FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-forensische Untersuchung einer S7-1500

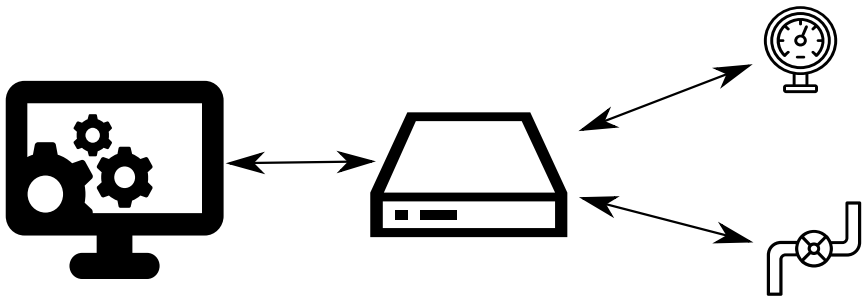
Cornelius Hons

07.06.2017

Inhaltsverzeichnis

Begriffserklärung

- Speicherprogrammierbare Steuerung (SPS)
- Gerät zur Steuerung und Kontrolle von Anlagen
- SPS verbunden mit Sensoren und Aktoren



Motivation

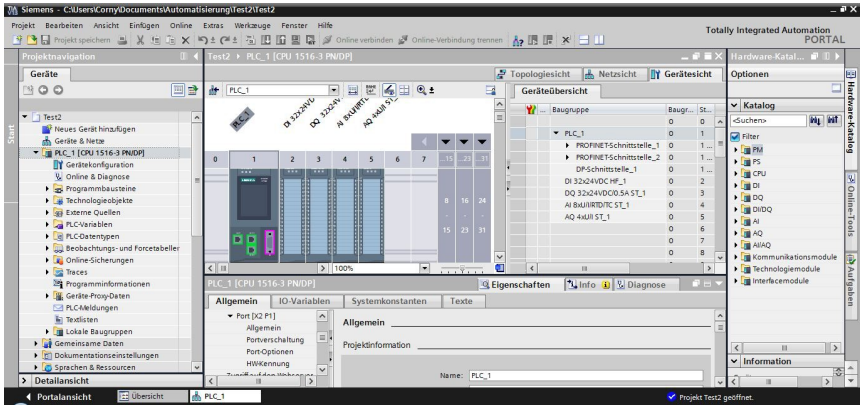
- SPS vermehrt über andere Geräte des Firmennetzes erreichbar
- Angriffe könnten in Zukunft zunehmen
- Forensische Auswertung der Angriffe gewinnt ebenfalls an Bedeutung

Details zur SPS

- S7-1500 von Siemens
- 1516-3 PN/DP (6ES7 516-3AN01-0AB0)
- Erscheinungsdatum 2013
- Proprietäres Betriebssystem
- Schnittstellen
  - 2x Profinet
  - 1x Profibus

TIA Portal

- Totally Integrated Automation Portal
- Version V13 SP1 Update 9
- Step-7 Professional
  - Programmierung von SPSs der S7 Baugruppe
- WinCC Advanced
  - Automatisierungsprozesse visualisieren



Untersuchung des verbundenen PC´s

- Speicherorte der Software
  - C:\Program Files\Siemens
  - C:\ProgramData\Siemens (versteckt)
  - C:\Program Files\Common Files\Siemens
- Speicherorte der Projekte
  - C:\User\<Benutzer>\My Documents\Automatisierung\
  - <Projekt-Name>.info enthält Name des Benutzers, der Projekt aktuell geöffnet hat

Untersuchung des verbundenen PC´s

- Registry
  - HKEY_CURRENT_USER\Software\SIEMENS\
  - HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\
  - Version und Sprache der Softwarekomponenten

