Ausfallsicherheit und Zukunftsfähigkeit der Feuerwehr Bergisch Gladbach

Prof. Dr. Johannes Berens, M.Sc.
concepture GmbH

Wer wir sind

Wir sind interdisziplinäre SpezialistInnen in den Bereichen:
Managementsysteme, Informationssicherheit, BCM, Sicherheitsberatung und Cybersicherheit

SEIT
2001
arbeiten wir für Ihre Sicherheit

Durchschnittsalter
36 Ø

4
Standorte
vom Bodensee bis zur Nordsee

6
Sprachen

Mehr als
2.500
Projekte seit Gründung
in verschiedenen Sicherheitsdisziplinen

29
zertifizierte Mitarbeiter
im Team

Auftrag

Auftrag:

Die IT der Feuerwehr Bergisch Gladbach soll auf Ausfallsicherheit geprüft werden.

Hintergrund

- In den letzten zwei Dekaden wurden zunehmend analoge Geschäftsprozesse digitalisiert.
- Häufig ist die Digitalisierung durch Dritte vorgegeben und nicht optional
- Nach einer betrieblichen Gewöhnung entfallen zunehmend analoge Redundanzen.
- Ein Ausfall digitaler Dienste führt meist zu einem Ausfall analoger Geschäftsprozesse.
- Bisherige Ausfälle und Störungen der IT tragen zur Sorge der Ausfallsicherheit der Feuerwehr bei

Der Anspruch an die Ausfallsicherheit der IT ergibt sich aus dem Schutzbedarf der Geschäftsprozesse der Feuerwehr.

Betroffene Geschäftsprozesse innerhalb der Feuerwehr:

- Brandschutz und Rettungsdienst
- Städtischen Krisenmanagement
- Bevölkerungsschutz

Module und Vorgehen

Modul 1: Schutzbedarfsanalyse

- Aufstellen einer Prozesslandkarte
- Ermitteln der Ausfallzeiten
- Zuordnen notwendiger Hard- und Software

Ergebnis Modul 1: Rangfolge der Prozesse nach Kritikalität und Schutzbedarf (Ist-Zustand)

Modul 2: Inventarisierung IT Dienste der städtischen IT

- Inventarisieren der korrespondierenden Hard- und Software bei der städtischen IT
- Ermitteln der maximalen Wiederherstellzeiten
- Vergleich maximaler Ausfallzeiten zu Wiederherstellzeiten

Ergebnis Modul 2: Rangfolge der IT-Dienste nach Abweichung von Ist-Schutz zu Soll-Schutz

Modul 3: Konzeption und Implementation der Maßnahmen

- Risikobewältigungsstrategien (Vermeiden, Mitigieren, Transferieren), Auswählen der geeigneten Maßnahmen
- Festlegen von Redundanzen

Ergebnis Modul 3: Maßnahmenplan

Methodik Prozessinventarisierung

Stakeholder FW GL

1. Inventarisierung der Prozesse mit Fachabteilungsleitungen
2. Ermitteln der maximalen Ausfallzeit und zeitkritischen Prozesse
3. Ermitteln der benötigten Hard- & Software
4. Ermitteln möglicher Redundanzen

Stakeholder IT

1. Überprüfen der Prozesse
2. Konkretisieren der Hard- & Software städtischer IT
3. Vergleich maximalen Ausfallzeit und Wiederherstellzeiten

Prozess-Inventar

Prozesse (Beispiel)

Abteilung	Abt.	Kernprozess	Tätigkeit	MAZ Regelbetrieb	MAZ Notbetrieb
Einsatzdienst / Organisation	10-11	Alarmierung – Notrufannahme (Leitstelle RBK)	Annahme des Notrufes und Disponierung der Einheiten	1 min	1 min
		Alarmierung - DME	Auslösen der DME	1 min	1 min
		Alarmierung - Wache	Wachdurchsage, Alarmdrucker, Alarmlicht, Torsteuerung	1 min	1 min
		Einsatz abarbeiten		1 min	1 min
		Tages-Dienstplanung	Vorplanung für 24Std Dienst	72h	72h
		Fahrt zur Einstelle	Wache -Einsatzstelle und zurück	1 min	1 min
		Kommunikation Fahrzeuge - Leitstelle	Einsatzstellenfunk, Status	1 min	1 min
		Monats-Dienstplanung	Vorplanung für einen Monat	1 Woche	1 Woche
		Grundbedürfnisse Mitarbeiter	Essen, Trinken, Schlafen, Sanitär	4h	4h
		Einsatzbereitschaft wieder herstellen	Personal für die Werkstätten	1 h	1 h
		Einsatzkonzepte	Erstellen von Einsatzkonzepten (AAO, SER)	3 Monate	
		Bedarfsplanung	Brandschutzbedarfsplan	3 Monate	

Prozesse

Abteilung	Abt.	Kernprozess	MAZ Regelbetrieb	MAZ Notbetrieb	Hardware	Software
Einsatzdienst / Organisation	10-11	Alarmierung - Notrufannahme	1 min	1 min	Kreisleitstelle	
		Alarmierung - DME	1 min	1 min	DME	
		Alarmierung - Wache	1 min	1 min	eigenes VPN	AmobilePro
		Einsatz abarbeiten	1 min	1 min	Tablet	Alamos
		Tages-Dienstplanung	72h	72h	PC, Telefon	SIEDA (MS Planner)
		Fahrt zur Einstelle	1 min	1 min		
		Kommunikation Fahrzeuge - Leitstelle	1 min	1 min		
		Monats-Dienstplanung	1 Woche	1 Woche	PC, Telefon	SIEDA (MS Planner)
		Grundbedürfnisse Mitarbeiter	4h	4h		
		Einsatzbereitschaft wieder herstellen	1 h	1 h		
		Einsatzkonzepte	3 Monate		PC, Telefon	Office
		Bedarfsplanung	3 Monate		PC, Telefon	Office

Ergebnis kritische Ausfallzeiten

Kurzfristig: eine Minute bis vier Stunden

- Einsatzdienst
- Erhalt der Einsatzfähigkeit
- Stabsarbeit
- Reaktion auf Großveranstaltungen

Mittelfristig: ein Arbeitstag bis eine Woche

- Gerätewesen
- Planwesen
- Personalkoordination

Langfristig: mehrere Wochen und Monate

- Erstellen des Haushalts
- Ausschreibungen, Konzepte

Ergebnis IT Bedarf Feuerwehr

IT-Bedarf Feuerwehr

Benötigte Hardware

- PC ohne besondere Spezifikation
- Tablets / Smartphones
- Telefon
- Internetzugang
- Videokonferenzsysteme
- Satellitentelefone und Internetverbindung
- Drucker

IT-Bedarf Feuerwehr

Benötigte Software

- Acrobat Reader
- Alamos (Alarmierungs- und Einsatzführungssystem)
- Arigon (Personalmangement)
- Bugzilla (Digitale Reparaturverwaltung)
- Citko e-Soll (Finanzsoftware)
- Dräger-Ware (Software für Atemschutzwerkstatt)
- Geoservices (Geodaten zur Einsatzplanung und -lenkung)
- Infoma (Finanzsoftware)
- LIS (Abrechnungssoftware für Rettungsdienst)
- Microsoft Office
- Mitarbeiterportal SIEDA (Digitale Mitarbeiterplattform Dienstplanung)
- Sieda (Dienstplanungssoftware
- WebEx (Video, Telefonie - und Kommunikationsplattform des FB 10)
- X-Change

IT-Bedarf Feuerwehr

Hardware & Software mit besonderem Anspruch an die Ausfallsicherheit

- Telefon, Funk, Satellit
- Alamos auf Tablets für Einsatzbearbeitung
- Alamos zur Wachsteuerung
- Office, Sieda und Acrobat Reader auf PC
- Abgesetzter Einsatzleitplatz mit Zugriff auf Kreisleitstellen-Rechner

Inventarisierung städtische IT

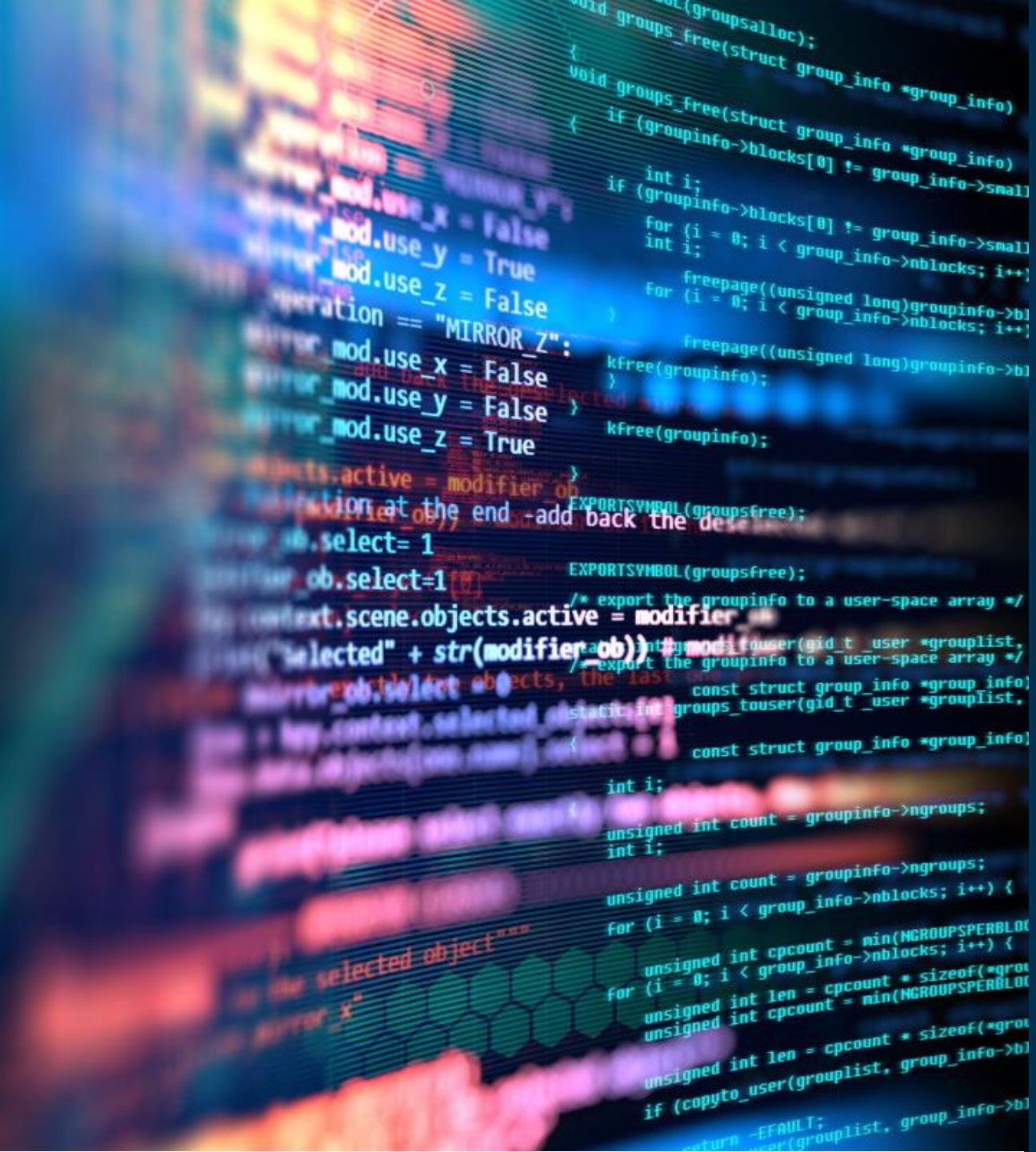
IT-Inventarisierung

Ergebnis der Inventarisierung mit der städtischen IT:

- Die Dienste auf Servern im Rathaus sind teilweise gespiegelt
- Ein weiteres RZ kann bestimmte Dienste übernehmen. Welche das sind, ist nicht definiert und dokumentiert. Grad der Redundanz ist nicht bekannt.
- Wegen fehlender Erfahrung und fehlenden Ressourcen kann die Wiederherstellungsdauer nicht beziffert werden

