ERNW Newsletter 37 / November 2011

Security Reflections on Multifunction Devices

Version: 1.0

Date: 14.11.2011

Author: Michael Maria Schaefer (mschaefer@ernw.de)

ERNW Enno Rey Netzwerke GmbH

Breslauer Str. 28

69124 Heidelberg

Tel. +49 6221 480390

Fax +49 6221 419008

www.ernw.de

Inhaltsverzeichnis

1 INTRODUCTION

This Newsletter is a follow up on the talk[1] my colleague Matthias Luft (mluft@ernw.de) and I gave on this year's TROOPERS11[2] conference in Heidelberg. When we started digging into that topic we surprisingly discovered the topic to be almost exhaustively addressed over the last years. In line with this knowledge we decided to less focus on vulnerability research as such but more on developing a guideline for secure operation and reducing risk of Multifunction Devices (MFD) in a corporate environment. This newsletter describes how we approached the topic of MFD security, which results we ended up with and what we recommend in order to increase the security level of MFDs within a corporate environment.

1.1 Motivation

The motivation to deeply dig into the topic of MFD security as well as to give a talk on that topic was heavily driven by experiences we made during our daily business as security consultants and pentesters. While today almost every company operates a considerable amount of MFDs, security evaluations of the generic IT infrastructure (such as penetration tests) typically do not involve such devices as a considered target. However, due to the diversity of environments we approach in our daily business, we have been able to examine the role and application, MFDs are assigned in small, mid-range and large enterprises. It turned out, that the impact such devices may have for the overall security state, is seriously underestimated. Concrete projects, which actually just negligibly concentrated on such devices, revealed MFDs not only as - how we later used to name them - *aggregator of sensitive data*, but also as completely unrecognized concerning internal security and hardening processes.

The field of MFD security is far from unexplored. Quite the opposite is actually the case. Over the last decade several groups of researchers have shown, that the security state of MFDs is not sufficiently addressed by the vendors and thus secure operation requires additional effort when integrating such devices into productive environments. Meanwhile vendors offer security solutions and extensions which should be considered as mandatory, when sensitive data come into play. However, our experiences show that the significance of MFDs in business environments is threateningly underestimated. In our understanding this is due to lack of awareness concerning the sensitivity of processed data as well as due to missing hardening processes which include such devices.

It appears that MFDs are not understood as critical parts of the overall security. Since vulnerability research on MFDs has been exhaustively done over the last years, as well as meanwhile vendors addressed common security concerns, the lack of solutions does not hold as an explanation of what we found in practice. Consequently we will focus on highlighting the potential threads which can arise from an insufficiently hardened MFD, as well as on developing a structured approach which allows secure productive operation with a manageable risk level.

1.2 Multifunction Devices

The SANS Institute[3] defines MFDs as *"single devices that are not only printers, but also copiers, scanners and fax machines"*. In addition it is claimed, that *"these networked [...] devices are increasingly common in enterprise environments [...]"*. In fact the market share of MFDs has significantly increased over the last decade. Manifold fields of operation attract companies, as it becomes possible to fulfill several tasks which arise from daily office routines with a single device. Typically integration into existing administrative processes is easily possible due to the compatibility to established directory services like LDAP or Microsoft Active Directory.

[1] See http://www.troopers.de/wp-content/uploads/2011/04/TR11_Schaefer_Luft_Multifunction_devices.pdf.

[2] See http://www.troopers.de/troopers11.

[3] See http://www.sans.org/reading_room/whitepapers/networkdevs/auditing-securing-multifunction-devices_1921.

Even though a wide range of different models, offered by a lot of vendors is available on the market, almost all MFDs share the same properties. Since printing, scanning and faxing is the standard feature set today's MFDs implement, a printing unit, an image scanner, as well as a modem is typically part of such a device. However, more important for security related considerations are other components which unify modern MFDs, such as a network interface as well as typical PC parts like processor, RAM, flash drives and hard disks, which will turn out as a particularly critical part.

