Workshop Notfallmanagement M5

Cybersecurity in der Produktion

13.12.2023

Mittelstand-Digital
Zentrum
Saarbrücken

Notfallmanagement

Worüber reden wir heute?

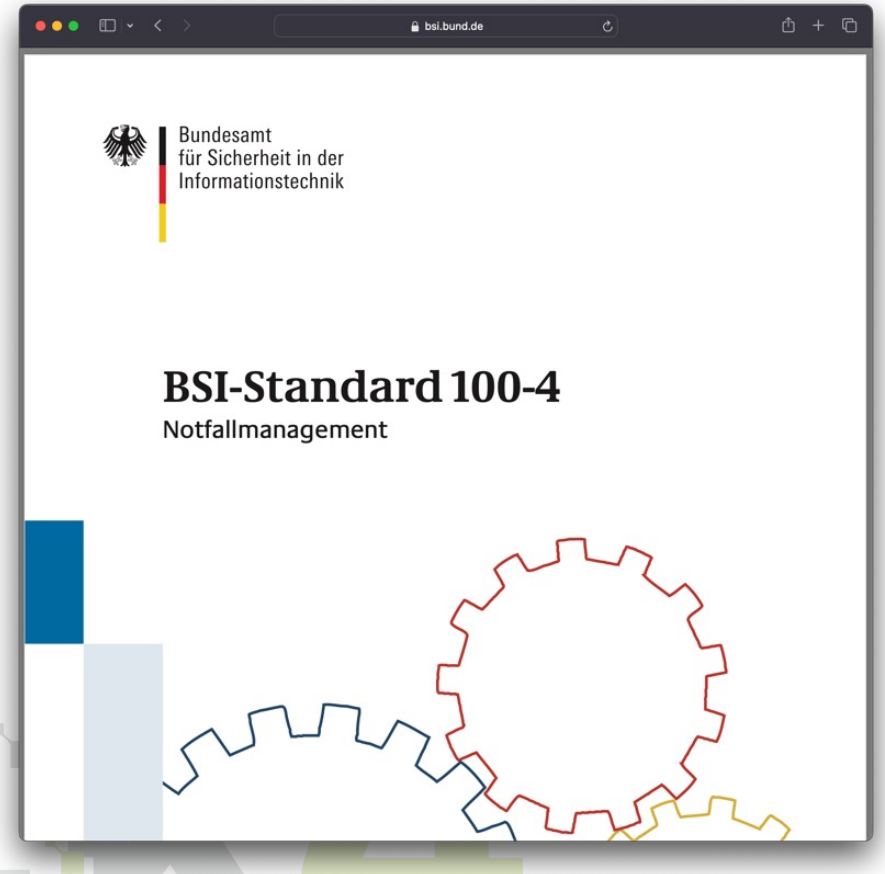
Notfallmanagement: Was?

- Was kann präventiv getan werden, damit Institutionen Notfälle und Krisen möglichst unbeschadet überstehen?
- Was ist zu tun, um bei der Unterbrechung wichtiger Prozesse deren raschen Wiederanlauf zu bewerkstelligen?
- Was sind überhaupt die kritischen Ressourcen und Prozesse einer Institution?

Notfallmanagement: Warum?

Unternehmen und Behörden reagieren besser auf Notfälle und Krisen, wenn sie sich hinreichend auf Ausnahmesituationen vorbereitet haben.

Notfallmanagement: Wie?



BSI – 100-4 Übersicht

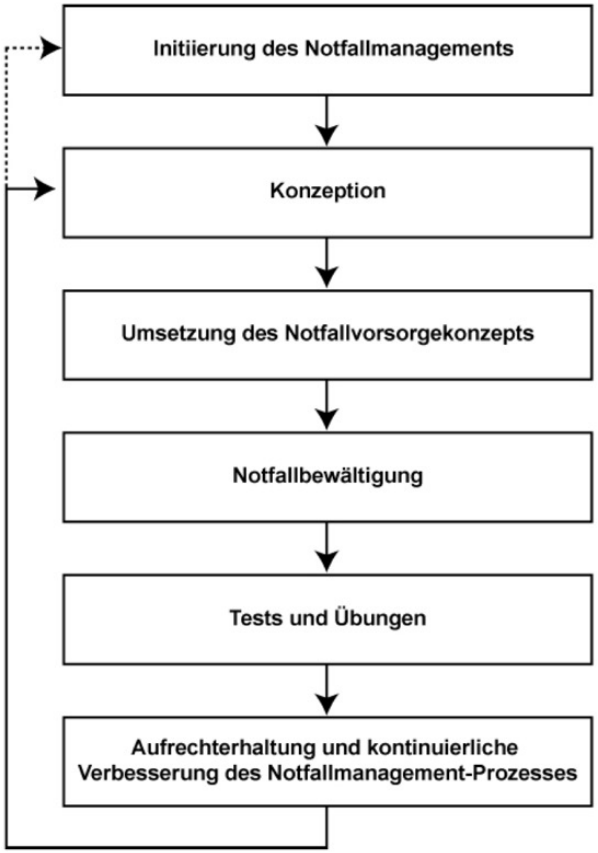
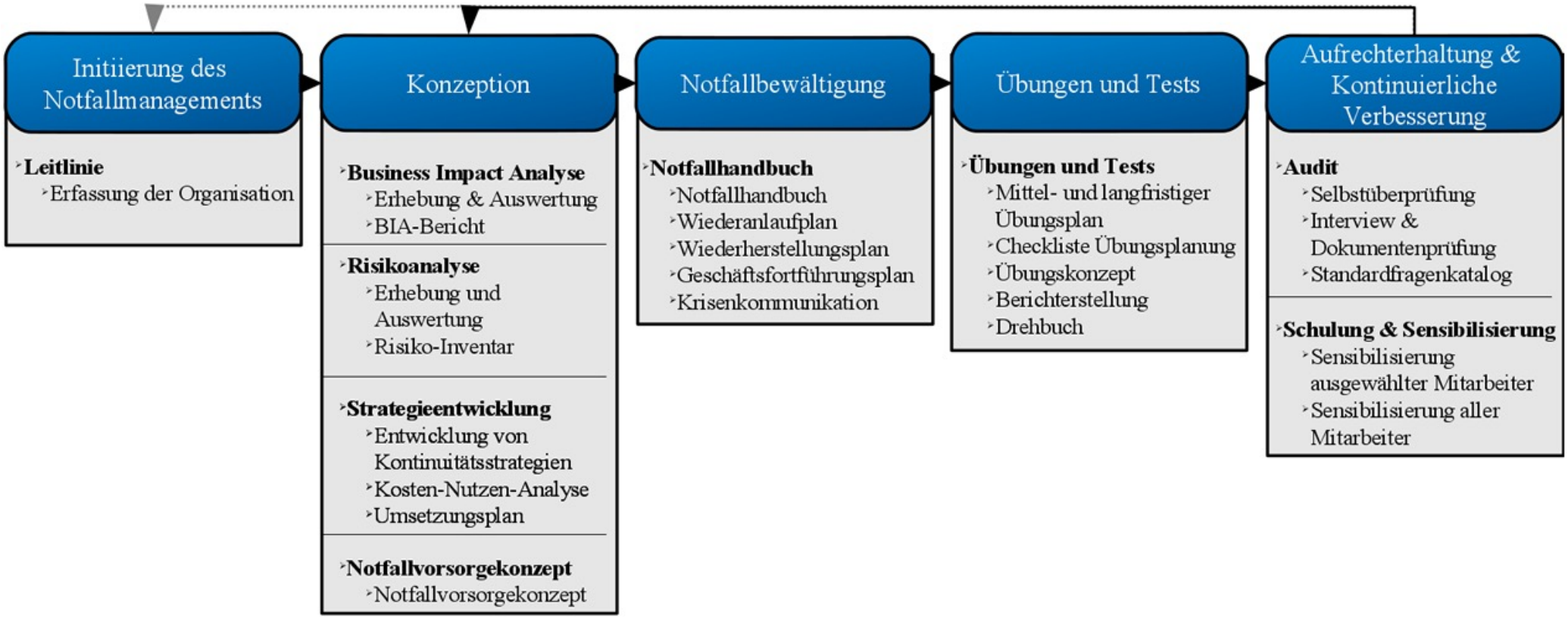


Abbildung 1: Notfallmanagement-Prozess

BSI – 100-4 Übersicht



BSI 100-4 - Übersicht

Beispiele für zu erstellende Dokumente sind:

- Leitlinie zum Notfallmanagement,
- Notfallvorsorgekonzept mit den Berichten zur Business Impact Analyse und Risikoanalyse,
- Notfallhandbuch mit aktuellen Kontaktdaten,
- Übungshandbuch, Übungsplan, Übungskonzepte und -protokolle,
- Schulungs- und Sensibilisierungskonzept,
- Auswertungen von Notfallbewältigungen,
- Revisionsberichte
- sonstige Berichte sowie
- Entscheidungsvorlagen an die Leitungsebene.