ABER:

- Eine Wiederherstellung eines Dienstes in weniger als 24h kann ausgeschlossen werden
- Wie lange eine Wiederherstellung jenseits der 24h benötigt, kann nicht beziffert werden. Es gilt Gründlichkeit vor Schnelligkeit
- Ein Notdienst außerhalb der Regelarbeitszeit ist nicht vorgesehen und personell nicht leistbar



Zwischenfazit und Empfehlung

Zwischenfazit

Bei einem Ausfall von Hard- oder Software von mehr als 24h:

- Werktags: überschreiten mindestens **46 von 155 Prozesse** die maximale Ausfallzeit
- Wochenende / Feiertag: überschreiten mindestens **74 von 155 Prozesse** die maximale Ausfallzeit

Ergebnis:

- Bereits Stromausfall führt zu einem Totalverlust der städtischen IT
- Die städtische IT für die Feuerwehr ist nicht ausreichend vor Ausfall geschützt
- Eine städtische Notfallplanung „IT-Ausfall“ liegt nicht vor und eine Lösung muss während eines Ausfalls gesucht werden.

Würdigung:

Die Resilienz der städtischen IT entspricht jeder Organisation, die viele Stakeholder bedient, über Dekaden historisch gewachsen ist, dabei situativ erweitert wurde und Dienste für neue Anforderungen teils kurzfristig adaptieren musste. Während frühe Phasen der Digitalisierung die Effizienz adressierte, rücken Anforderungen an die IT-Sicherheit und das Notfallmanagement erst in den letzten Jahren vermehrt in den Fokus. Die städtische IT ist im kommunalen Umfeld und auch im Vergleich zu kleinen und mittelständischen Unternehmen keine Ausnahme.

Conclusion: Optionen zur Sicherung der IT FW BG

Lösung:

Option 1 – Ertüchtigung der städtischen IT:

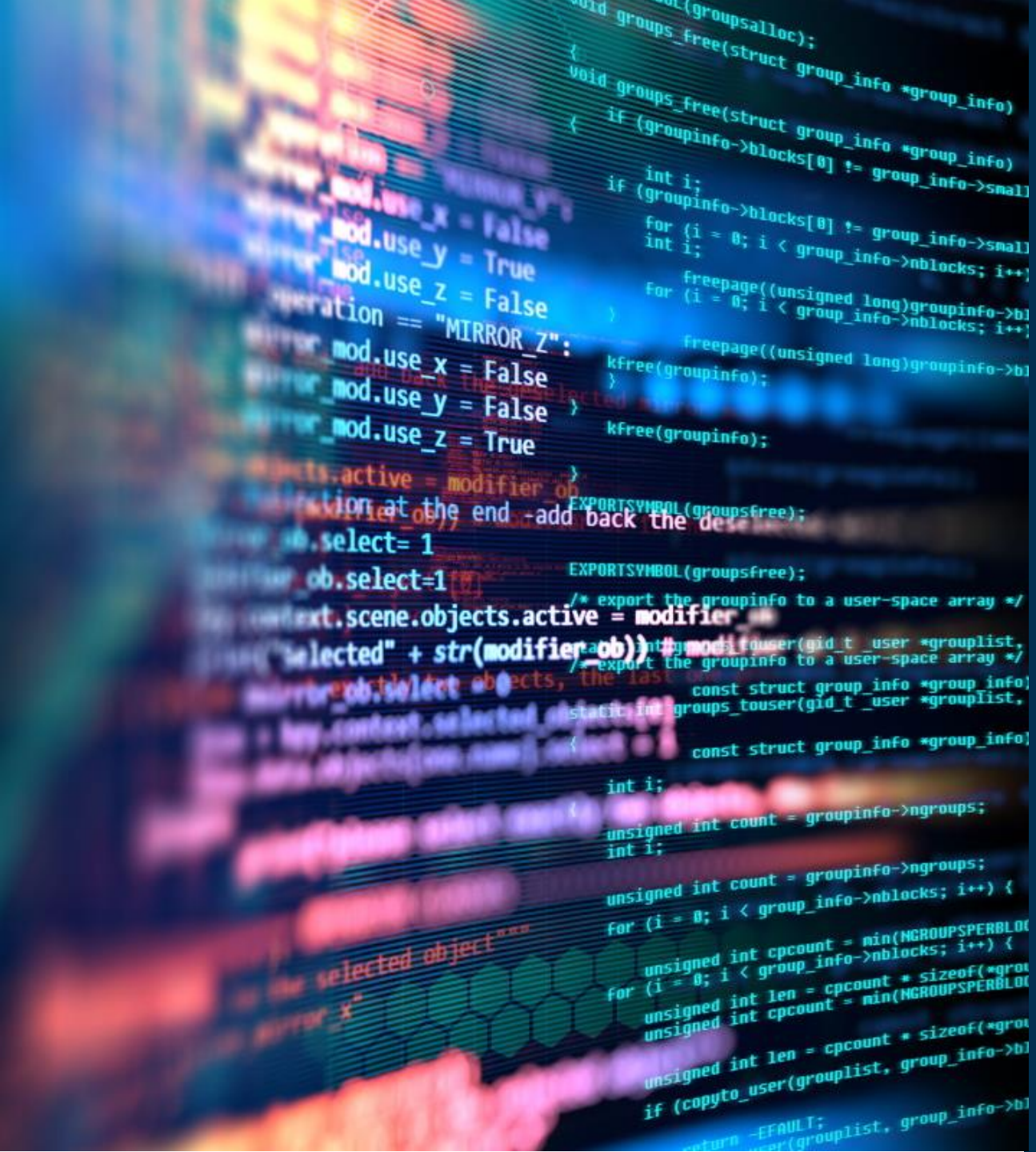
Wenn IT-Dienste durch die Stadt gestellt werden, dann wird zeitnah benötigt:

