What are embedded systems, and what kind of cybersecurity do they need?

Embedded systems

kaspersky bring on the future

Tempting targets

Embedded systems handle valuable data – financial, personal, etc. – and therefore represent a very attractive target for cybercriminals.

Embedded systems are all around us

We use embedded systems every day. ATMs, in-store POS systems, vending machines, ticket kiosks, medical CT scanners, and even automatic gas stations — these are all specialized devices operating on embedded Windows or Linux systems.

These devices handle valuable data – financial, personal, etc. – and therefore represent a very attractive target for cybercriminals. That is why reliable protection of these devices is vital for any company that uses them.

However, businesses don't always think about the security of embedded systems as they do about standard office systems, and their security is often put on the back burner. But protecting them is very important, and the unique specifics of these systems can't just be ignored.

Embedded systems: industries and types of devices

Industries

- Financial Services
- Transportation & Tourism (Ticketing)
- Retail
- Restaurants & Hospitality
- Healthcare
- Government & Non-commercial
- Entertainment

Devices

- ATMs
- Ticketing machines
- Fuel dispensers
- Checkouts
- Point-of-Sale
- Medical equipment
- Legacy endpoints
- Slot & arcade machines

Features of Embedded Systems

Although embedded systems may seem little different from conventional workstations, this is not the case. They have several significant differences that must be taken into account when developing a protection strategy.

Usage model

A typical embedded system is fundamentally different from a regular desktop computer, which is used by a single user for a wide range of tasks. Embedded systems, on the other hand, are typically used by an almost unlimited number of users, and perform a very narrow range of tasks.

There are also other differences. For example, interaction with embedded systems is often carried out using specific input devices (a numeric keypad and/or a touch screen with a highly specialized user interface), making it impossible to enter arbitrary data and commands.

Exchange ports that allow external peripheral devices to be connected are usually only available to technical specialists. Communication with 'the outside world' takes place via the internet, via a local network, or using information storage devices with limited functionality, such as bank cards.

An ATM is obviously not used to read e-mail or visit websites, so these channels can't be used as attack vectors. At the same time, network connection becomes increasingly important. This is one of the main channels used for attacks on embedded systems because almost all types of embedded systems are connected to the company's local network. This means that after penetrating it, an attacker can try to compromise these specialized devices via the network. As for ports, malicious actors may even benefit from the particular physical location of an embedded system.

Physical location

Most computer appliances based on embedded systems are located in public spaces, in accordance with the usage model. A durable steel case and limited means for interaction with the device are designed to protect against unplanned access to the system's hardware and software elements. However, since no device can be created completely maintenance-free, even the most durable case can be opened with a key — which means that an intruder can also open it. Having gained access to the computer appliance hardware, they can then attach a standard mouse and keyboard, plug in a pen drive with malware or even an externally bootable operating system that will allow them to turn the computer appliance on, bypassing its own OS.

In some cases, it may even be a single-board computer, which can be used to hack into the system or, for example, to analyze commands that make the dispenser issue banknotes to the user. It's plain sailing from then on, all the attacker has to do is embed their tools of choice into the system and use them to make the built-in computer do whatever they want—from issuing money or performing shadow transactions to stealing user data. Unless the embedded system is properly secured...

Security challenges:

The high risk of direct tampering with onboard software, including the OS, specialized software, and the security solution itself.

Long service life and limited system resources

Being built with a specific task in mind, embedded systems often have no more than a "necessary and sufficient" level of processor performance. And since computer appliances that use embedded computer systems tend to have a long service life, it's not unusual to come across, for example, an operating ATM with weak and outdated hardware.

Security challenges:

Outdated and weak hardware pose a significant problem, and are insufficient for many modern security solutions.

Outdated and vulnerable software

Another side effect of the long life of expensive computer appliances based on embedded systems is outdated software. Their modest system configuration often doesn't allow for using a newer operating system, and newer versions of specialized application software often don't work with an old OS (or, conversely, there may not be a newer version of the middleware available, while an older version won't work with a new OS). As a consequence, there are systems in active use for which security updates are no longer being released, meaning that any vulnerability can be exploited by a malicious actor in the absence of special protection.

Security challenges:

The increased risk of an attack due to software vulnerabilities combined with an extremely limited choice of security solutions; it is very difficult to find a modern security product that is compatible with an old OS such as Windows XP. The vast majority of manufacturers no longer support them.

A weak internet connection

Some devices, such as ATMs, ticket terminals, and automatic fuel filling stations, are situated in remote locations with no wired internet, or slow or unreliable wireless internet. The application software can account for such scenarios — for example, transactions can be handled asynchronously, "when the connection allows". Many modern security solutions, on the other hand, are much more dependent on a good internet connection. To reduce installation time and the size of installed software, their developers reduce the volume of local components and, instead, rely heavily on cloud infrastructure.

Security challenges:

The lack of a stable, reliable, high-speed internet connection gives criminals additional opportunities for compromising transactions. At the same time, the effectiveness of many modern solutions that are overly dependent on communication with the vendor's cloud infrastructure can be significantly reduced.

