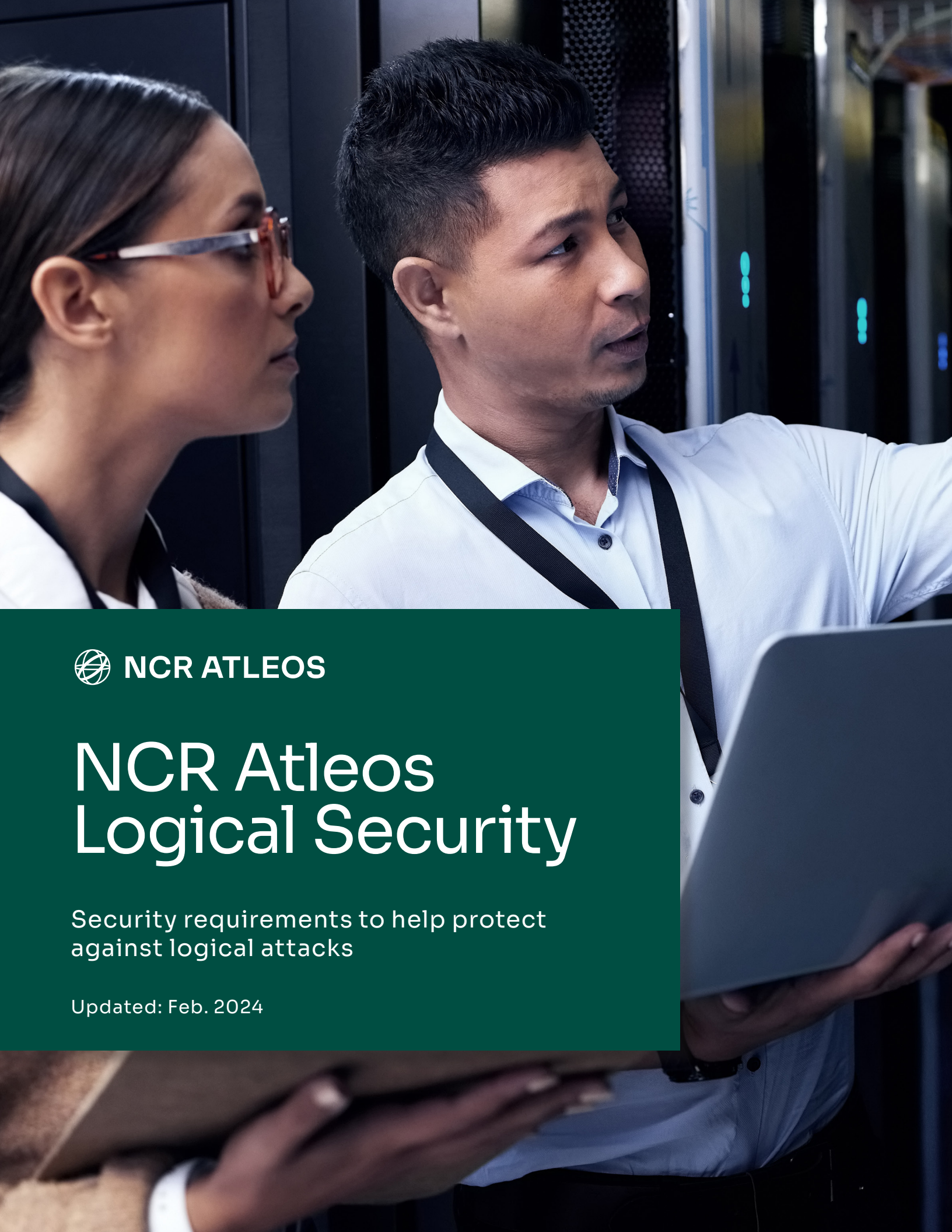


NCR ATLEOS

NCR Atleos Logical Security

Security requirements to help protect against logical attacks

Updated: Feb. 2024

Introduction

For far too many years, security played a minor role in the purchasing decision of ATMs and ATM services, but with the continued evolution of criminal attacks on ATMs and pressure from industry bodies such as PCI and EMV, security and compliance is now a fundamental part of the ATM landscape.

This document describes the primary activities required to be performed to maximize the security and integrity of an ATM estate to help protect against logical attacks.

NCR Atleos security model defines a layered approach. This provides the best protection from a variety of attack vectors and having all the security layers in place maximizes the security of an ATM estate.