- Ausfallsichere Infrastruktur: georedundant gespiegelte, notstromversorgte Rechenzentren nach BSI-C5
- personellen Ressourcen für einen 24/7 Notdienst
- Aufbau eines ISMS und eines BCMS inklusive Notfall- und Krisenmanagements bei der IT

Option 2 – Schaffen einer unabhängigen IT-Infrastruktur FW BG

Erweiterung und damit Entkopplung der vorhandenen feuerwehreigenen IT durch

- Aufbau eigener redundanter Server
- Anmietung weiterer Cloudlösungen



Prüfung „eigene IT“

Option 2 – eigene IT-Infrastruktur FW BG

Bereits vorhandene selbst gestellte Lösungen:

- Alarmierungssystem (HPE HW)
- Eldis (Einsatzleitplatz)
- Firewall Sophos
- Führungsunterstützung (LARDIS)
- Ipads (Einsatzunterstützung)
- Netzwerk (VPN, Remote Desktop)
- Nextcloud
- Sat-Anbindung (Starlink, Iridium)
- Server-Infrastruktur (AV Raum, Racks, USV)
- Switch Cisco
- Telefonie Cisco
- Telekom-Anbindung
- ViKo Cisco
- Wachalarm
- Wlan Cisco Meraki

Option 2 – eigene IT-Infrastruktur FW BG

Bereits vorhandene Lösungen

- Auswahl eines Hochsicherheitsrechenzentrum
- Mehrfachanbindung an dieses Hochsicherheitsrechenzentrum
- Einsatz nur von sicherheitszertifizierten Kommunikationsplattformen
- Komplette Notstromversorgung der Standorte inkl. aller Endgeräte

Fehlende Lösungen

- Einbindung städtischer Software (~~Outlook~~, **Infoma**, Session, **Kosy**, Citko.esoll, OKVS)
  - Die meisten städtischen Anwendungen sind bereits webbasiert und werden bis auf Outlook und citko.esoll nur gelegentlich benötigt.
- Applikationsserver
- Backupserver
- Datenbankserver
- Fileserver
- Lizenzmanagement
- Support

- Endgeräte
- Endpoint Security

- Voll- oder Teil-Ausschreibung/Erweiterung: Jörg, Frank, Simon

- Treffen zentrale Dienste: Finanzsoftware auf zwei Systemen?
- Make or buy: Server : Frank/Jörg/Benny, André, Sascha, Timo, Andreas, tbd (zzgl Simon ab Mitte)
  - Ausfallsicherheit vs Abhängigkeit von Dritten vs Sicherheits- und Supportniveau

