TÜV SÜD AG Honeynet

Technische Beschreibung

23.07.2015

1 Inhalt

2 Virtuelle Standorte

Drei logische Standorte, haben einzelne IP Adressbereiche, FW01 bietet diese nach außen so an, dass die drei Bereiche wie unterschiedliche Netze erscheinen (TTL Werte und Paketlaufzeiten werden entsprechen durch Einstellungen auf FW01 geändert)

3 Systeme

3.1 ROUTER01

3.1.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Fa0/0	212.114.128.129		Internes Netz 1
Fa0/1	212.114.130.97	255.255.255.240	Internes Netz 2
Ser0/0	212.104.101.74	255.255.255.240	Anbindung zu M-Net

3.1.2 Hardware

- bei Ebay gekauft, CISCO Router, Anbindung WAN-Seite X.21, 2 Mbit, geht auf das Modem von M-Net

3.1.3 Betriebssystem

- CISCO IOS

3.1.4 Rollen und Funktionen

- Schickt syslog und Netflow Version 5 Daten an Logserver (SERVER01)
- ACLs konfiguriert für Eigenschutz, keine Firewall-Funktion für das Honeynet

Aufgabe des Routers ist es, den Internet-Anschluss von MNet auf zwei, nach den beiden von MNet bezogenen Adressbereichen, intern über zwei Ethernet-Schnittstellen zur Verfügung zu stellen. Der Router besitzt auf des WAN-Seite eine X.21 Schnittstelle mit 2 Mbit und auf der LAN-Seite zwei Ethernet-Schnittstellen mit jeweils 10 Mbit.

Der Router loggt die Zugriffe, die über die lokalen ACLs protokolliert werden und schickt diese über einen NAT-Adresse per Syslog an SERVER01. Das NAT erfolgt dabei auf FW01.

Zudem generiert der Router aus dem Verkehr über seine Netzwerkschnittstellen Netflow Version 5 Daten, die er an den auf Server01 laufenden Flow-Kollektor sendet. Der Versand erfolgt dabei ähnlich wie bei Syslog über eine öffentliche IP-Adresse, die auf FW01 auf die interne Adresse von SERVER01 genattet wird.

3.2 Firewall FW01

3.2.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	10.0.1.1	255.255.255.0	Admin-LAN
Eth1	192.168.0.1	255.255.240.0	Honeynet
Eth2	192.168.84.2	192.168.84.255	TÜV SÜD Labornetz mit DSL-Anschluss
Eth3			Frei
Eth4	10.0.2.1	255.255.255.0	VPN-Zugang, zu FW03

Eth5	10.0.3.1	255.255.255.0	VPN-Zugang, zu FW03
Eth6	212.114.128.130	255.255.255.240	M-Net, zu Router01, phy. IP der FW
Eth6:1	212.114.128.131	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:2	212.114.128.132	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:3	212.114.128.133	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:4	212.114.128.134	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:5	212.114.128.135	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:6	212.114.128.136	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:7	212.114.128.137	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:8	212.114.128.138	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:9	212.114.128.139	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:10	212.114.128.140	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:11	212.114.124.141	255.255.255.240	M-Net, zu Router01, für NAT
Eth6:12	212.114.124.142	255.255.255.240	M-Net, zu Router01, für NAT
Eth7	212.114.130.98	255.255.255.240	M-Net, zu Router01, phy. IP der FW
Eth7:1	212.114.130.99	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:2	212.114.130.100	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:3	212.114.130.101	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:4	212.114.130.102	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:5	212.114.130.103	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:6	212.114.130.104	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:7	212.114.130.105	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:8	212.114.130.106	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:9	212.114.130.107	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:10	212.114.130.108	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:11	212.114.130.109	255.255.255.240	M-Net, zu Router01, für NAT
Eth7:12	212.114.130.110	255.255.255.240	M-Net, zu Router01, für NAT

3.2.2 Hardware

- Nexcom NSA3130-C8
- 8 Ethernet-Schnittstellen 10/100/1000
- 4 GB RAM
- Festplatte 250 GB SATA-2

3.2.3 Betriebssystem

- secXtreme Generische Security Appliance Release 5.0

3.2.4 Software

- ngrep
- whois
- Erweiterungen der Firewall für das Honeynet
- QoS Erweiterungen der Firewall

3.2.5 Rollen und Funktionen

- Kontrolliert den Zugriff auf das Honeynet
- Generische Security Appliance Version 5.0 von secXtreme
- Mechanismen für Notabschaltung
- Layer 3 Firewall

- NAT
- Fortgeschrittenes Routing anhand von Policy-Routing (es wird mit verschiedenen Routing-Tabellen gearbeitet)
- Sendet die Logdaten per Syslog auf SERVER01
- Holt sich per NTP die Zeit von SERVER01
- Sendet E-Mails an SERVER01

3.3 Firewall FW02

3.3.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	10.0.1.2	255.255.255.0	Admin-LAN
Eth1			Transparentes Layer-2 Interface zu FW01
Eth2			Transparentes Layer-2 Interface zu Switch
Eth3			Frei
Eth4			Frei
Eth5			Frei
Eth6			Frei
Eth7			Frei

3.3.2 Hardware

- Nexcom NSA3130-C8
- 8 Ethernet-Schnittstellen 10/100/1000
- 4 GB RAM
- Festplatte 250 GB SATA-2

3.3.3 Betriebssystem

- secXtreme Generische Security Appliance Release 5.0

3.3.4 Software

- Snort IDS (scxt-idsipssensor, scxt-barnyard2, scxt-idsipstools, scxt-libdaq, scxt-libdnet, scxt-snort 2.9.6.0) (paketiert und zur Verfügung gestellt von secXtreme)
- Erweiterungen der Firewall für das Honeynet

3.3.5 Rollen und Funktionen

- Nicht als FW eingesetzt, sondern inline als IPS (snort) transparent auf Layer-2
- Es werden aber aktiv keine Pakete geblockt (daher Inline-IDS)
- Aufgesetzt auf die generische Security Appliance Version 5.0 von secXtreme
- Mechanismen zur Notabschaltung
- IPS (snort) reportet in die Datenbank auf APPLIANCE01
- Sendet die Logdaten per Syslog auf SERVER01
- Holt sich per NTP die Zeit von SERVER01
- Sendet E-Mails an SERVER01