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
{C8A94EBE-6C1...	REG_SZ	V13.00.01.09_07.01.00.01
Company	REG_SZ	Siemens AG
CreationDate	REG_SZ	2014.12.17
DeliveryLangua...	REG_SZ	1031;1033;3082;1036;1040;2052;1033,1031;1041;
Msp_Active	REG_SZ	STEP7V13_upd_V13.00.01.09_07.01.00.01_{7183D762-1D8D-46
Path	REG_SZ	C:\Program Files\Siemens\Automation\Portal V13\
ProdGroup	REG_SZ	Siemens TIAP
ProdType	REG_SZ	
ProductName	REG_SZ	Siemens Totally Integrated Automation Portal V13 - STEP 7
Release	REG_SZ	V13.00.01.09_07.01.00.01
SetupType	REG_SZ	EDITION_CLIENT
TechnVersion	REG_SZ	V13.00.01.09
Version	REG_SZ	13.00.0100
VersionString	REG_SZ	V13.0 SP1 UPD9

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
Applications	REG_SZ	GERMAN,ENGLISH,FRENCH,SPANISH,ITALIAN,JAPANESE,CHINESE

Untersuchung des verbundenen PC´s

- Logfiles
  - C:\ProgramData\Siemens\Automation\Logfiles
  - Informationen
    - Ablauf der Installation
    - Hardware des PCs

```
------------------------------------ System Information ------------------------------------
12:08:14|          |RAM Size                          |2.00 GB
12:08:14|          |Processor 1                       |Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz
12:08:14|          |Processor 2                       |Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz
12:08:14|          |Computer name                     |CORNY-PC
12:08:14|          |Space Info on Drive: C:\ (NTFS)   |Total Space: 49.90 GB  Used space: 33.95 GB
12:08:14|          |OSVersion                         |OS Version : 6.1.7601.2
12:08:14|          |OSVersion                         |Major Version : 6
12:08:14|          |OSVersion                         |Minor Version : 1
12:08:14|          |OSVersion                         |Product Type : 1
12:08:14|          |System Language                   |German (1031)
12:08:14|          |UI Language                       |German (1031)
```

Untersuchung des verbundenen PC´s

- Prozesse
  - 13 Prozesse
  - Step-7, WinCC, OPC und Automation License Manager

Untersuchung des verbundenen PC´s

Prozess	Nur aktiv wenn TIA Portal aktiv
Siemens.Automation.ObjectFrame.FileStorage.Server.exe	nein
Siemens.Automation.SoftwareUpdater.exe	nein
Siemens.Automation.Portal.exe	ja
s7otbxsx.exe	ja
ALMPanelPlugin.exe	nein
almsrvx.exe	nein
SmartServer.exe	nein
s7oiehsx.exe	nein
pniomgr.exe	nein
s7epasrv32x.exe	nein
S7TraceServiceX.exe	nein
s7oPNDiscoveryx.exe	nein
Opc.Ua.DiscoveryServer.exe	nein

Kommunikation

- Portscan mit Nmap:

  „nmap -p - -T4 -A -v 192.168.0.10“

- Port 80 (http)

- Port 443 (https)

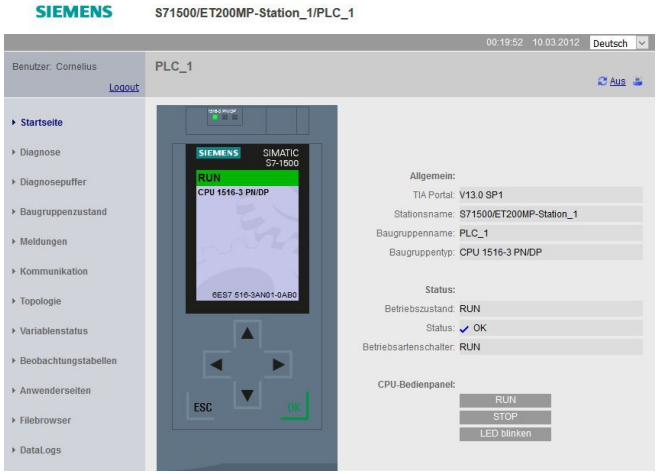
- Port 102 (Connection Oriented Transport Protocol)

Connection Oriented Transport Protocol

- Paket-basiert
- Weitere Untersuchungen mit Wireshark
- COTP auf TPKT auf TCP
- TPKT „emuliert“ COTP auf TCP

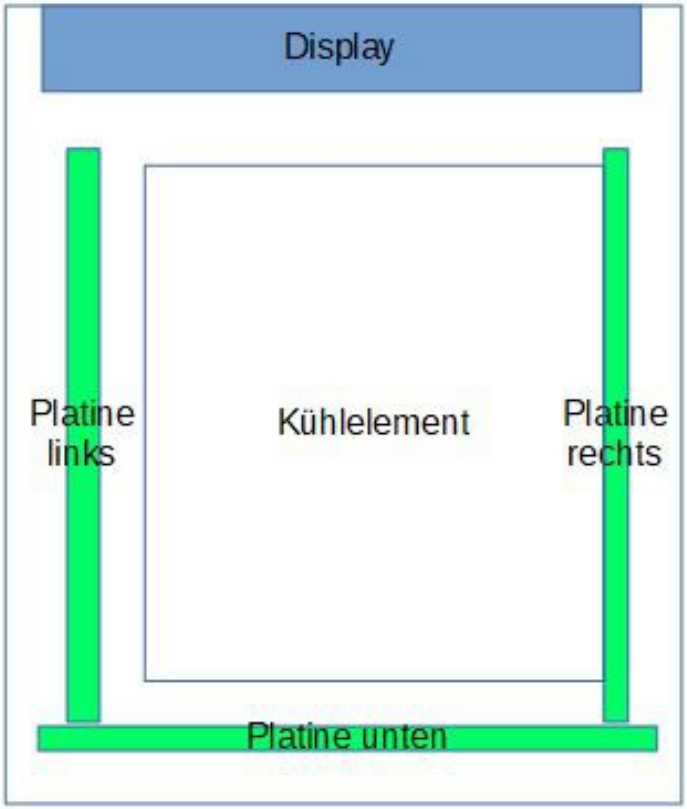
Webserver

- Informationen über
  - SPS und Input/Output-Module
  - Schnittstellen



- Ausgabe von Variablen
- MiniWeb Server Language kompatibel
- Anwenderseite (CSS und Javascript kompatibel)