Concerning the software, most vendors chose embedded operating systems for their MFDs. Typically they provide a web-based front end for generic administration as well as for user-specific job control, meaning users can submit jobs, review scanned or printed documents, as well as manage stored files. Additional features like *scan-to-email* or *scan-to-fax* have become state of the art even for small office devices. Consequently the majority of MFDs is granted (at least limited) access to the internet as well.

In order to achieve a maximum level of integration into a manifold range of environments, MFDs support a wide variety of protocols which allow file transfer of actual documents on the one hand but also device management on the other hand. Thus, protocols like SMB, FTP, SMTP, POP3 are as well in place as are HTTP, Telnet, SNMP, etc. Obviously protocols for actual printing communication like IPP, JetDirect, PJL, PCL are part of the common feature set as well.

1.3 Role of MFDs in Corporate Networks

The classic purpose of a MFD is to unify typical tasks which arise in daily office operation in one machine. This applies for small businesses as well as for medium sized and large enterprises. Consequently such devices often show an enormous throughput of scanned and printed documents. In contrast to the legacy setup of having an average printer, shared only by a few people of one particular office, a MFD nowadays aggregates documents of a large group of people. Even inter-divisional usage isn't unusual.

Since processed documents usually are understood as non-public data, using MFDs is a critical business case. Access controls appear as a logical and mandatory mean of increasing the security level of operation. However, we rarely found such means in place when examining actual implementations in practice. The same applies for the segregation of devices according to the sensitivity of data which are processed. Dedicated and thus exclusive devices for higher management seems appropriate but is hardly implemented in productive environments.

Frame agreements with established vendors often accompany service contracts for corresponding devices. As maintenance is typically preferred to be done remotely (to reduce costs), this particular scenario may imply internet access for the MFDs or at least remote access by a specific machine, located somewhere within the corporate network and accessible by the manufacturer from the outside. Maintenance in general may also imply MFDs (or specific parts, such as a hard disk) leaving the company and thereby losing administrative control over the device. While the risk seems manageable at first glance, the situations impact changes if assuming that thousands of sensitive or even confidential documents remain on that particular device or hard disk.

2 Threats and Vulnerabilities

When talking about security, it is always important to approach certain assets in a structured way. Consequently it is indispensable to understand the security impact that arises when integrating MFDs into corporate networks. As we would like to raise awareness on such impact, we concentrate on highlighting and assessing threats and vulnerabilities which have been shown in the past, rather than on repeatedly proving such vulnerabilities for other models or vendors.

2.1 Methodology

In order to examine known vulnerabilities and rate their impact as well as to dig into such devices with our own methods we set up a lab, consisting of several MFDs from almost all established manufacturers. While looking into the software and the corresponding features on the one hand, we especially concentrated on threats which could arise from physical access. As already mentioned, the typical environment does not provide any access control to such devices. Consequently the scenario of a compromise due to physical access is much more likely as it is for dedicated servers or other systems, located in a separated computing center.

By means of methods used for a common web-application pentest we examined the web-interfaces, which were offered by all lab devices. Additional pentest techniques were used to dig into offered protocols as mentioned earlier. In addition we used methods like fuzzing to inspect the robustness of the implemented feature set as well as of the underlying operating system.

Special attention was given to such devices which were equipped with additional storage hardware like flash drives or hard disks. We checked for the effort necessary to remove or replace such storage devices and applied forensic techniques in order to get insight about data management and processing of sensitive data.

2.2 Vulnerabilities

As mentioned, vulnerability assessment has been done on MFDs for quite some years. Obviously we didn't want to blindly rely on corresponding results. The recent state of such devices could only be determined by validating known vulnerabilities, check if those have been fixed and of course by applying our own methods of vulnerability research. One doesn't anticipate too much if stating that the results were quite sobering.