Regulatory requirements

Most embedded systems handle valuable financial and personal data, and therefore any work with them is regulated by law. Regulatory authorities require reliable protection in order to minimize the risk of incidents and ensure that detailed data is available for investigation if an incident does occur. Certain specific technologies may be included in the recommended list, such as system integrity monitoring.

Security challenges:

Increased data protection requirements demand highly efficient countermeasures while, at the same time, recommend technologies that are not readily available as part of standard EPP-class solutions (or are only provided as part of specialized server protection).

In search of a compromise

In summary, we can conclude that multi-user, single-task, low-power embedded systems have specific attack vectors (network, direct access to the device). At the same time, they operate with extremely valuable data (in addition to financial data, this may be sensitive personal data, as, for example, in the case of medical equipment), for which not only confidentiality but also immutability is important. Implementing generic protection solutions for such systems may cause a number of issues, because a typical EPP-class solution won't work well on weak hardware, and will not be compatible with outdated operating systems. Even if it starts and seems fine, there are still likely to be performance and compatibility issues.

Many manufacturers of security solutions have opted to completely prohibit everything that is not required to perform the primary task of the device

The application control technology in Default Deny mode blocks outright any programs that are not initially listed in the so-called "allowlist".

In theory, this eliminates the need for threat detection mechanisms because the malware simply won't start and the approach requires very few resources.

However, this strategy may not work against some attacks, such as “file-less”, “memory-only” types capable of injecting malicious code into a legitimate process that is already running in the memory (vulnerabilities in outdated software can provide a way to do this).

In general, a weaker system offers fewer opportunities to hackers, but a business using embedded systems, such as a bank or retailer, is unlikely to use only one generation of technology.

So, how do you protect such sensitive assets?

Use different solutions?

For weak systems, use a Default Deny solution, and for more powerful ones, try to implement a regular EPP app, hoping that no compatibility issues arise?

Or find a truly universal solution?

Special protection for special devices

If we look at the protection options for embedded systems currently available on the market, most vendors offer two options:

Option 1. An "economical", resource-efficient solution

That is compatible with outdated systems but which offers the simplest, single-layer protection based on application control technology and Default Deny mode. In addition to the lack of tools to counter a number of attacks typical for embedded systems, this type of specialized solution is most often stand-alone and managed separately from other products in the vendor's ecosystem.

Option 2. Traditional endpoint security

For embedded systems, most manufacturers suggest using the same solution that protects conventional workstations. Although such a solution undoubtedly has a modern stack of security technologies and can be integrated into the vendor's ecosystem, it typically does not take into account the specifics of embedded systems mentioned above. In addition, such solutions only work effectively on the most modern and powerful computer appliances, leaving the still functioning but outdated devices behind.

Even using both options at the same time, the problem isn't solved. In addition, a mixed management approach (especially involving different manufacturers) can significantly complicate the work of IT and cybersecurity teams.

The ideal security solution

So, what does the ideal security solution that is suitable for a wide range of embedded systems and scenarios look like?

The solution must provide the highest level of protection possible

In contemporary conditions, this means a stack of different technologies to protect against the relevant (that is, typical for embedded systems of all types) range of attack vectors and techniques used.

The solution must provide the maximum possible protection on systems of every level

Old, low power, and the latest ones, with sufficient performance and system resources.

However, as it is virtually impossible to run everything available within the technology stack on top of weak hardware at the same time, scalability is essential.

In other words, the solution must allow for separate management of layers of protection, turning the set that gives maximum protection on or off for a given set of hardware and a system usage scenario.

The solution must support the most common operating systems

The most common operating systems used to create embedded systems. At a minimum, this means Windows and Linux.

The solution must support legacy OS versions

Legacy OS versions used in embedded systems that are still running.

The solution must meet regulatory requirements

The solution must have the technologies they recommend in its security stack, and be able to log event details in a centralized security event monitoring system (SIEM).

The solution must be thoroughly tested for compatibility

At least with typical configurations of embedded systems of different types. Ideally, it must be supplied as part of a computer appliance, all components having been tested by the manufacturer (or assembler) of this computer appliance, to ensure trouble-free operation.

The solution must have centralized management

Ideally integrated with other products in the vendor's ecosystem, to create a unified security system that provides monitoring and protection of all levels of the company's IT infrastructure through a single console.

Kaspersky Embedded System Security

Kaspersky Embedded Systems Security

Based on our experience of previously using applications from the Kaspersky Security for Business product line to protect embedded systems, we realized that a specialized solution to protect the unique specifics of embedded systems was essential.

This is why we developed **Kaspersky Embedded Systems Security**, which today supports Windows and Linux.

The solution offers:

An exceptionally rare combination

on the market of a multi-layer technology stack for different platforms featuring an opt-in approach to enable the protective layers

Very modest

system requirements

Support for outdated OS versions

down to Windows XP SP2

It is also part of the multifunctional

Kaspersky security ecosystem

Can be managed from the same management console

as other Kaspersky security products

Protection of embedded systems becomes an integral part of the company's overall security strategy

and is seamlessly integrated into existing information security processes.

To learn more about the product's key benefits and features, visit the product web page.

Learn more

Technical specifications can be found on the support site in the sections covering product applications for Windows

Learn more

Technical specifications can be found on the support site in the sections covering product applications for Linux.

Learn more

Kaspersky Embedded System Security

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture