Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Thema:

Unified Monitoring

Mehrwerte mit Geschäftsprozessen

Referent/in:
Hr.Diener

Datum:
18.4.2018

Der Saarländer

Das Klinikum Saarbrücken

Gemeinnützige Gesellschaft (gGmbH)

100% Tochter der Stadt Saarbrücken

Einer der größten Arbeitgeber im Saarland

Krankenhaus der Maximalversorgung
(16 Fachabteilungen)
ca. 128.Mio Umsatz

2.000 Beschäftigte
27.000 stationäre Patienten jährlich
80.000 ambulante Patienten jährlich

IT-Abteilung

Die EDV Abteilung betreut mit 13 Vollstellen:

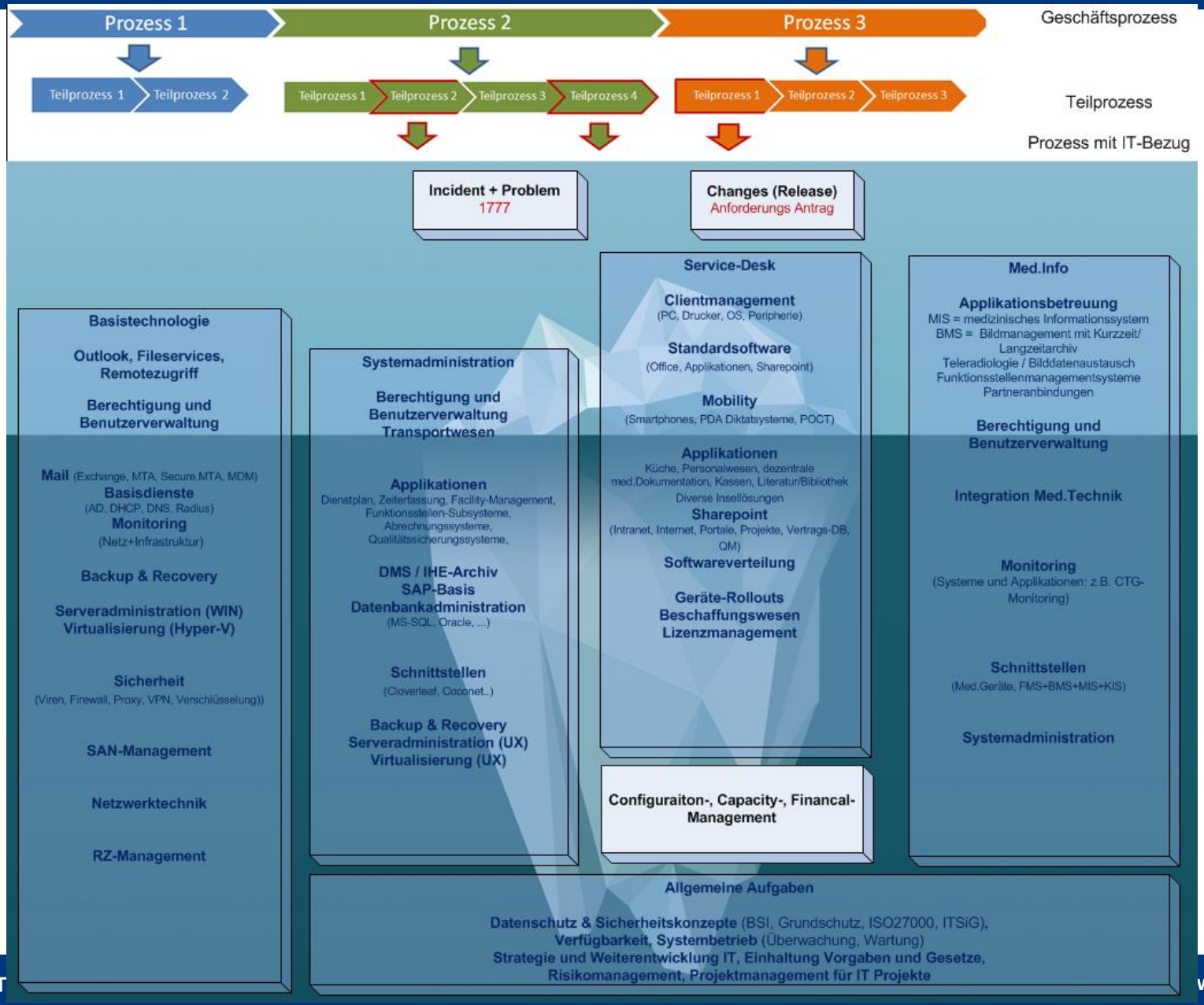
- 5000 Netzwerkports (> 100 aktive Komponenten, 37 Verteiler)
- 1700 Benutzer
- 1000 PCs
- 470 Drucker
- 120 Server (80 virtualisiert, 40 Hardware)
- 80 Systeme / 150 Applikationen
- 35 externe Dienstleister
- 3 Standorte

- 30 TB Speichervolumen im PACS o. Langzeitarchiv
- 20 TB digitale Patientenakten

- IT-Budget ~ 1,5% vom Umsatz

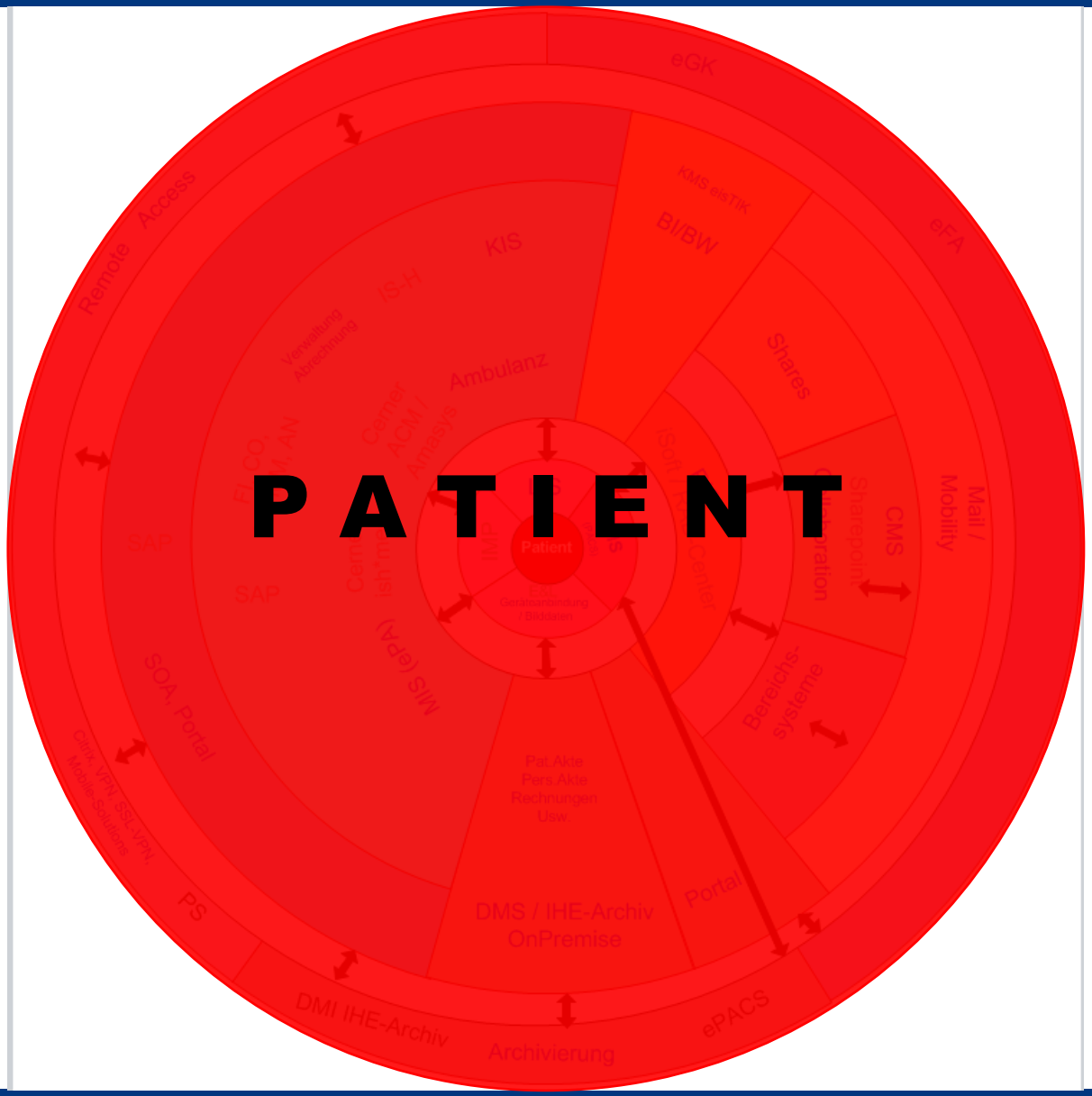
IT-Abteilung

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken



Prio "EDV-Triage"
4 Clients + Peripherie, Einzelpatzlösungen
3 Unterstützende Systeme Patientenversorgung, Mobility, Backup, Spezial- & Bereichssysteme, Intranet + Portale, BQS, DMS
2 Partner- und Remotezugänge, Dateidienste, Mailsystem, Labor, Patho, SAP-ERP, FMS , BSZ, Medizinisches Monitoring (CTG)
1 RIS, BMS, MIS
1 Schnittstellenserver, SAP-Basis, Basisdienste, Server, Virutalisierung, LAN-Firewall
1 Storage, Netzwerk, RZ

Leitbild: **Die uns anvertrauten Menschen bestimmen unser Handeln; ihr Wohl steht im Mittelpunkt.**



