CYBERSECURITY FOR THE NEXT GENERATION OF BRANCH BANKING

KEEPING THE DIGITAL SERVICES NETWORK OPEN AND SAFE

WHITE PAPER

THE # NEXTGENBANK

AURIGA
the banking e-volution

www.aurigaspa.com

The COVID-19 pandemic has accelerated technological transformation; we have all been driven to everything that gives us remote access. This includes a move to transacting digitally; something that cybercriminals are actively looking to exploit.

Now that digital services have been widely embraced, the importance of banking cybersecurity has taken on new impetus. There is a pressing need to have every angle covered and to be able to pre-emptively protect consumers – no matter what channel they are using. New processes and barriers to prevent and mitigate attacks are needed.

It is therefore important to look at banking and cybersecurity from different angles.

The ATM ecosystem is vulnerable due to its complexity and because it is often running on obsolete, unpatched operating systems. ATMs are made up of esoteric hardware and software which means that they can be tricky to update from a systems perspective as well as a cost one.

A further problem is that ATMs need to be available to customers 24/7 and so downtime needs to be limited. This has an impact on finding the right time to perform testing and upgrades. Indeed, the balance between availability and upgrades means the temptation to delay making changes or upgrades is high. As a result, improvements to ATM networks get left behind and banks struggle to get an up to date picture of their overall vulnerability in terms of both potential surface attack areas and specific points of vulnerability.

Thus, the management and maintenance of these machines is often fragmented. In addition too many people can legitimately access the systems and the hardware, which increases the risk of an attack taking place. And the issue with dealing with any attack is that an upgrade is then needed - something that is very costly to deploy. Even when vendors have implemented upgrades as a remedy to this, attackers have found ways to bypass them.

The solution to all of these conundrums is to look at cybersecurity solutions that are tailormade to reduce the cyber-attack risks associated with them.

EXPLOITS ON THE RISE

Firstly, the main cyber-attacks that the ATM network falls victim to need to be identified and then banks can work out how best to protect them.

ATM logical attacks, for one, have been growing relentlessly in the last decade as the rewards are high and the attack can be done quietly. For example, criminals can carry out an attack in an ATM network in several ATMs simultaneously instead of blowing up just a single ATM. There are different type of logical attacks and they are constantly evolving and becoming more and more sophisticated.

The man in the middle attack' is another trend that is set to continue. This is when a cybercriminal attempts to hijack an operation on an ATM. For example, a banking customer needs to execute a transaction, it goes to an authorisation centre that will then check whether this is a valid transaction. Attackers will try and take advantage of this by manipulating the messages that are asking for the authorisation of the transaction. If they can gain access to those messages, they can fool potential victims.

Another attack that is set to rise in 2021 is called a 'black box attack', which is a physical attack that is not based on malware or technology, but rather on the connecting and physical external device such as the ATM dispenser. By connecting to the dispenser, the external device can then issue dispensing commands, which therefore leads to cash coming out of the ATM.

The fact that most ATMs often have poor physical barriers contributes to the rise of black box attacks - criminals can easily access the physical hardware. Another reason why black box attacks are on the rise is due to the fact that the technique itself is cheaper and simpler to perform than other fraudulent techniques, such as cloning cards or ATM skimming. Also, lower-skilled criminals can easily purchase the equipment to carry out black box attacks.

While most cybercriminals exercise black box attacks on non-bank ATMs, the recent rise in attacks on bank branch ATMs have proven that they are just as vulnerable.

Jackpotting is a similar technique to the black box attack, whereby cybercriminals use malware to trick an ATM into dispensing cash. Jackpotting is very easy to commit and has been on the rise for several years. There is no doubt that it will continue into 2021.

One reason why jackpotting will continue trending is due to the fact that cybercriminals are putting a lot of effort into developing innovative ways of attacking through the XFS layer. The issue again with the ATM channel is that ATMs are physically accessible, attackers can tap into them through infiltrating the banking infrastructure and then gaining access to the cash. They also contain sensitive data, such as credit card and pin numbers.

Again, the vulnerabilities in the outdated ATM systems have contributed to the global rise of jackpotting. As mentioned before, many ATMs run on decade-old versions of Windows. This gives hackers the opportunity to infiltrate the software layers in the ATMs and exploit the hardware to trigger the cash dispenser.

NEW SELF-SERVICE DEVICES BEING TARGETED

And ATMs are not the only target for criminals. Indeed with the increasing prevalence of home office and remote working, bank employees only have access to their systems through remote access. This area also reveals weaknesses that can be exploited by cybercriminals. Special cybersecurity solutions on employees' computers will be unavoidable.