3.4 Firewall FW03

3.4.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Port 1	10.0.2.2	255.255.255.0	An FIREWALL01 Port eth4
Port 2	Frei		
Port 3	10.0.3.2	255.255.255.0	An FIREWALL01 Port eth5
Port 4	Frei		

3.4.2 Hardware

- Endian Firewall
- Desktop-Bauform

3.4.3 Rollen und Funktionen

- VPN Gateway für Out of band Administration

Diese Firewall stellt das VPN für den Out-of-Band Zugang zum Honeynet zur Verfügung. Die Firewall selbst ist mit ihren zwei Schnittstellen an der FW01 angeschlossen, die den eingehenden und ausgehenden Verkehr kontrolliert. FW03 sorgt primär nur für die Terminierung des VPN-Tunnels. Als Protokoll kommt dabei OpenVPN auf der Basis von SSL zum Einsatz. Die Authentifizierung erfolgt dabei mit Zertifikaten. Auf den Clients läuft dazu entsprechend ein OpenVPN-Client.

Der Zugang war eingerichtet für ein Notebook von TÜV SÜD Rail und für ein Notebook von secXtreme.

3.5 Switch SWITCH01

3.5.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
LAN	192.168.0.254	255.255.255.0	Admin-Interface im Honeynet

3.5.2 Portbelegung

Port	Gerät	Beschreibung
1	Frei	
2	HUB01	
3	Frei	
4	APPLIANCE01 eth1	honeyBox im Honeynet
5	Frei	
6	Frei	
7	Frei	
8	Frei	
9	Frei	
10	Frei	
11	Frei	
12	Frei	
13	Frei	
14	Frei	
15	Frei	
16	Frei	
17	Frei	
18	Frei	

19	Frei	
20	Frei	
21	Frei	
22	Frei	
23	SWITCH02 Port 1	
24	FIREWALL02 eth2	Administration Firewall
25	SERVER02	GBIC Kupfer
26	Frei	GBIC Kupfer

3.5.3 Hardware

- CISCO 3750-24 Serie

3.5.4 Betriebssystem

- CISCO IOS Version 1.2(20)SE4

3.5.5 Rollen und Funktionen

- Folgende Geräte des Honeynets sind daran angeschlossen:
  - Drei SPS S7-1200 von Siemens
  - FW02
  - APPLIANCE01 (honeyBox) mit Interface eth1
  - SERVER01 über Monitorport des SWITCH01
  - SERVER02

Der Switch bildet zudem VLANs ab. Das Administrationsinterface mit der Adresse 10.0.1.60 liegt dabei im VLAN 10. Der Switch ist per Telnet aus dem Adminnetz erreichbar.

3.6 HUB01

3.6.1 Portbelegung

Port	Gerät	Beschreibung
1	Frei	
2	Frei	
3	SWITCH02 Port 2	
4	Frei	
5	SPS02	
6	SERVER02	
7	SPS01	
8	SPS03	

3.6.2 Hardware

- 3COM OfficeConnect HUB/TPO

3.6.3 Rollen und Funktionen

Der Hub ermöglicht das Sniffen des Verkehrs zwischen den SPS Geräten. Der Cisco Switch SWITCH01 konnte leider mit den Multicast-Adressen des Netzwerks keine komplette Ausleitung des Verkehrs ermöglichen, so dass zu diesem Hub gegriffen werden musste.

3.7 WASSER-GW03 (virtuell auf SERVER02)

3.7.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung

Eth0	192.168.0.5	255.255.0.0	
Eth1	10.0.5.2	255.255.255.0	

3.7.2 Hardware

- Virtualisiert auf SERVER02
- 1GB RAM

3.7.3 Betriebssystem

- Ubuntu 14.04.1 LTS

3.7.4 Software

- Apache2 mit Konfiguration durch TÜV SÜD als HTTPS Reverse Proxy

3.7.5 Rollen und Funktionen

- Reverse Proxy, um HTTPS-Anfragen an die SPSen in http zu wandeln und an die SPSen weiter zu senden, damit der Verkehr mitgelesen werden kann

3.8 WASSER-MGMT01 (virtuell auf SERVER02)

3.8.1 Hardware

- Virtualisiert auf SERVER02
- 1GB RAM

3.8.2 Rollen und Funktionen

Das System war nicht im aktiven Aufbau des Honeynets aktiv und ist herunter gefahren.

3.9 WASSER-MGMT02 (virtuell auf SERVER02)

3.9.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	10.0.1.22	255.255.0.0	

3.9.2 Hardware

- Virtualisiert auf SERVER02
- 1GB RAM

3.9.3 Betriebssystem

- Ubuntu 14.04.1 LTS

3.9.4 Software

- Apache2
- Nprobe
- Pfring

3.9.5 Rollen und Funktionen

- Auswertung der Netflow-Daten mit ntop (wurde aber wegen der Auswertung mit iSILK nicht weiter genutzt)

3.10 SCADA01 (virtuell auf SERVER02)

3.10.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
LAN	192.168.0.20	255.255.255.0	

3.10.2 Hardware

- Virtualisiert auf SERVER02
- 2 GB RAM

3.10.3 Betriebssystem

- Windows Server 2008 R2 Standard SP 1 English 64 Bit
- Hostname in Virtualbox: Wasser_SCADA_SRV
- Hostname in Windows: WIN-CDHA5UO1MSI

3.10.4 Software

- TIghtVNC 2.7.10
- UltraVnc 1.2.0.3
- OPC Core Components
- OPC .NET API 2.00
- SIMATIC WinCC/Audit Viewer 2008 SP2
- Simatic OPC – XML Gateway V11.0 + SP2 DE
- Simatic WinCC Runtime Advanced V11.0 – SP2 SE
- Snare Version 4.0.2
- Wibukey Setup

3.10.5 Rollen und Funktionen

- Anzeige der Anlagenvisualisierung

3.11 SVENGINEERINGWKS01 (virtuell auf SERVER02)

3.11.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
LAN	192.168.0.25	255.255.255.0	