As typical computer systems, MFDs are potentially vulnerable through all technologies and services implemented. Quite known and repeatedly demonstrated flaws include the following:

- Insufficient filtering / input validation on spoken protocols
- Default credentials
- *Phone home* features (maintenance, updates, etc…)
- Vulnerable web-interfaces (XSS, SQLi, authentication bypass, …)
- Vulnerable implementation of technologies and protocols (postscript, PJL)

```
Starting Nmap 5.51
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
9101/tcp open  jetdirect
9102/tcp open  jetdirect
9103/tcp open  jetdirect
```

A typical NMAP listing of a MFD

While we could confirm flaws on almost all sort of the above mentioned, we found an insufficient file management to reveal one of the most fragile aspect of MFDs in general. This topic will be particularly covered in section 2.4.

2.3 Arising Threats

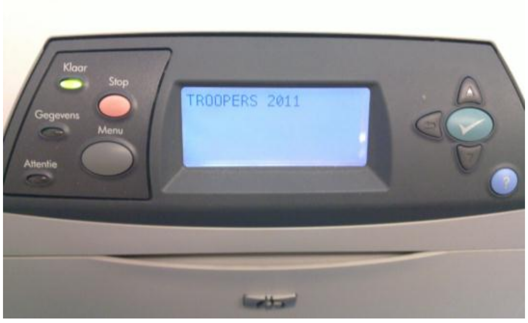
Potential threats are as multilateral as are the attack vectors. The obviously most critical scenario is a complete device compromise. The malicious attempts a potential attacker could raise, are almost endless. While the complete access to all documents processed with the MFD reveals all kind of sensitive data, a compromised device could also be used to give or send out manipulated documents of every kind. Without going too much into detail, one can imagine the potentially wide impact. Even though a complete compromise of a MFD is not observed to much in practice, it has to be emphasized that modern MFDs are nothing but an embedded PC with adjusted software for device control. After all it's just a PC with a potentially well-known but stripped down operating system, running a standard TCP/IP stack on standard hardware. Therefor one has to keep in mind, that vulnerabilities arising from such components may affect MFDs as well.

The typical usage scenario of a MFD implies physical access by a large and often uncontrolled group of users. Therefor the thread model of physical access has to be considered in more detail. Physical access may allow an attacker not only to change configuration parameters but also to remove or replace components (such as e.g. a hard disk). A case study, later demonstrated in this document, will illustrate potential risks which may occur as a result from accessing the hard disk.

The maybe most feared result of an exploited weakness in the IT infrastructure is an information disclosure scenario. Since MFDs' main task is to process documents, which often contain sensitive information, they appear as a highly endangered target to a corresponding attack. While insufficiently secured management interfaces may reveal documents or credentials of other users, software flaws like XSS will result in an equal scenario. In addition, inadequate hardening of the device results in multilateral ways of accessing sensitive data over various channels, such as FTP, PJL or HTTP.

As MFDs are fully adequate components of a corporate network, they're potentially vulnerable to eavesdropping on a network channel. As a result of unencrypted network traffic, an eavesdropping attacker may extract credentials, reconstruct processed documents or get in possession of stateful information, which allow stealing a session between a user and the MFD. As a consequence a compromised account could be used to steal sensitive information or as a starting point for further attempts (e.g. in order to completely compromise the device). Getting in possession of a privileged account could enable an attacker to change configuration, to extensively extract sensitive data or to create inconspicuous accounts for further attempts.

Last but not least the manipulation of a screen messages allows for abuse in a social engineering scenario. While simple deception of a malfunction just poses a negligible thread, the request to call a specific number could serve as a starting point for further social engineering attempts (such as credential fishing or even the supposed legalization of a hardware replacement, which again may result in further threads such as data leakage).