Bundesamt
für Sicherheit in der
Informationstechnik

RECPLAST GmbH

Eine fiktive GmbH des BSI

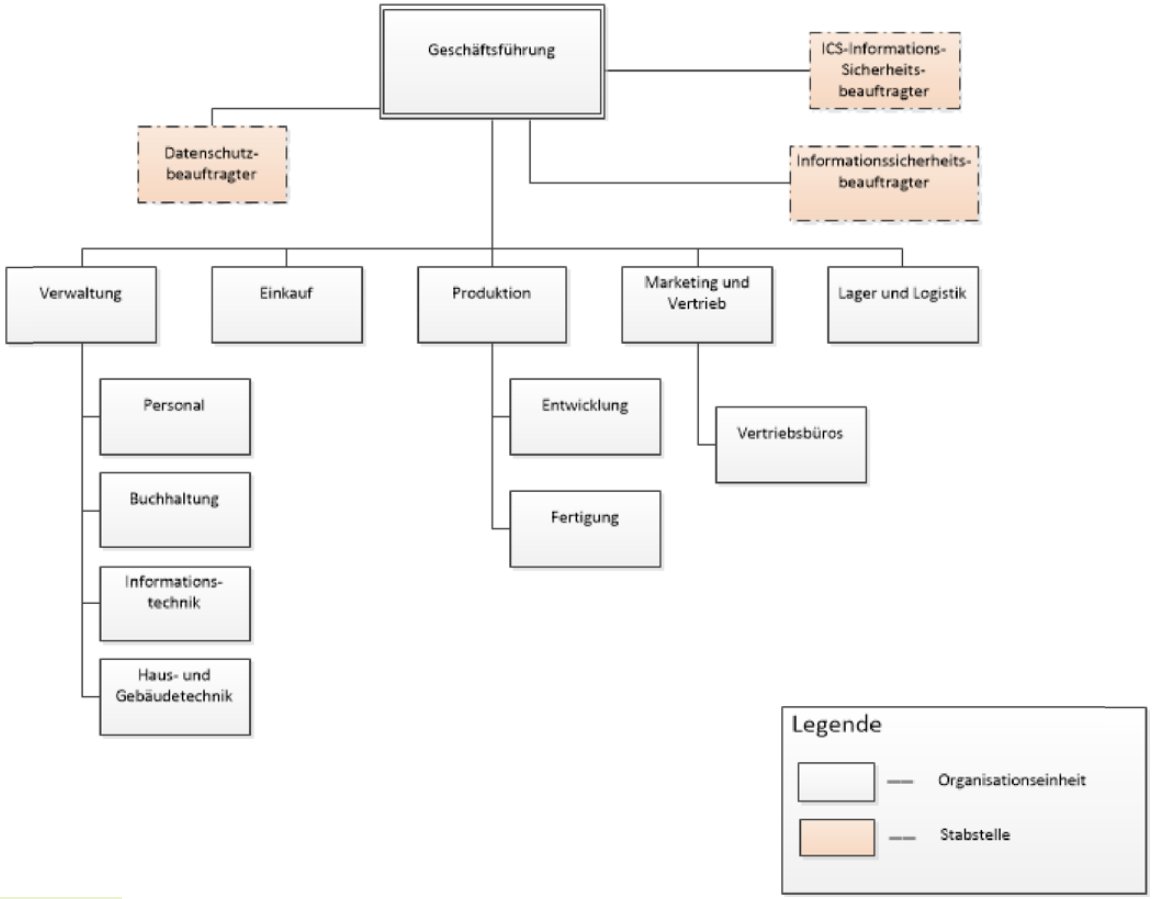
K4

RECPLAST: Demo GmbH des BSI

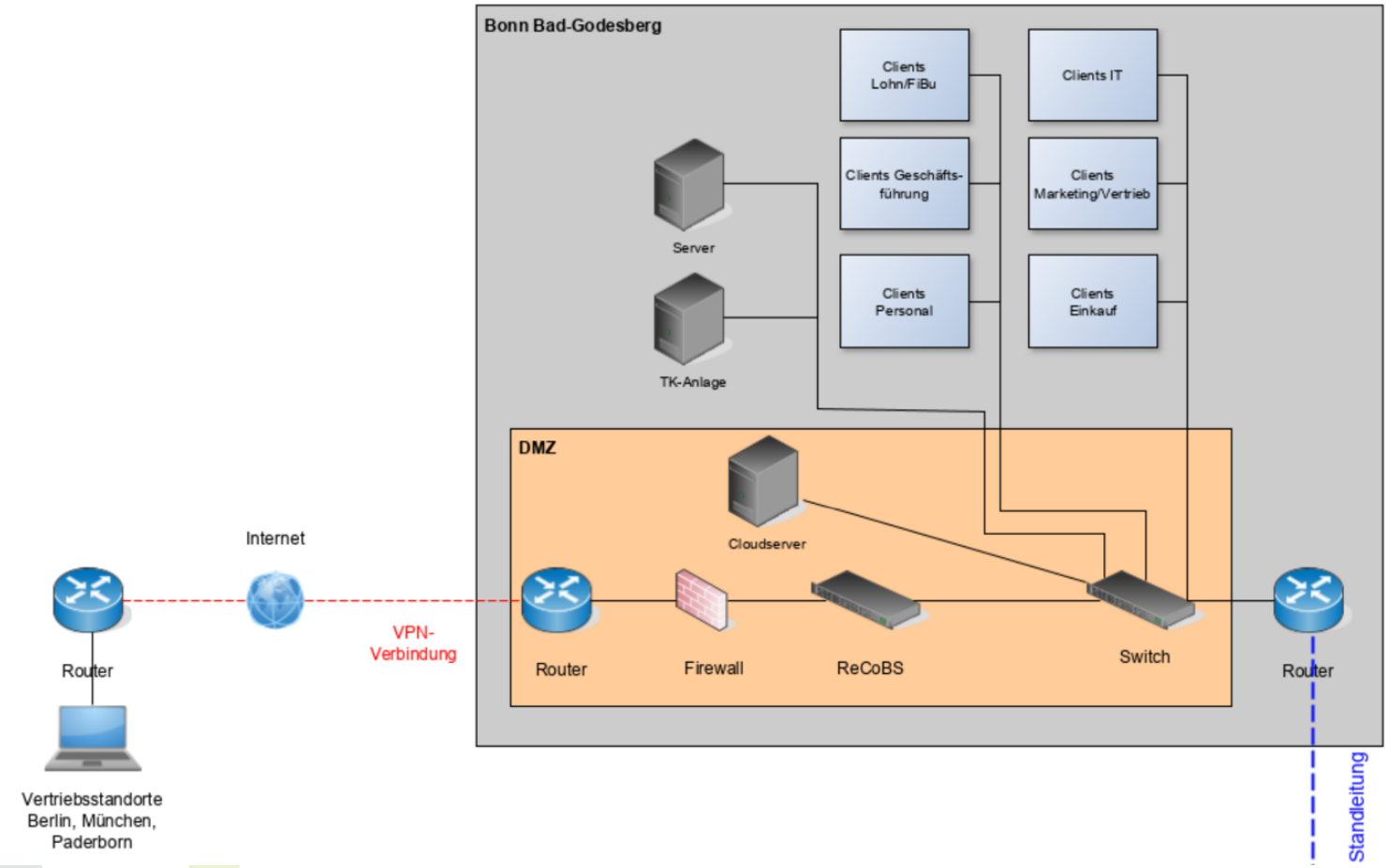
RECPLAST: Demo GmbH des BSI

- Mittelständiges Unternehmen
- Produkte: Recycelt verschiedene Kunststoffe zu “Regranulat“ und stellt daraus neue Werkstücke her
- Kunden: Teilweise Einzelbestellungen, teilweise Großabnehmer
- Mitarbeiter: etwa 500 (175 Verwaltung, 315 Produktion)
- Standorte: Verwaltung (Bonn), Produktion (Beuel), + Vertriebsstandorte
- Umsatz: 50 Mio/Jahr, etwa 1 Mio/Jahr Gewinn

