KONICA MINOLTA

SECURITY EVALUATION REPORT BY NTT DATA

ABLE TO WITHSTAND 80 HOURS OF WHITE HAT HACKING

Independent testing by a respected global security expert

Any network-connected device with a CPU and operating system introduces a security risk. To protect data and comply with security regulations such as PCI, HIPAA, FERPA and GDPR, global organizations continually monitor emerging threats from all devices, including printers. Recently, some news outlets have depicted sensationalized scenarios where printers were being used as an easy point of access into company networks to wreak havoc and steal all kinds of data. Konica Minolta customers are naturally concerned about vulnerabilities that may apply to their businesses.

Although Konica Minolta can provide customers with design specifications and internal test data that demonstrates how Konica Minolta MFPs are secure against attack, we decided that having a third-party expert try and hack one of our leading devices would be the best way to provide peace of mind to customers. Working with NTT DATA and NTT Security, thorough penetration tests, including scripted attacks and advanced hacking tactics, have been performed on a best-selling Konica Minolta MFP.

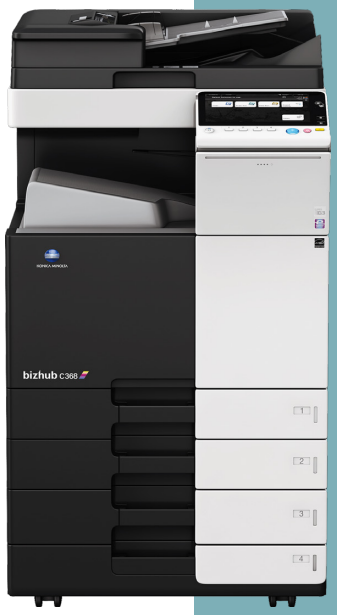
As security experts with global credibility, NTT DATA and NTT Security were the clear choice to carry out the testing. Konica Minolta provided the engineers with an MFP and the device's source code, so that the "white hat" hacking could be completed to the broadest and most aggressive standard possible. Testing spanned several weeks, totaling around 80 hours of trying to hack the device, and found no major security vulnerabilities, showing that Konica Minolta MFPs are well fortified against attacks, including brute-force tactics.

NTT DATA

Giving Shape to Ideas

SECURITY EVALUATION REPORT BY NTT DATA

KONICA MINOLTA MFP SECURITY FEATURES



bizhub

Up-to-date & certified

Konica Minolta develops and provides the newest security features to protect customer information. Most Konica Minolta devices have been awarded ISO 15408 certification and FIPS140-2 certification.

A secure network

Devices equipped with user authentication ensure that only those with permission can use them. Administrator authentication is needed to access the whole address book, preventing the address book being tampered with all at once. Unneeded MFP ports and protocols can be switched to OFF to prevent outside intrusions. The fax line only supports fax protocol, and if any other communication protocol attempts to use the line it will not be supported. Encryption, bi-directional certificate verification and quarantine network options are also available.

Stay virus free

Konica Minolta MFPs use a Linux kernel OS which is kept updated with all necessary security patches to operate safely with Windows OS devices, such as servers. If an infected USB device is connected to the MFP, there is no mechanism by which a run file can be booted, so run file viruses have no effect.

Your data in safe hands

Data contained in internal HDDs is encrypted and can be password locked, so in the unlikely event that an HDD is removed, your data stays safe (this is an option on some devices). Data stored temporarily is overwritten page by page, making it impossible to output again. And finally, to prevent printed documents from being taken from the print tray by a third-party, use the secure print feature. Print will start after the password is entered on the MFPs operation panel.

Link to original article from NTT DATA

KONICA MINOLTA, INC.
2-7-2 Marunouchi Chiyoda-ku, Tokyo, Japan