PROTECTING YOUR ATMS FROM LOGICAL ATTACKS

An NCR white paper

Protecting against an emerging threat

Over the past several years there has been a dramatic rise in the use of electronic devices and malware to gain access to ATM computer systems or components with the purpose of obtaining cash or other sensitive data from ATMs.

These logical attacks can be broadly categorized into three major categories:

Black Box Attacks

Malware in the network

Malware on the ATM

In each of these cases there is a potential risk for criminals to gain access to all of the cash in the ATM. Also, in these coordinated attacks, many ATMs can be affected. As a result the losses from these forms of attacks can quickly become extremely significant.

To help financial institutions protect their ATMs and customers, NCR has compiled a list of guidelines that will provide defenses against this form of attack.

Recommended practices to defend against Logical Attacks

01	Secure your BIOS
02	Establish an adequate operational password policy for all passwords
03	Implement communications encryption (TLS encryption or VPN)
04	Establish a firewall
05	Remove unused services and applications
06	Deploy an effective anti-virus mechanism
07	Establish a patching process for Operating System Patches
08	Establish a regular patching process for ALL software installed
09	Disable Windows® Auto-Play
10	Ensure the application runs in a locked down account with minimum privileges required
11	Define different accounts for different user privileges
12	Deploy a network authentication based Hard Disk Encryption Solution
13	Ensure there is protected communications to the dispenser of the ATM
14	Perform a Penetration Test of your ATM production environment annually

Don’t forget the Physical Security

Traditional attacks on ATMs still remain and are increasing in many regions. A comprehensive security solution strategy needs to also include protection against:

- Card Skimming and Trapping
- Cash Trapping
- Robbery and other Physical Attacks on the ATM

NCR has a complete portfolio of solutions, and services that need to be part of all ATM operators plans. Security is not an option for NCR and should not be an option for Financial Institutions.

Contact NCR for an assessment of your solutions strategy and learn how you can protect your ATMs.

For more informatiom about how to secure your ATM netwrok, visit ncr.com or email financial@ncr.com to contact an NCR account representative today.

Contact us

Learn more

Sign up for NCR Alerts

Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.

NCR Corporation | 3097 Satellite Boulevard . Duluth, Georgia 30096 . USA

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice. All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR representative or NCR office for the latest information. NCR Secure is a registered trademark of NCR Corporation in the United States and/or other countries. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.

©2015 NCR Corporation 15FIN3754-0915 www.ncr.com