3.11.2 Hardware

- Virtualisiert auf SERVER02
- 1 GB RAM

3.11.3 Betriebssystem

- Windows 7 Prof. 32 Bit
- Hostname: Wasser_ENG_WKS

3.11.4 Software

- TIghtVNC 2.7.10
- UltraVnc 1.2.0.3
- OPC Core Components
- OPC .NET API 2.00

- Snare Version 4.0.2
- Microsoft SQL Server Native Client
- Microsoft SOAP Toolkit 3.0
- SIMATIC Prosave V9.0 incl. SP3
- Siemens Automation License Manager V5.1 + SP1 + Upd3
- Siemens Totally Integrated Automation Portal V11
- Microsoft SQL Server 2005

3.11.5 Rollen und Funktionen

- Engineering der SPS-Software

3.12 DBSERVER01 (virtuell auf SERVER02)

3.12.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
LAN	192.168.0.30	255.255.255.0	

3.12.2 Hardware

- Virtuell auf SERVER02
- 1 GB RAM

3.12.3 Betriebssystem

- Windows 7 Prof. SP 1 32 Bit
- Hostname: Wasser_DB_SRV01

3.12.4 Software

- TIghtVNC 2.7.10
- Microsoft SQL Server 2005

3.12.5 Rollen und Funktionen

- Ein weiteres Element der Wasser-Infrastruktur

3.13 SWITCH02

3.13.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
LAN	10.0.1.50	255.255.255.0	

3.13.2 Portbelegung

Port	Gerät	Beschreibung
1	SWITCH01 Port 24	
2	NAS01 Port 1	Anbindung NAS01
3	SERVER02 eth0 (onboard)	Anbindung SERVER02
4	APPLIANCE01 eth0	Administration honeyBox
5	FIREWALL01 eth0	Administration Firewall
6	FIREWALL02 eth0	Administration Firewall
7	NAS01 Port 1	Anbindung NAS01
8	Frei	
9	Frei	

10	Frei	
11	Frei	
12	Frei	
13	Frei	
14	Frei	
15	Frei	
16	Frei	
17	Frei	
18	Pentest1	Auswerte-Notebook
19	Frei	
20	Frei	
21	Frei	
22	Frei	
23	Frei	
24	Frei	

3.13.3 Hardware

- HP Procurve 2524
- Keine Transceiver-Port Module bestückt

3.13.4 Betriebssystem

- HP eigenes Betriebssystem Version F.05.17

3.13.5 Rollen und Funktionen

Der Switch bildet das Management-Netzwerk des Honeynets ab. Er ist per SSH und Telnet administrativ erreichbar.

3.14 SERVER01

3.14.1 Netzwerkschnittstellen

Schnittstelle	**IP-Adresse**	**Subnetzmaske**	**Beschreibung**
Eth0	10.0.1.10	255.255.255.0	Admin-LAN
Eth1			Frei
Eth2	10.0.5.1	255.255.255.0	Logging der VMs von SERVER02
Eth3			Frei
Eth4			Frei
Eth5			Frei
Eth6			Frei
Eth7	Ohne IP (stealth)		Sniffing Interface im Honeynet

3.14.2 Hardware

- Hardware Nexcom NSA3180-C8, 19 Zoll, 8 x Gigabit Ethernet
- 2 TB SATA-2 Festplatte
- 4 GB RAM

3.14.3 Betriebssystem

- Betriebssystem Generische Security Appliance Version 5.0 von secXtreme

3.14.4 Software

Folgende zusätzliche Software wurde installiert:

- SiLK Netflow Collector (scxt-netsa-silk) (paketiert und zur Verfügung gestellt von secXtreme)
- FlowViewer
- Snort IDS (scxt-idsipssensor, scxt-barnyard2, scxt-idsipstools, scxt-libdaq, scxt-libdnet, scxt-snort 2.9.6.0) (paketiert und zur Verfügung gestellt von secXtreme)
- Apache2 Webserver (für FlowViewer)
- Netrec (scxt-netrec) (secXtreme)
- Auswerte-Skripte (TÜV Süd)

3.14.5 Rollen und Funktionen

- Syslog Server (Standard syslog-ng des Betriebssystems)
- PCAP-Daten (Netzwerkrecorder netrec von secXtreme der Daten vom Interface eth7 im Round-Robin Verfahren)
- Rolle des Zeitservers (NTPv3, Standard Betriebssystemdienst, holt aus dem Internet (DSL Anschluss) die Zeit, über SWITCH02 und FW01, DSL Laboranschluss (nicht M-Net für Honeynet))
- Rolle des E-Mail Servers (Standard exim4 Server des Betriebssystems), versendet E-Mail an den web.de wasser.bayern@web.de Account
- Rolle des E-Mail-Relais für interne Komponenten ,(Komponenten des Honeynet schicken Mails an SERVER01, dieser schickt weiter an Web.de)
- Intrusion Detection System (snort, projektspezifisch gepackt und zur Verfügung gestellt von secXtreme), gleiches Interface, das pcap Daten sammelt; reportet an die DB auf APPLIANCE01; überwacht internen Honeynet Traffic)
- Webinterface für FlowViewer (Software für die grafische Auswertung der Netflow-Daten)

3.15 SERVER02

3.15.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	Keine IP		Anbindung der VMs in Honeynet
Eth1	Keine IP		Logging der VMs
Eth2	10.0.1.20	255.255.255.0	Admin-Interface im Honeynet

3.15.2 Hardware

- Dell Optiplex 490 Workstation
- 2 Festplatten je 1 TB im RAID 1
- RAID 1 Controller
- 3 Ethernet-Netzwerkschnittstellen
- 16 GB RAM
- Xeon X5355 mit 2,66 Ghz, 4 aktive Cores
- Serieller Port (Anbindung an Out-of-Band Konsole von ROUTER01)
- Serieller Port (Anbindung an Not-Aus Schalter)

3.15.3 Betriebssystem

- Ubuntu 14.04 LTS

3.15.4 Software

- Virtualbox 4.3.10
- emergencyButton.py (TÜV SÜD)

3.15.5 Installierte virtuelle Machinen

- SCADA
- DBSERVER01
- WIKI
- Engineering Workstation
- PROXY01 192.168.0.5 SSL Entschlüsselung (Umleitung HTTPS Kommunikation mit SPS auf Server 02, hier Apache Webserver als Reverse-Proxy)

3.16 WSCLIENT01

3.16.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	10.0.1.21	255.255.255.0	

3.17 WSCLIENT02

3.17.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	10.0.1.22	255.255.255.0	

3.18 WIKI (virtuell auf SERVER02)

3.18.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	10.0.1.	255.255.255.0	

3.18.2 Rollen und Funktionen

Es wurde ein internes Wiki aufgebaut, in dem Änderungen und Arbeiten am Honeynet dokumentiert wurden.

3.19 APPLIANCE01 (honeyBox)

3.19.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	10.0.1.40	255.255.255.0	Interface im Management-LAN
Eth1	192.168.0.3	255.255.0.0	Interface im Honeynet, nicht sichtbar

3.19.2 Hardware

- secXtreme honeyBox industrial 2-Port

3.19.3 Betriebssystem

- secXtreme honeyBox Release 5.0

3.19.4 Software

- Watersim (TÜV Süd) inkl. Überwachungstools

- Snort IDS (scxt-idsipssensor, scxt-barnyard2, scxt-idsipstools, scxt-libdaq, scxt-libdnet, scxt-snort 2.9.6.0) (paketiert und zur Verfügung gestellt von secXtreme)

3.19.5 Rollen und Funktionen

- Honeybox von secXtreme, Modell Industrial 2-Port
- Ein Interface im Honeynet (eth1)
- Ein Interface im Admin-Netz (eth0)
- Datenbank: sammelt Honeybox, IDS und IPS Events von APPLIANCE01, FW02 und SERVER01
- Hier laufen Honeypots, zum Beispiel Drucker-Server
- Hier laufen 4 Modbus/TCP Honeypots, mit denen die SPS01 für die Simulation spricht

Auf dem System wurde eine Reihe von Honeypots konfiguriert. Da auf den echten SPS Modus/TCP betrieben wird, wurde das vorhandene Template tmpl_for_plc_1200 um den Dienst Modbus/TCP erweitert (my_tmpl_for_plc_1200_with_modbus).

3.19.6 Aktive Honeypots

Folgende Honeypots sind aktiv:

Template	IP-Adresse	Name	Beschreibung
tmpl_for_hp_lj	192.168.0.100	PRINTER01	HP Jetdirect Printer Server
my_tmpl_for_plc_1200_with_modbus	192.168.13.2	SPS_PUMPSTATION01	SPS, Bestandteil der Simulation
tmpl_for_industrial_switch	192.168.13.25	SWITCH03	Industrial Switch
my_tmpl_for_plc_1200_with_modbus	192.168.14.2	SPS_PUMPSTATION02	SPS, Bestandteil der Simulation
tmpl_for_industrial_switch	192.168.14.25	SWITCH03	Industrial Switch
my_tmpl_for_plc_1200_with_modbus	192.168.15.2	SPS_HOCHBEHAELTER01	SPS, Bestandteil der Simulation
my_tmpl_for_plc_1200_with_modbus	192.168.15.10	SPS_TEST01	SPS
my_tmpl_for_plc_1200_with_modbus	192.168.15.11	SPS_TEST02	SPS
my_tmpl_for_plc_1200_with_modbus	192.168.15.12	SPS_BRUNNEN_NOT	SPS, Bestandteil der Simulation
tmpl_for_industrial_switch	192.168.15.25	SWITCH04	Industrial Switch

3.20 NAS01

3.20.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Eth0	10.0.1.30	255.255.255.0	Interface im Management-LAN
Eth1			Frei

3.20.2 Hardware

- QNAP TS-420U Turbo NAS Appliance 19 Zoll
- 4 x 3 GB SATA-2 Festplatten im RAID-5 Verbund
- 1 GB RAM

3.20.3 Betriebssystem

- QNAP eigenes Betriebssystem Version 4.1.1 Build 20140916

3.20.4 Rollen und Funktionen

- NFS-Server
- Datensicherung von SERVER01

3.21 SPS01

3.21.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	192.168.0.12	255.255.0.0	Interface im Honeynet

3.21.2 Hardware

- Siemens S7-1200 CPU 1214C DC/DC/DC

3.21.3 Betriebssystem

- Firmware 3.0.2

3.21.4 Software

- Die Software WA wurde von ausecus erstellt und über die Engineering-Workstation auf die SPS geladen

3.21.5 Rollen und Funktionen

- Eine SPS für Steuerung und Simulation, Verbindung zu SCADA

3.22 SPS02

3.22.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	192.168.0.13	255.255.0.0	Interface im Honeynet

3.22.2 Hardware

- Siemens S7-1200 CPU 1212C DC/DC/RLY

3.22.3 Betriebssystem

- Firmware 3.0.2

3.22.4 Software

- Es ist keine Software auf der SPS installiert, die Teil der Wassersimulation ist

3.22.5 Rollen und Funktionen

- Test SPS, nicht Bestandteil der Simulation, soll dem Angreifer vorgaukeln, dass hier eine SPS für interne Tests zur Verfügung steht.

3.23 SPS03

3.23.1 Netzwerkschnittstellen

Schnittstelle	IP-Adresse	Subnetzmaske	Beschreibung
Lan	192.168.0.14	255.255.0.0	Interface im Honeynet

3.23.2 Hardware

- Siemens S7-1200 CPU 1212C DC/DC/RLY

3.23.3 Betriebssystem

- Firmware 3.0.2

3.23.4 Software

- Es ist keine Software auf der SPS installiert, die Teil der Wassersimulation ist

3.23.5 Rollen und Funktionen

- SPS im Stop-Modus; damit wird überwacht, ob ein Angreifer diese SPS in den RUN-Zustand schaltet

3.24 Schwachstellen der SPSen

Die eingesetzten SPS S7-1200 laufen mit der Software-Version 3.0.2. Für diese Version ist eine Reihe von Schwachstellen bekannt. Es wurde gezielt diese ältere Version (aktuell Stand 09/2015 Version 4.x) eingesetzt, um dem Angreifer eine Reihe von bekannten Angriffen zu ermöglichen.

CVE-2014-2249 Cross Site Request Forgery (CSRF)

Der Web-Server auf der SPS (Ports 80 und 443 TCP) ist für einen CSRF Angriff anfällig. Damit kann die Vertraulichkeit, Verfügbarkeit und Integrität der SPS beeinträchtigt werden, wenn der Angreifer dem Opfer über Sozial Engineering einen präparierten Link sendet und das Opfer diesen aufruft.

CVE-2014-2258 Improper Resource Shutdown or Release

Ein Angreifer kann die SPS in den Defect-Mode bringen und damit einen DoS durchführen. Das ist möglich durch ein speziell gebautes Paket, das an Port 443/TCP gesendet wird. Es ist ein Kaltstart notwendig, um das System danach wieder in Betrieb zu nehmen.

CVE-2104-2250 Insufficient Entropy

Ungenügende Entropie bei der Authentifiizerung am Web-Server der SPS kann dazu führen, dass ein Angreifer eine bestehende Session übernehmen kann.

CVE-2014-2252 Improper Resource Shutdown or Release

Ein Angreifer kann die SPS in den Defect-Mode bringen und damit einen DoS durchführen. Das ist möglich durch ein speziell gebaute Profinet-Pakete, die an die SPS gesendet werden. Es ist ein Kaltstart notwendig, um das System danach wieder in Betrieb zu nehmen.

CVE-2014-2254 Improper Resource Shutdown or Release

Ein Angreifer kann die SPS in den Defect-Mode bringen und damit einen DoS durchführen. Das ist möglich durch ein speziell gebautes Paket, das an Port 80/TCP gesendet wird. Es ist ein Kaltstart notwendig, um das System danach wieder in Betrieb zu nehmen.

CVE-2014-2256 Improper Resource Shutdown or Release

Ein Angreifer kann die SPS in den Defect-Mode bringen und damit einen DoS durchführen. Das ist möglich durch ein speziell gebautes Paket, das an Port 102/TCP gesendet wird. Es ist ein Kaltstart notwendig, um das System danach wieder in Betrieb zu nehmen.

3.25 Stromversorgung 24 Volt

3.25.1 Hardware

- SITOP PSU 100L
- DC 24V/10 A

3.25.2 Versorgte Geräte

Folgende Geräte werden damit versorgt:

- SPS01
- SPS02
- SPS03
- APPLIANCE01

4 Weitere Honeynet-Bestandteile

4.1 Remote-Zugang

Für die Remote-Administration wurde ein eigener VPN-Zugang über einen vom M-Net Honeynet Anschluss unabhängigen Weg eingerichtet.

- DSL-Router
- DynDNS-Account: wgffgfgsdf.selfhost.eu
- Der DSL-Router ist an das Labor-Netz angeschlossen
- Es existiert eine Portweiterleitung von Port UDP/6032 auf die externe IP-Adresse von FW03

4.2 Alarmierung per E-Mail

4.2.1 Account für interne Statusmeldungen

Der Versand von internen Statusinformationen und –meldungen erfolgt per E-Mail. Dazu wurde bei web.de eingerichtet: wasser.bayern@web.de. Die Mails an diesen Account werden von SERVER01 gesendet. Für den Versand der E-Mails muss sich SERVER01 an dem Mail-Server von web.de anmelden. Das hat bisher zweimal zu Problemen geführt, da Web.de „Unregelmäßigkeiten beim Zugriff auf Ihren Web.de Account“ festgestellt hat und den Account vorsorglich gesperrt hat. Um das Problem zu beheben, musst das Passwort für den Mail-Account jeweils neu gesetzt werden.

Im Web.de-Account erfolgt die Weiterleitung auf zwei aktive E-Mail Adressen von Projektbeteiligten.

4.2.2 Fake-Email-Account

Für die Registrierung der IP-Adressen wurde eine weitere E-Mail Adresse verwendet, die keinen Zusammenhang mit der von Web.de für die internen Nachrichten hat. Es wurde dafür bei Google-Mail ein Account wasser.bayern@gmail.com eingerichtet.

4.3 Registrierung der IP-Adressen

Um den Bezug des Wasserwerks im Raum München herzustellen, wurden IP-Adressen des Providers M-Net beantragt, da dieser in der Zielregion aktiv ist. Um den Anschein von mehreren Standorten zu erreichen, wurden zwei getrennte, nicht aufeinander folgende IP-Adressbereiche mit jeweils 16 IPv4-Adressen beantragt.

Die Registrierung wurde durchgeführt als

```
Wasser Bayern OHG
Barthstr. 16
80339 München
```

4.4 Aus dem Internet erreichbare Systeme

System	Öffentliche IP	Interne IP	Typ	Modell	TCP	UDP	TCP	UDP
Hauptstandort								
PROXY01		192.168.0.5	Real (VM)	Apache2 Reverse Proxy für HTTPS zu HTTP Konvertierung	8012 8013 8015			
SPS01	212.114.128.132	192.168.0.12	Real	Siemens SPS S7-1200	80 102 443	161	(80) 443 ANY	ANY
SPS02	212.114.128.133	192.168.0.13	Real	Siemens SPS S7-1200	80 102 443	161	(80) 443 ANY	ANY
SPS03	212.114.128.135	192.168.0.14	Real	Siemens SPS S7-1200	80 102 443	161	(80) 443 ANY	ANY
SCADA01	212.114.128.131	192.168.0.20	Real (VM)	Windows Server 2008 R2	80 102 5901		5901	
SVENGINEERINGWKS01	212.114.128.139	192.168.0.25	Real (VM)	Windows 7			5901	
DBSERVER01		192.168.0.30	Real (VM)	Windows 7				
PRINTER01	212.114.128.140	192.168.0.100	HP	tmpl_for_hp_lj	21 23 80 280 515 631 9100	161 427		
PRINTER02	212.114.128.141	192.168.0.101	HP	tmpl_for_hp_lj	21 23 80 280 515 631 9100	161 427		
SWITCH01	212.114.128.142	192.168.0.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024		
Pumpstation 1								