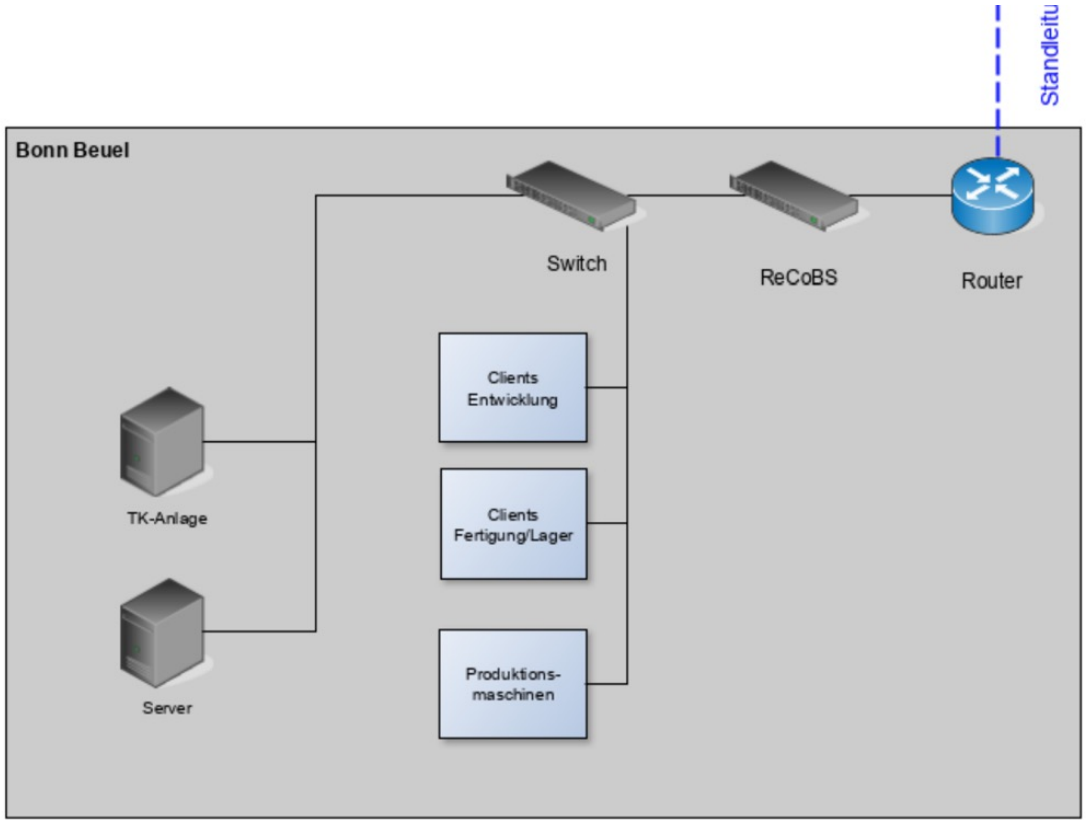
Organigramm RECPLAST



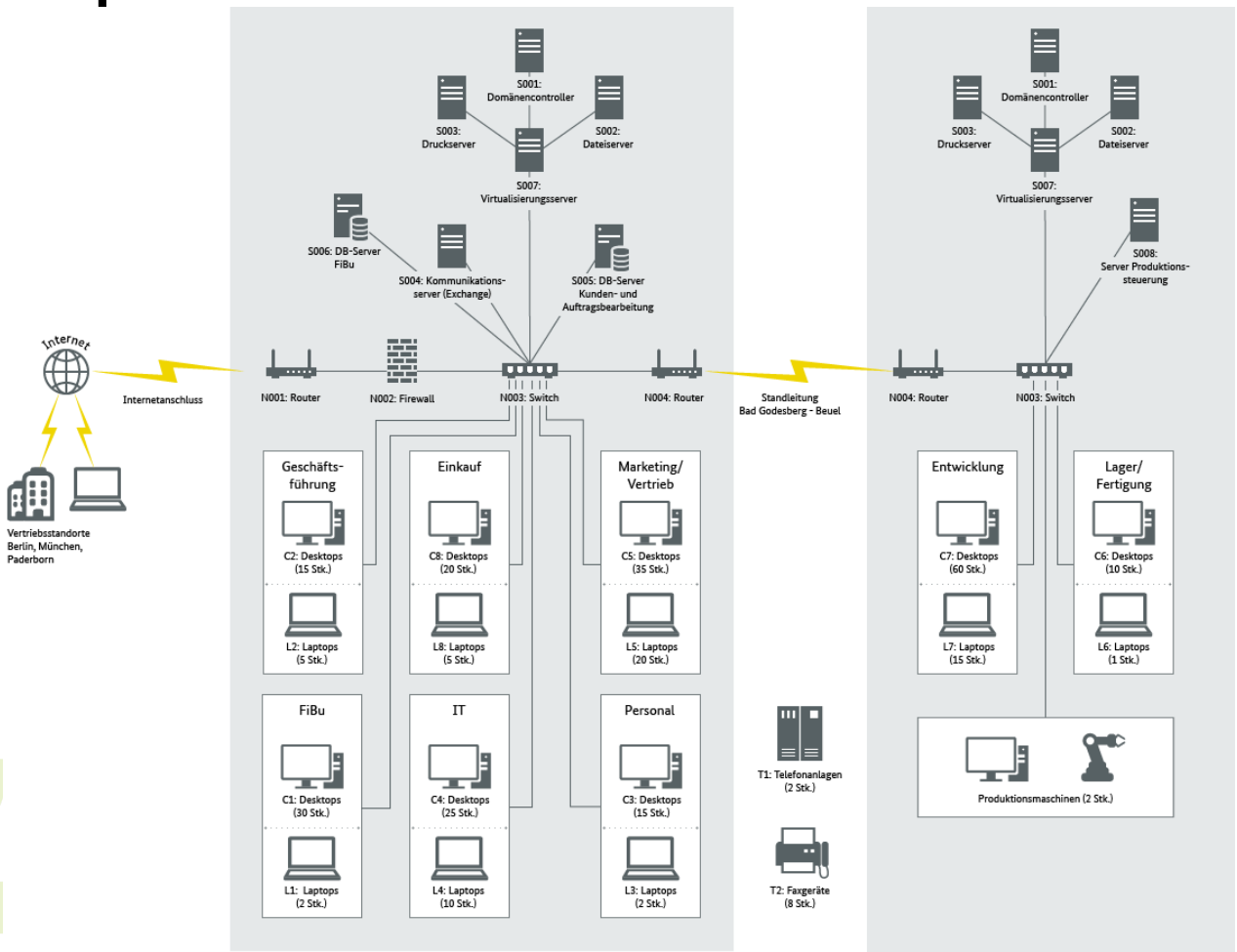
Vereinfachter Netzplan



Vereinfachter Netzplan

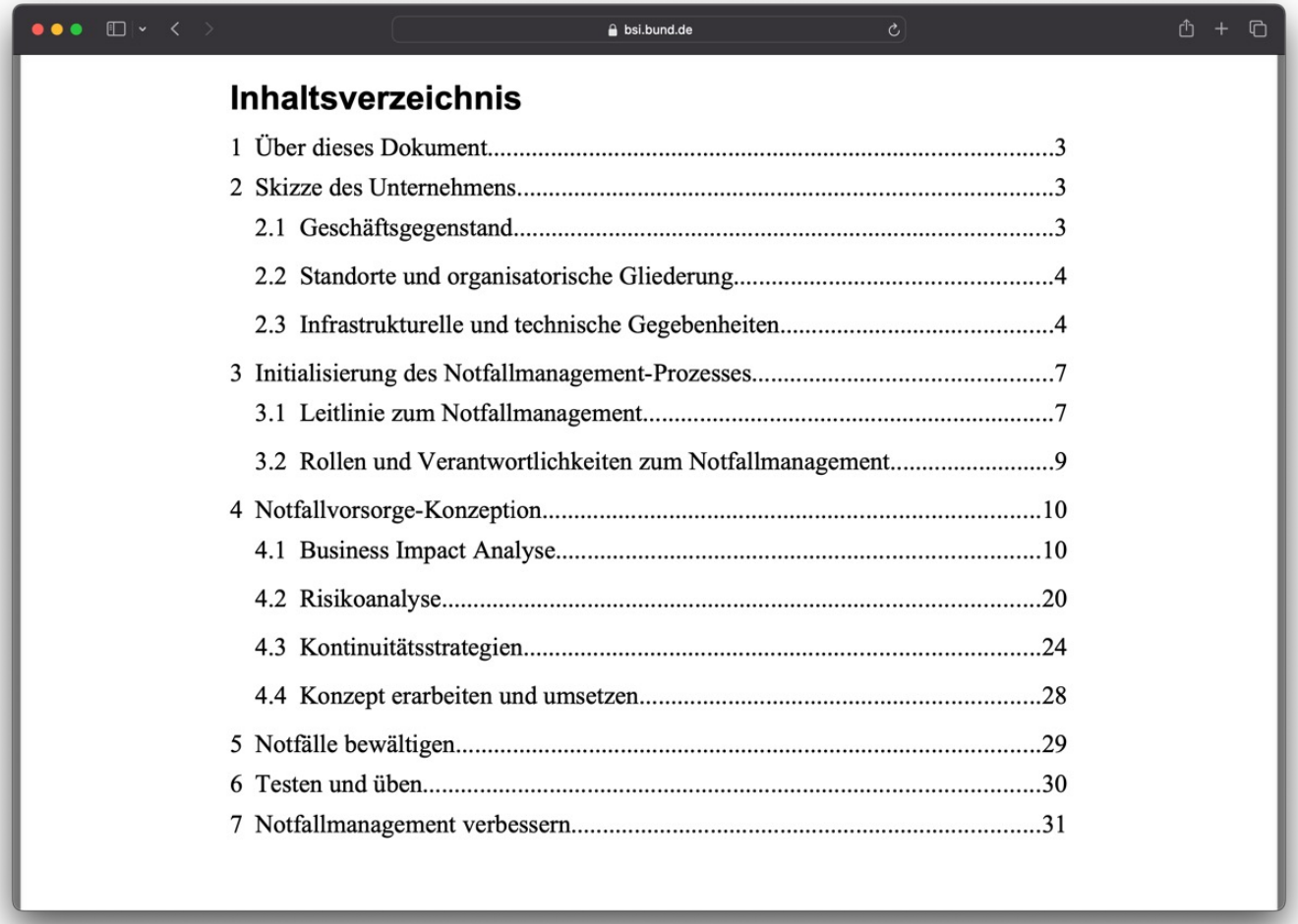


Netzwerkplan: RECPLAST



BSI – RECPLAST GmbH Notfallmanagement

BSI – RECPLAST GmbH Übersicht



Inhaltsverzeichnis

Kapitel 2: Skizze des Unternehmens

- Geschäftsgegenstand
  - Was tun wir? (Allgemein, grobe Arbeitsabläufe)
  - Wer sind unsere Kunden?
  - Umsatz und Gewinn

Kapitel 2: Skizze des Unternehmens

- Standorte und organisatorische Gliederung
  - Standorte
  - Mitarbeiter an Standorten
  - Was wird wo gemacht? (Verwaltung/Produktion)

Kapitel 2: Skizze des Unternehmens

- Infrastrukturelle und technische Gegebenheiten
  - Aufgliederung von Abteilungen und Gebäuden (Wer sitzt wo?)
  - IT-Infrastruktur pro Standort
  - Eventuell Lageplan
  - Welche Software an welchem Standort? (Verwaltung: eher Office, Produktion: auch CAD)

Kapitel 3: Initialisierung des Notfallmanagement-Prozeesses

- Voraussetzungen
  - Unterstützung durch Management