Hardware



- NDA auf Datenblätter der Speicher-Chips

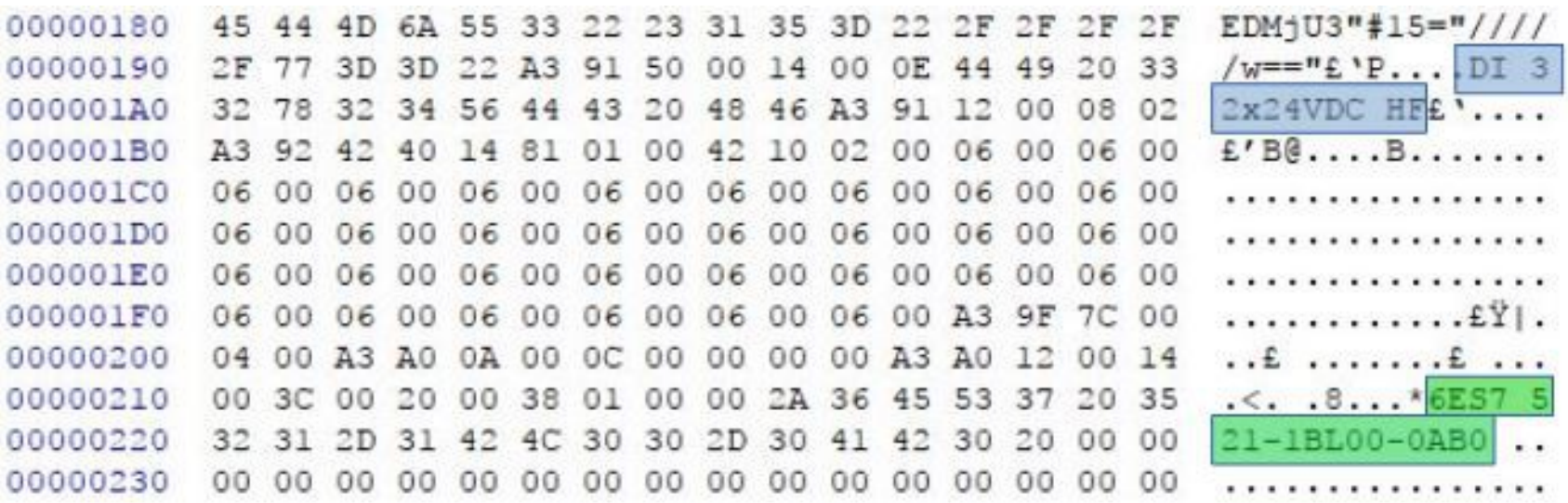
Speicherkarte

- SPS ohne Speicherkarte nicht lauffähig
- 24MB
- FAT32
- Variablennamen des Programms in ASCII
- Produktnummern der Module in ASCII
- HTML-Quellcode der Anwenderseite in ASCII
- Dateien mit Infos zu den Benutzern