Warum NetEye …

Produkt	Einsatzzeit	Basis	Bemerkung
WOTAN	5 Jahre	Nagios	Unflexibel, keine sinnvolle Weiterentwicklung, Aufwendig, Lizenzsierung nach IPs = zu teuer
SCOM	2 Jahre	Microsoft	Im EA-Vertrag enthalten Probleme schon bei einfachstem Netzmonitoring Business Prozesse nur mit Add-On‘s Sehr teuer >50T€ Lizenzen und > 30T€ Dienstleistung Adminaufwand zu hoch
PRTG	Eval	Nagios	Nur „einfaches“ IT Monitoring. Zu wenig Mehrwerte
~~Realtech~~	~~Eval~~		~~Tolle Funktionen~~ ~~Zukunft ungewiss~~ ~~Basissystem 100T€~~ ~~Sehr teuer wenn Business Prozesse abgebildet werden sollen~~
SHD SM-Box	Eval	Nagios	Einzige neben Neteye die Business Prozesse gut abbilden. Teuer >50T€ für Geschäftsprozesse Lizenzierung nach IPs

Neteye/Würth wegen

- Gesamtkonzept,
- Ausbaubarkeit,
- Flexibilität
- **UND Bereitschaft Kundenanforderungen aufzunehmen**

Status NetEye & EriZone am Klinikum

Erizone für ITSM nach ITIL

- Incident, Problem, Change, Release, Capacity, Finance
- Anbindung an Neteye um aus „Problem“-View direkt Ticket zu eröffnen

Neteye:

- OCS, SafedAgent -> GLPI Assetverwaltung + alle Verträge und Supportinfos
- Nedi
- Wiki für Dokumentation
- Nagios für Monitoring
- Business Process Monitoring
- Capacity Management
- NagVis
- Logmanager, Kibana, Grafana
- SMS Tool

ToDo:

- Real- & EndUser Monitoring
- Log-Management ausbauen
- Netzwerkmonitoring nTop
- Vulnerability Scan integrieren
- Erizone Workflow‘s
- Shutdown Management / Event Management

Herausforderung: Komplexität ↑↑

Facility-Management:

- Immer mehr in IT eingebunden
- IT: Feuchtigkeit, Brand, Temperatur
- Temperatur (Blutprodukte, Essentransport),
- Reinraum (Zytostatika),
- Zeit-/Zugangsterminals
- …

Unified Communication

- Rohrpost
- Telefonie (VoIP), Fax
- Patientenentertainment (Telefon, WLAN, TV)
- Schwesternruf und Alarmierung
- …

Medizin Technik / Patientenmonitoring

- 4.500 Geräte
  (CT, MRT, Sono, Ultraschall, Spritzenpumpen, Beamtmungsgeräte, EKG, EEG, EMG …)
- Zukünftig noch IoT
  (Blutdruck, Blutzucker, Temperatur …)
- …

Fazit

- Mehr als klassische IT Themen
- IT Dienste immer Komplexer
- Immer mehr Abhängigkeiten der System untereinander
- ABER nicht mehr Spezialisten verfügbar.

→ **Baselining**

Gesamtheitlich

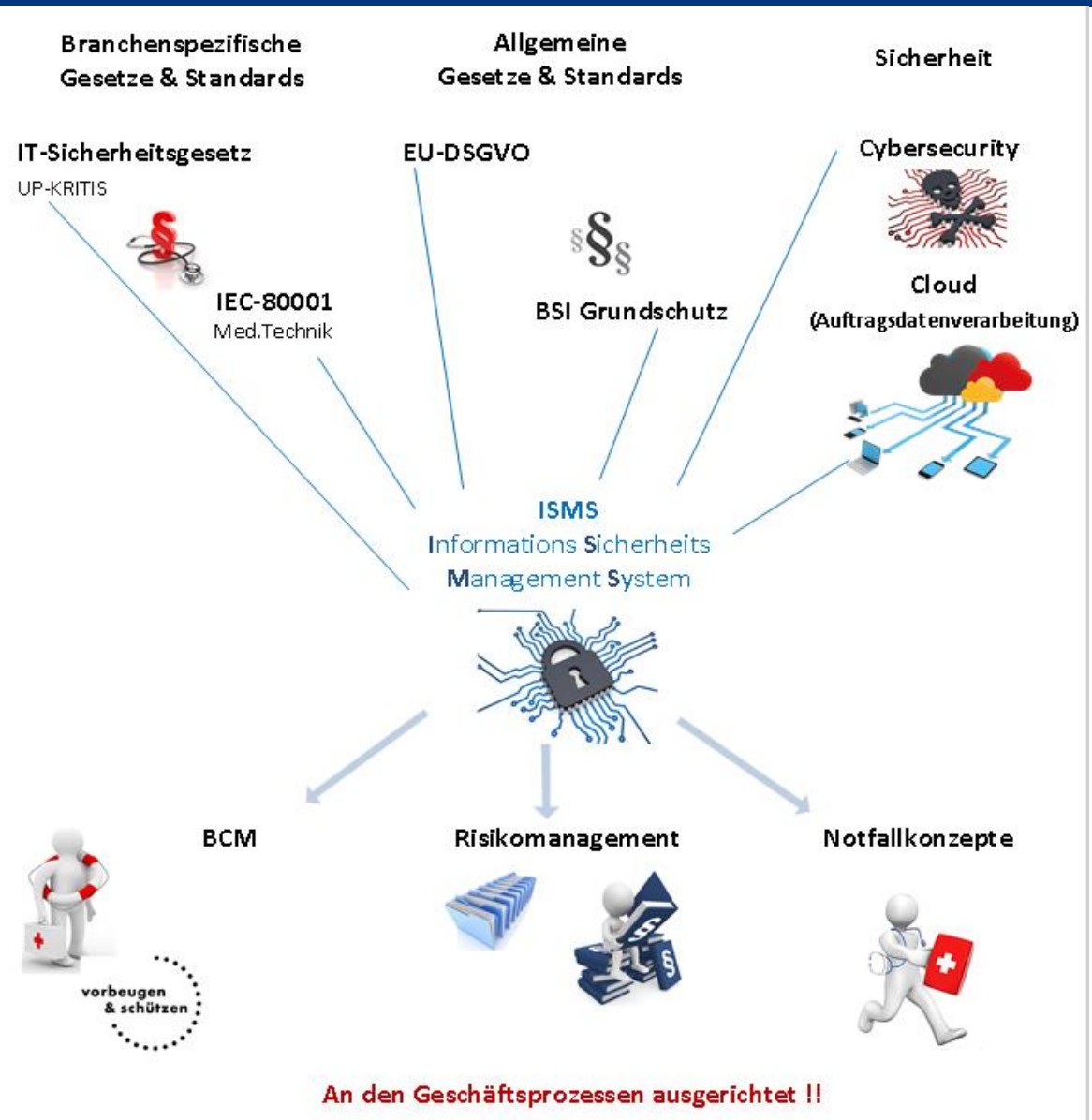
Herausforderungen: § + Normen = ↑↑

Viele
- Gesetze
- Handlungsempfehlung
- Sicherheitsvorgaben

fokussieren auf

ein **ISMS** (ISO/IEC 27001)

Themen:
- Dokumentation
- Nachvollziehbarkeit
- Logging / Auditing
- Schwachstellenmanagement
- Notfallkonzepte
- Risikomanagement
- BCM



Herausforderung gestalten

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Dokumentation
Geschäftsprozesse

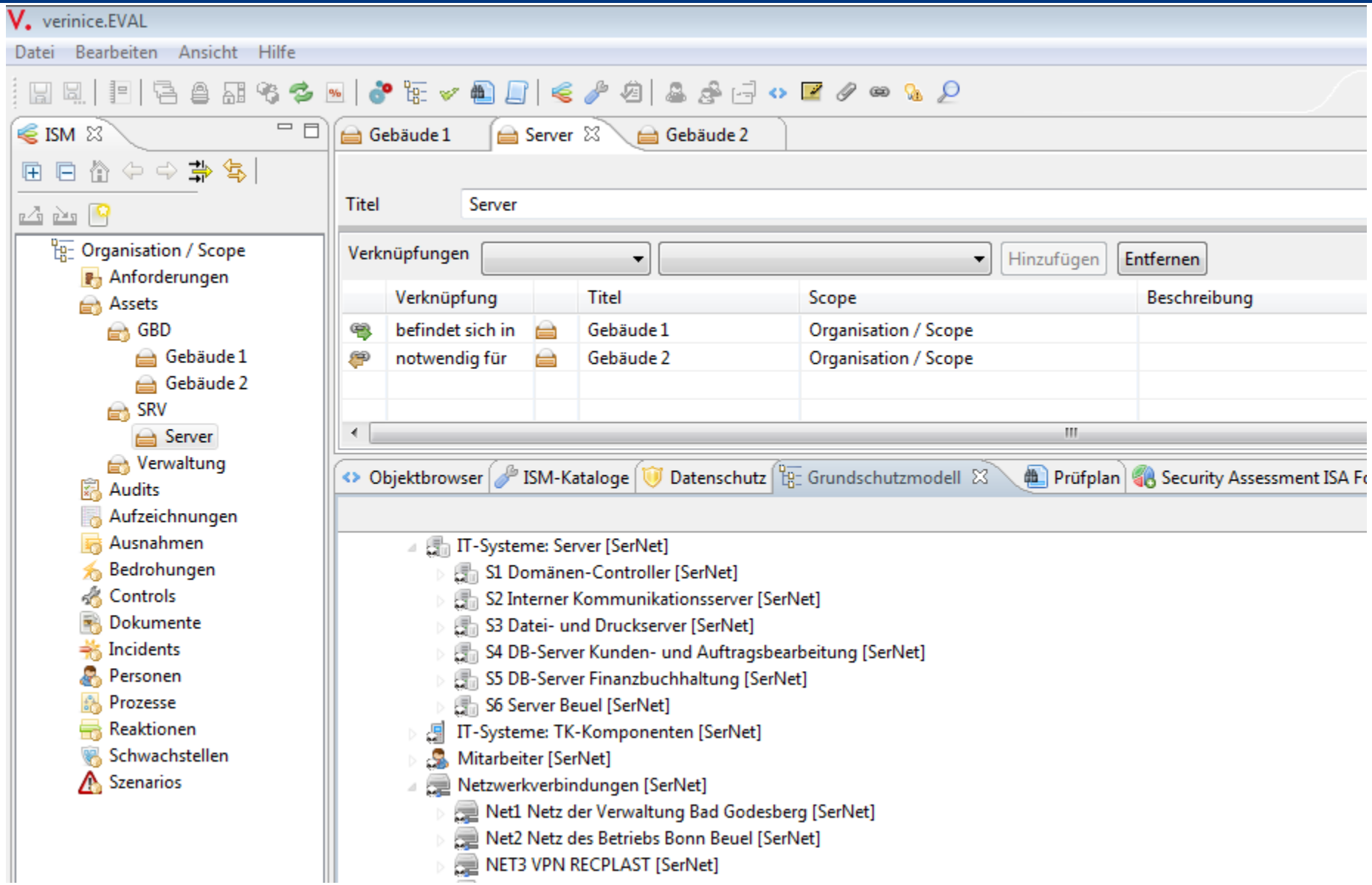
- Dokumentation **= Wiki**
- Asset-Management **= OCS, GLPI, Nedi**
- Risikomanagement + ISMS Doku