NCR Atleos secure minimum configuration

This paper defines what NCR Atleos considers to be the minimum security configuration guidelines for a ATM environment. Whilst some details may relate to NCR Atleos ATMs only, the guidelines are considered to be applicable to all vendors ATMs

All NCR Atleos ATMs MUST be configured as per the guidelines outlined in this document. These minimum security requirements are necessary to defend/protect against currently known logical attacks on an ATM. All of these recommendations provide protection to the different layers within the environment, complementing each other to provide a secure holistic coverage across all the layers.

A multi-layered security ensures that if one layer has a weakness/failure, then the other layers will mitigate the risk of that weakness or failure being exploited. If all the layers of protection are not applied then it may allow compromise of another layer.

The layered approach to security and the importance of having the layers is critical to preventing different types of attack on the ATM environment. These guidelines should not be considered as optional - they should be viewed as essential to protect the ATM in today's environment.

NCR Atleos Secure: software configuration and implementation guidelines

RULE 1

Secure the BIOS

The UEFI firmware/BIOS is a set of programs, typically in firmware (PROM, EEPROM or flash memory), that enables a computer's CPU to communicate with peripheral devices. The BIOS provides start-up Power-On Self-Test (POST) and then bootstraps the operating system on power-on or bus-reset. The BIOS consists of code (typically operating CPU in real mode) and configuration settings. The configuration settings are used to control the operation of the BIOS programs and also the hardware parameters that are exposed to the operating system.

Securing the BIOS is fundamental to the security of the ATM. Administration of the BIOS must adhere to the following principles:

- During normal operations, you should configure the BIOS to boot from the primary Hard Disk only. All other bootable mechanisms should be removed from the boot order to prevent booting from any other unauthorized device
- BIOS updates must be reviewed and tested before deployment.
- Performing BIOS operations must be password (non-default / unique) protected. Passwords should be non default and unique.
- UEFI Secure Boot, where at all possible, to protect against boot vector attacks

To manually configure the ATM BIOS on your NCR ATMs, please contact your NCR Account Manager for a copy of **Manually Securing the BIOS**.

NCR Atleos recommends the use of Secure Boot and solutions to manage the BIOS remotely. NCR Atleos offers solutions which perform the following operations :

- Remotely, through software distribution, secures and updates the BIOS for most NCR cores
- Configures boot from primary Hard Disk only
- Sets a customer specific BIOS password
- Allows remote update of
  - ATM boot order
  - ATM BIOS Password
  -ATM UEFI firmware/BIOS to latest version.

RULE 2

Establish an adequate operational password policy for all passwords

It is up to each and every ATM deployer to ensure that they implement a secure user account and password policy. Banks should use an account management system that will allow them to manage accounts centrally, e.g. Microsoft Active Directory. Moreover, they should ensure that all passwords are secure.

- ALL default passwords MUST be changed as per PCI 4.0 requirement 2.2
- User account passwords must be unique per ATM and per account. This gives maximum protection at each ATM, as a successful attack at one ATM cannot lead to a successful attack at another ATM
- NCR Atleos recommends user passwords be at least 14 characters long and must not contain more than two consecutive characters from the user name
- User passwords should also be complex and must contain at least three of the following 4 categories
  - English uppercase alphabet characters (A-Z)
  - English lowercase alphabet characters (a-z)
  - Base 10 digits (0-9)
  - Non alphanumeric characters (for example !@#$%)
- User and Administrator account passwords must be changed every 90 days (as required by PCI DSS 4.0 requirement 8.3
- BIOS passwords are often limited by length and complexity. Nonetheless, BIOS passwords should be as complex as the BIOS allows. NCR Atleos has solutions for managing BIOS passwords.

RULE 3

Implement communications encryption

Transmission of sensitive cardholder data across ALL networks must be encrypted. Cyber criminals may be able to intercept transmissions of cardholder data over networks, so it is important to prevent their ability to view this data. Encryption is one technology that can be used to render transmitted data unreadable by any unauthorised person.

PCI DSS 4.0 Requirement 4.2.1 states to use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission.

SSL and early TLS encryption have been demonstrated to have weaknesses which can be exploited and must not be used as a security control to meet PCI requirements.

As a minimum the PCI DSS guidance below should be followed for migrating away from SSL and early TLS.

- Since June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place
- New implementations must not use SSL or early TLS as a security control
- Existing implementations must migrate to a secure TLS version (now 1.2)
- All use of SSL and early TLS as a security control must be stopped

- Configure TLC Securely. Ensure your TLS implementation is configured securely m- ensure you're supporting secure TLS cipher suites and key sizes, and disable support for other cipher suites that are not necessary for interoperability. Use certificate pinning and certificate check.