Weiteres:
- Datenschutzkonzept
- Operatives Geschäft
  - Archivierung von Daten: Speicherfristen

0. Voll- oder Teil-Ausschreibung/Erweiterung: Frank, Simon, Sascha, Johannes

1. Make or buy: Frank/Benny, André, Sascha, Timo, Andreas, Sarut (zzgl Simon ab Mitte): 06.05. 10:00-11:00

- Applikationsserver
- Backupserver
- Datenbankserver
- Fileserver
- Schließanlage (SQL-Datenbank)
- Virtualisierungsgrad / Workplace-Methode / mobiles Arbeiten

Vorgehen: kick off, Inventarisieren der Anforderungen an Hardware und Abhängigkeiten, Konzepterstellung

2. MDM: Frank/Jörg/Benny, André, Andreas, PC-Team (Lückoff), Sarut - (Microsoft intunes bereits im Einsatz)

- Endgeräte & Endpoint Security

3. Betrieb

- Lizenzmanagement
- Support (Wartungsfenster)

Concept „buy“

Parameter:

Anzahl Endgeräte: 80, 60 oder 40 Usern

Anzahl Lizenzen 80, 60 oder 40 Usern

Anzahl Endpointsecurity: 80, 60 oder 40 Usern

Nutzungsdauer in Jahren: 5 Jahre

FW IT-Personal: Ein Sys-Admin & ein First-Level Support (nicht weiter betrachtet, da ohnehin benötigt)

fehlende Lösungen	80 User	60 User	40 User
Backup gespiegelt on premise		4.000,00 €	
File,- Applikation-, Datenbankserver		12.000,00 €	
Data-Center-Lizenz		5.600,00 €	
Support		24.000,00 €	
Endgeräte	32.000,00 €	24.000,00 €	16.000,00 €
Endpoint-Security	9.600,00 €	7.200,00 €	4.800,00 €
Lizenzen Office 365	10.400,00 €	7.800,00 €	5.200,00 €
Support	24.000,00 €	24.000,00 €	24.000,00 €
Kosten pro Jahr	97.600,00 €	84.601,00 €	71.602,00 €

Ergebnis

Ausblick

Ergebnis:

Die Feuerwehr ist nicht ausreichend vor einem Ausfall geschützt. Außerhalb ihrer eigenen Systeme führt das Versagen einer Einzelkomponenten zum Systemversagen.

Würdigung:

Die Feuerwehr stellt eine besondere Einheit der Stadt mit ganz besonderen Anforderungen an die Ausfallsicherheit dar. Diese Anforderungen, mit maximalen Ausfallzeiten von stellenweise maximal einer Minute zu jedem Zeitpunkt eines Jahres, in einem städtischen Verwaltungsnetz abzubilden, ist nicht zielführend.

Empfehlung:

Es wird empfohlen die IT der Feuerwehr von der städtischen IT zu trennen und eine stand-alone Lösung zu erstellen.

Gründe:

- Die Feuerwehr hat wesentliche IT-Bestandteile bereits in Eigenregie angeschafft. Es müssen lediglich Komponenten hinzugefügt werden.
- Die städtische IT quantitativ und qualitativ zu ertüchtigen ist der aufwändigere und teurere Weg

Ausblick

Vorteile:

- Redundante IT-Dienste von Feuerwehr und Stadt können sich im Ausfall gegenseitig substituieren
- Die IT-Dienste können exakt auf die Bedürfnisse der Feuerwehr abgestimmt werden, ohne das Kompromisse mit den Bedürfnissen anderer städtischer Stakeholder getroffen werden müssen.
- Veränderte Anforderungen an die Feuerwehr können kurzfristig berücksichtigt werden.
- Es entfällt der Vermittlungsaufwand zwischen Kreisleitstelle und städtischer IT.

Prof. Dr. Johannes Berens

Partner
Concepture Gruppe

+49 (0)173 3871025
j.berens@concepture.de

Vielen Dank für Ihre Aufmerksamkeit!