SPS_PUMPSTATION01	212.114.130.99	192.168.13.2	HP	my_tmpl_for_plc_1200_with_modbus Wird von SPS01 angesprochen, Teil der Simulation	80 102 443 502	161		
SWITCH02	212.114.130.100	192.168.13.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY
Pumpstation 2								
SPS_PUMPSTATION02	212.114.130.101	192.168.14.2	HP	my_tmpl_for_plc_1200_with_modbus Wird von SPS01 angesprochen, Teil der Simulation	80 102 443 502	161		
SWITCH03	212.114.130.102	192.168.14.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY
Hochbehälter und Notbrunnen								
SPS_HOCHBEHAELTER01	212.114.130.102	192.168.15.2	HP	my_tmpl_for_plc_1200_with_modbus Wird von SPS01 angesprochen, Teil der Simulation	80 102 443 502	161		
SPS_TEST01	212.114.130.104	192.168.15.10	HP	my_tmpl_for_plc_1200_with_modbus	80 102 443 502	161	502	161
SPS_TEST02		192.168.15.11	HP	my_tmpl_for_plc_1200_with_modbus	80 102 443 502	161		
SPS_BRUNNEN_NOT	212.114.130.109	192.168.15.12	HP	my_tmpl_for_plc_1200_with_modbus Wird von SPS01 angesprochen, Teil der Simulation	80 102 443 502	161		
SWITCH04	212.114.130.110	192.168.15.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY

Legende Real: physikalisch vorhanden, nicht virtualisiert; Real (VM): virtualisiert; HP: Honeypot auf der Honeybox

4.5 Physikalischer Not-Aus-Schalter

An dem technischen Aufbau des Honeynets wurde ein Not-Aus-Schalter angebracht, der die Verbindung des Honeynets zum Internet trennt. Dabei wurde das Signal des Schalters auf den

Parallelport des SERVER02 gegeben. Dort wird es mit einem Skript überwacht. Wenn der Schalter betätigt wird, wird auf dem ROUTER01 die WAN-Schnittstelle herunter gefahren. Dazu sendet SERVER01 über einen seriellen Port, an dem der serielle Konsolenport des Routers angeschlossen ist, eine Reihe von Kommandos.

5 Simulation

5.1 Aktoren und Sensoren

Die realen Komponenten der Anlage (Aktoren und Sensoren) sowie deren Verhalten werden simuliert, da sie nicht real vorhanden sind.

5.2 Industrie-Bus Modbus/TCP

Wie bei einem echten System werden die Sensoren und Aktoren über einen Industriebus angebunden. Für das Honeynet wurde als Protokoll Modbus/TCP gewählt. Zum einen bietet die honeyBox eine weitgehende Implementierung von Modbus/TCP. Zum anderen wurde bewusst eine TCP/IP-basierte Kommunikation gewählt, um die Aufzeichnung und Auswertung zu erleichtern und einem potentiellen Angreifer eine weitere Flanke zu öffnen.

Die SPS01 spricht dabei vier virtuelle SPS auf der honeyBox an.

5.3 Simulationssoftware

Die eigentliche Simulation des Wasserwerks erfolgt auf der honeyBox mit einem Script (watersim.py). Dieses Skript läuft in einer Schleife und führt folgende Aktionen aus:

- Einlesen der Steuerungsdaten der SPS01
- Verarbeitung der Eingabewerte
- Schreiben der Ausgabewerte in die XML-Dateien

In der Simulation sind typische Verbrauchswerte über einen Tag und ein einfacher Feiertagskalender hinterlegt.

Die Simulation startet über das Startskript /etc/init.d/watersim beim Start der honeyBox automatisch mit. Zudem ist ein cron-Job „simcheck“ angelegt, der zyklisch prüft, ob die vorhandenen XML-Dateien well-formed sind. Das soll verhindern, dass korrupte XML-Dateien die Simulation abbrechen lassen. Falls XML-Dateien defekt sind, werden sie durch eine Sicherungskopie ersetzt und die notwendigen Dienste neu gestartet und ein Alarm per E-Mail versendet.

5.4 XML-Schnittstelle

Die Kommunikation zwischen den virtuellen SPS mit Modbus/TCP und der Simulation erfolgt über XML-Dateien auf der honeyBox. Die Modbus/TCP-Module der virtuellen SPS schreiben die über das Netzwerk von der SPS01 erhaltenen Daten in die XML-Dateien und lesen die Daten dort aus, die die SPS01 über Modbus/TCP anfordert.

Die Simulation wiederum liest die aktuellen Werte aus den XML-Dateien und schreibt die Ergebnisse nach dem Ende eines Durchlaufs wieder in die XML-Dateien. Für die Speicherung interner Zustände nutzt die Simulation eine weitere XML-Datei (127.0.0.1).

Die Synchronisation zwischen den Lese- und Schreibzugriffen der verschiedenen Prozesse erfolgt über Locking auf Dateiebene je XML-Datei.

5.5 Datenstrukturen der virtuellen Modbus/TCP Devices

5.5.1 Interne Verwaltungsdaten der Simulation 127.0.0.1

Dabei handelt es sich um kein Modbus/TCP Device, das von außen auf der Honeybox (Appliance01) angesprochen werden kann. Vielmehr werden darin Daten der Simulation persistent gehalten. Die Daten liegen dort im Verzeichnis /var/lib/honeypot/honeyd_if_eth1/modules.

Die XML-Daten werden von der Simulationssoftware watersim.py gelesen und geschrieben. Die Synchronisation der Zugriffe zwischen Honeypot-Prozess und der Simulation wird über File-Locking-Mechanismen auf Betriebssystemebene hergestellt.

```
<data>
 <log>
    <ok>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>127.0.0.1</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </ok>
    <error>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>127.0.0.1</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </error>
  </log>
  <terminate-after-transaction>0</terminate-after-transaction>
  <read-before-read>1</read-before-read>
  <write-after-write>1</write-after-write>
  <write-if-not-changed>0</write-if-not-changed>
  <service-module-options name="modbus_tcp">
    <ignore-invalid-register-range>1</ignore-invalid-register-range>
  </service-module-options>
  <ipv4-address>127.0.0.1</ipv4-address>
  <port>0</port>
  <description>SPS Hochbehaelter INTERNAL DATA</description>
  <registers>
        <register num="1015">
                <type>output_register</type>
                <value>300696</value>
                <value-min>0</value-min>
                <value-max>400000</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>Intern.Status.Liter_1</description>
    </register>
                <register num="1016">
                <type>output_register</type>
```

```
                <value>300696</value>
                <value-min>0</value-min>
                <value-max>400000</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>Intern.Status.Liter_2</description>
        </register>
  </registers>
</data>
```

5.5.2 192.168.13.2 SPS_PUMPSTATION01 (Honeypot aber Teil der Simulation)

Es handelt sich um einen Honeypot, der auf der honeyBox Appliance läuft und eine Siemens SPS S7-1200 mit Modbus/TCP emuliert. Das System wird von SPS01 per Modbus/TCP über zwei TCP-Verbindungen (einmal je für Lesezugriffe und für Schreibzugriffe) angesprochen.