NCR Atleos solutions support TLS version 1.2 and is stronger when combined with the environment hardening guidelines provided in this document.

Never send unencrypted cardholder data via end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)

MAC-ing of sensitive authorization messages is also recommended. This prevents data from being modified by establishing a shared secret with the legitimate host, so it prevents takeover or replacement attacks. NCR Atleos recommends usage of TLS 1.2 with Macing enabled for all message fields.

RULE 4

Install and maintain a Firewall

The ATM firewall must be configured to only allow known authorized incoming and outgoing connections necessary for an ATM environment. The connections must be configured per program rather than per port.

For example, the default configuration of the Windows 10 firewalls blocks all incoming communication connections and any applications that require incoming connections must be explicitly configured. All outgoing communications are allowed by default.

Detailed configuration options for the Windows firewalls and lots more are provided within the NCR Atleos Base/Enhanced OS Hardening products. For further information, please refer to the documentation for your firewall product.

RULE 5

Remove unused services and applications

It is recommended that you remove any unused services and applications from the system to reduce the attack surface area. By adopting the principle of 'If you don't use it, disable it', you remove potential attack vectors.

For example, if your application does not use output caching, you should disable the ASP.NET output cache module. Thereafter, if future security vulnerabilities are found in this module, your application is not vulnerable.

The following table lists **examples** of the recommended applications that should be removed from the ATM software stack if they are not used. However, you should review your software stack to determine if there are further binaries that can be removed:

Application	File Name	Description/ Purpose
Address Resolution Protocol	arp.exe	Display/edit network address
File Attribute	attrib.exe	Display/edit file attributes
File Transfer Protocol	ftp.exe	Transfer files between two hosts
NetBios over TCP/IP	nbtstat.exe	Display network information
Network Statistics	netstat.exe	Display network information
Name Server Lookup	nslookup.exe	Display network information
Remote Copy Program	rcp.exe	Copy files
Registry Editor	regedit.exe	Display/edit Windows registry
Registry Editor	regedt32.exe	Display/edit Windows registry
TCP/IP Route Command Application	route.exe	Display/edit network settings
Remote Shell Application	rsh.exe	Execute command on remote computer

NCR Atleos recommends using NCR Secure Allowlisting - Solidcore to assist in blocking executables that cannot be removed.

RULE 6

Deploy an effective anti-malware mechanism

Anti-malware software will:

- Maintain the integrity of your ATM software stack and prevent malicious software compromising your ATM.

An effective white-listing solution will provide online protection beyond known malware threats. For example, memory protection, zero-day attacks and threat alerting.

We recommenced using NCR Atleos Secure Allowlisting - Solidcore as it is:

Solidcore Suite:

- is more effective than anti- virus software alone in preventing known and unknown malware from executing.
- is an active whitelisting application for increased malware protection
- prevents execution of malware copied onto an environment
- prevents unauthorized software from execution
- alerts on execution of unauthorized software and malware
- provides runtime memory protection
- protects against zero-day attacks, known, and unknown threats
- can evaluate its own status, and send alerts if its agent becomes disabled

To complement Solidcore Suite you should use a traditional reactive signature-based Anti- Virus (AV) solution to ensure any known malware copied onto your ATM is removed.

Major points to consider when deploying AV:

- Anti-Virus only protects and cleans up known malware and is as effective as its last set of signatures, these signatures must be kept up to date
- Scan reports/logs must be reviewed regularly to determine if the ATM is infected or not
- AV should be run on a weekly basis on an ATM to detect if known malware exists
- AV on an ATM should be configured to:
  - Run in silent mode with no pop-ups
  - Do not have the AV running in real-time mode, do not check log files too frequently because they are updated too often
  - If the AV software is running in the background, consider process priorities
  - Put the ATM out of service prior to scanning and run during quiet periods
  - Update the signature files prior to running the scan

If Solidcore Suite Alerts or AV scan reports indicate malware has been found, best practice malware incident procedures must be followed, which may include the following (dependent on the malware found and on law enforcement):

- Take the impacted ATMs out of service
- Quarantine the malware
- For forensic analysis to be done, the hard disks must be removed and a forensic image taken
- To restore the ATM to normal functionality, the ATM should be reimaged with a new hard disk using a known master image
- Scan the rest of the ATM estate for the malware found.