  - Ressourcen werden bereitgestellt (Zeit, Geld, Infrastruktur)
  - Leitlinie wird entwickelt oder ist schon vorhanden
  - Strukturen werden aufgebaut
  - Mitarbeiter werden aktiv eingebunden

Kapitel 3: Initialisierung des Notfallmanagement-Prozesses

- Leitlinie
  - Rollen und Verantwortlichkeiten
  - Hauptverantwortlicher + Vertretung
  - Notfallbeauftragter + Vertretung
  - Temporäre Notfallvorsorgeteams
  - Notfallbewältigung

Kapitel 3: Initialisierung des Notfallmanagement-Prozesses

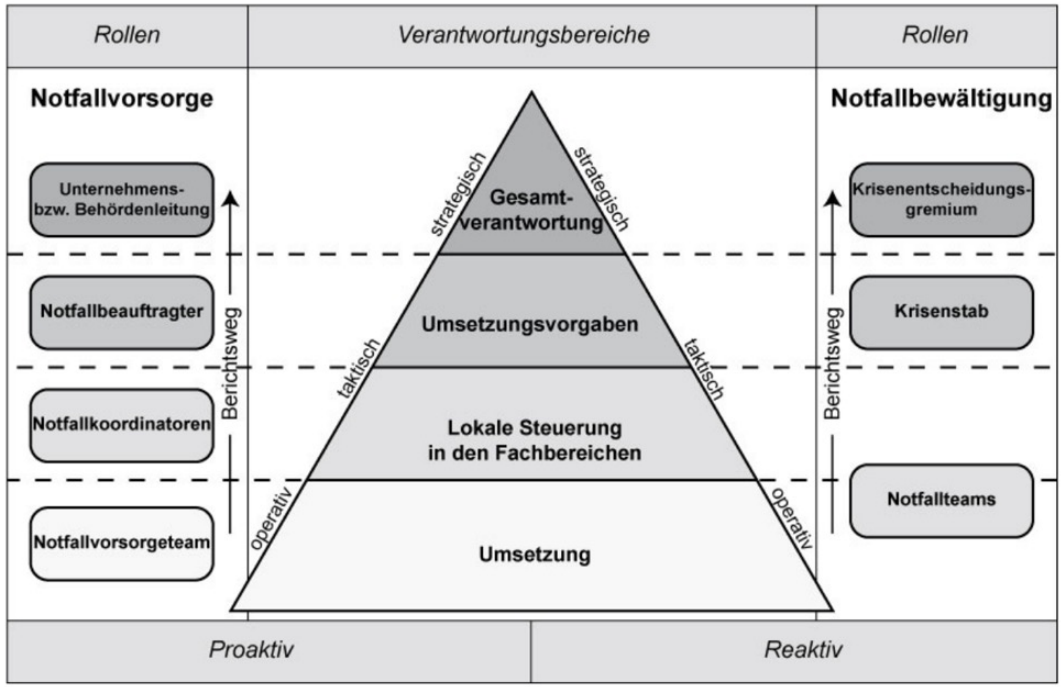


Abbildung 2: Rollen und Verantwortungsbereiche

Kapitel 4: Notfallvorsorge-Konzeption

- Konzept wird erarbeitet auf Basis von
  - Business Impact Analyse
  - Risikoanalyse
  - Kritische Prozesse absichern mit entsprechenden Ressourcen
  - „Kronjuwelen“ absichern

Kapitel 4: Notfallvorsorge-Konzeption

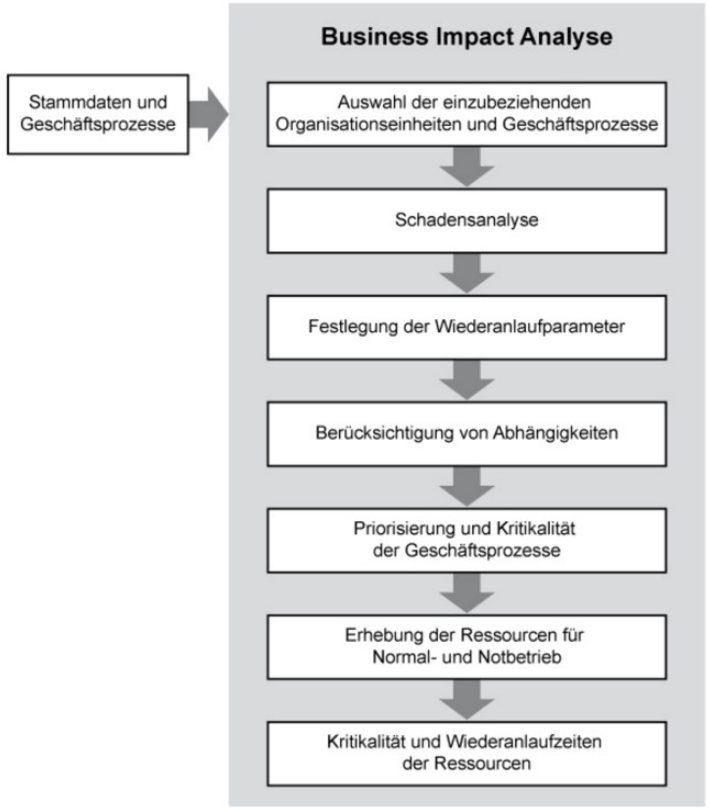


Abbildung 3: Übersicht Business Impact Analyse

Kapitel 4: Notfallvorsorge-Konzeption

- Business Impact Analyse
  - Kritische Prozesse identifizieren
  - Schadenskategorien festlegen
  - Bewertungsperioden festlegen