Speicherkarte
Variablennamen

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000   A6 92 00 00 01 00 AC 00 1B 04 74 65 73 74 00 07  ¦'....¬...test..
00000016   61 75 73 67 61 62 65 00 03 6D 6F 64 00 05 63 6C  ausgabe..mod..cl
00000032   6F 63 6B 00 00 00 A6 90 01 00 00 00 AC 00 15 05  ock...¦.....¬...
00000048   54 61 67 5F 32 00 05 54 61 67 5F 34 00 05 54 61  Tag_2..Tag_4..Ta
00000064   67 5F 35 00 00 00 A6 90 02 00 00 00 AC 00 07 05  g_5...¦.....¬...
00000080   54 61 67 5F 33 00 00 00 A6 90 03 00 00 00 AC 00  Tag_3...¦.....¬.
00000096   77 0A 43 6C 6F 63 6B 5F 42 79 74 65 00 0A 43 6C  w.Clock_Byte..Cl
00000112   6F 63 6B 5F 31 30 48 7A 00 09 43 6C 6F 63 6B 5F  ock_10Hz..Clock_
00000128   35 48 7A 00 0B 43 6C 6F 63 6B 5F 32 2E 35 48 7A  5Hz..Clock_2.5Hz
00000144   00 09 43 6C 6F 63 6B 5F 32 48 7A 00 0C 43 6C 6F  ..Clock_2Hz..Clo
00000160   63 6B 5F 31 2E 32 35 48 7A 00 09 43 6C 6F 63 6B  ck_1.25Hz..Clock
00000176   5F 31 48 7A 00 0D 43 6C 6F 63 6B 5F 30 2E 36 32  _1Hz..Clock_0.62
00000192   35 48 7A 00 0B 43 6C 6F 63 6B 5F 30 2E 35 48 7A  5Hz..Clock_0.5Hz
```

Speicherkarte
Produktnummer Modul



00000180	45	44	4D	6A	55	33	22	23	31	35	3D	22	2F	2F	2F	2F	EDMjU3"#15="////
00000190	2F	77	3D	3D	22	A3	91	50	00	14	00	0E	44	49	20	33	/w=="£'P....DI 3
000001A0	32	78	32	34	56	44	43	20	48	46	A3	91	12	00	08	02	2x24VDC HF£'....
000001B0	A3	92	42	40	14	81	01	00	42	10	02	00	06	00	06	00	£'B@....B.......
000001C0	06	00	06	00	06	00	06	00	06	00	06	00	06	00	06	00	.....
000001D0	06	00	06	00	06	00	06	00	06	00	06	00	06	00	06	00	.....
000001E0	06	00	06	00	06	00	06	00	06	00	06	00	06	00	06	00	.....
000001F0	06	00	06	00	06	00	06	00	06	00	06	00	A3	9F	7C	00	.....£Ÿ|.
00000200	04	00	A3	A0	0A	00	0C	00	00	00	00	A3	A0	12	00	14	..£ .....£ ...
00000210	00	3C	00	20	00	38	01	00	00	2A	36	45	53	37	20	35	.<. .8...*6ES7 5
00000220	32	31	2D	31	42	4C	30	30	2D	30	41	42	30	20	00	00	21-1BL00-0AB0 ..
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

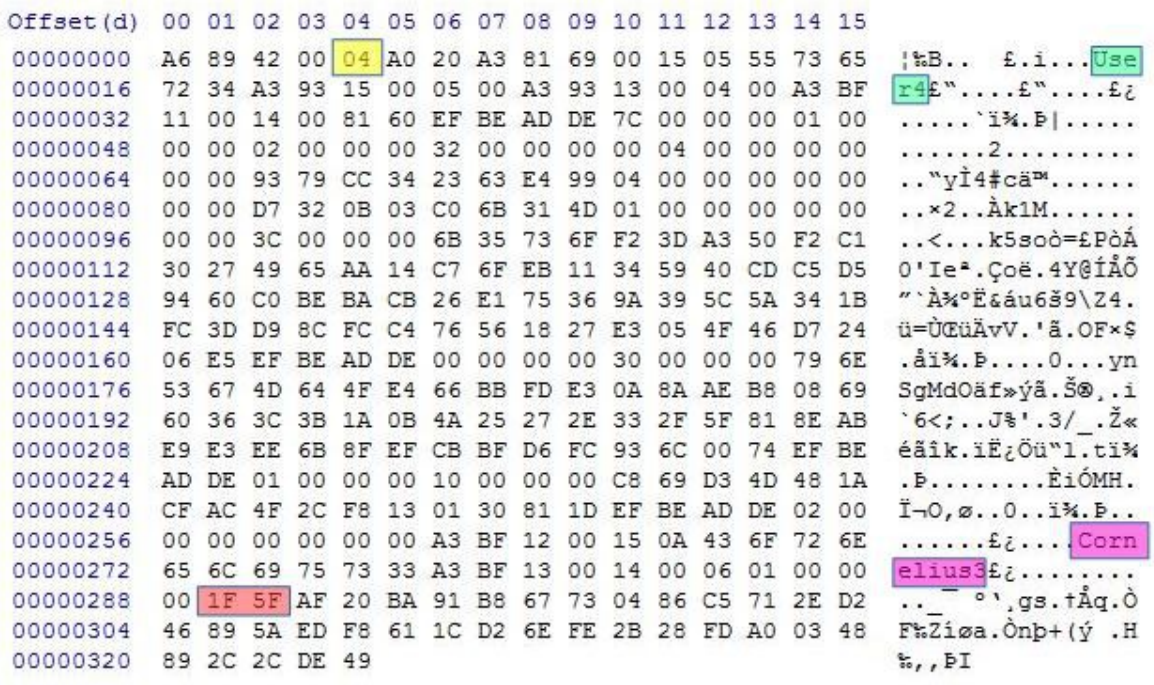
– Modulname

– Produktnummer

Speicherkarte
Anwenderseite Quellcode