RULE 7

Establish a regular patching process for all software installed

Keep all software running on the ATM up to date with the latest security patches for all software. This ensures that attackers do not take advantage of known vulnerabilities within the deployed software.

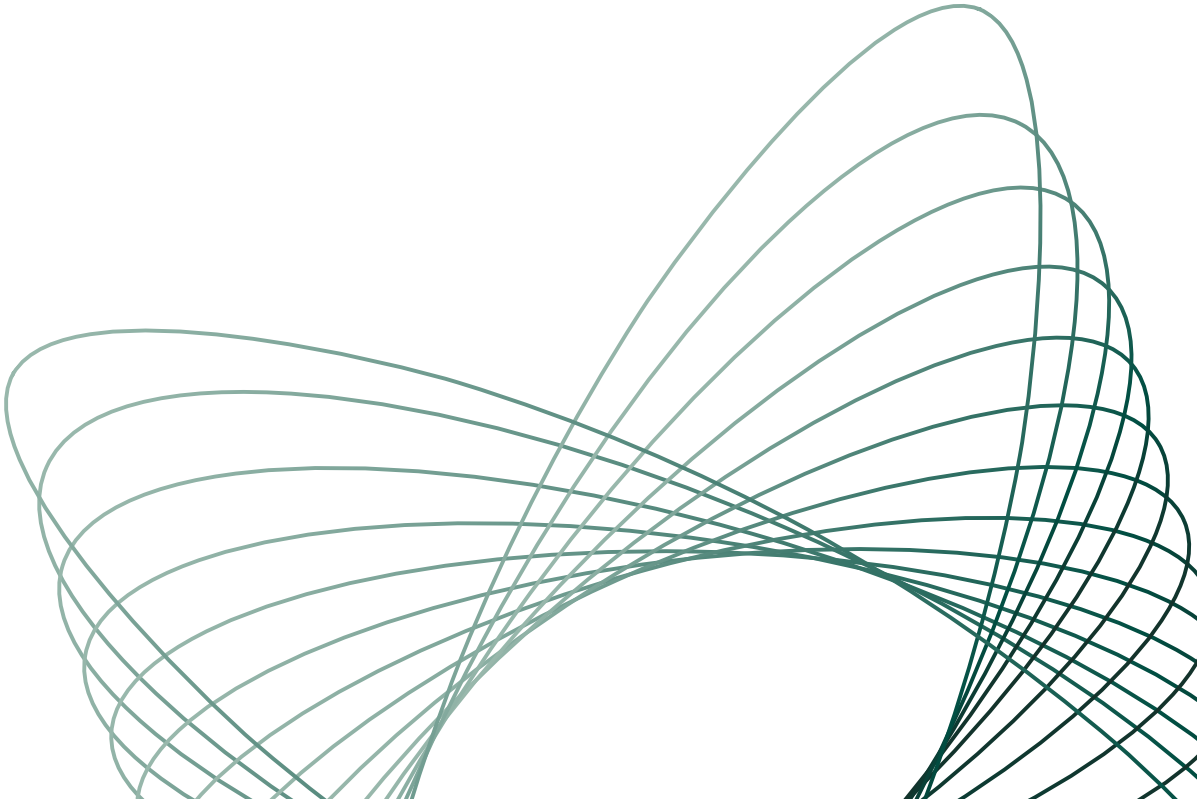
Weaknesses may allow malware to be installed onto the ATM or allow attackers access to the ATM software stack. If a vulnerability within the software stack has been addressed by a patch which has been installed onto the ATM then it will no longer be exploitable.

Keeping up to date with Microsoft security hotfixes ensures that attackers do not take advantage of known vulnerabilities within the operating system. The unpatched vulnerabilities may allow malware to be installed onto the ATM or allow attackers access to the ATM software stack.

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met.

It is important to ensure that ATMs are running on a supported operating system – industry reports would suggest that a substantial number of ATM's still run older OS versions, and migration to a supported operating system environment should be planned to take place as soon as possible.

Without critical Windows security updates, your ATM may become vulnerable to harmful viruses, spyware, and other malicious software which can steal cardholder data or damage your business data and information.



RULE 8

Hardening the Windows operating system (OS)

The Windows operating system must be hardened to restrict the privileges and behavior of the ATM to allow only the functions necessary for a self-service environment. This consists of setting up a locked down OS environment on a standalone ATM based on the following high level requirements:

- Disable Windows Auto-play
  - Auto-play is a feature of Windows operating systems which allows software to run from removable media as soon as it is detected on a USB, DVD or CD. Disabling the auto-play feature within the operating system will prevent malware being automatically run when it is detected on removable media.
- Implement a locked-down user account for automatically running self-service application functionality, with the least privileges and no interactive desktop access
- Implement a keyboard disabler to block keypresses being interpreted within the locked down account
- Apply file, folder and registry permissions to restrict access to the minimum required for the ATM to function
- Apply computer and user policies to restrict to the minimum functionality required for the ATM application to function correctly and securely

All the above configuration options and many more are provided within the OS Hardening solutions provided by NCR Atleos.

These solutions protect the operational security of an ATM creating a secure locked down environment to protect the ATM's assets. The secure environment encompasses a comprehensive set of security features including: preventing the automatic running of programs on removable media, providing a locked down account for automatically running self-service functionality, controlling access to external devices and running of software which effectively locks down the runtime environment of the ATM at the registry level. In excess of 500 settings are automatically set when the software is installed in 'Secure Mode'. These settings are a balance between the minimum settings required to operate an ATM in a stand-alone environment, and the industry-accepted system hardening standards. Which include, but are not limited to:

- Center for Internet Security (CIS)
- Microsoft Windows Security Baseline using Security Compliance Toolkit
- International Organisation for Standardisation (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

RULE 9

Implement role based Access Control

The more people with access to cardholder data environment, the greater risk that a consumer's account will be used maliciously. Restricting access to those with a legitimate business reason helps you prevent mishandling of cardholder data, and protect against ATM jackpotting. PCI-DSS requirements identifies a need to restrict access to data on a "business need to know" basis.

For all users accessing the ATM environment, their account permissions should be based on the roles they have and should be given only the permissions required for the role. For example, branch staff who need to change the printer paper should only be assigned the level of access needed to effectively perform that task. Once you define all roles and corresponding access needs, you can grant permissions accordingly.

Remote desktop access for ATMs is not recommended. If there is a business need for remote access being required then role based access control must also be implemented and a least privileges approach should be taken. PCI-DSS requirement 8.4 must be enforced for that access which means multi-factor authentication with at least two of the methods below be used for all remote access to the payment application environment.

Authentication methods for all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Payment application vendors must provide instructions for configuring the application to support multi-factor authentication.

NCR Atleos PCA-SSF compliant applications provide guidance on how to meet this requirement.

RULE 10

Deploy a network authenticated hard disk encryption solution

Deploying full hard disk encryption protects from offline attacks and ensures the integrity of the ATM hard disk.

This means that the ATM is protected against malware attacks even when the ATM hard disk is offline e.g. where:

- The ATM is booted from bootable removable media
- The hard disk is removed from the ATM and mounted as a secondary drive
- The core is removed from the ATM

NCR Atleos Secure Hard Disk Encryption protects against the above attack vectors by rendering the contents of the hard disk unreadable which maintains the confidentiality and integrity of the data against:

- Data harvesting from the ATM hard disk
- Reverse engineering software on the ATM hard disk (if using network authentication)

NCR Atleos Secure Hard Disk Encryption solution supports three deployment modes:

1. Server Provisioned Autoboot (recommended)
   - Provides a centralized encryption status of the ATMs being managed (PCI DSS requires all encryption keys to be managed)
   - Provides remote administration
   - Provides the ability to perform a crypto-erase of the hard disk either to react to threats (e.g. if a disk is believed to be stolen and then tries to reconnect to the server it will be automatically erased) or to allow for secure disk disposal
   - Provides automatic encryption key backup
   - Can allow for authorized hard disk decryption
2. Network Authenticated Autoboot
   - As above but with a higher level of security by only allowing the encrypted hard disk to boot once it has been authorized by the HDE authorization server.

- Requires a high level of infrastructure and network stability to maintain high availability.

3. Standalone Autoboot (for no network connectivity environments)
   - Not recommended but can provide for scenarios where network connectivity is unreliable on non-existent.
   - Encryption key management is performed manually.

RULE 11

Protect communication between the ATM core and the dispenser

Encrypting the communications between the ATM core and the dispenser will prevent black box attacks. If attackers attempt to send commands to the dispenser directly, the dispenser will recognize these commands as invalid. Only commands from the ATM software stack will be authenticated and processed by the dispenser.