Kapitel 4: Notfallvorsorge-Konzeption

- Dokumentation der Schadensanalyse pro Prozess

Kapitel 4: Notfallvorsorge-Konzeption

Prozess:	Aufbereitung Recycling-Materialien		**Organisationseinheit:**		Fertigung	
Bearbeiter:	P. Muster (Notfallbeauftragter)		**Interviewpartner:**		M. Müller (Abteilungsleiter)	
Schadensszenario	**Schaden nach Bewertungsperiode**					**Anmerkungen**
	12 Std.	**1 Tag**	**3 Tage**	**7 Tage**	**28 Tage**	
finanzielle Auswirkungen	1	1	1	1	2	Wenn in größerem Umfang Regranulate zugekauft werden müssen, entstehen hohe Mehrkosten.
Verstoß gegen Gesetze, Vorschriften oder Verträge	1	1	1	1	1	Solange Regranulate zugekauft werden können, werden Verträge nicht verletzt.
Beeinträchtigung der Aufgabenerfüllung	1	1	1	1	1	Der Zukauf beeinträchtigt auch langfristig die Abläufe im Unternehmen nicht stark.
negative Innen- und Außenwirkung	1	1	1	2	2	Längere Ausfälle wirken sich negativ auf die Motivation der Mitarbeiter aus.

Tabelle 3: Beispieltabelle für den Schadensverlauf eines Geschäftsprozesses (1 = niedriger Schaden, 2 = mittlerer Schaden)

Kapitel 4: Notfallvorsorge-Konzeption

- Dokumentation der Schadensanalyse - Prozessübersicht

Kapitel 4: Notfallvorsorge-Konzeption

Prozess	Schadensszenario	Schaden nach Bewertungsperiode				
		12 Std.	1 Tag	3 Tage	7 Tage	28 Tage
Aufbereitung Recycling-Materialien	finanzielle Auswirkungen	1	1	1	1	2
	Verstoß gegen Gesetze, Vorschriften oder Verträge	1	1	1	1	1
	Beeinträchtigung der Aufgabenerfüllung	1	1	1	1	1
	negative Innen- und Außenwirkung	1	1	1	2	2
	Summe	**4**	**4**	**4**	**5**	**6**
Fertigung Endprodukte	finanzielle Auswirkungen	1	2	3	4	4
	Verstoß gegen Gesetze, Vorschriften oder Verträge	1	1	1	2	3
	Beeinträchtigung der Aufgabenerfüllung	2	2	3	3	4
	negative Innen- und Außenwirkung	1	1	2	2	3
	Summe	**5**	**6**	**9**	**11**	**14**
IT-Wartung	finanzielle Auswirkungen	1	1	2	3	3
	Verstoß gegen Gesetze, Vorschriften oder Verträge	1	1	1	2	3
	Beeinträchtigung der Aufgabenerfüllung	1	2	2	3	3
	negative Innen- und Außenwirkung	1	1	2	3	3
	Summe	**4**	**5**	**7**	**11**	**12**

Kapitel 4: Notfallvorsorge-Konzeption

- Wiederanlaufparameter
  - Was darf wie lange maximal ausfallen?
  - Wie viel Kapazität muss der Notbetrieb bereitstellen?
  - Wie lange darf der Notbetrieb laufen?
  - Wie lange darf die Wiederherstellung dauern?

