Sorting out cybersecurity for modern warehouse logistics

05 March 2024

In a world where cyber-attacks are international news, cybersecurity has become a top priority for the logistics and e-commerce industry for protecting operations and brand reputation. However, the operational technology (OT) that controls modern logistics operations has created more potential security vulnerabilities than ever before. In response, experts such as Prime Vision are providing businesses with a holistic, but also agnostic, continuous approach to cybersecurity that safeguards software and hardware.

Fleur Baars, Business Development & Sales Director and Julian Gonzalez Verbeek, Director of Technology at Prime Vision, a global leader in computer vision integration and robotics for logistics and e-commerce, explore cybersecurity in logistics, potential threats and how to be prepared.

The zero-trust environment

In the past, networks were not necessary for sorting centres as there was no exchange of information from outside. Eventually, as they were introduced, firewalls were able to create trusted, closed environments. For a time, this was fine for protecting data, as warehouse and sorting operations were still not communicating with the outside world. However, all this has changed.

The facets of a modern logistics chain have opened sorting centres to the outside world. Track and trace, as well as communications with customers and suppliers, embody this shift. This interconnectivity comes at a price though – OT is now much

harder to secure as there are so many points of entry for malware. A zero trust environment where everything must be protected and authenticated is prevalent.

The risks of malware for an organisation are enormous. A successful cyber-attack can disable key equipment, halt operations, steal data and cause nationwide delivery interruptions – all resulting in almost incalculable financial and reputational losses. For example, in January 2023, the UK's Royal Mail was hit by a ransomware attack which prevented it from posting letters and parcels overseas for almost six weeks.[1] Effective preparation for this scenario is difficult, as it's hard to know what kind of threat will be faced. Therefore, taking an integrated approach is best.

Being prepared and responding effectively

A good start is to evaluate the total enterprise design and continuously scan and monitor the complete environment to detect any possible threats. Following that, segmentation is important. By building a 'security perimeter' around systems, malware can be quarantined in the event of infection to protect other parts of the operation, including physical equipment. Thanks to the zero trust architecture and centrally managed software and hardware environments of modern warehouses and sorting centres, continuous proactive monitoring is also possible, with observability platforms ready to alert the security team to any issues.

Using hardware that features endpoint protection helps prevent against threats introduced into the system via USB and other methods. Strict security protocols for personnel, whether restricting access to server rooms or introducing two factor authentication, help reduce human errors. Key information regarding processes and actions, including historic access and activity reports, can be stored for full traceability, all available to authorised people at any time.

[1] Royal Mail resumes overseas deliveries via post offices after cyber-attack – The Guardian

Beyond prevention, in a worst-case scenario, it is critical to have a robust contingency plan in place with the security team, partners and suppliers. Identifying the threat and what it does is crucial before deciding to close systems down.

It is essential to decipher what malware wants - whether that is to encrypt or steal information, shutdown or disrupt operations mostly resulting in a financial request. Its removal is then conducted on a case-by-case basis. For particularly aggressive threats, a complete wipe or even replacing untrusted hardware may be needed.

Working with non zero trust solutions

However, logistics operations are not uniform, which presents additional cybersecurity challenges.

Take legacy equipment for example. Sorting machines can cost tens of millions of dollars and are expected to work for decades. Anything can be replaced, but large costs and potential downtime are often prohibitive. This means that cybersecurity experts are required to work with dated infrastructure, programming languages and equipment from a plethora of vendors.

To understand legacy systems and develop secure solutions for them requires decades of experience and experts understanding all languages and systems. A cyber security expert must create interface layers that can communicate with older systems, while passing information to newer, more secure systems. This is something that Prime Vision specialises in.

However, the optimal approach is security-by-design, which is only possible when cybersecurity is engrained early on in a project.

Security-by-design for zero downtime

When a leading e-commerce business in central Europe required cybersecurity for its new warehouse sorting operations, it approached Prime Vision. The business

processes millions of parcels a day, with customers expecting same or next day delivery - so no downtime could be tolerated.

Security-by-design allows cybersecurity to be built into the foundations of a warehouse or sorting operation. Rules regarding software, hardware, protocols and personnel can be established early, allowing partners, vendors and suppliers to easily understand and adopt the measures. Prime vision applied this methodology with the e-commerce business.

Segmentation also meant that Prime Vision could change the usual customer policy of installing a large update every quarter. Instead, continuous upgrades and patches could be rolled out “on the fly” without any downtime. Secure encryption, automation of updates and regular market monitoring for the latest global malware threats allowed cybersecurity to stay up-to-date seamlessly.

