PayThink The Oracle MICROS attack is a call to fix point of sale security

paymentssource.com/opinion/the-oracle-micros-attack-is-a-call-to-fix-point-of-sale-security

Attacks on point-of-sale (POS) systems usually target immediate gain through fraud with payment card data, which is why any organization that uses point of sale devices or processes payment details needs to be on constant alert.

The numerous point-of-sale security breaches should serve as a reminder to each company that deploys this technology to reorient their business strategy around security. Without focusing on encryption, a holistic security check - and by consequence compliance, organizations are leaving themselves open to potential malicious attacks.

In the recent case of the data breach at Oracle's MICROS point-of-sale division, the weak link was in legacy systems running the network of payment terminals, which were infected with malicious code.

Image: Bloomberg News

POS systems run on a diverse range of operating systems like Windows, Unix, Linux and DOS and several communications protocols are used, so each organization is responsible for applying the best data security solutions and practices for each network of POS devices.

But point-of-sale data breaches have also reached the cloud. The most recent case is Lightspeed's data breach, a cloud-based POS provider in Canada that serves more than 38,000 business clients, that was hacked against retail POS systems. The incident exposed sensitive information related to sales, products, clients' encrypted passwords.

In order to effectively secure POS systems, companies should look at:

Encryption: Ensuring encryption between the POS payment applications and their card readers is recommended

to protect all sensitive data including things like usernames and passwords for businesses and individual accounts.

A rigorous security check: This should be done to all components of complex infrastructures that support POS terminals – servers, payment processors, websites, cash registers, and others.

Compliance: The debate “security versus compliance” also comes up, since - going back to Oracle again - Oracle is PCI compliant, yet attackers found a loophole. Organizations should have security as a primary objective and, in consequence, compliance is met, since regulations are usually built upon security best practices.

Roman Foeckl

Roman Foeckl is CEO of CoSoSys.