可以考虑此类情况，例如，交易可以异步处理，"当连接允许时"。另一方面，许多现代的安全解决方案更依赖于良好的互联网连接。为了减少安装时间和安装软件的大小，他们的开发人员减少了本地组件的体积，转而严重依赖云基础设施。

安全挑战：

缺乏稳定，可靠、高速的互联网连接为犯罪分子提供了更多破坏交易的机会。与此同时，许多现代解决方案过度依赖与供应商云基础设施的通信，其有效性可能会显著降低。

监管要求

大多数嵌入式系统处理关键的财务和个人数据，因此与它们的任何工作都受法律监管。监管机构需要可靠的保护，以最大限度地降低事故风险，并确保在事故发生时有详细的数据供调查之用。某些特定技术可包括在推荐列表中，例如系统完整性监控。

安全挑战：

越来越多的数据保护要求采取高效的对策，与此同时，建议采用不是作为标准 EPP 级解决方案的一部分现成可用（或仅作为专用服务器保护的一部分提供）的技术。

寻求妥协

总之，我们可以得出结论，多用户、单任务、低功耗嵌入式系统具有特定的攻击向量（网络，直接访问设备）。同时，它们使用极其关键的数据（除了财务数据之外，这可能是敏感的个人数据，例如医疗设备），对此不仅保密性而且不变性同样重要。为此类系统实施通用保护解决方案可能会导致许多问题，因为典型的 EPP 级解决方案在弱的硬件上无法很好地工作，并且无法与过时的操作系统兼容。即使它能启动且看起来不错，仍然可能存在性能和兼容性问题。

许多安全解决方案制造商选择完全禁止非主要任务所需的所有事情

一般来说，较弱的系统为黑客提供的机会较少，但使用嵌入式系统的企业（如银行或零售商）不太可能只使用一代技术。

默认拒绝模式下的应用程序控制技术会阻止所有最初未在所谓的"允许列表"中列出的程序。

从理论上讲，这消除了对威胁检测机制的需求，因为恶意软件根本不会启动，并且这种做法只需要很少的资源。

但是，这种策略可能不适用于某些攻击，例如能够将恶意代码注入已在内存中运行的合法进程的"无文件"、"仅内存"类型（过时软件中的漏洞可以提供方法这样做）。

那么，如何保护此类敏感资产呢？

使用不同解决方案？

对于弱系统，使用默认拒绝解决方案；对于更强大的系统，尝试实施常规的 EPP 应用，希望不会出现兼容性问题？

或者找一个真正通用的解决方案？

给特殊设备特殊保护

如果我们看看目前市场上可用的嵌入式系统的保护选项，大多数供应商提供两种选择：

选项 1。"经济"、资源高效的解决方案

这与过时的系统兼容，但提供的是基于应用程序控制技术和默认拒绝模式的最简单的单层保护。除了缺乏应对众多针对嵌入式系统的典型攻击的工具之外，这种类型的专业解决方案通常是独立的，与供应商生态系统中的其他产品分开管理。

选项 2。传统端点安全

对于嵌入式系统，大多数制造商建议使用保护传统工作站的相同解决方案。虽然这样的解决方案无疑具有现代安全技术堆栈，可以被集成到供应商的生态系统中，但它通常没有考虑到上面提到的嵌入式系统的具体细节。此外，这些解决方案只能在最现代、最强大的计算机设备上有效工作，而将仍在运行但过时的设备抛在后面。

即使同时使用这两个选项，问题也没有解决。此外，混合管理方法（特别是涉及不同制造商）会使 IT 和网络安全团队的工作大大复杂化。

理想的安全解决方案

那么，适用于各种嵌入式系统和场景的理想安全解决方案是什么样的呢？

该解决方案必须提供可能的最高保护级别

在当代条件下，这意味着采用各种不同技术抵御使用的相关（即典型的所有类型的嵌入式系统）范围内的攻击向量和技术。

解决方案必须在每个级别的系统上提供足够的保护

旧系统、低功耗系统和最新系统，具有足够的性能和系统资源。

然而，由于几乎不可能同时在弱的硬件之上运行技术堆栈中的所有可用内容，因此可扩展性至关重要。

换句话说，解决方案必须允许对保护层进行单独管理，为给定的一组硬件和系统使用场景打开或关闭提供最大保护的集合。

解决方案必须支持最常见的操作系统

用于创建嵌入式系统的最常见操作系统。至少包含 Windows 和 Linux。

解决方案必须支持老操作系统版本

仍在运行的嵌入式系统中使用的老操作系统版本。

解决方案必须满足法规要求

解决方案必须具有他们在其安全堆栈中推荐的技术，并且能够在集中式安全事件监控系统 (SIEM) 中记录事件详情。

解决方案必须彻底经过兼容性测试

至少具有不同类型的嵌入式系统的典型配置。理想情况下，它必须作为计算机设备的一部分提供，所有组件都经过计算机设备制造商（或装配商）的测试，以确保无故障运行。

解决方案必须有集中管理

理想地与供应商生态系统中的其他产品集成，以创建一个统一的安全系统，通过单个控制台提供对所有级别的公司 IT 基础架构进行监控和保护。

卡巴斯基
嵌入系统安全

卡巴斯基嵌入系统安全解决方案

根据我们以前使用卡巴斯基网络安全解决方案产品线的应用程序来保护嵌入式系统的经验，我们意识到，使用专业解决方案保护嵌入式系统的独特细节必不可少。

这就是我们开发 **卡巴斯基嵌入式系统安全** 的原因，它如今支持 Windows 和 Linux。

解决方案提供：

非常罕见的组合

突显在多层技术堆栈市场上，适用于不同平台，采用选择加入的方法启用保护层

非常简朴的

系统要求

支持过时的操作系统版本

直到 Windows XP SP2

它也属于多功能

卡巴斯基安全生态系统

可以和其他卡巴斯基安全产品一样

从同一管理控制台进行管理

嵌入式系统保护成为公司整体安全战略的一个组成部分

并无缝集成到现有的信息安全流程中。

要进一步了解产品的主要优点和功能，请访问产品网页。

了解更多

技术规格可以在支持网站上介绍 Windows 产品应用程序的部分中找到

了解更多

技术规格可以在支持网站上介绍 Linux 产品应用程序的部分中找到

了解更多

卡巴斯基
嵌入系统安全

了解更多

www.kaspersky.com.cn

#卡巴斯基
#引领未来