Kapitel 4: Notfallvorsorge-Konzeption

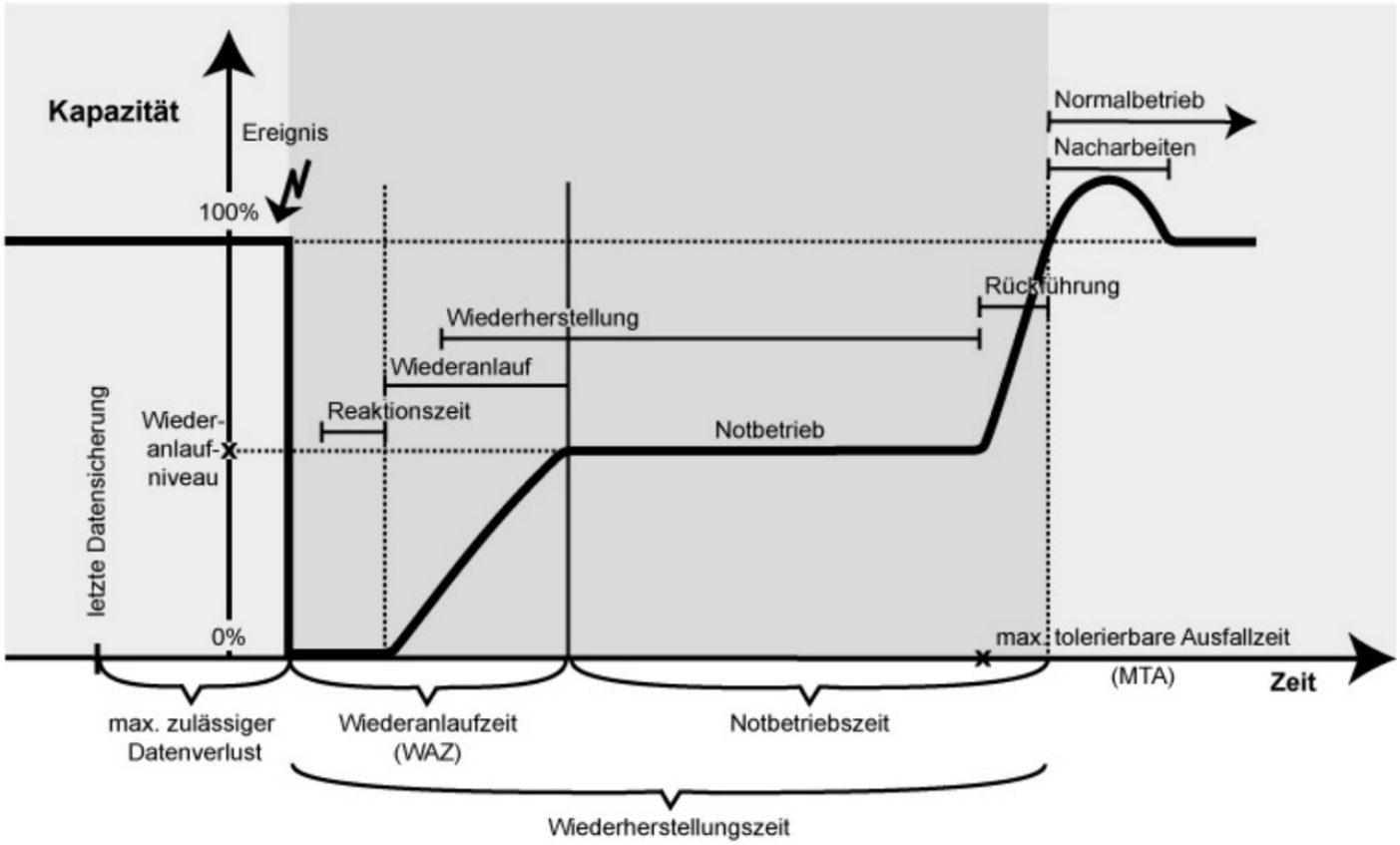


Abbildung 6: Wiederanlaufparameter

Kapitel 4: Notfallvorsorge-Konzeption

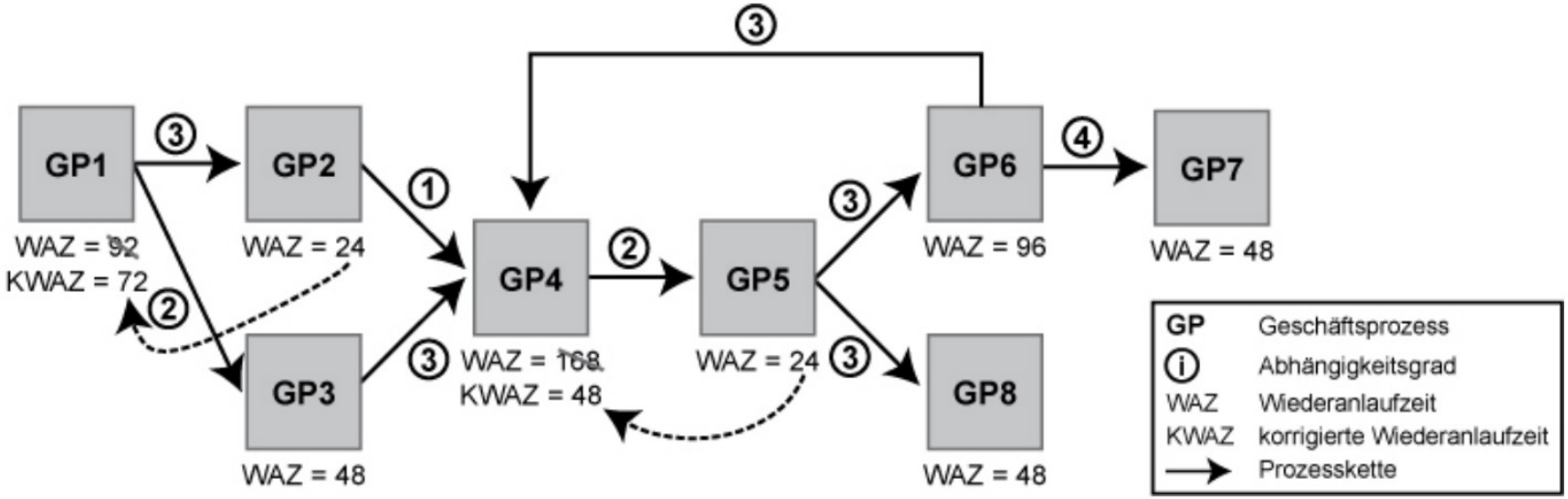


Abbildung 7: Vererbung der Wiederanlaufzeit in Richtung Vorgänger

Kapitel 4: Notfallvorsorge-Konzeption

Parameter	Aufbereitung Recycling-Materialien	Fertigung Endprodukte	IT-Wartung	Server-Betrieb
Maximal tolerierbare Ausfallzeit (MTA)	4 Wochen	3 Tage	1 Woche	3 Tage
Wiederanlaufzeit (WAZ)	3 Woche	2 Tage	3 Tage	2 Tage
Wiederanlauf-Niveau	80 Prozent	80 Prozent	75 Prozent	80 Prozent
Maximal tolerierbare Notbetriebszeit (MTN)	6 Wochen	2 Wochen	4 Wochen	2 Wochen
Maximal tolerierbare Wiederherstellungszeit (MTW)	9 Wochen	3 Wochen	6 Wochen	3 Wochen

Tabelle 5: Wiederanlaufparameter ausgewählter Prozesse bei der RECPLAST GmbH

Kapitel 4: Notfallvorsorge-Konzeption

- Kritikalitätsbewertung von Prozessen

Kategorie	Wiederanlaufzeit	Maximal tolerierbare Ausfallzeit	Gesamtschaden nach einer Woche	Allgemein
unkritisch	länger als vier Wochen	länger als vier Wochen	niedrig	Ausfälle haben allenfalls geringfügige Auswirkungen
wenig kritisch	zwei bis vier Wochen	zwei bis vier Wochen	mittel	Ausfälle haben spürbare Auswirkungen
kritisch	zwischen drei Tagen und zwei Wochen	zwischen drei Tagen und zwei Wochen	hoch	Ausfälle haben beträchtliche Auswirkungen
hoch kritisch	weniger als drei Tage	weniger als drei Tage	sehr hoch	Ausfälle haben existenziell bedrohliche Auswirkungen

Tabelle 6: Beispiel für die Definition von Kritikalitätskategorien

Kapitel 4: Notfallvorsorge-Konzeption

- Kritikalitätsbewertung von Prozessen
  - der Prozess „Aufbereitung Recycling-Materialien“ als **weniger kritisch,**
  - der Prozess „IT-Wartung“ als **kritisch**,
  - der Prozess „Fertigung Endprodukte“ als **hoch kritisch** und
  - der Prozess „Server-Betrieb“ ebenfalls als **hoch kritisch**.

Kapitel 4: Notfallvorsorge-Konzeption

- Risikoanalyse

Wahrscheinlichkeit	Auswirkung/Schaden			
	Niedrig	Mittel	Hoch	Sehr hoch
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
Wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Tabelle 8: Matrix zur Bewertung der Risiken bei der RECPLAST GmbH

Kapitel 4: Notfallvorsorge-Konzeption

- Risikoanalyse

Risikogruppe (-szenario)	Risiko-Bewertung (Erläuterung)	Gewählte Strategie (Alternativen)
Verlust des Serverraums (z. B. durch Brand)	hoch (geringe Wahrscheinlichkeit, aber große Auswirkungen)	Risikoreduktion (ggf. auch Risikotransfer oder Risikoakzeptanz)
Hacker	mittel (die Bewertung berücksichtigt bereits vorgenommene Absicherungen, ohne die das Risiko sehr hoch wäre)	Risikoreduktion (Risikoakzeptanz)
usw.	usw.	usw.

Tabelle 9: Dokumentation der Risikoanalyse bei der RECPLAST GmbH

Kapitel 4: Notfallvorsorge-Konzeption

- Kontinuitätsstrategien
  - Verschiedene Optionen pro Prozess
    - Minimal
    - Klein
    - Mittel
    - Groß

Kapitel 4: Notfallvorsorge-Konzeption

- Kontinuitätsstrategien

Strategieoption	Prozess „Fertigung Endprodukte“	Prozess „IT-Wartung“
Mittlere Lösung	Ein Vertrag mit einem externen Dienstleistungsunternehmen wird geschlossen, von dem im Notfall Produkte zugekauft werden.	Ein Rahmenvertrag bindet ein externes Unternehmen zur Wartung der IT-Systeme an die RECPLAST GmbH. Dieses Unternehmen übernimmt im Notfall die IT-Wartung.
Große Lösung	Ein zweiter Produktionsstandort wird aufgebaut, der die Produktion übernehmen kann. Dieser zweite Standort kann auch genutzt werden, um die Produktion auszuweiten und Nachfragespitzen zu befriedigen.	Es existieren zwei vollständige Teams für die Wartung der IT-Systeme.

Tabelle 10: Kontinuitätsstrategien für zwei Beispielprozesse bei der RECPLAST GmbH

Kapitel 4: Notfallvorsorge-Konzeption

- Kosten und Nutzen analysieren
  - Welche Strategie kostet mich wie viel? Einmalige Kosten? Laufende Kosten?
  - Bringen bestimmte Strategien auch weitere Vorteile mit sich?

Kapitel 4: Notfallvorsorge-Konzeption

- Beispiel:
  - Server-Betrieb

- **„Cold Standby“**, die billigste Lösung: Die erforderliche Hardware und Software muss am zweiten Standort noch beschafft und in Betrieb genommen werden. Der dafür erforderliche zeitliche Aufwand wurde auf zwei Wochen geschätzt.
- **„Warm Standby“**, die mittlere Lösung: Die Hardware ist am zweiten Standort bereits vorhanden, ebenso alle Software, deren Installation einen höheren Aufwand erfordert. Im Notfall müssen lediglich einfach zu installierende Software sowie Datenbestände eingespielt werden. Der zeitliche Aufwand für diese Lösung wurde mit zwei Tagen kalkuliert.
- **„Hot Standby“**, die teuerste, aber im Notfall auch schnellste Lösung: Alle Server werden parallel betrieben, so dass im Notfall binnen weniger Stunden der Normalbetrieb der Server wiederhergestellt werden kann.

Die Zuständigen der RECPLAST GmbH entschieden sich für die zweite Lösung („Warm Standby“), da diese – anders als ein „Cold Standby“ – den Wiederanlauf-zielen der Prozesse genügt, gleichzeitig aber auch kostengünstiger ist als ein „Warm Standby“. Es entstehen zwar Kosten für Hardware und Softwarelizenzen, aber weitaus geringere Personalaufwände als bei der großen Lösung.