Die XML-Daten werden von der Simulationssoftware watersim.py gelesen und geschrieben. Die Synchronisation der Zugriffe zwischen Honeypot-Prozess und der Simulation wird über File-Locking-Mechanismen auf Betriebssystemebene hergestellt.

```
<data>
 <log>
    <ok>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </ok>
    <error>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </error>
  </log>
  <terminate-after-transaction>0</terminate-after-transaction>
  <read-before-read>1</read-before-read>
  <write-after-write>1</write-after-write>
  <write-if-not-changed>0</write-if-not-changed>
  <service-module name="modbus_tcp">
    <ignore-invalid-register-range>1</ignore-invalid-register-range>
  </service-module>
  <ipv4-address>192.168.13.2</ipv4-address>
  <port>502</port>
  <description>SPS Pumpe 1</description>
  <registers>
        <register num="0">
                <type>output_register</type>
                <value>1</value>
                <value-min>0</value-min>
```

```
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Watchdog_SND</description>
        </register>
        <register num="1">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung</description>
        </register>
        <register num="2">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Pumpe_On | SND.Schieber_On</description>
        </register>
        <register num="1000">
                <type>output_register</type>
                <value>1</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Watchdog_RCV</description>
        </register>
        <register num="1001">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druck</description>
        </register><register num="1002">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
```

```
                <description>RCV.Status.Durchfluss</description>
        </register>
        <register num="1003">
                <type>output_register</type>
                <value>912</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Grundwasserstand</description>
        </register>
        <register num="1004">
                <type>output_register</type>
                <value>100</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Stellung</description>
        </register>
        <register num="1005">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Endschalter |
RCV.Status.Pumpe_Rueckmeldung | RCV.Status.Alarm_Ueberstrom |
RCV.Status.Alarm_Drehmoment | RCV.Status.Alarm_Betretung</description>
        </register>
</registers>
```

5.5.3 192.168.14.2 SPS_PUMPSTATION02 (Honeypot aber Teil der Simulation)

Es handelt sich um einen Honeypot, der auf der honeyBox Appliance läuft und eine Siemens SPS S7-1200 mit Modbus/TCP emuliert. Das System wird von SPS01 per Modbus/TCP über zwei TCP-Verbindungen (einmal je für Lesezugriffe und für Schreibzugriffe) angesprochen.

Die XML-Daten werden von der Simulationssoftware watersim.py gelesen und geschrieben. Die Synchronisation der Zugriffe zwischen Honeypot-Prozess und der Simulation wird über File-Locking-Mechanismen auf Betriebssystemebene hergestellt.

```
<data>
 <log>
    <ok>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
```

```
      </ipv4-addresses>
    </log-ignore-src>
  </ok>
  <error>
    <do-log>1</do-log>
    <log-ignore-src>
      <ipv4-addresses>
        <ipv4-address>192.168.0.12</ipv4-address>
      </ipv4-addresses>
    </log-ignore-src>
  </error>
</log>
<terminate-after-transaction>0</terminate-after-transaction>
<read-before-read>1</read-before-read>
<write-after-write>1</write-after-write>
<write-if-not-changed>0</write-if-not-changed>
<service-module name="modbus_tcp">
  <ignore-invalid-register-range>1</ignore-invalid-register-range>
</service-module>
<ipv4-address>192.168.14.2</ipv4-address>
<port>502</port>
<description>SPS Pumpe 2</description>
<registers>
      <register num="0">
              <type>output_register</type>
              <value>1</value>
              <value-min>0</value-min>
              <value-max>65535</value-max>
              <random-rate>0</random-rate>
              <mode>rw</mode>
              <log-success>1</log-success>
              <log-fail>1</log-fail>
              <description>SND.Watchdog_SND</description>
      </register>
      <register num="1">
              <type>output_register</type>
              <value>0</value>
              <value-min>0</value-min>
              <value-max>65535</value-max>
              <random-rate>0</random-rate>
              <mode>rw</mode>
              <log-success>1</log-success>
              <log-fail>1</log-fail>
              <description>SND.Schieber_Stellung</description>
      </register>
      <register num="2">
              <type>output_register</type>
              <value>0</value>
              <value-min>0</value-min>
              <value-max>1</value-max>
              <random-rate>0</random-rate>
              <mode>rw</mode>
              <log-success>1</log-success>
              <log-fail>1</log-fail>
              <description>SND.Pumpe_On | SND.Schieber_On</description>
      </register>
      <register num="1000">
              <type>output_register</type>
              <value>1</value>
```

```
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Watchdog_RCV</description>
        </register>
        <register num="1001">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druck</description>
        </register><register num="1002">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Durchfluss</description>
        </register>
        <register num="1003">
                <type>output_register</type>
                <value>915</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Grundwasserstand</description>
        </register>
        <register num="1004">
                <type>output_register</type>
                <value>33</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Stellung</description>
        </register>
        <register num="1005">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
```

```
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Endschalter |
RCV.Status.Pumpe_Rueckmeldung | RCV.Status.Alarm_Ueberstrom |
RCV.Status.Alarm_Drehmoment | RCV.Status.Alarm_Betretung</description>
        </register>
</registers>
</data>
```

5.5.4 192.168.15.2 SPS_HOCHBEHAELTER (Honeypot aber Teil der Simulation)

Es handelt sich um einen Honeypot, der auf der honeyBox Appliance läuft und eine Siemens SPS S7-1200 mit Modbus/TCP emuliert. Das System wird von SPS01 per Modbus/TCP über zwei TCP-Verbindungen (einmal je für Lesezugriffe und für Schreibzugriffe) angesprochen.

