Auriga announces new enhancements to its ATM zero trust cybersecurity solution.

London, 5th December 2023
Auriga, a leading software provider for the banking and payment industries, today unveiled new enhancements to its **Lookwise Device Manager (LDM)**, amplifying its capabilities in securing ATMs against increasingly sophisticated cyber threats.

Auriga's Lookwise Device Manager already sets the standard for protecting fixed-purpose devices that are crucial to business operations, such as ATMs. The latest iterations of LDM are engineered with a zero-trust approach, transforming vulnerabilities in the self-service sector into fortified points of trust and reliability.

The **Zero Trust model** makes suspicious assumptions about the vulnerability of the infrastructure that manages ATM and ASST devices, for example, that the remote access system can be manipulated or a software image installed on the ATM may be compromised even before being deployed. Additionally, maintenance technicians may not have ATM security as their priority or attackers may find common SW update processes useful for introducing their malware. This way nothing is executed on an ATM or ASST unless it has been previously authorised.

New features in LDM are being added as ATM cyber attack threats are evolving. For example, in 2023 **a new ATM jackpotting malware variant was revealed, dubbed FiXS**, infecting ATMs in Mexico. ATM jackpotting attacks use malware to steal large amounts of cash from an ATM without having to use a credit or debit card.

With cyber threats evolving at a breakneck pace, the newest versions of LDM now have improved **communications protection** features that focus on securing the ATM processes that could access the network. By only allowing trusted connections, ATMs are safeguarded against potential cyber-attacks, such as remote access and Man-in-the-middle attacks from untrusted hosts/ports.

Moreover, the updates introduce a more secure way to certify and protect the software from the very beginning of its deployment. These enhancements are designed to prevent any malicious interference before the ATMs are operational, making sure the ATM has all and only the authorised SW and policies deployed. Additionally, Auriga has expanded its **encryption features** to secure even systems without Hardware Security Modules (HSM), meeting the needs of more clients.

> "In an age where digital security is paramount, Auriga is dedicated to providing the highest level of protection for our clients' ATM networks," **said Vincenzo Fiore, CEO, and Founder of Auriga** "These enhancements to our Lookwise Device Manager are more than just upgrades; they are a recommitment to our promise of security and trust in a sector that relies on confidentiality and reliability. Looking ahead, Auriga's future for LDM includes further advancements in the remaining key operational processes, with a keen emphasis on on-site maintenance operations and reducing the attack surface during software update processes."

Auriga's LDM is currently being used to secure ATMs across various customers all around the world and has been designed based on the knowledge of the ATM infrastructure and the attacker's tactics and techniques. That is why it provides with the most comprehensive layered protection model to protect an ATM at all stages of the attack life cycle while ensuring full availability to services for customers.

About us

Auriga is a specialist in software applications for ATMs and payment systems. The company has also been an important innovator in online and mobile banking, offering solutions that promote process optimisation and a long-term competitive advantage. Over 74% of ATMs in Italy are managed with Auriga's WWS software. Auriga is a global company with a presence in Western and Eastern Europe, Latin America and Asia-Pacific.

For more information about Auriga:
https://www.aurigaspa.com/en/

For information

Daniel Couzens
Allison+Partners
auriga@allisonpr.com
+44(0)20 3971 4305