WINCOR NIXDORF

BEETLE /moPOS Tablet

Mobile POS solution

Windows 8.1 Security Advice
(July 2015)

We would like to know
your opinion on this publication.

Please send us a copy of this page
if you have any constructive criticism on:
- the contents
- the layout
- the product.

We would like to thank you in advance
for your comments.
With kind regards,

Wincor Nixdorf International GmbH
R&D, SAT11
Wohlrabedamm 31

D-13629 Berlin

E-Mail: retail.documentation@wincor-nixdorf.com

Your opinion

Contents

1 Introduction

THIS WINDOWS 8.1 SECURITY ADVICE FOR THE BEETLE /moPOS TABLET (“ADVICE”) ONLY INFORMS ABOUT SOME POSSIBLE PREVENTIVE MEASURES TO ENABLE USERS OF THE BEETLE /moPOS TABLETS TO BETTER SECURE SUCH AGAINST FRAUD ATTACKS. EVEN WHEN FOLLOWING THE COMPLETE ADVICE, THIS MAY NOT SECURE AGAINST BREACHES, SECURITY ISSUES AND POSSIBLE DATA LOSSES. THE RESPONSIBILITY TO SECURE THE USE AND OPERATION OF THE BEETLE /moPOS TABLET NEED TO BE CAREFULLY AND INDIVIDUALLY CONSIDERED BY THE USER.

This document provides a baseline guide to securing the Windows 8.1 Professional and Industry as recommended by WINCOR NIXDORF International GmbH (hereinafter “Wincor Nixdorf”).

The following recommendations in this baseline guide are intended for use on the tablets of a moPOS System, but most are product-independent.

Following chapters describe different aspects of Windows security and their recommended configuration.

2 General recommendations

The following contains some general recommendations you can use whenever self-service devices are being considered.

- Set the computer name in the way that it doesn't allow the attacker to derive its function from the name.
- Install anti-malware software to protect your device.
- Use Microsoft security patches and security packs.
- Configure your device in a way which makes it complaint with PCI DSS standards.
- Enable for example the built-in Windows firewall or install and enable the one you favor.
- Use hard disk encryption software (e.g. Microsoft BitLocker).
- Do not use unencrypted WLAN connections.
- Disable IPv6 if it is not needed.

These configurations make your device more resistant to unauthorized access and malware.

3 Account policies

Like the majority of operating systems, per-default standard Operating System accounts are not compatible to the various security standards and best practice e.g. PCI, SANS, NIST etc. Using the Account Policy's accounts can be configured so that they conform to industry recognized best practice and standards.

Configuration examples:

- You can enforce the password history to raise the value of remembered passwords, so you can monitor that you don't use old passwords again
- PCI DSS recommends to change your user passwords at least every 90 days
- Set the minimum password age down to 0
- Configure your password length up to a minimum of 8 characters
- set up the account lockout duration
- limit the logon attempts

To configure use the following path:

Control Panel> System and Security

4 Audit policies

Being able to record who, performed what and when is not only essential but a key PCI – DSS requirement. Check the settings in Advanced Audit Policy Configuration and set them to your needs and internal policies.

To configure use the following path:

Control Panel> System and Security> Administrative Tools> Local Security Policy> Advanced Audit Policy Configuration

5 Event Logs

The settings will deliver the means whereby service and support personal will be able to have, and retrieve the information required to perform the necessary tasks.

Configuration examples:

- Set up the correct max. log size
- Achieve the log when max. log size is reached
- Choose a warning level to inform you about the log size

To configure use the following path:

Control Panel> System and Security> Administrative Tools> Event Viewer

6 Groups and User

The configuration of local users and groups depends on the topology and the network of which the target device shall become a member of.

To protect and obscure the group and user configurations

- Use strong passwords
- Rename the user and group names (for example: WNUsers00, WNUsers01, WNUsers02, …)
- Rename built-in administrator account from Administrator to Application and set a strong password
- Interchange guest and user account names
- Interchange global and local account names
- Create a dummy user account named Administrator and set a strong password as honey trap

To configure use the following path:

Control Panel> User Accounts and Family Safety

7 Logon

Make sure the device is always secured via a user login. The access to the operating system and its software shall not be possible without any password. Make sure the device will be locked in case of a short time of inactivity. After inactivity of an appropriate time re-login with password is required. The time of inactivity should be definitely less that one hour.