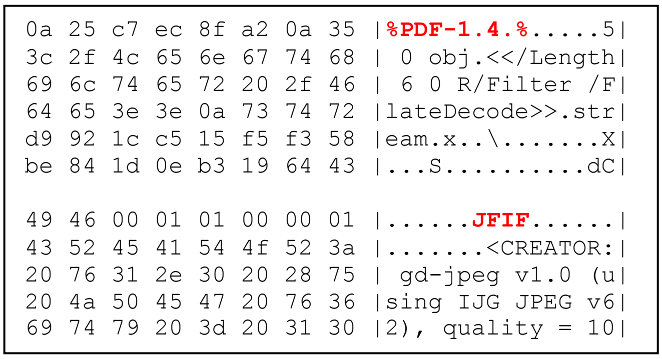
2.4 Case Study: Encryption & secure file deletion on built-in hard disks

Driven by a particular scenario we found in practice, we dug more deeply into the actual file management of MFDs. As mentioned, modern devices are equipped with standard hard disk, which are not only used for the operating system itself, but also to store scanned documents and to buffer data corresponding to print jobs and other tasks. At this point it should become clear, what the term of *aggregator of sensitive information* is all about.

But let's start at the beginning: As described above, all data which are to be processed by a MFD are potentially buffered somewhere on the device. Our investigation (unsurprisingly) revealed that in the majority of cases no dedicated flash-based (and thus volatile) memory is sued for that kind of caching, but data is buffered somewhere on the hard disk. The important detail to understand is, that once data is stored on a hard disk, it will remain on the disk as long as it is not explicitly and securely deleted or overwritten by other data. In other words: If an attacker can get in possession of such a hard disk he may be able to extract or recover an enormous amount of sensitive information, which have been processed by the device. To get an idea of the dimension we want to emphasize, that on one particular device we were able to recover all [sic!] documents which have been processed (meaning scanned or printed) by this MFD. Forensic examination of the hard disk revealed thousands of files going back 1,5 years up to the day the device had been setup.

An obvious countermeasure against information leakage in case of a removed or compromised hard disk is encryption. While several approaches for an according key management exist, it has to be stated, that the operational effort to maintain a considerable amount of MFDs and corresponding hard disk encryption keys may increase. However, it constitutes the most effective protection against unauthorized file access on a hard disk level. However, it turned out that none of the devices we investigated had file encryption in place. The alternative to a complete disk encryption is a secure delete mechanism, which makes sure that buffered data erased securely from the hard disk after it has been processed and is not necessary anymore. Even though that kind of protection does only hold for buffered data and will not help against extraction of data which is stored on purpose (such as scanned document stored in a personal document box). Unfortunately the previous described observation holds for a secure deletion mechanism as well. We were not able to confirm such a mechanism being in place on the devices we examined.

It appears that vendors are aware of the obvious attack vectors of build-in hard disks being removed or replaced. During our investigation we examined almost all vendors making use of so called *pseudo-file-systems*. That is, even though partitions could be detected, we were not able to detect known file systems, resulting in not being able to mount the partition for comfortable file management.



```
0a 25 c7 ec 8f a2 0a 35 |%PDF-1.4.%.....5|
3c 2f 4c 65 6e 67 74 68 | 0 obj.<</Length|
69 6c 74 65 72 20 2f 46 | 6 0 R/Filter /F|
64 65 3e 3e 0a 73 74 72 |lateDecode>>.str|
d9 92 1c c5 15 f5 f3 58 |eam.x..\.......X|
be 84 1d 0e b3 19 64 43 |...S..........dC|

49 46 00 01 01 00 00 01 |......JFIF......|
43 52 45 41 54 4f 52 3a |.......<CREATOR:|
20 76 31 2e 30 20 28 75 | gd-jpeg v1.0 (u|
20 4a 50 45 47 20 76 36 |sing IJG JPEG v6|
69 74 79 20 3d 20 31 30 |2), quality = 10|
```