Überwachung
Geschäftsprozesse
(SLA‘s)

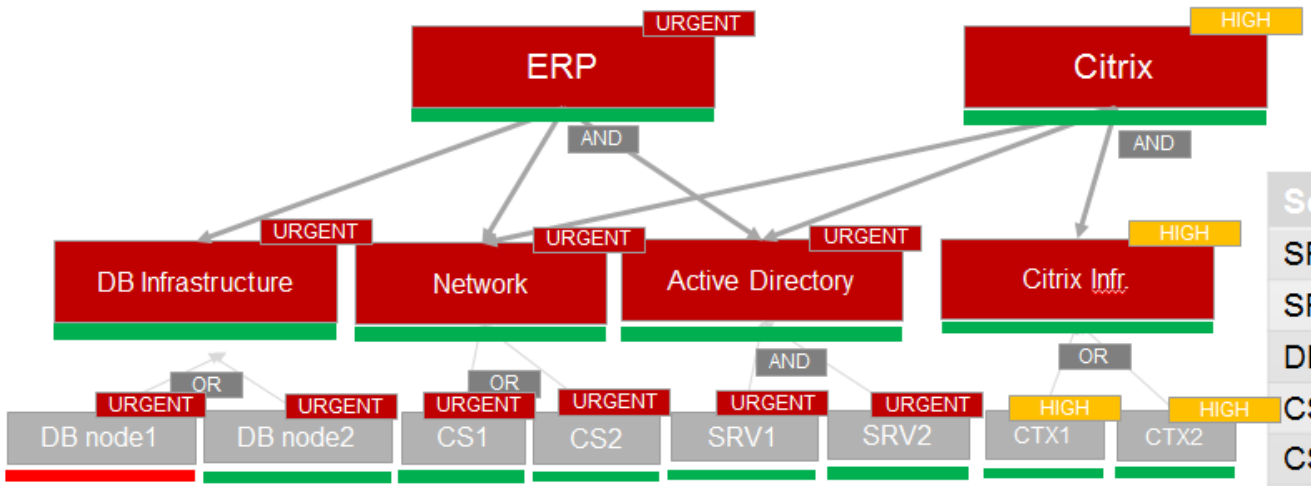
- Business Process Monitoring **= NagVis, Process View, Business Impact**
  - Real & Enduser Monitoring **= Alyvix, nTop**
  - Network Monitoring **= Nedi**
  - Facility Monitoring **= nBox**
  - System-, Storage-Monitoring = Nagios
- Capacity Management
  - Netzwerk+Server Performance, **= Cacti**
  - Application Performance **= Alyvix**

Logging,
Auditing

- Vulnerability Management
- Benachrichtigungen = Mail, SMS, Tickets **= OTRS / EriZone**
- Log-Management **= elasticSearch, Kibana, Grafana, Log Manager**
- Event Handler **= Event Console**
- Automatische Aktion **= Shutdown-Management**


verinice.EVAL
Datei Bearbeiten Ansicht Hilfe
ISM
Organisation / Scope
Anforderungen
Assets
GBD
Gebäude 1
Gebäude 2
SRV
Server
Verwaltung
Audits
Aufzeichnungen
Ausnahmen
Bedrohungen
Controls
Dokumente
Incidents
Personen
Prozesse
Reaktionen
Schwachstellen
Szenarios
Gebäude 1
Server
Gebäude 2
Titel
Server
Verknüpfungen
Hinzufügen
Entfernen
Verknüpfung
Titel
Scope
Beschreibung
befindet sich in
Gebäude 1
Organisation / Scope
notwendig für
Gebäude 2
Organisation / Scope
Objektbrowser
ISM-Kataloge
Datenschutz
Grundschutzmodell
Prüfplan
Security Assessment ISA Fo
IT-Systeme: Server [SerNet]
S1 Domänen-Controller [SerNet]
S2 Interner Kommunikationsserver [SerNet]
S3 Datei- und Druckserver [SerNet]
S4 DB-Server Kunden- und Auftragsbearbeitung [SerNet]
S5 DB-Server Finanzbuchhaltung [SerNet]
S6 Server Beuel [SerNet]
IT-Systeme: TK-Komponenten [SerNet]
Mitarbeiter [SerNet]
Netzwerkverbindungen [SerNet]
Net1 Netz der Verwaltung Bad Godesberg [SerNet]
Net2 Netz des Betriebs Bonn Beuel [SerNet]
NET3 VPN RECPLAST [SerNet]

NetEye Business Services



=Business Service

=Tech Srv

Service view	Priority	Status
SRV1	Urgent	OK
SRV2	Urgent	OK
DB node 2	Urgent	OK
CS 1	Urgent	OK
CS 2	Urgent	OK
CTX 1	High	OK
CTX 2	High	OK

Risk Management for Business Services

- Sample matrix of Impact x Urgency and Priority mapping example:

Impact X Urgency		Impact		
		1 = High	2 = Med	3 = Low
Urgency	1 = High	2	3	4
	2 = Med	3	4	5
	3 = Low	4	5	6

Impact + Urgency -> Priority mapping.

Fill into above matrix a priority mapping according the priorioriity to be attributed:

Priority	Label	Priority description
2	Urgent	Immedately
3	High	Within the next 4 hours
4	Med	Within a week
5 - 6	Low	When possible

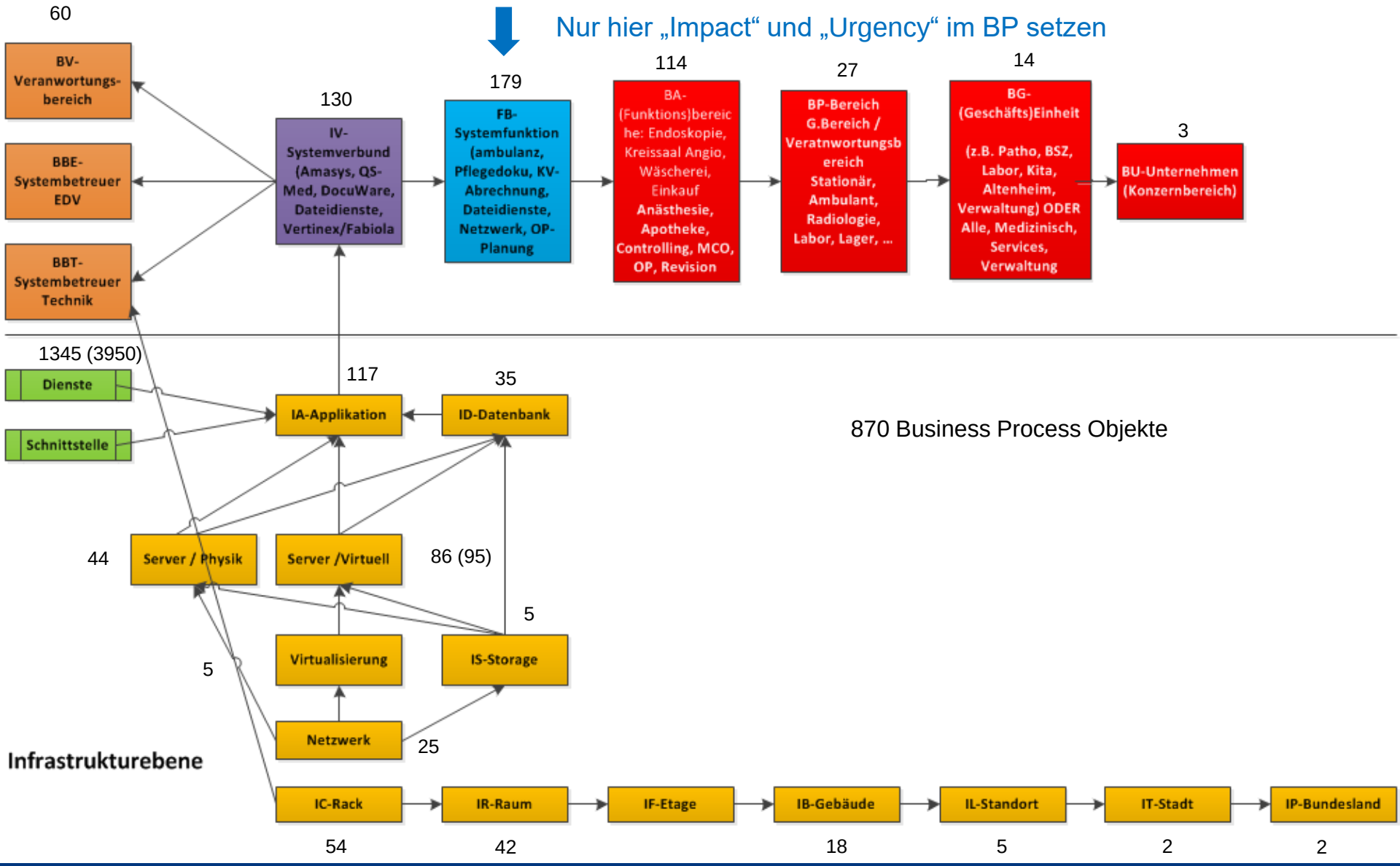
Examples of Application:

Urgent	ERP System
Urgent	Phone
High	Accounting Application in Backoffice
Medium	Office Printer of a User is broken
Low	The monitor in the entrance hall is off