Die XML-Daten werden von der Simulationssoftware watersim.py gelesen und geschrieben. Die Synchronisation der Zugriffe zwischen Honeypot-Prozess und der Simulation wird über File-Locking-Mechanismen auf Betriebssystemebene hergestellt.

```
<data>
 <log>
    <ok>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </ok>
    <error>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </error>
  </log>
  <terminate-after-transaction>0</terminate-after-transaction>
  <read-before-read>1</read-before-read>
  <write-after-write>1</write-after-write>
  <write-if-not-changed>0</write-if-not-changed>
  <service-module-options name="modbus_tcp">
    <ignore-invalid-register-range>1</ignore-invalid-register-range>
  </service-module-options>
  <ipv4-address>192.168.15.2</ipv4-address>
  <port>502</port>
  <description>SPS Hochbehaelter</description>
  <registers>
        <register num="0">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
```

```
                <log-fail>1</log-fail>
                <description>SND.Watchdog_SND</description>
        </register>
        <register num="1">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung_1</description>
        </register>
        <register num="2">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung_2</description>
        </register>
        <register num="3">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung_Entwaesserung</description>
        </register>
        <register num="4">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung_Notversorgung</description>
        </register>
        <register num="5">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_ON_1 | SND.Schieber_ON_2 |
SND.Schieber_ON_Entwaesserung | SND.Schieber_ON_Notversorgung</description>
        </register>
```

```
        <register num="1000">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Watchdog_RCV</description>
        </register>
        <register num="1001">
                <type>output_register</type>
                <value>300</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Hoehenstand_1</description>
        </register>
        <register num="1002">
                <type>output_register</type>
                <value>300</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Hoehenstand_2</description>
        </register>
        <register num="1003">
                <type>output_register</type>
                <value>300</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Leitfaehigkeit</description>
        </register>
        <register num="1004">
                <type>output_register</type>
                <value>4</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Durchfluss</description>
        </register>
        <register num="1005">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
```

```
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Durchfluss_Notversorgung</description>
        </register>
        <register num="1006">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druckmessung</description>
        </register>
        <register num="1007">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druckmessung_Notversorgung</description>
        </register>
        <register num="1008">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Stellung_1</description>
        </register>
        <register num="1009">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Stellung_2</description>
        </register>
        <register num="1010">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
```

```
                <log-fail>1</log-fail>

<description>RCV.Status.Schieber_Stellung_Entwaesserung</description>
        </register>
        <register num="1011">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>

<description>RCV.Status.Schieber_Stellung_Notversorgung</description>
        </register>
        <register num="1012">
                <type>output_register</type>
                <value>768</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Endschalter_1 |
RCV.Status.Schieber_Endschalter_2 | RCV.Status.Schieber_Endschalter_Entwaesserung |
RCV.Status.Schieber_Endschalter_Notversorgung | RCV.Status.Alarm_Betretung
</description>
        </register>
        <register num="1013">
                <type>output_register</type>
                <value>444</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druck_1</description>
        </register>
        <register num="1014">
                <type>output_register</type>
                <value>446</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druck_2</description>
        </register>
  </registers>
```

5.5.5 SPS_BRUNNEN_NOT 192.168.15.12 (Honeypot aber Teil der Simulation)

Es handelt sich um einen Honeypot, der auf der honeyBox Appliance läuft und eine Siemens SPS S7-1200 mit Modbus/TCP emuliert. Das System wird von SPS01 per Modbus/TCP über zwei TCP-Verbindungen (einmal je für Lesezugriffe und für Schreibzugriffe) angesprochen.

Die XML-Daten werden von der Simulationssoftware watersim.py gelesen und geschrieben. Die Synchronisation der Zugriffe zwischen Honeypot-Prozess und der Simulation wird über File-Locking-Mechanismen auf Betriebssystemebene hergestellt.

```
<data>
 <log>
    <ok>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </ok>
    <error>
      <do-log>1</do-log>
      <log-ignore-src>
        <ipv4-addresses>
          <ipv4-address>192.168.0.12</ipv4-address>
        </ipv4-addresses>
      </log-ignore-src>
    </error>
  </log>
  <terminate-after-transaction>0</terminate-after-transaction>
  <read-before-read>1</read-before-read>
  <write-after-write>1</write-after-write>
  <write-if-not-changed>0</write-if-not-changed>
  <service-module name="modbus_tcp">
    <ignore-invalid-register-range>1</ignore-invalid-register-range>
  </service-module>
  <ipv4-address>192.168.15.12</ipv4-address>
  <port>502</port>
  <description>SPS Pumpe Not</description>
<registers>
        <register num="0">
                <type>output_register</type>
                <value>1</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Watchdog_SND</description>
        </register>
        <register num="1">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
```

```
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Schieber_Stellung</description>
        </register>
        <register num="2">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>SND.Pumpe_On | SND.Schieber_On</description>
        </register>
        <register num="1000">
                <type>output_register</type>
                <value>1</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Watchdog_RCV</description>
        </register>
        <register num="1001">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Druck</description>
        </register><register num="1002">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>rw</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Durchfluss</description>
        </register>
        <register num="1003">
                <type>output_register</type>
                <value>911</value>
                <value-min>0</value-min>
                <value-max>65535</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Grundwasserstand</description>
        </register>
        <register num="1004">
```

```
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Stellung</description>
        </register>
        <register num="1005">
                <type>output_register</type>
                <value>0</value>
                <value-min>0</value-min>
                <value-max>1</value-max>
                <random-rate>0</random-rate>
                <mode>r</mode>
                <log-success>1</log-success>
                <log-fail>1</log-fail>
                <description>RCV.Status.Schieber_Endschalter |
RCV.Status.Pumpe_Rueckmeldung | RCV.Status.Alarm_Ueberstrom |
RCV.Status.Alarm_Drehmoment | RCV.Status.Alarm_Betretung</description>
        </register>
</registers>
</data>
```