File headers can be easily detected on raw device access

Even though further investigations revealed some of the *magic*, vendors put into such file systems in order to make them look non-standard, it is important to understand, that this particular effort does not add any security to the whole scenario, as long as data is still stored unencrypted and not deleted securely. Without going too much into inner details of file systems it can be stated, that the file systems job is mainly to arrange data in an efficient and robust way. In turn, data are still stored *as they are* (meaning typically in one piece) somewhere on the hard disk. What we miss when neglecting the file system type itself is the ability to actually manage and browse the data. However, it is still possible to operate on the raw device and the data stored on it. As files are masked by so called file-headers which identify the file type as well as reveal additional information, it is possible to scan the file for files we're interested in. In our particular case we concentrated on PDF and JPG files, as those are the common formats used to store processed documents. While this can be done with custom scripts, tools like *foremost*[4] exist, which implement the basic functionality on detection and recovery of known file types.

HDD disassembly

Additional investigation revealed the frighteningly minimal effort to get access to the inner hardware. As a result on optimized disassembly and maintenance processes, components such as hard disk or flash drives are located quite central and easily accessible. While some vendors at least hide those parts behind screwed covers, other vendors make use of screw-less, modular plug-in systems, which allow the removal or replacement within a few seconds. But even those old-fashioned screwed assemblies allow removing a hard disk within very few minutes. In other words: Once an attacker knows about the aspired model and has physical access he will be able to remove a corresponding hard disk though a few practiced movements. All in all the typical operational model of MFDs does not imply any means of physical security against hard disk removal at all.

All in all our investigations revealed tons of sensitive documents by means of very limited effort and a little bit of file system understanding. It can be stated, that professional forensic solutions may support and simplify the process, but at the bottom line they're not necessary for simple file recovery. In all cases we were able to recover documents which had been processed by that particular MFD, mostly retrieving highly sensitive and historical data of several months. This all was possible due to no measures being in place, such as file encryption or secure deletion.

Last but not least it has to be kept in mind, that in case of maintenance or hardware replacement, specific parts (hard disks in particular) might leave the company. As a result administrative and physical control is lost. Even though vendors guarantee the responsible handling or even elimination of such drives, replacement hardware has quite frequently been found available on the internet in the past. To avoid potential complication with data leakage resulting from replacement hardware it appears obvious, that appropriate encryption and secure deletion has to be enforced by the operating company instead of relying on vendors and service providers.

2.5 Additional Observations

Since we spent quite some time with our test-lab, we gained a *feeling* about robustness and handling of MFDs. Without going too much into detail, our summary about these properties can be entitled as *moderate*. For almost all devices we were able to observe arbitrary crashes and reboots. While for some devices these effects were even reproducible, some of our candidates showed completely undefined behavior and even complete system failures, which in one particular case were not repairable, not even after a complete system restart. In other words: The system broke just as a result of our research attempts (without touching the hardware at all of course). While these results do not influence the security state of such devices directly, they imply some notes on the quality of the corresponding software stacks. Again we want to raise awareness on these facts. Especially small and mid-size devices

[4] See http://foremost.sourceforge.net.

are not constructed for a long-lasting support window and lifetime support. The simple reality is, that they are constructed to be replaced within foreseeable future. This in turn implies evidence about long term support and quality assurance strategies by the vendors.

3 Sisters' Act of MFD Security

As mentioned, the goal of our work was to develop a tiny but straight catalog, which helps integrating MFDs in corporate environments in a secure way and which can hold as a guideline for secure operation. When it comes down to Information Security we often quote a catalog of cornerstones, which we at ERNW call *The Seven Sisters*. They form the framework of measures, recommendations and thoughts we believe to be essential on Information Security. Derived from this framework, the following *Sister's Act of MFD Security* is an adaptation to the special needs for secure MFD operation, which sums up the important aspects to mind, when integrating such devices into productive corporate environments.

3.1 Access Control

As the concept of physical access control is typically not a feasible one in daily work environments it appears obvious to even more concentrate on other access control measures. However, our experiences show quite the opposite. Privileged accounts were often accessible through **default passwords** and SNMP (which is almost always activated by default) communities could be read or even written by default **community strings** like *public* and *private*.