Logon settings apply to both, automatic and interactive user logon, therefore it is recommended to configure the auto logon and the interactive settings

- Don’t show the username of the last login
- authentication should necessary to unlock the workstation
- Ease of access opportunities should not enabled
- key combination to ease the access should be enabled
- Fast user switch should not be possible

To configure use the following path:

Control Panel> User Accounts and Family Safety> User Accounts

8 User Account Control

It is recommended to configure the UAC to get prompt the needed information of your system inside your allowed framework.

To configure use the following path:

Control Panel> User Accounts and Family Safety> User Accounts

9 Services

Double check the list of services started, especially those started when the system is starting. Reduce the number to required minimum in your environment. This will speed up the system start, provide additional capacity for needed services and applications enables you to identify critical tasks more easy and limits the number of security risks.

To configure use the following path:

Control Panel> Administrative Tools> Services

10 User rights and privileges

It is recommended to configure the settings of rights and privileges of the members according their tasks and your internal policies.

To configure use the following path:

Control Panel> User Accounts and Family Safety> User Accounts

11 File system

It is recommended to maximize data availability, scales efficiently to very large data sets across diverse workloads, and guarantees data integrity by means of resiliency to corruption (regardless of software or hardware failures) operated by using ReFS format.

12 TCP/IP

It is recommended to protect your system against network attacks, for example against SYN, ICMP, SNMP, AFD, SYS to filter the TCP/IP and set up the protection settings.

To configure use the following path:

Control Panel> Network and Internet> Network and Sharing Center

13 Network connections

The settings of the network connections are essential for the security of the whole system. It is recommended to:

- Allow access only with strong passwords.
- Hide the computer from the browse list.
- Make sure that only selected members are able to change settings like passwords.
- Send passwords only encrypted to third-party servers.
- Limit the logon hours and restrict the access for anonymous users.

To configure use the following path:

Control Panel> Network and Internet> Network and Sharing Center

14 Hardware

To protect data on the hardware restrict the access to external storage devices, e. g. the DVD drive. Do not download drivers or print over HTTP and prevent the computer from writing to USB block storage devices. The auto run of all kinds of drivers should be restricted and it should not be possible for users to install printer drivers.

To disable the automatic update and recovery of drivers:

Settings> Change PC Settings> Update and Recovery> Recovery

15 Internet Explorer

It is very important to increase and set the possible security configurations because of the increased usage of the Microsoft Internet Explorer and internet based user interfaces.

It is recommended to allow only selected members the changing of general and security zones settings. Functions of online pages should not be available on offline page.

To change rights and privileges of members:

Control Panel> User Accounts and Family Safety> User Accounts

To change limit functions of certain offline pages:

Control Panel> Network and Internet

16 Other settings

It is recommended to check the settings concerning the power down of the system. Open files for example should not be saved for the next session and the power down should not be possible without having to log on.

To change the power down settings:

Control Panel> Hardware and Sound> Power Options

17 EFFECT; ENFORCEABILITY; DISCLAIMER

THIS ADVICE DOES NOT CONSTITUTE AN OFFER TO PURCHASE OR LICENSE, NOR AN AGREEMENT OF ANY KIND, AND BY THIS ADVICE NO SUCH AGREEMENT SHALL BE DEEMED TO EXIST. THIS ADVICE IS NOT INTENDED TO NAME, AND DOES NOT CONSTITUTE BINDING NOR COMPLETE NOR INDIVIDUALIZED RECOMMENDATIONS BY WINCOR NIXDORF, BUT IS MERELY INTENDED TO NAME SOME BASIC AND ABSTRACT PROPOSALS; THEREFORE NO CLAIM NOR ANY LEGAL RIGHTS AGAINST WINCOR NIXDORF MAY BE BASED ON THIS DOCUMENT. FOR THE NAMED PROPOSALS AND RECOMMENDATIONS ANY WARRANTY IS EXCLUDED. WINCOR NIXDORF SHALL HAVE NEITHER LEGAL NOR FINANCIAL OBLIGATIONS WITH RESPECT TO THE ADVICE, UNLESS SUCH HAVE BEEN MUTUALLY AGREED IN A WRITTEN AND BINDING CONTRACT, WHICH HAS BEEN PROPERLY EXECUTED AND AT LEAST SIGNED BY WINCOR NIXDORF.

Wincor Nixdorf International GmbH
D-33094 Paderborn

Order No.: ***01750280322A***