Problem view	Priority	Status
DB node 1	Urgent (No impact)	Critical

Business Process Hierarchien

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken



Namenskonvention

s. Excelsheet Klassifikation BPs für Filterung BP-View

Filter für Prioritätenansicht

	Anfangsbuchstaben der BP	Prionummer = Tag in Neteye	Tag Headline	Tag Description	Risikobewertung Schutzziel
Step 1	Allen BPs einen Defaultwert geben.				
		999 Defaultwert	Defaultwert	Defaultwert	
Step 2	Allen BPs nach Typen einen Defaultwert geben (idealerweise direkt auf DB per SQL?)				
Bereiche	BB*	920 Bereiche	Verantwortungsbereiche	Verantwortungsbereiche	
Verantwortliche	BV*	910 Verantwortliche	Verantwortliche	Leitungen	
Geschäftsprozesse	BU* BG* BT* BA* BP*	850 Geschaeftsbereiche	Geschäftsbereiche	Geschäftsbereiche	
Applikationen	IA* ID*	750 Applikationen	Applikationen	Applikationen	
Server	SE* SA* ST* VE* VA* VT*	650 Server	Server	Server	
Storage	IS*	550 Storage	Storage	Storage	
Netzwerk	NF* NR* NS*	450 Netzwerk	Netzwerk	Netzwerk	
Standort	IC* IB* IR* IL* IT* IP*	350 Standort	Standort	Gebäude, Etagen, Räume	
Systemverbund	IV*	250 IV S P	Systemverbund Prio: normal	Schutzziel: Allgemeine Funktion	
Systemfunktion	FB*	150 FB S P	Systemfunktion Prio: normal	Schutzziel: Allgemeine Funktion	
Step3	FB wird von Hand die Prios der Risikoanalyse zugeordnet				
FB	Systemfunktion	111 FB S1 P1	Systemfunktion Prio: sehr hoch	Schutzziel: Sicherheit Patientenversorgung	Sicherheit Patientenversorgung
FB	Systemfunktion	112 FB S1 P2	Systemfunktion Prio: hoch	Schutzziel: Sicherheit Patientenversorgung	Sicherheit Patientenversorgung
FB	Systemfunktion	121 FB S2 P1	Systemfunktion Prio: sehr hoch	Schutzziel: Erhaltung lebensnotwengider Funktionsbereiche	Erhaltung lebensnotwendiger Funktionsbereiche
FB	Systemfunktion	122 FB S2 P2	Systemfunktion Prio: hoch	Schutzziel: Erhaltung lebensnotwengider Funktionsbereiche	Erhaltung lebensnotwendiger Funktionsbereiche
FB	Systemfunktion	131 FB S3 P1	Systemfunktion Prio: sehr hoch	Schutzziel: Wirtschaftliche und rechtliche Existenz	Wirtschaftliche und rechtliche Existenz
FB	Systemfunktion	132 FB S3 P2	Systemfunktion Prio: hoch	Schutzziel: Wirtschaftliche und rechtliche Existenz	Wirtschaftliche und rechtliche Existenz
FB	Systemfunktion	141 FB S4 P1	Systemfunktion Prio: sehr hoch	Schutzziel: Begrenzung wirtschaftlichen Schaden	Begrenzung Wirtschaftlicher Schaden
FB	Systemfunktion	142 FB S4 P2	Systemfunktion Prio: hoch	Schutzziel: Begrenzung wirtschaftlichen Schaden	Begrenzung Wirtschaftlicher Schaden

s. Excelsheet Namenskonvention

Namenskonvention NetEye (KONZEPT)

Monarch

Aliase werden grundsätzlich gleich benannt wie die Objekte selbst, um Fehler im System zu vermeiden.
Die Größe bzw. Länge der Namen wird begrenzt auf 40 Zeichen, da bei mehr als 40 Zeichen die Übersichtlichkeit des Systems leidet.

Aufbau	Beispiel	Erläuterungen
Host hier wird der tatsächliche Name des Hosts verwendet.	1. ve-rpdoc01-01 2. NS-14001	**Funktion eines Objekts:** NOTIFY: Gruppen mit diesem Term im Namen dienen lediglich der Alarmierungsübermittlung durch das System. Die Kontakte, die diesen Gruppen zugewiesen sind, haben grundsätzlich keinerlei Berechtigungen System. VIEW: Gruppen mit diesem Term im Namen dienen der Berechtigungsverwaltung im System. Kontakte in diesen Gruppen dürfen ausschließlich die LDAP-user enthalten. Für grundlegende Berechtigungen gibt es zwei Templates; das "login" Template, durch welches der Kontakt lediglich Leserechte auf alle Objekte im System erhält, und das "login-administrators" Template, durch welches der Kontakt alle Berechtigungen im System erhält. Sollten diese beiden Optionen nicht den Anforderungen entsprechen, kann man diese manuell pro Kontakt durch das setzen und entfernen von Häkchen im Berechtigungsbereich des LDAP-Contacts verändern. Hierbei gilt es zu beachten, dass das vordere "inheritance"-Häkchen vor der zu verändernden Berechtigung entfernt werden muss; ansonsten passt sich die Einstellung trotz Speichern wieder an das vergebene Template an!
Host Groups Block 1: **Objekt im System + Kürzel für Funktion der Gruppe** Block 2: **Abteilungs-/Bereichscode** Block 3: **Name der Gruppe**	1. **HGN-ESD-SharePoint** (Host Gruppe Notify-EDV Service Desk-SharePoint) 2. **HGV-EDV-Alle_Systeme** (Host Gruppe View-EDV Abteilung-Alle_Systeme)	
Host Profile Block 1: **Objekt im System + Kürzel für Art der Komponente** Block 2: **Abteilungs-/Bereichscode** Block 3: **Name des Profils**	1. **HPN-EBA- Extreme** (Host Profil Netzwerk-EDV Basis- Extreme) 2. **HPS-TFT-Telefonanlage** (Host Profil Server-Fernmeldetechnik-Telefonanlage)	
Contact Block 1: **Objekt im System + Kürzel für Art des Contacts** Block 2: **Abteilungs-/Bereichscode** Block 3: **Mail-Verteiler Name oder Name der Person**	1. **CGN-EDV-Basistechnologie** (Contact Mail-EDV Abteilung-Basistechnologie (-> *Verteiler!)* 2. **CTS-ELT-jdiener** (Contact SMS-EDV Leitung-jdiener)	
Contact Groups Block 1: **Objekt im System + Kürzel für Funktion der Gruppe** Block 2: **Abteilungs-/Bereichscode** Block 3: **Name der Gruppe**	1. **CGN-EDV-SysAdmin** (Contact Gruppe Notify-EDV Abteilung-SysAdmin) 2. **CGV-EDV-Alle_Systeme** (Contact Gruppe View-EDV Abteilung-Alle_Systeme)	**Arten von Kontakten:** LOGIN: Das ist der Kontakt, mit dem sich die entsprechende Person am System authentifiziert. Es handelt sich dabei um einen vom System automatisch angelegten LDAP User, welcher aus dem AD importiert wird. Er trägt immer den Namen des AD; d.h. das "LOGIN" kommt in diesem Namen nicht vor. Er wird ebenfalls für die Berechtigungen im System eingesetzt. MAIL: Das ist der Kontakt, über den die E-Mail Alarmierung stattfindet. SMS: Das ist ein spezieller Kontakt, der nur als Zusatzkontakt für eine Person angelegt wird, die zusätzlich per SMS benachrichtigt werden soll.
Service Block 1: **Objekt im System + Kürzel für Art des Checks** Block 2: **Abteilungs-/Bereichscode** Block 3: **Name des Service**	1. **SVS-TAG-APC_Akkustatus** (Service SNMP-Technik-Abt.-APC_Akkustatus) 2. **SVN-EBA-Windows_CPU** (Service NRPE-EDV Basis-Windows_CPU)	
Service Profile Block 1: **Objekt im System + Kürzel für Art der Komponente** Block 2: **Abteilungs-/Bereichscode** Block 3: **Name des Profils**	1. **SPS-EBA-Hyper_V** (Service Profil Server-EDV Basisadministration-Hyper_V) 2. **SPN-EBA-Extreme_Default** (Service Profil Netzwerk(-Switch)-EDV Basis-Extreme Default)	
Business Process Monitoring Da alle Business Prozesse als Services unter einem einzigen, "virtuellen" Host aufgeführt werden, sollte das Namensschema auf den ersten Blick eine Auskunft über seine tatsächliche Funktion geben.		
Generelle Konvention für Business Processes: Block 1: **Code für Art des Business Prozesses** Block 2: **betroffener Bereich** Block 3: **Name des BP; lang und verständlich!**	1. **BBW - EDV - Netzwerk Cores Alle** (BereichsBP-EDV Abteilung-Netzwerk_Cores_Alle) 2. **BGH-ZNA-SAP Applikation** (GeschäftsBP Alle Großbereiche-ZNA-SAP_Applikation)	
SMSTool: Kontakte im SMSTool werden stets nach dem Namenschema für SMS-Contacts (s.oben: Contacts) vergeben!	1. **CTS-ELT-jdiener** (Contact SMS-EDV Leitung-jdiener) 2. **CTS-EDV-modul** (Contact SMS-EDV Abteilung-modul)	
Time Periods: Block 1: **Abteilungs-/Bereichscode** Block 2: **Name/Bezeichnung der Zeitperiode**	1. **EDV-Bereitschaft** (einheitliche Bereitschaft) 2. **TFT-Bereitschaft** (Bereitschaft pro Bereich i.d. Abteilung) 3. **TET-Bereitschaft** (Bereitschaft pro Bereich i.d. Abteilung)	