While LDAP or AD integration is easy and comfortable for personalized usage, local standard accounts for administration and maintenance often remain disregarded even though they're not necessarily overwritten by those managed through the directory service. It is quite not a pioneering security advice, however it has to be raised again and again, that every kind of default credentials has to be changed with those of an adequate security level. This implies even more for devices which are ready-to-use and thus implicate a *setup and forget* mentality. Well maintained user account and integration of a directory service do not help security wise, if the machine is accessible with a full privileged admin account with default credentials, which are stored locally.

3.2 Isolation

Even though difficulties of access control apply as well for isolation attempts, isolation can and should be done on the network layer. What is common standard on network infrastructure management should apply for MFDs as well. That's why we recommend managing and potentially even addressing such devices through a **dedicated VLAN**. This allows minimizing the attack surface or enables locking out potential attack vectors completely.

3.3 Restriction

Restriction in the context of MFDs can be understood in several ways and does not have to be applied directly or exclusively at the device itself. Implementing the above addressed isolation through dedicated VLANs, allows filtering **traffic** within this VLAN and to decide infrastructure-wise, which protocol is allowed to be spoken with the printer by whom. It is obvious that this decision cannot be maintained on a per-user basis, but different network segments can have different trust-levels and thus can be granted different **communication methods** with the device (keep in mind about external maintenance access or network segments for external employees). It has to be mentioned, that this kind of restriction does not necessarily have to be enforced through the infrastructure but through the MFD itself.

While restriction appears most meaningful in the context of communication methods, it is obvious, that this measure can be applied on different aspects of a MFD as well. User should be restricted to those **services** they really need and should not be granted all (potentially unknown) services available. Of course, the ideal approach here is to grant and not to restrict...

3.4 Encryption

While encryption is not the most obvious measure to apply for an MFD, it turned out to be the most important one. When examining the data management, we were negatively surprised on how easy it was to recover files. In combination with the even more scary state of physical security when it comes to protection of the actual hard drive, it becomes obvious, that data security has to be enforced at data creation. In order to avoid uncontrollable data leakage, files have to be encrypted when stored on the device. Especially the fact, that data remain on the device even though they have not intentionally been stored, requires secure data management, which can only be achieved through **data encryption**. Even though almost all enterprise level devices offer features like *ATA passwords* or *HDD encryption*[5], we never found these features activated in practice. Although encryption might imply additional effort on key management, it is worth to integrate such mechanisms.

What applies for data management should not be neglected on a network level. Almost all modern devices offer administrative access through remote connections. Since **encrypted and well authenticated protocols** like SSH are typically available, the secret on why not to enable such protocols by default but use those, which are proven to be insecure and outdated since decades remains at the vendors. Consequently the responsibility to dry out protocols like telnet (at least for their local network) is given to the administrative staff of the companies. Depending on how sensitive the processed data are, even transport encryption can become appropriate, especially if the data cross untrusted networks or infrastructure on their way to the MFD.

3.5 Hardening

What is common standard for productive systems like server and infrastructure components should apply for MFDs as well. Unfortunately it turned out to not be the case for the devices we examined in the wild. Due to the straight forward management and the reduced subset of features available, hardening of MFDs is a manageable venture. Even though MFDs offer a large range of **printing and communication protocols**[6], typically only a very reduced subset is really needed in the actual environment. Especially protocols like PJL, which offers device manipulation by design, should be evaluated in terms of necessity and deactivated if other protocols offer the same functionality. The same applies for administrative and remote management protocols and methods. Especially in the case of web interfaces (which are offered by all modern devices) it has to be evaluated if access is necessary and how it can be restricted to the user group actually requiring such access method.

