

NCR PERSPECTIVE

When prevention is better than cure

By Paul Race, Director of Financial Industry Communications, NCR

Technologies that have transformed the ATM channel have also acted as a catalyst for the introduction of malware

The ATM has changed, as has the environment in which it operates. The most-used banking channel now provides a wide range of services, and the technologies that enable this have also evolved.

With these new technologies come new risks. The technologies that have transformed the ATM channel – open environments, Web technologies and new integrated services – have also acted as a catalyst for the introduction of malware such as viruses, worms and Trojans.

Recently in Russia, criminals attacked eighteen ATMs, installing Trojan malware designed to steal PIN and card information. Examples such as this provide evidence of growing ATM threats and demonstrate how essential it is to protect the integrity of the self-service channel in a Windows™ environment. In order to define an appropriate response, it is first necessary to fully identify the nature of the threat.

Traditional threat – traditional response

A fundamental issue that needs consideration is whether in the current environment the traditional reactive approach to security threats is appropriate.

The majority of solutions currently available are reactive in nature (firewalls to guard against worms, anti-virus products, intrusion detection for malware). That is to say, whether they are signature-based, rule-based or behaviour-based, they work knowing or learning what is bad. This is effective in reacting to known risks, but what of the new and unidentified? One can only react to a threat once it is recognised, so until then the system remains at risk. In the case of zero-day attacks, for example, such a reactive approach is initially ineffective. What is needed is a solution that provides protection against known and *unknown* future risks. The challenge is to future-proof ATM security in the Windows environment.

Multi-faceted nature of risks

In addition to traditional threats such as viruses, worms and Trojans, there are three other types: emerging risks such as zero-day attacks by increasingly sophisticated malware authors; the danger of insider error or malicious attack from insiders (a growing trend); and the business risk introduced by increasing demands for regulatory compliance. Brian Bailey, NCR's vice president of financial solutions management, said "*traditional*

What is needed is a solution that provides protection against known and unknown future risks



solutions may address traditional problems but there is a changing landscape out there and we need to be innovative in how we defend against it”.

Attacking the cause not the symptoms

NCR has developed a simple yet unique complementary approach to future-proofing the security of ATM software for all Windows environments. It integrates new technology from Solidcore, the leading developer of IT control solutions, and tailors it to the specific requirements of the ATM and self-service environment.

The multi-vendor solution can run on all ATMs and has already been deployed by more than 100 customers, with NCR issuing over 60,000 licences worldwide. The solution addresses all four categories of ATM channel risk (traditional threats, emerging threats, business risks and internal threats) in that it attacks the cause rather than the symptoms. It is also unique in offering security control and compliance in one product.

Solidcore for APTRA™ tackles the real underlying problem – the introduction, from whatever source, of unauthorised code. It is therefore dealing with the cause of the threat rather than ‘after the event’ symptoms such as worms and viruses. No other single technology or ATM vendor can do this today: provide protection against known and unknown threats.

How does it work? Solidcore for APTRA will not allow any unauthorised code (such as viruses, worms or Trojans) to run. Code cannot be tampered with, modified or deleted, and running code is protected from being hijacked or tricked into unauthorised actions. This is very important for protecting ATMs from common attacks like buffer overflows and other types of code injection.

As well as protecting against external threats, the solution is also effective against insider attacks, accidental modification or lack of control. Even fully authorised administrators cannot run new software or modify existing software apart from authorised downloads.

In summary, by ensuring that the ATM is always operating as intended, Solidcore for APTRA negates all potential attacks – internal or external, known or unknown.

Removing the pressure of exposure

One significant problem faced by the ATM channel

is the insider threat due to patching. This involves an operator applying a patch, change or update with good intentions, but bringing the system down. The potential for this will increase as centralised solutions such as Active Directory and Software Management are employed, potentially multiplying any mistakes across the network.

When a patch is issued, there is a need to ensure it is relevant to the ATM environment and that it doesn't compromise network stability. Fear of leaving the network exposed might lead an institution to rush the process and introduce a patch without having made all the necessary checks. A number of banks have recognised that with Solidcore for APTRA they have in place a buffer against this vulnerability. Should they choose to introduce a patch, they can do so in a measured and efficient way, as the pressure of exposure has been alleviated.

Supporting compliance

NCR has found that banks migrating to Windows are looking beyond short-term security fixes – they are considering the challenges introduced by data security standards and regulatory compliance.

In the current environment there is no doubt that regulatory compliance requirements such as Sarbanes Oxley (SOX) and the Payment Cards Industry Association (PCI) will eventually impact the ATM industry. Included in the Solidcore for APTRA solution is the capability to provide real-time audit information on the changes made at any ATM with a tamper-proof record of activity. It thereby supports standard compliance reporting on the security and state of deployed ATMs. Changes can be identified, reconciled against authorisations, remediated or prevented.

Complex problem – comprehensive solution

Software security is complex. Thankfully there is a simple and comprehensive solution. Solidcore for APTRA is unique in addressing the root cause of software risk. Rather than applying ad hoc fixes after the event, Solidcore for APTRA prevents the introduction of unauthorised code and thereby protects against the threats you know and, more importantly, those you don't. As a bonus, it also enables you to demonstrate to third party auditors that adequate IT controls are in place, future-proofing you against further demands for greater regulatory compliance. ■

In addition to traditional threats, there are three other types: emerging risks, insider threats, and business risk

Solidcore for APTRA tackles the real underlying problem – the introduction, from whatever source, of unauthorised code