Prio-Matrix aus Risikomanagement

Prioritäten	Prionummer	Kürzel	Label	Beschreibung	
Schutzziel1: Sicherheit Patientenversorgung					
		2	*ZD-1*	*ZD Sehr hoch*	Zentrale IT-Dienste Umgehend
		3	*ZD-2*	*ZD hoch*	Zentrale IT-Dienste schnellstmöglich
		4	S1-1	S1 Sehr hoch	Med.Prozesse Patientenversorgung Umgehend
		5	S1-2	S1 Hoch	Med.Prozesse Patientenversorgung schnellstmöglich
Schutzziel2: Erhaltung lebensnotwendiger Funktionsbereiche					
		8	S2-1	S2 Sehr hoch	Med.Prozesse Funktionsdienste Umgehend
		9	S2-2	S2 Hoch	Med.Prozesse Funktionsdienste schnellstmöglich
Schutzziel3: Wirtschaflich und rechtliche Existenz					
		10	S3-1	S3 Sehr hoch	Wirtschaftl. Existenz Umgehend
		11	S3-2	S3 Hoch	Wirschaftl. Existenz schnellstmöglich
Schutzziel4: Begrenzung Wirtschaftlicher Schaden					
		12	S4-1	S4 Sehr hoch	Wirtschaftl. Schaden Umgehend
		13	S4-2	S4 hoch	Wirtschaftl. Schaden schnellstmöglich
Normale Prioritäten					
		18	N-1	Sonstige Sehr hoch	IT-Systeme Umgehend (keine Schutzziele)
		19	N-2	Sonstige Hoch	IT-Systeme schnellstmöglich (keine Schutzziele)
		21	*ZD-3*	*ZD normal*	Zentrale IT-Dienste normale SLA
		23	S1-3	S1 normal	Med.Prozesse Patientenversorgung normale SLA
		27	S2-3	S2 normal	Med.Prozesse Funktionsdienste normale SLA
		29	S3-3	S3 normal	Wirtschaftl. Existenz normale SLA
		31	S4-3	S4 normal	Wirtschaftl. Schaden normale SLA
		37		Sonstige normal	IT-Systeme mit normlen SLA
		>=38	N-4	Niedrig	IT-Systeme mit geringer Priorität

Prio-Matrix Berechnung

		Impact					
		1	3	7	9	11	17
Urgency		ZD	S1	S2	S3	S4	N
1	Very High	2	4	8	10	12	18
2	High	3	5	9	11	13	19
20	Normal	21	23	27	29	31	37
37	Low	38	40	44	46	48	54

Performance

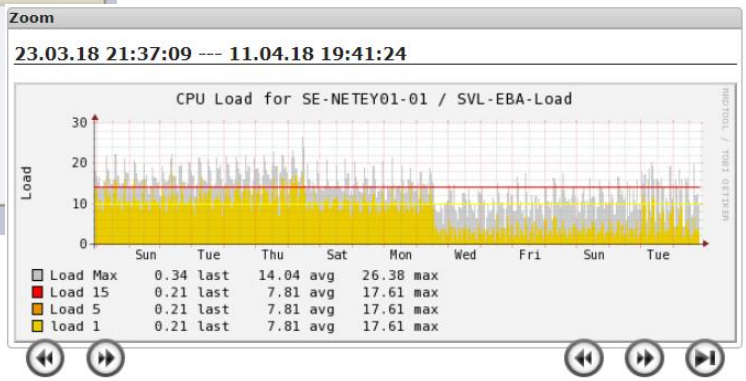
Select configuration interface: Business Process Monitoring Management

bu-kl

Name	Logical op	Info	Urgency	Impact	Number of children	Tag
BU-KL	Linear (AND)	Klinikum			70239	850

Services Actively Checked:

Time Frame	Services Checked
<= 1 minute:	1517 (38.0%)
<= 5 minutes:	3865 (96.8%)
<= 15 minutes:	3992 (100.0%)
<= 1 hour:	3992 (100.0%)
Since program start:	3992 (100.0%)



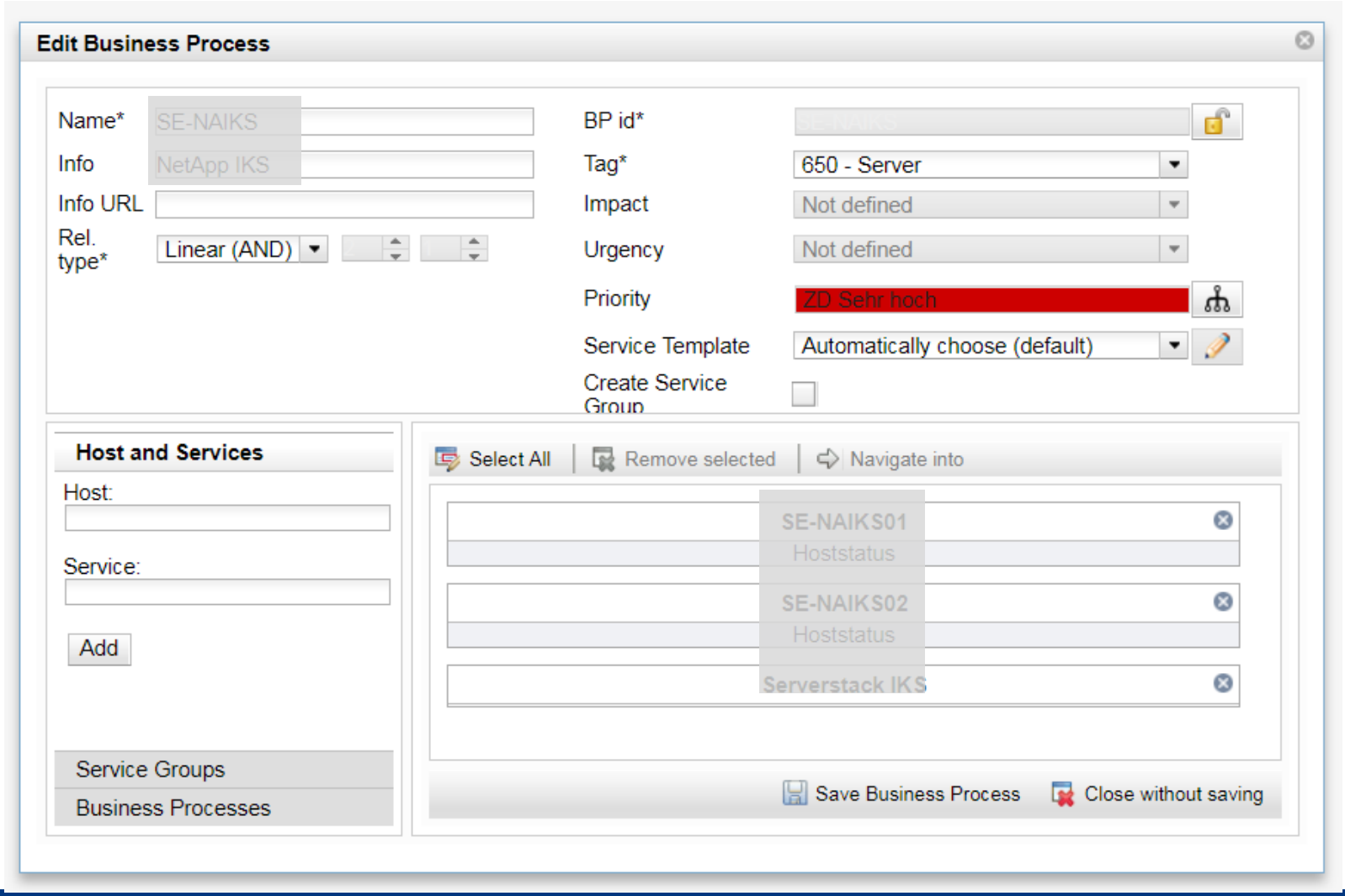
1x CBS+ Appliance 1xXeon 12Cores, 64GB RAM
1x CBS virtuell 2x virt. Kerne, 4GB RAM

Livestatus Statistics:

Type	Total	Rate	Cached
Servicechecks:	431,477	25.47 /sec	
Hostchecks:	19,599	0.93 /sec	
Forks:	6,756	0.23 /sec	
Connections:	21,634	1.33 /sec	
Requests:	26,086	1.51 /sec	
NEB Callbacks:	1,028,281	53.48 /sec	
Log Messages:	250	0.00 /sec	5,161

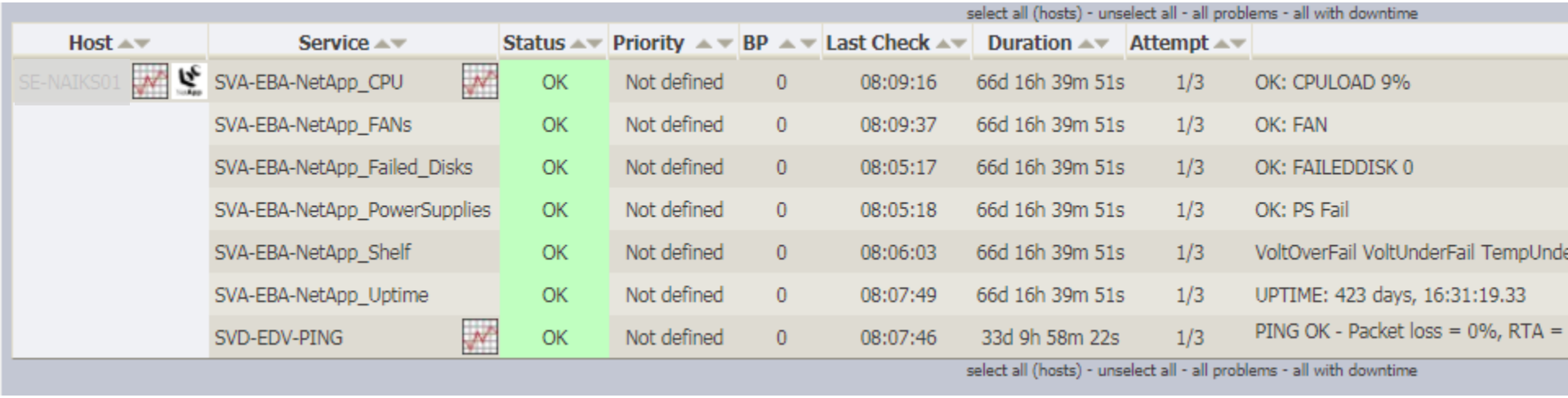
Praxis Tipps …

Im BP müssen alle wichtigen Host-Stati für die „Problem“-View Anzeige aufgenommen werden.
Hier schlechtes Beispiel mit nur Hoststatus!

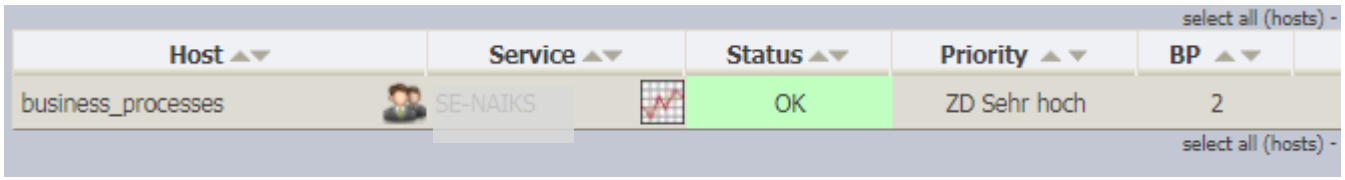


Praxis Tipps …

Physikalische Hosts der Netapp



Jeder physikalische Host bekommt einen gleichnamigen BP



Warum?

- Sonst werden in der „Problems“ View die Prios nicht korrekt angezeigt
- Der Status wäre nur unter „Host Detail“ und „Service Detail“ zu sehen.

Praxis Tipps …

Monitoring -> „Host Detail“

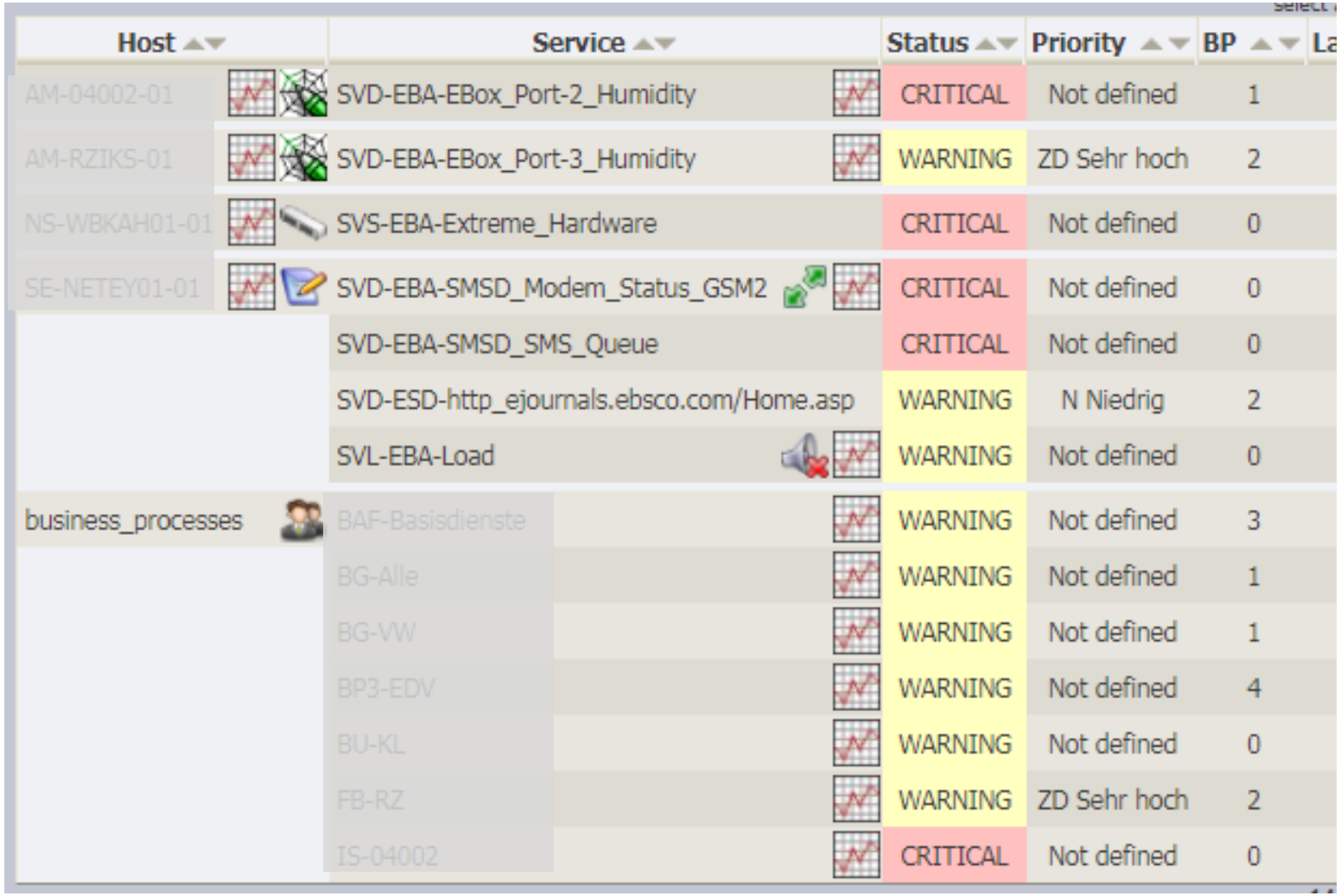
Host	Status	Priority	BP	Last Check
VE-NETEY01-01	UP	ZD hoch	2	16:11:48

Monitoring -> „Service Detail“

Host	Service	Status	Priority
VE-NETEY01-01	SVD-EDV-PING	OK	Not defined
	SVL-EBA-Disks_FreeSpace	OK	Not defined
	SVL-EBA-Load	OK	Not defined
	SVL-EBA-LoggedIn_Users	OK	Not defined
	SVL-EBA-Nagios_Log_NotificationProblem	OK	Not defined
	SVL-EBA-NetEye_HardwareStatus	OK	ZD hoch
	SVL-EBA-Total_Processes	OK	Not defined
	SVL-EBA-Uptime	OK	Not defined

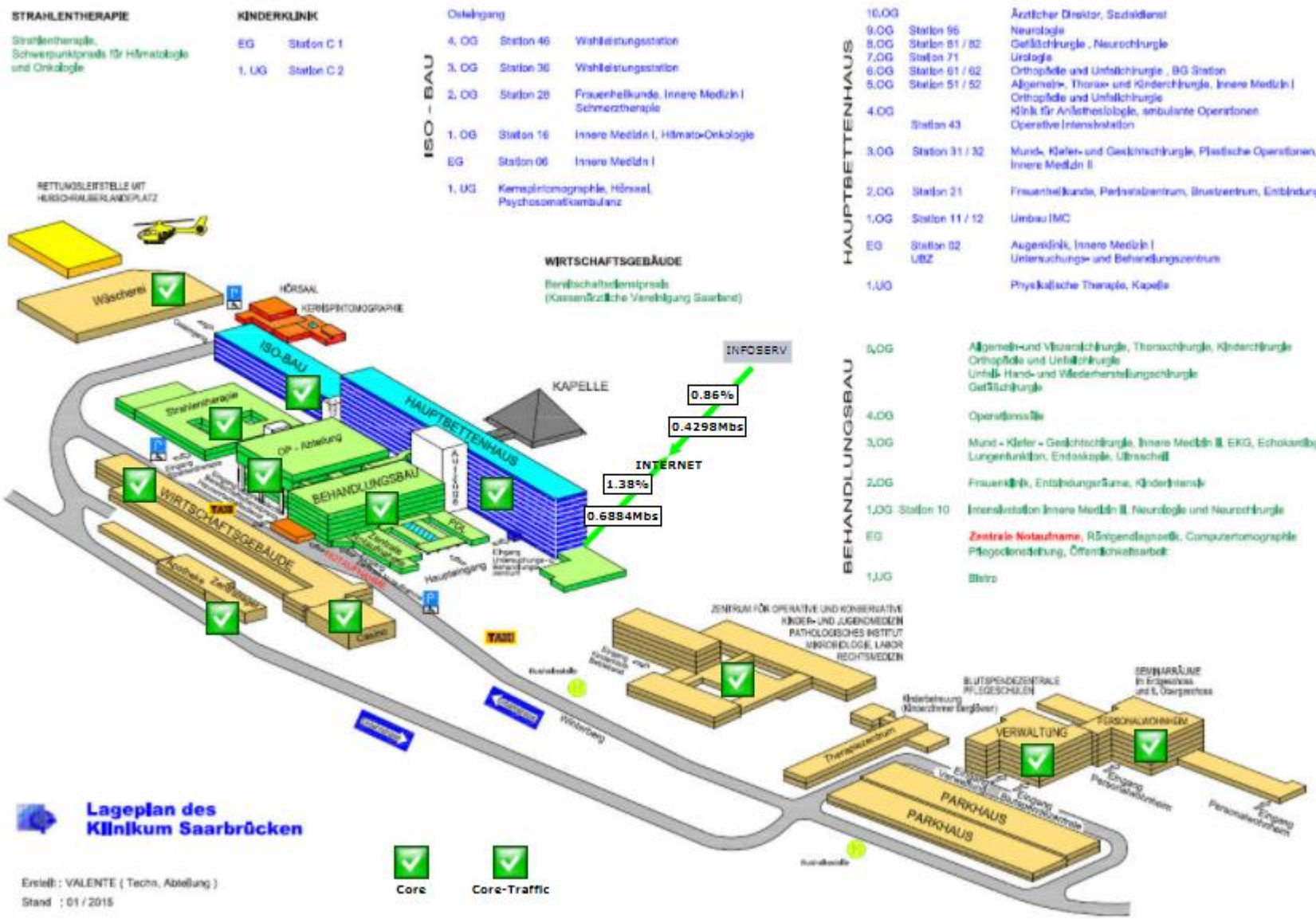
Praxis Tipps …

- Se-neteye01-01 -> nicht alles Service lösen „Alarm“ aus
- B* -> nicht alle Business Services haben Priorität