Kapitel 4: Notfallvorsorge-Konzeption

4.4 Konzept erarbeiten und umsetzen

Maßnahme	Personalaufwand		Sachkosten	
	einmalig	wiederkehrend	einmalig	wiederkehrend
Beschaffung, Installation und Wartung von Hardware für zusätzliche Server in Bad Godesberg und Beuel	3 PT	0,5 PT/Monat (einschließlich Funktionstests)	8.000 Euro	200 Euro/Jahr (Reparaturen)
Beschaffung, Installation und Wartung der wichtigsten Software	2 PT	0,5 PT/Monat (einschließlich Funktionstests)	2.000 Euro	300 Euro/Jahr (Aktualisierung der Lizenzen)
Anpassung des Serverraums in Bonn-Beuel an die zusätzlichen IT-Systeme (USV, bessere Klimatisierung usw.)	5 PT	0,5 PT/Monat	6.000 Euro	500 Euro/Jahr (höhere Kosten für Strom)
Summe	**10 PT**	**1,5 PT/Monat**	**16.000 Euro**	**1.000 Euro**

Tabelle 12: Kostenaufstellung zu Vorsorgemaßnamen der RECPLAST GmbH (PT = Personentage)

Kapitel 5: Notfälle bewältigen

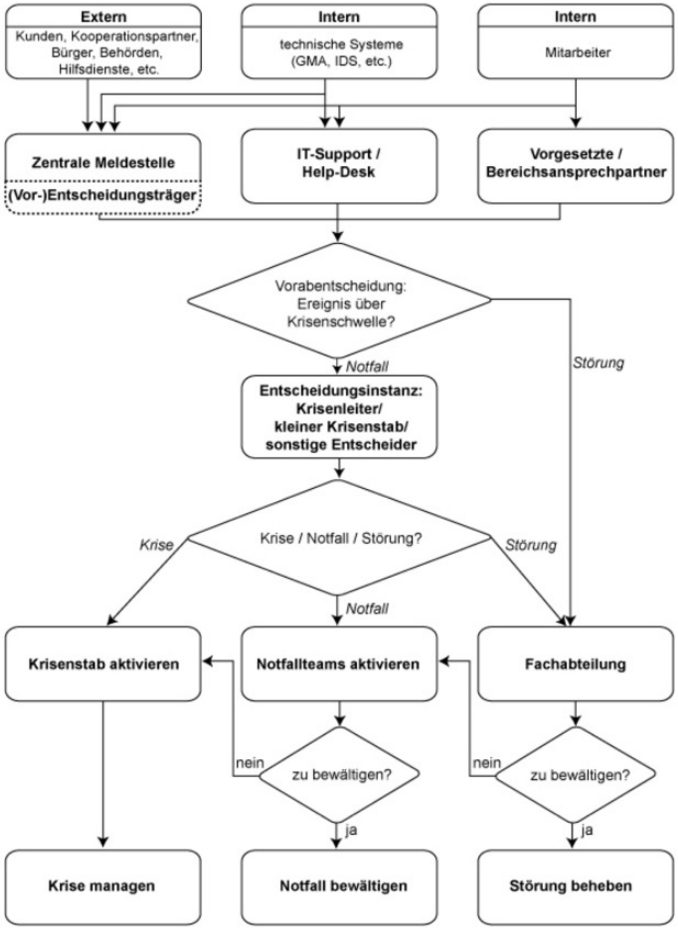


Abbildung 10: Alarmierung und Eskalation

Kapitel 5: Notfälle bewältigen

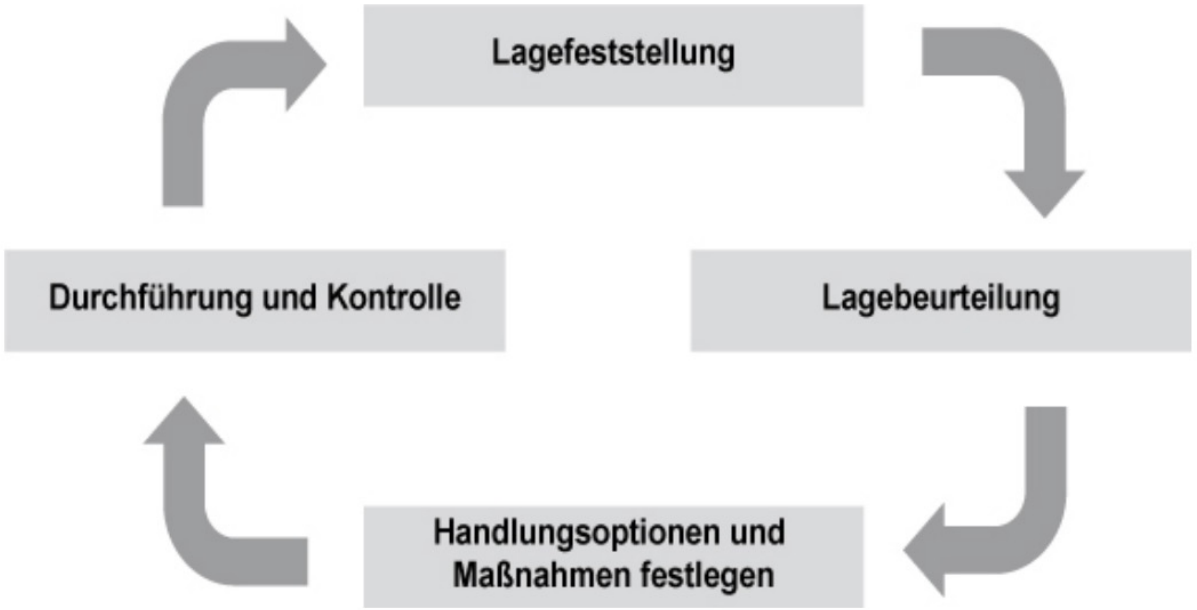


Abbildung 11: Bewältigungsprozess

Kapitel 5: Notfälle bewältigen

Ein Notfallplan enthält alle zur Behandlung von Krisen und Notfällen wichtigen Angaben. Dazu zählen:

- Sofortmaßnahmen zur unmittelbaren Abwehr von Gefahren,
- Aufgabenbeschreibungen für bestimmte Situationen und Personen,
- Zuständigkeiten und Festlegungen für das Krisenmanagement (Rollen, Meldewege, Treffpunkte, Regelungen zur Arbeit in Krisenstäben),
- Regelungen zur Öffentlichkeitsarbeit im Krisenfall,
- Detaillierte Beschreibungen zur Wiederherstellung von Ressourcen und zur Wiederaufnahme und Fortführung des Geschäftsbetriebs, sowie
- Angaben dazu, wie Personen und Institutionen, die zur Bewältigung des Notfalls beitragen, erreicht werden können.

Kapitel 6: Testen und üben

- Wie wird das Notfallmanagement getestet?
- Wie oft wird getestet?
- Was passiert mit den Ergebnissen?
- Gibt es verschiedene Tests?
  - Szenarien, Drehbücher, externe Unterstützung, …

Kapitel 6: Testen und üben

Übungsart	Zielgruppe			Ablauf		Aufwand/ Umfang
	strategisch	taktisch	operativ	diskussions-basiert	handlungs-orientiert	niedrig/-mittel/ hoch/ sehr hoch
Test der technischen Vorsorgemaßnahmen			X		X	niedrig
Funktionstest			X		X	mittel
Plan-Review		x	x	X		niedrig
Planbesprechung		X	x	X		niedrig-mittel
Stabsübung	x	X		X		niedrig-mittel
Stabsrahmenübung	x	X	x	X	x	mittel-hoch
Kommunikations- und Alarmierungsübung		x	X		X	niedrig
Simulation von Szenarien		X	X		X	hoch
Ernstfall- oder Vollübung	X	X	X		X	sehr hoch

Tabelle 18: Übungsarten

Kapitel 6: Testen und üben

Übung: XYZ											
Nr.	**Real-Zeit**	**Szenario-Zeit**	**Stichwort**	**Aktivität**	**Ziel/ erwartete Reaktion**	**Ein-spielender**	**Akteure**				**Hilfsmittel/ Werkzeug/ Art der Einspielung**
							A	**B**	**C**	**…**	
1	…		…		…		…	…	…	…	…
2	10:10		Meldung an LZ	*(Beschreibung der Einlage mit Hintergrundin-formationen)*	Überprüfung der Meldung, Eskalation	Hr. Jansen		X	X		Handy
3	…		…	…	…		…	…	…	…	…

Tabelle 19: Beispiel Übungsdrehbuch

Kapitel 7: Notfallmanagement verbessern

- Wann muss aktualisiert werden?
- Ergebnisse der Übungen einfließen lassen
  - Was kann verbessert werden?
  - Was lief gut?
  - Was ging gar nicht? (Backups? Server Updates...)
  - Externe Überprüfung alle x Jahre?