NCR Atleos Recommends for NCR Atleos ATM's:

1. Deploy the latest version of Dispenser Platform Software/Firmware. NCR apply critical security patches to the dispenser platform software, and it is imperative that customers maintain their platform software to the latest version. The minimum version which must be used is XFS Dispenser Security Update 01.01.00
   - The firmware updates are available in the latest released NCR Atleos platform software. Firmware is packaged with the corresponding drivers as platform software components for the dispensers. Firmware is therefore deployed by installing the platform components. This can be done either by a complete upgrade of the NCR platform software or by integrating the new software components into an existing supported platform. NCR Professional Services can assist with a new platform upgrade nor platform component upgrades.
2. Set the Dispenser Protection Authentication level to Level 3, Physical Protection.
3. Set the Dispenser Authentication Sequence to:
   - Level 2 for S1 dispensers
   - Level 1 for S2 dispensers
4. For high risk locations e.g. Mexico, or for high risk ATM models, set the Dispenser Authentication Sequence to:
   - Level 4 for S1 dispensers
   - Level 2 for S2 dispensers
5. Disable diagnostic dispense (for S1) and disable SYSAPP configuration of settings.

RULE 12

Perform a penetration test of your ATM annually

It is best practice to have a penetration test performed on your ATM by an organization external to your company. It should be done against a full software stack, network access points and physically hardened environment as per the recommendations in this document. At a minimum, follow the PCA-SSF requirements section 6.2 requirements for ensuring applications are not vulnerable to common coding vulnerabilities.

The test should comprise of various simulated attacks in an attempt to find misconfiguration, weaknesses and vulnerabilities that could be exploited by an attacker in a production level ATM. The penetration test will allow you to identify any areas that need to be addressed to ensure your ATM is optimally secure.

RULE 13

Deploy a software distribution tool that will assist in maintaining the confidentiality, integrity and availability of your ATMs

A software distribution capability with industry best practice security controls, role based account control, authorization and authentication is an essential layer that will help maintain the confidentiality, Integrity and availability of your ATMs.

To meet rule 7, it is essential to have remote software distribution capabilities.

If malware is found or suspected to be on an ATM, software distribution will expedite the clean-up and update malware signature files across an ATM estate. This will help put the ATMs into a more secure state, prevent attacks occurring and help limit damage to those ATMs that may be compromised.

NCR Recommends Vision Software Distribution

RULE 14

Consider the physical environment of ATM deployment

The physical environment that an ATM is deployed within and the ATM type will influence the risk of an ATM being attacked. Lobby ATM's should not be deployed in 24/7 unattended environments without compensating physical security controls. A "through-the- Wall" ATM may be more suitable for these locations. Additionally, any network hardware/routers should be appropriately secured.

NCR Atleos recommends:

Through-the-wall ATMs, which may be more suitable for unattended environments. UL-rated, pick-resistant, Top Box locks, or a Smart Locks solution as a configuration option or upgrade kit with appropriate key management.

RULE 15

Consult an enterprise security specialist to assess and deploy industry best-practice security controls within your enterprise.

Ensure you follow industry best-practices within your wider organization to minimize the risk of a compromise occurring within your enterprise, for example:

- Security Awareness Training for employees to minimize the risk of spear phishing and other social engineering attacks.
- Having a tried and tested incident response plan in place
- A robust patching process is in place across the FI's enterprise.
- Role-based access control
- Network Intrusion Detection/Prevention systems. Creating custom rules to detect and respond to unusual traffic behavior, e.g., block and alert on any ATM to ATM traffic
- Network Access Control for endpoint authentication to only allow authorised authenticated devices (ATMs) and applications access to the network and services.

NOTE: These are just examples. Your enterprise security specialist should advise on best-practice controls.

NCR ATLEOS

Why NCR Atleos?

NCR Atleos solutions power more than 15,000 financial institutions across the globe, We have the largest independent ATM network offering convenient self-service banking across four continents, are the largest ATM deployer with an 800K global ATM install base, and deliver exceptional customer experiences as #1 in multi-vendor ATM software.

Contact us at NCRAtleos.com today

NCR Atleos (NYSE: NATL) is a leader in facilitating banks and retailers to deliver best-in-class self-service banking experiences for consumers. Atleos helps customers expand their reach, provide greater financial access for customers and reduce operational complexity through industry-leading technologies, unmatched global services capabilities, the largest surcharge-free network and expertise in running ATM networks. Atleos is headquartered in Atlanta, Georgia, with 20,000 employees globally.

NCR Atleos Corporation
864 Spring St NW
Atlanta, GA 30308

Patents Pending

ncratleos.com