Host	Service	Status	Priority	BP
AM-04002-01	SVD-EBA-EBox_Port-2_Humidity	CRITICAL	Not defined	1
AM-RZIKS-01	SVD-EBA-EBox_Port-3_Humidity	WARNING	ZD Sehr hoch	2
NS-WBKAH01-01	SVS-EBA-Extreme_Hardware	CRITICAL	Not defined	0
SE-NETEY01-01	SVD-EBA-SMSD_Modem_Status_GSM2	CRITICAL	Not defined	0
	SVD-EBA-SMSD_SMS_Queue	CRITICAL	Not defined	0
	SVD-ESD-http_ejournals.ebsco.com/Home.asp	WARNING	N Niedrig	2
	SVL-EBA-Load	WARNING	Not defined	0
business_processes	BAF-Basisdienste	WARNING	Not defined	3
	BG-Alle	WARNING	Not defined	1
	BG-VW	WARNING	Not defined	1
	BP3-EDV	WARNING	Not defined	4
	BU-KL	WARNING	Not defined	0
	FB-RZ	WARNING	ZD Sehr hoch	2
	IS-04002	CRITICAL	Not defined	0

Netzwerkübersicht



NetEyeThruk | NetEyeThruk | Bereichssicht.htm

se-netey01-01/thruk/#/main.php

WÜRTHPHOENIX NetEye

- Home
- Monitoring
- Reporting
- Configuration
- Extensions
  - Business Monitoring
  - Capacity Mgmt
  - Network Analisys
  - Net Monitor
  - NagVis
  - NagMap
  - Event Console
  - Action Launchpad
  - Log Manager
  - Shutdown Management
  - Kibana Dashboard
  - SMS Tool
  - Grafana Dashboard

WÜRTHPHOENIX NetEye

Version 3.12

"Sun Dec 31 2017"

Check for NetEye updates

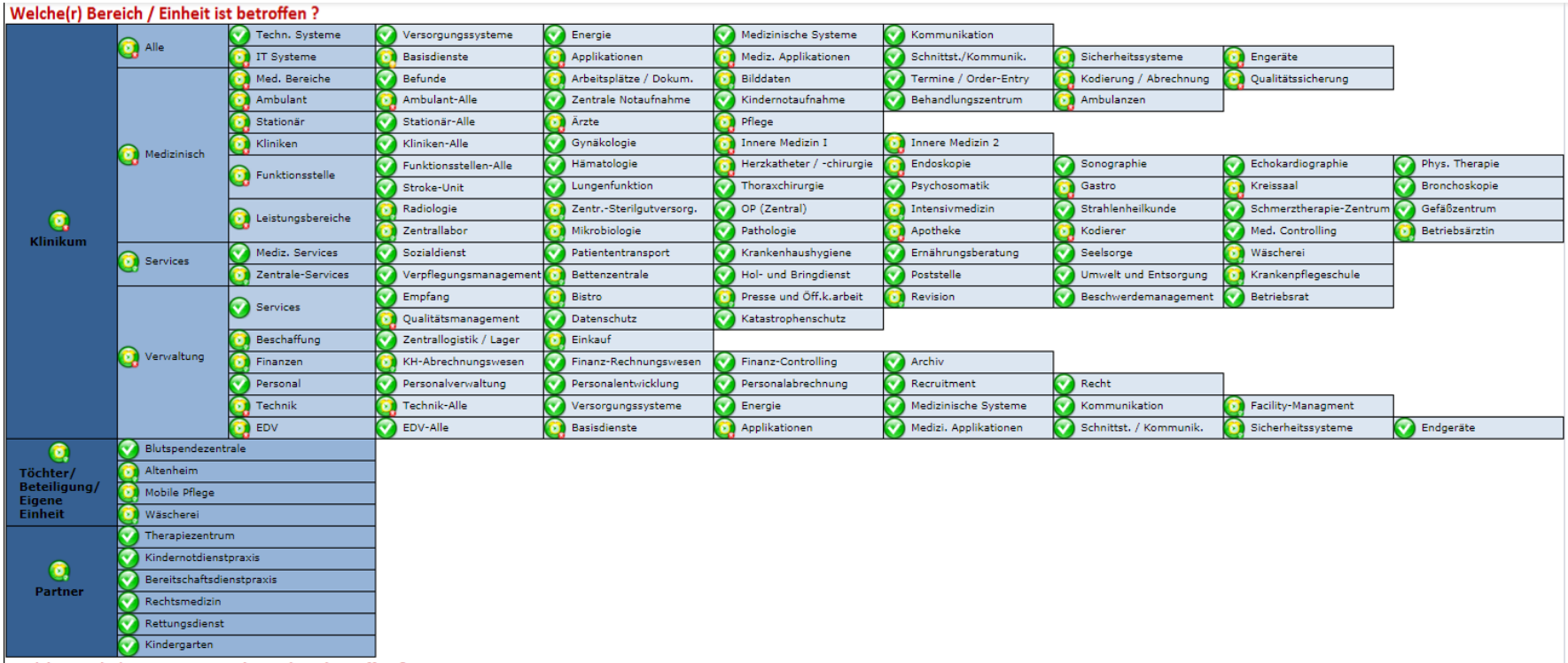
Powered by:

WÜRTHPHOENIX

Verknüpfungen | Desktop | Bibliotheker | 10:00

Bereichssicht / Geschäftsprozesse

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken



Startseite des IT-Monitoring / Auskunftssystem

Bereichssicht

Beantwortet die Fragen

- Welche(r) Bereich / Organisationseinheit ist betroffen?
- Welcher Fach-/Verantwortungsbereich ist betroffen?
- Welcher Servicebereich ist Zuständig / soll informiert werden?

Info: Diese Sicht gibt eine generelle Information zu den Systemstati. Sie dient nicht zur Bewertung von Eskalationen z.B. gibt es Systeme die Nachts und am Wochenende keine Relevanz haben.

Risikomanagement

Schutzziele

1. Patientenversorgung (Sehr hoch / Hoch)
2. Wichtige Funktionsbereiche (Sehr hoch / Hoch)
3. Wirtschaftlich & rechtliche Existenz (Sehr hoch / Hoch)
4. Begrenzung wirtschaftlicher Schaden (Sehr hoch / Hoch)
5. Systeme mit normaler Priorität (Normal)

Beantwortet die Fragen

- Welche Relevanz hat ein Systemausfall aus der Bereichssicht für die Nacht und das Wochenende?

Info: Diese Sicht dient der Unterstützung zur Einschätzung ob ein Systemausfall eskaliert werden muss

Infrastruktursicht

Mit den Teilsichten:

- Standorte
- Netzwerk
- Server (Hardware)
- Applikationen

Beantwortet die Fragen

- Welche Infrastruktur ist betroffen (Hardware/Raum)
- Wo befindet sich die Lokation der betroffenen Komponenten

Info: Die Sicht dient primär der EDV, Technik und Dienstleistungspartner zur schnellen Lokation des Problems

Netzwerkübersicht

Beantwortet die Frage

- Liegen Netzwerkstörungen vor?
- Wo sind die betroffenen Komponenten zu finden?
- Hat das Netzwerk Lastprobleme?

Info: Die Sicht dient primär der EDV, Technik und Dienstleistungspartner zur schnellen Lokation des Problems

NetEyeThruk

NetEyeThruk

monitoring/thruk/#/main.php

WÜRTHPHOENIX NetEye

- Home
- Monitoring
  - Tactical Overview
  - Service Detail
  - Host Detail
  - Host Groups
  - Service Groups
  - Problems
  - Comments
  - Downtime
  - Status Map
  - Nagios Status Map
- Reporting
- Configuration
- Extensions

WÜRTHPHOENIX NetEye

Version 3.12

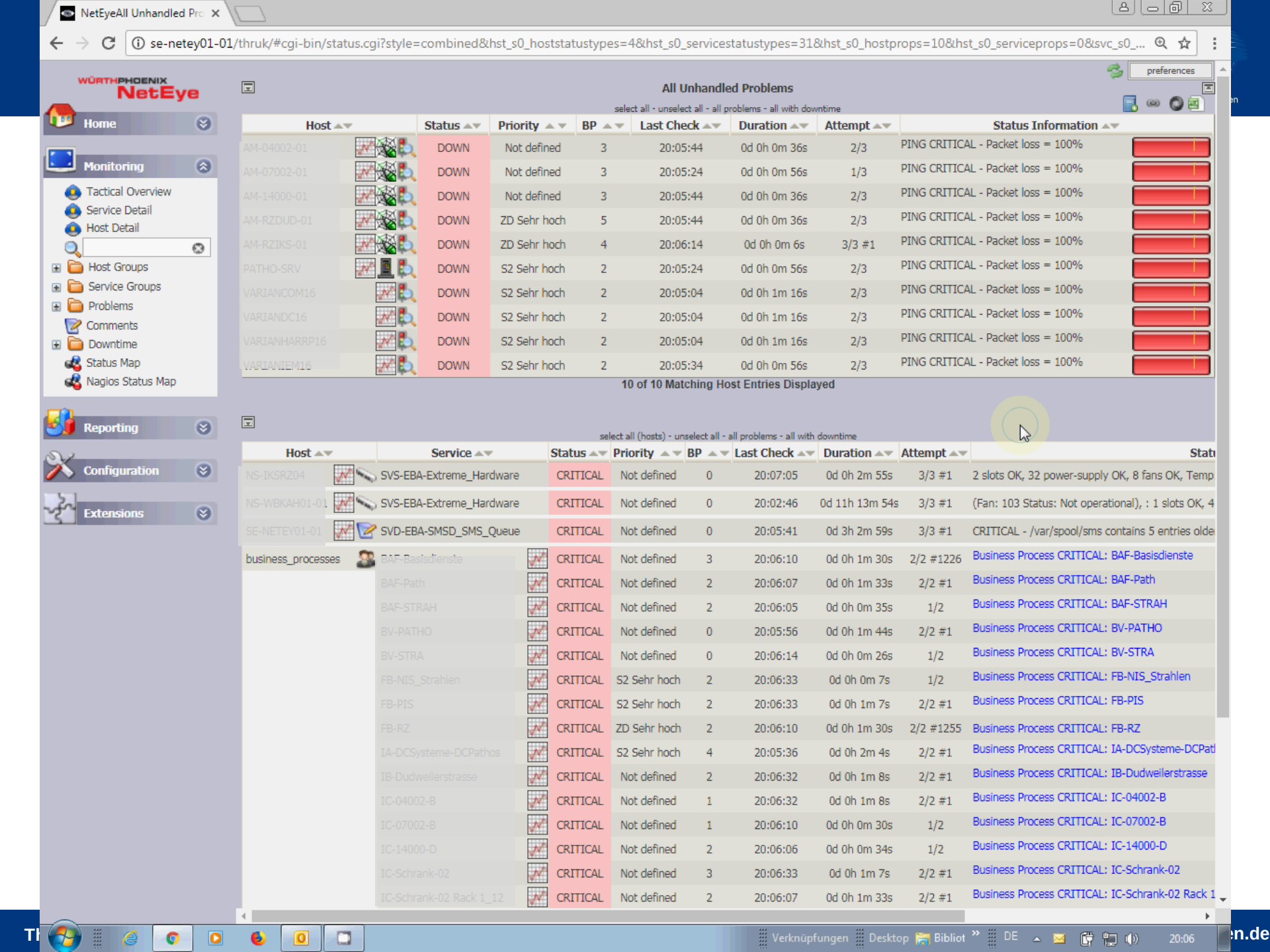
"Sun Dec 31 2017"

