NTT DATA SECURITY EVALUATION REPORT

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. Some customers are worried about scenarios where printers can be used as an easy point of access into company networks to wreak havoc and steal all kinds of data.

Konica Minolta provides customers with design specifications and internal test data that demonstrates how Konica Minolta MFPs are secure against attack, however we decided that having a third-party expert try and hack one of our leading line of 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 the best-selling bizhub i-Series MFPs.

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.

UP-TO-DATE & CERTIFIED. In addition to meeting the industry standard Common Criteria for IT security, ISO/IEC 15408, we further validate our printers through the bizhub SECURE service. Prior to sending a device to a client's network, bizhub SECURE configures the device with additional encryption and security settings. Together, the Common Criteria validation and the bizhub SECURE service enable us to assure customers that all our bizhub devices are highly secured.

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 storage media is encrypted and can be password locked, so in the unlikely event that an SSD/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.

VIEW FULL REPORT HERE

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446

CountOnKonicaMinolta.com