By taking a security-by-design approach, Prime Vision delivers continuous cybersecurity with zero downtime, ensuring 24/7 sorting is uninterrupted by the installation of new updates and infrastructure.

Staying secure

As well as its expertise providing cybersecurity for legacy equipment or new projects – Prime Vision holds itself to high security standards and continually innovates to keep pace with the latest threats.

The business is ISO 27001 certified and is accredited to ISAE 3402 Type II. To maintain these industry standards, all procedures and controls are regularly checked by multiple persons, both in internal and external certified audits. The high internal security level is evidenced by the fact that Prime Vision manages customer server spaces, ensuring highly restricted access.

Additionally, Prime Vision experts continuously scan the market for new cybersecurity technologies and assess ways in which to improve them.

Experimentation and testing allow the company to build comprehensive contingency plans, which can be passed on to customers.

An integral approach for any logistics operation

As a world-leading supplier of software and hardware solutions for logistics, e-commerce and postal operations, Prime Vision has exceptional experience securing OT infrastructure in legacy and new-build projects. Furthermore, it will work tirelessly with customers to advise the chief information officer (CIO), chief information security officer (CISO) and other relevant personnel, providing expert technical guidance where necessary.

Lessons learned are applied to its hardware and software development, so customers benefit from secure products backed by knowledgeable support. More than that, its holistic approach aims to make cybersecurity part of company culture, combining people, technology and regulation together to provide a robust, integrated response to potential threats.

More from Prime Vision - https://primevision.com/sorting-out-cybersecurity-for-modern-warehouse-logistics/

Image captions:

Image 1: Cybersecurity has become a top priority for the logistics and e-commerce industry for protecting operations and brand reputation.

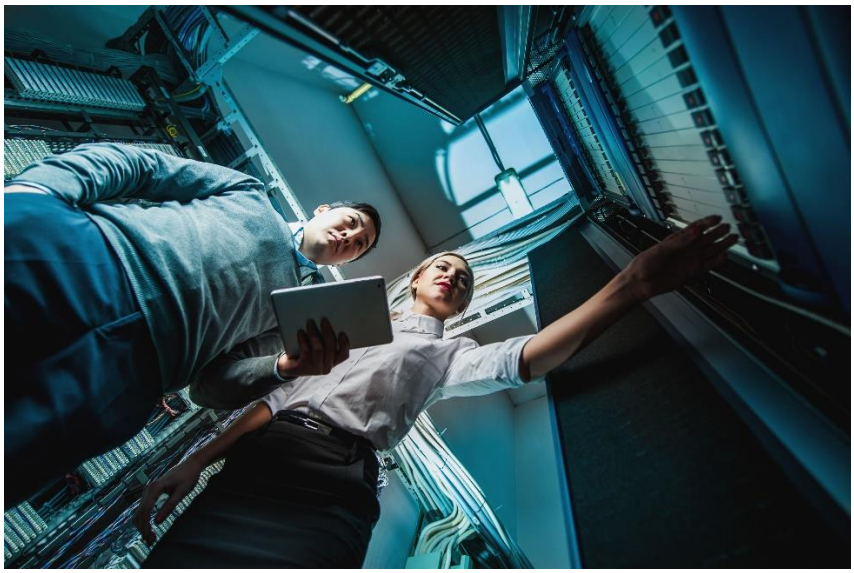

Image 2: Prime Vision specialises in integrating legacy systems with new, more secure systems.

About Prime Vision

Prime Vision is a global leader in computer vision integration and robotics for logistics and e-commerce. As an award-winning company, Prime Vision designs and integrates solutions using the latest recognition, identification, and robotics techniques to optimize the automation of sorting processes.

Headquartered in Delft, The Netherlands, more than 170 experts provide comprehensive market and domain knowledge to digital companies around the world.

For more information, visit https://primevision.com/

Editorial Contact:
DMA Europa: Ollie Eggleton
Tel: +44 (0)1905 917477
Web: news.dmaeuropa.com
Email: press-team@dmaeuropa.com
Address: Progress House, Midland Road, Worcester, Worcestershire, WR5 1AQ, United Kingdom

Reader Contact:
Prime Vision: Ellen Brender à Brandis
Web: https://primevision.com/
Tel.: +31 15 219 2090
Email: info@primevision.com
Address: Olof Palmestraat 10, P.O. Box 6034, 2600 JA Delft, KVK 08068458