While **replacement of default passwords** has already been mentioned, an important addition in the context of secure file management are features like **instant disk wiping** or **secure delete**, which ensure that data are securely erased after they have been buffered or processed. In case file/hdd encryption is not available on your device, secure delete can help to minimize the risk of data leakage. However one has to keep in mind, that it is not a fully adequate replacement for encryption, since it does not secure files, which have been stored on purpose (e.g. in personal folders or mailboxes).

Coming back to common standard on secure IT operation, appropriate **patch management** should be self-evident for MFDs as well. However we didn't saw those devices integrated in patch management processes at all. Even though potential vulnerabilities do not gain that much public attention, they can introduce even more noteworthy threats for a corporate environment.

It should have become clear, that the core of hardening is basically about **disabling unneeded features** to reduce the attack surface. Since not all potential features (like PXE, **-to-scan*, etc.) are covered in this article, the responsibility on comprehending and consequently disabling unnecessary functionalities remains at the administrative staff.

[5] This is at least available via additional modules.

[6] Which unfortunately are typically all enabled by default in order to ensure maximum integration and compatibility.

3.6 Secure Management

What has almost entirely been covered by the other *Sisters* can be summed up here again. It is important to understand, that management methods typically imply full privileged access to the according device. As hijacking or eavesdropping such a management session may imply a complete device compromise, it is important to protect such sessions through secure management method. Those imply **secure protocols** (e.g. HTTPS), usage of appropriate **network segmentation** (e.g. through VLANs) and **appropriate authentication** (e.g. by directory services).

3.7 Visibility

The last but not least important *Sister* addresses visibility and consequently traceability. While directory services introduce a certain (and important) amount of visibility, we found one similarly important aspect often to be neglected. **Logging** is often sensed as a - in several respects - resource-intensive process without too much valuable outcome. However the potential value is typically experienced (and then oftentimes missed) in case of a real incident. Therefor logging should be one of the most important and highly integrated processes of secure IT management. Needless to say, simple collection of log files doesn't gain any value at all. The value of a logging process increases with the amount invested in understanding log messages and filtering out important anomalies which may reveal early indicators on strange things happening in your corporate.

4 Conclusion

Our studies revealed a frighteningly low level of security awareness in the context of Multifunction Devices. While the comparatively little effort vendors invest to setup their devices with a basic level of security is not surprising, the lack of awareness about a MFD's role for the overall Information Security level of a company, raised significance on addressing this topic from an appropriate perspective. When rethinking the documents one has processed, meaning scanned, printed or faxed, with a MFD over the last year, it becomes clear why MFDs should be part of the overall risk assessment process.

Even though the variety of potential attack vectors on MFDs is quite large, solutions for almost all scenarios exist, which allow to minimize risk down to a manageable level. Over the last year, vendors have published hardening guides as well as developed security features like HDD encryption and secure deletion in order to address common threats in a corporate environment. Without disturbing daily work processes it becomes possible, to securely operate such devices by simply evaluating concrete needs and adapting the feature set of the present device appropriately. Understanding MFDs as *aggregators of sensitive data* implies a certain mindset, which allows to adequately realize potential threats which arise from careless integration.

The *Sister's Act of MFD Security* provides a framework on secure operation and management, based on a cornerstone-like catalog which allows addressing certain threats accordingly. The *Sister's Act of MFD Security* consequently helps to raise awareness on why it is important to integrate MFDs in established hardening processes such as patch management, secure management and logging and monitoring.

5 FURTHER READING

- http://www.sans.org/reading_room/whitepapers/networkdevs/auditing-securing-multifunction-devices_1921
- http://www.konicaminolta.co.uk/fileadmin/CONTENT_local/Business_Solutions/Press-Office/White-Papers/Fundamentals-of-Security.pdf
- http://www.hp.com/united-states/business/catalog/nist_checklist.pdf
- http://www.troopers.de/wp-content/uploads/2011/04/TR11_Schaefer_Luft_Multifunction_devices.pdf
- http://its.dal.ca/depts/security/events/canheit2007/mfds.pdf