For example, assisted self-service devices, which are fully owned and secured by a financial institution, will be the interface between the customer and the bank in the bank of the future. These devices must be sufficiently

secured in order to gain the trust of customers. The security aspect may become an important differentiator against other channels, such as online or mobile, which the customer is also responsible for protecting.
In terms of risks, financial fraud would obviously remain to be one of the key factors for a cyber-attack, but an even more damaging threat for the lean bank branch concepts of trust and security would be a targeted attack. This would lead to a customer data breach, business continuity interruption, reputational damage for the financial institution, and loss of customer confidence in the service (versus other banking channels).

Like ATMs, assisted self-service devices are physically accessible and dependent on remote communications and interconnection with the IT infrastructure, inheriting some of its risks and vulnerabilities. Thus an effective OT cybersecurity strategy needs to be put in place. A comprehensive and robust cyber-protection approach is an absolute must, but it needs to be complemented with the proactive monitoring of the device; in terms of service availability, security status, and the ability to have real-time access to investigate and remediate any potential security incident.

Financial institutions will have to look more intensively at cybersecurity and corresponding solutions this year and actively work to ensure that both their customers' personal data and their systems are protected.

RELYING ON AI AND ML FOR CYBERSECURITY

Artificial intelligence (AI) and machine learning (ML) are playing an increasing role in cybersecurity, with security tools analysing data from millions of cyber incidents, and using it to identify potential threats -- an employee account acting strangely by clicking on phishing links, for example, or a new variant of malware. A key benefit of machine learning in cybersecurity is that it identifies and reacts to suspected problems almost immediately, preventing potential issues from disrupting business.

By deploying AI-based cybersecurity to automate some of the defence functions, the aim is to ensure that the network is going to be safe, without relying on humans having to perform the impossible task of monitoring everything at once.

But although AI-based cybersecurity has many benefits, it is not a complete replacement for human security staff; and like any other software on the network, you cannot just install it and forget about it – there needs to be regular evaluation. You cannot assume that AI and machine learning are going to solve all the problems.

PROVEN SOLUTIONS FOR HOLISTIC DEVICE SECURITY

Auriga’s Lookwise Device Manager (LDM) allows bank security teams to monitor the security status of the banking network from a single graphical interface, avoiding the need to manage multiple independent solutions.

This centralised approach also means that device and infrastructure management can be done within a single hub and actions can be executed remotely to quickly establish new defences, via techniques including network segmentation and the implementation of new firewalls.

The various layers of protection required include file integrity protection, application whitelisting, full disk encryption, and hardware protection. These act singularly and together to provide a robust deterrent to would-be attackers. And because they can be managed centrally they allow the bank visibility over where a vulnerability might lie and how to patch that to stop it becoming a wider, systemic issue.

Elida Policastro, Regional VP – Cybersecurity Division at Auriga explains:

> *"The LDM is an integrated multi-vendor security solution that provides the most advanced layered protection model for self-service devices, allowing users to monitor the operating system or XFS status and relevant security events."*

The solution also has a remote key loading (RKL) module, which is integrated into the other layers and provides different modules to remotely control the ATM devices, thus facilitating operations, security investigations and maintenance activities.

> *"The manager works by adding an extra control layer so that the operation teams can manage the Remote Key Loading process and run custom remote actions to investigate or react to the new generation of logical and physical attacks based on malware",* Policastro says.

This provides a central and effective means to manage the security of individual bank endpoints. The manager covers all types of attack by blocking attempts to infect the ATMs with malware and then preventing any successful malware penetration from being executed.
In practice this means that once an attack has been attempted, the bank can take steps to stop it spreading throughout the ATM network by closing down the affected area, rather that the entire ATM network.

Providing adequate security measures to protect every workstation in an organisation is an essential mission. Secure workstations are the foundation of secure networks. If a hacker can access a workstation, the entire network could be compromised. Any security solution must include antivirus, backup prevention, firewalls, remote maintenance and monitoring. LDM offers a comprehensive package/solution for workstations that simplifies the security and monitoring process. The technology used uses the concept of whitelisting to allow access to system resources in a controlled manner.

Ultimately, not investing in the right technology means that banks risk opening themselves up to the very real possibility of experiencing security breaches, loss of sensitive customer data, and of course stolen cash. The reputational damage of this is simply too big to contemplate. It is time to act.

AURIGA
the banking e-volution

Building 3, 566 Chiswick High Road
London W4 5YA - United Kingdom
london@aurigaspa.com
www.aurigaspa.com