```
00000400  41 5B 3C 21 44 4F 43 54 59 50 45 20 68 74 6D 6C  A[<!DOCTYPE html
00000410  3E 0D 0A 0D 0A 3C 68 74 6D 6C 3E 0D 0A 09 3C 68  >....<html>...<h
00000420  65 61 64 3E 0D 0A 09 09 3C 74 69 74 6C 65 3E 41  ead>....<title>A
00000430  6E 77 65 6E 64 65 72 73 65 69 74 65 3C 2F 74 69  nwenderseite</ti
00000440  74 6C 65 3E 0D 0A 09 3C 2F 68 65 61 64 3E 0D 0A  tle>...</head>..
00000450  09 0D 0A 09 3C 62 6F 64 79 3E 0D 0A 09 09 3C 68  ....<body>....<h
00000460  31 3E 41 6E 77 65 6E 64 65 72 73 65 69 74 65 3C  1>Anwenderseite<
00000470  2F 68 31 3E 0D 0A 09 09 0D 0A 09 09 46 65 68 6C  /h1>........Fehl
00000480  65 72 20 41 75 73 67 61 62 65 20 28 49 6E 74 2C  er Ausgabe (Int,
00000490  20 30 20 6B 65 69 6E 20 46 65 68 6C 65 72 29 3A   0 kein Fehler):
000004A0  20 3C 74 64 20 63 6C 61 73 73 3D 22 6F 75 74 70   <td class="outp
000004B0  75 74 20 66 69 65 6C 64 22 3E 3A 3D 22 44 61 74  ut field">:="Dat
000004C0  65 6E 62 61 75 73 74 65 69 6E 5F 31 22 2E 61 75  enbaustein_1".au
000004D0  73 67 61 62 65 3A 3C 2F 74 64 3E 3C 62 72 3E 0D  sgabe:</td><br>.
000004E0  0A 09 09 43 6C 6F 63 6B 3A 20 3C 74 64 20 63 6C  ...Clock: <td cl
000004F0  61 73 73 3D 22 6F 75 74 70 75 74 20 66 69 65 6C  ass="output fiel
00000500  64 22 3E 3A 3D 22 44 61 74 65 6E 62 61 75 73 74  d">:="Datenbaust
00000510  65 69 6E 5F 31 22 2E 63 6C 6F 63 6B 3A 3C 2F 74  ein_1".clock:</t
00000520  64 3E 3C 62 72 3E 0D 0A 09 09 44 42 20 33 33 33  d><br>....DB 333
00000530  20 54 65 73 74 3A 3C 74 64 20 63 6C 61 73 73 3D   Test:<td class=
00000540  22 6F 75 74 70 75 74 20 66 69 65 6C 64 22 3E 3A  "output field">:
00000550  3D 22 44 42 20 33 33 33 22 2E 64 62 5F 76 65 72  ="DB 333".db_ver
00000560  73 69 6F 6E 3A 3C 2F 74 64 3E 3C 62 72 3E 0D 0A  sion:</td><br>..
```

Speicherkarte
Benutzerdatei



Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
00000000	A6	89	42	00	04	A0	20	A3	81	69	00	15	05	55	73	65	¦‰B.. £.i...Use
00000016	72	34	A3	93	15	00	05	00	A3	93	13	00	04	00	A3	BF	r4£“....£“....£¿
00000032	11	00	14	00	81	60	EF	BE	AD	DE	7C	00	00	00	01	00	.....`ï¾.Þ|.....
00000048	00	00	02	00	00	00	32	00	00	00	00	04	00	00	00	00	......2.........
00000064	00	00	93	79	CC	34	23	63	E4	99	04	00	00	00	00	00	..“yÌ4#cä™.....
00000080	00	00	D7	32	0B	03	C0	6B	31	4D	01	00	00	00	00	00	..×2..Àk1M.....
00000096	00	00	3C	00	00	00	6B	35	73	6F	F2	3D	A3	50	F2	C1	..<...k5soò=£PòÁ
00000112	30	27	49	65	AA	14	C7	6F	EB	11	34	59	40	CD	C5	D5	0'Ieª.Çoë.4Y@ÍÅÕ
00000128	94	60	C0	BE	BA	CB	26	E1	75	36	9A	39	5C	5A	34	1B	”`À¾ºË&áu6š9\Z4.
00000144	FC	3D	D9	8C	FC	C4	76	56	18	27	E3	05	4F	46	D7	24	ü=ÙŒüÄvV.'ã.OF×$