Check for NetEye updates

Powered by:

WÜRTHPHOENIX

Verknüpfungen Desktop Bibliotheker DE 15:58


NetEyeAll Unhandled Pro
se-netey01-01/thruk/#cgi-bin/status.cgi?style=combined&hst_s0_hoststatustypes=4&hst_s0_servicestatustypes=31&hst_s0_hostprops=10&hst_s0_serviceprops=0&svc_s0_...
WÜRTHPHOENIX NetEye
preferences
Home
Monitoring
Tactical Overview
Service Detail
Host Detail
Host Groups
Service Groups
Problems
Comments
Downtime
Status Map
Nagios Status Map
Reporting
Configuration
Extensions
All Unhandled Problems
select all - unselect all - all problems - all with downtime
Host
Status
Priority
BP
Last Check
Duration
Attempt
Status Information
AM-04002-01 DOWN Not defined 3 20:05:44 0d 0h 0m 36s 2/3 PING CRITICAL - Packet loss = 100%
AM-07002-01 DOWN Not defined 3 20:05:24 0d 0h 0m 56s 1/3 PING CRITICAL - Packet loss = 100%
AM-14000-01 DOWN Not defined 3 20:05:44 0d 0h 0m 36s 2/3 PING CRITICAL - Packet loss = 100%
AM-RZDUD-01 DOWN ZD Sehr hoch 5 20:05:44 0d 0h 0m 36s 2/3 PING CRITICAL - Packet loss = 100%
AM-RZIKS-01 DOWN ZD Sehr hoch 4 20:06:14 0d 0h 0m 6s 3/3 #1 PING CRITICAL - Packet loss = 100%
PATHO-SRV DOWN S2 Sehr hoch 2 20:05:24 0d 0h 0m 56s 2/3 PING CRITICAL - Packet loss = 100%
VARIANCOM16 DOWN S2 Sehr hoch 2 20:05:04 0d 0h 1m 16s 2/3 PING CRITICAL - Packet loss = 100%
VARIANDC16 DOWN S2 Sehr hoch 2 20:05:04 0d 0h 1m 16s 2/3 PING CRITICAL - Packet loss = 100%
VARIANHARRP16 DOWN S2 Sehr hoch 2 20:05:04 0d 0h 1m 16s 2/3 PING CRITICAL - Packet loss = 100%
VARIANIEM16 DOWN S2 Sehr hoch 2 20:05:34 0d 0h 0m 56s 2/3 PING CRITICAL - Packet loss = 100%
10 of 10 Matching Host Entries Displayed
select all (hosts) - unselect all - all problems - all with downtime
Host
Service
Status
Priority
BP
Last Check
Duration
Attempt
Stat
NS-IKSRZ04 SVS-EBA-Extreme_Hardware CRITICAL Not defined 0 20:07:05 0d 0h 2m 55s 3/3 #1 2 slots OK, 32 power-supply OK, 8 fans OK, Temp
NS-WBKAH01-01 SVS-EBA-Extreme_Hardware CRITICAL Not defined 0 20:02:46 0d 11h 13m 54s 3/3 #1 (Fan: 103 Status: Not operational), : 1 slots OK, 4
SE-NETEY01-01 SVD-EBA-SMSD_SMS_Queue CRITICAL Not defined 0 20:05:41 0d 3h 2m 59s 3/3 #1 CRITICAL - /var/spool/sms contains 5 entries olde
business_processes BAF-Basisdienste CRITICAL Not defined 3 20:06:10 0d 0h 1m 30s 2/2 #1226 Business Process CRITICAL: BAF-Basisdienste
BAF-Path CRITICAL Not defined 2 20:06:07 0d 0h 1m 33s 2/2 #1 Business Process CRITICAL: BAF-Path
BAF-STRAH CRITICAL Not defined 2 20:06:05 0d 0h 0m 35s 1/2 Business Process CRITICAL: BAF-STRAH
BV-PATHO CRITICAL Not defined 0 20:05:56 0d 0h 1m 44s 2/2 #1 Business Process CRITICAL: BV-PATHO
BV-STRA CRITICAL Not defined 0 20:06:14 0d 0h 0m 26s 1/2 Business Process CRITICAL: BV-STRA
FB-NIS_Strahlen CRITICAL S2 Sehr hoch 2 20:06:33 0d 0h 0m 7s 1/2 Business Process CRITICAL: FB-NIS_Strahlen
FB-PIS CRITICAL S2 Sehr hoch 2 20:06:33 0d 0h 1m 7s 2/2 #1 Business Process CRITICAL: FB-PIS
FB-RZ CRITICAL ZD Sehr hoch 2 20:06:10 0d 0h 1m 30s 2/2 #1255 Business Process CRITICAL: FB-RZ
IA-DCSysteme-DCPathos CRITICAL S2 Sehr hoch 4 20:05:36 0d 0h 2m 4s 2/2 #1 Business Process CRITICAL: IA-DCSysteme-DCPath
IB-Dudweilerstrasse CRITICAL Not defined 2 20:06:32 0d 0h 1m 8s 2/2 #1 Business Process CRITICAL: IB-Dudweilerstrasse
IC-04002-B CRITICAL Not defined 1 20:06:32 0d 0h 1m 8s 2/2 #1 Business Process CRITICAL: IC-04002-B
IC-07002-B CRITICAL Not defined 1 20:06:10 0d 0h 0m 30s 1/2 Business Process CRITICAL: IC-07002-B
IC-14000-D CRITICAL Not defined 2 20:06:06 0d 0h 0m 34s 1/2 Business Process CRITICAL: IC-14000-D
IC-Schrank-02 CRITICAL Not defined 3 20:06:33 0d 0h 1m 7s 2/2 #1 Business Process CRITICAL: IC-Schrank-02
IC-Schrank-02 Rack 1_12 CRITICAL Not defined 2 20:06:07 0d 0h 1m 33s 2/2 #1 Business Process CRITICAL: IC-Schrank-02 Rack 1
Verknüpfungen
Desktop
Bibliot
DE
20:06

NetEyeThruk | Buiness Process View | Buiness Process View | Buiness Process View | Buiness Process View | NetEyeThruk

se-netey01-01/thruk/#/main.php

WÜRTHPHOENIX NetEye

- Home
- Monitoring
- Reporting
- Configuration
- Extensions
  - Business Monitoring
    - Process View
    - Business Impact
  - Capacity Mgmt
  - Network Analisys
  - Net Monitor
  - NagVis
  - NagMap
  - Event Console
  - Action Launchpad
  - Log Manager
  - Shutdown Management
  - Kibana Dashboard
  - SMS Tool
  - Grafana Dashboard

WÜRTHPHOENIX NetEye

Version 3.12
"Sun Dec 31 2017"

Check for NetEye updates

Powered by: WÜRTHPHOENIX

Verknüpfungen | Desktop | Bibliotheker | DE | 15:11

NetEyeThruk | Business Impact Analyse

se-netey01-01/thruk/#/main.php

WÜRTHPHOENIX NetEye

- Home
- Monitoring
- Reporting
- Configuration
- Extensions
  - Business Monitoring
    - Process View
    - Business Impact
  - Capacity Mgmt
  - Network Analisys
  - Net Monitor
  - NagVis
  - NagMap
  - Event Console
  - Action Launchpad
  - Log Manager
  - Shutdown Management
  - Kibana Dashboard
  - SMS Tool
  - Grafana Dashboard

WÜRTHPHOENIX NetEye

Version 3.12
"Sun Dec 31 2017"

Check for NetEye updates

Powered by:
WÜRTHPHOENIX

Verknüpfungen Desktop Bibliotheker 15:22

Lessons Learned / Whishlist

Bei der Umsetzung

- Konzept sehr wichtig damit multifunktionalen Ansatz erfolgen kann
  → Synergie mit Risikomanagement und ISO/27001
- Commitment zu „Weg“
  -> Zeitaufwendig / Ressourcenbedarf nicht unterschätzen
- Hat EDV Mitarbeitern geholfen
  (Bereitschaft, 18:00 Uhr Dienst)

Danke an‘s Würth Team,
dass Sie bei der Umsetzung der Vision geholfen haben!

Im Produkt / Wunschliste

- Performance !
- Visuelle Aufbereitung verbessern
  - „Priority“ Ausweisung als eigene Spalten die man Filtern kann. Sortiert nach Prionummern
  - Priorität in Business-View bis auf Asset in Anzeige „vererben“
  - Ausweisung der „root cause“ / „Impact“
- Erizone Integration verbessern -> BP Downtime trägt alle abhängigen Objekte und Assets in ein Change-Ticket ein.
- Mehr vorgefertigte Standardkonfigurationen / Best-Practice
- Export für ISMS (Verinice) + ISMS View
- Integration Vulnerabilitymanagement (OpenVAS, Greenbone)

Vielen Dank für Ihre Aufmerksamkeit!