00000160	06	E5	EF	BE	AD	DE	00	00	00	00	30	00	00	00	79	6E	.åï¾.Þ....0...yn
00000176	53	67	4D	64	4F	E4	66	BB	FD	E3	0A	8A	AE	B8	08	69	SgMdOäf»ýã.Š®¸.i
00000192	60	36	3C	3B	1A	0B	4A	25	27	2E	33	2F	5F	81	8E	AB	`6<;..J%'.3/_.Ž«
00000208	E9	E3	EE	6B	8F	EF	CB	BF	D6	FC	93	6C	00	74	EF	BE	éãîk.ïË¿Öü“l.tï¾
00000224	AD	DE	01	00	00	00	10	00	00	00	C8	69	D3	4D	48	1A	.Þ.........ÈiÓMH.
00000240	CF	AC	4F	2C	F8	13	01	30	81	1D	EF	BE	AD	DE	02	00	Ï¬O,ø..0..ï¾.Þ..
00000256	00	00	00	00	00	00	A3	BF	12	00	15	0A	43	6F	72	6E	......£¿....Corn
00000272	65	6C	69	75	73	33	A3	BF	13	00	14	00	06	01	00	00	elius3£¿........
00000288	00	1F	5F	AF	20	BA	91	B8	67	73	04	86	C5	71	2E	D2	.._¯ º‘¸gs.†Åq.Ò
00000304	46	89	5A	ED	F8	61	1C	D2	6E	FE	2B	28	FD	A0	03	48	F‰Zíøa.Ònþ+(ý .H
00000320	89	2C	2C	DE	49												‰,,ÞI

– Nummer

- Benutzername

– Nummer in ASCII

- Benutzerrechte

Speicherkarte
Benutzer-Rechte

1F 5F

0001 1111 0101 1111

- Jedes Bit steht für ein Recht
- Ist ein Bit 1, hat der Benutzer dieses Recht

Speicherkarte
Benutzer-Rechte

Der Benutzer ist autorisiert...	Bit
...die Diagnose abzufragen	0000 0000 0000 0001
...die Variablen zu lesen	0000 0000 0000 0010
...die Variablen zu schreiben	0000 0000 0000 0100
...den Variablenstatus zu lesen	0000 0000 0000 1000
...den Variablenstatus zu schreiben	0000 0000 0001 0000
...Meldungen zu quittieren	nicht auswählbar
...anwenderdefinierte Seite aufzurufen	0000 0000 0100 0000
...in anwenderdefinierte Seite zu schreiben	0000 0000 1000 0000
...Dateien zu lesen	0000 0001 0000 0000
...Dateien zu schreiben/löschen	0000 0010 0000 0000
...den Betriebszustand zu ändern	0000 0100 0000 0000
...die LED blinken zu lassen	0000 1000 0000 0000
...ein Firmware-Update durchzuführen	0001 0000 0000 0000
Systemparameter ändern	nicht auswählbar
Anwendungsparameter ändern	nicht auswählbar

Speicherkarte
Benutzer-Rechte

- Benutzerrechte nicht einfach änderbar
- Letzten 32-Byte vermutlich Prüfsumme
- Abhängigkeit von Benutzername, Nummer und Name der Datei
- Dateinamen variabel, Dateipfade konstant

Zusammenfassung

- Erkennung von
  - schädlichen Prozessen
  - manipulierter Anwenderseite
  - falschen Variablen und falschen Werten von Variablen
  - manipulierten Benutzern des Webservers

Vielen Dank für ihre Aufmerksamkeit

Quellen

Icons made by Madebyoliver from www.flaticon.com is licensed by "Creative Commons BY 3.0"

Icons made by Freepik from www.flaticon.com is licensed by "Creative Commons BY 3.0"

Icons made by Vaadin from www.flaticon.com is licensed by "Creative Commons BY 3.0"

https://mall.industry.siemens.com/collaterals/files/42/jpg/P_ST70_XX_06248i.jpg