Fazit: Notfallmanagement BSI

- Hilfreicher Leitfaden
- Muss auf eigene Bedürfnisse angepasst werden
- Notfallmanagement ist viel Aufwand
- Ohne Übung und Tests ist der Plan nicht belastbar


K4

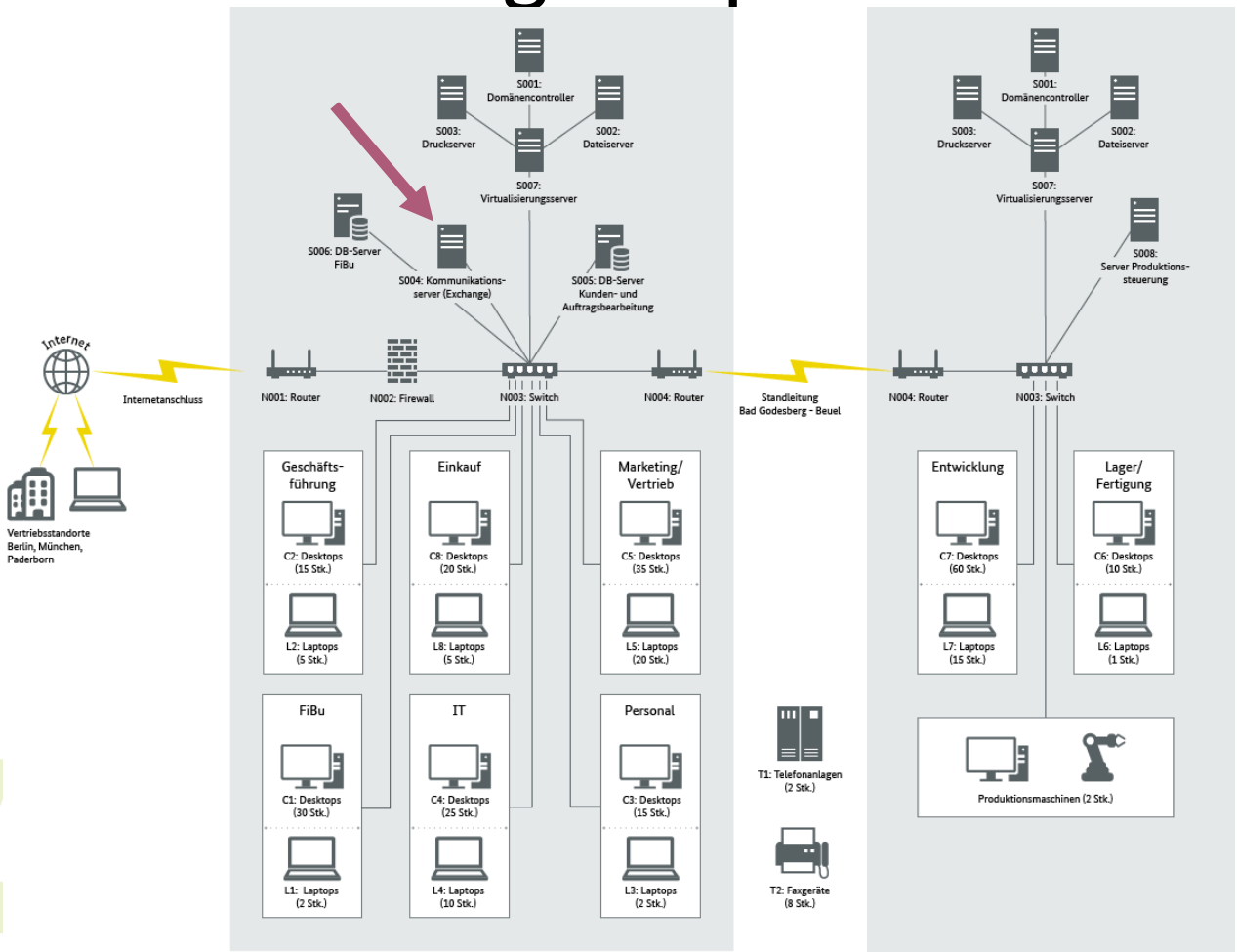
Angriffsszenarien

Was tun wenn es brennt?

Szenario 1

Einen Tag zu spät…

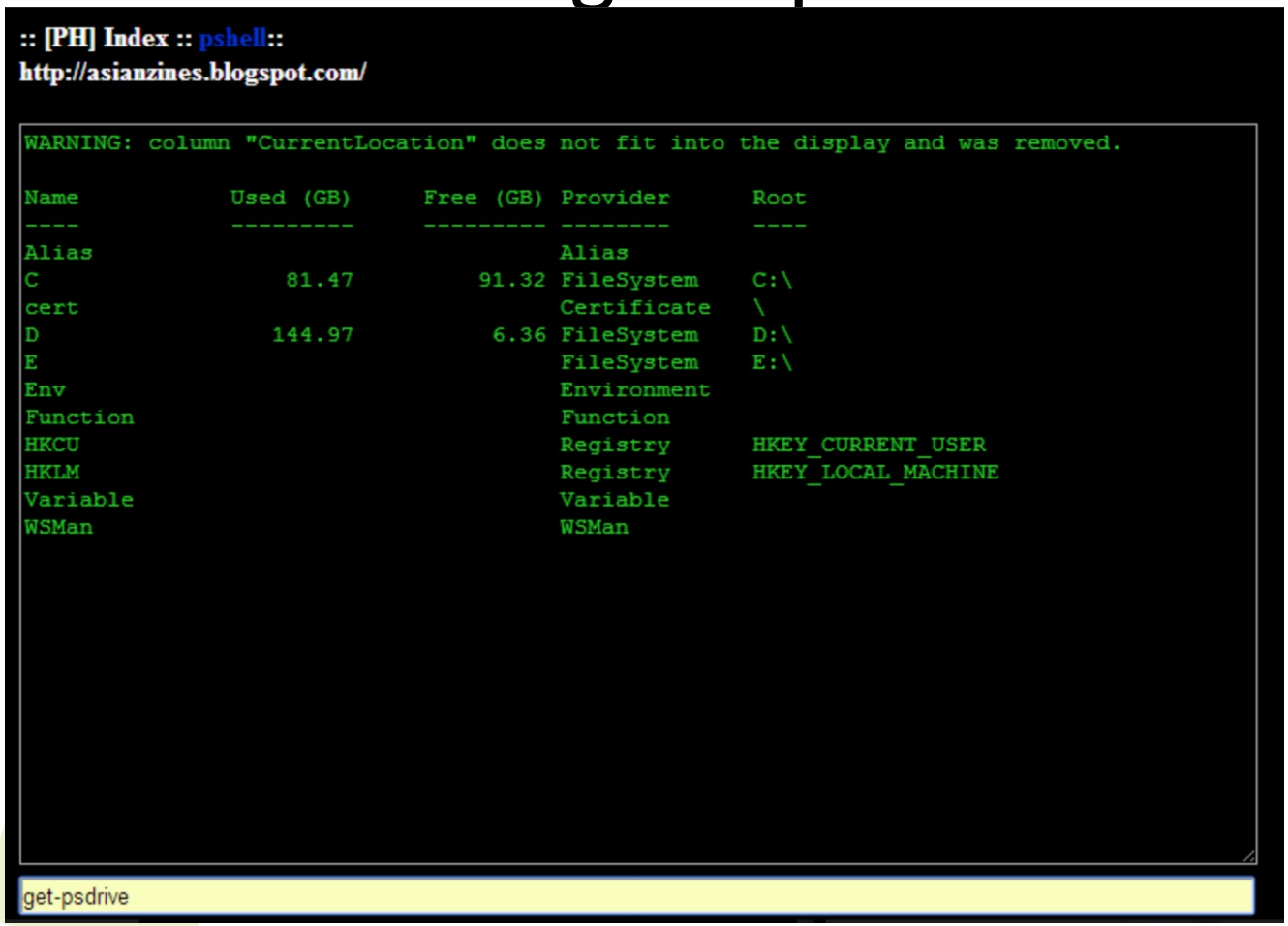
Szenario 1: Einen Tag zu spät



Szenario 1: Einen Tag zu spät

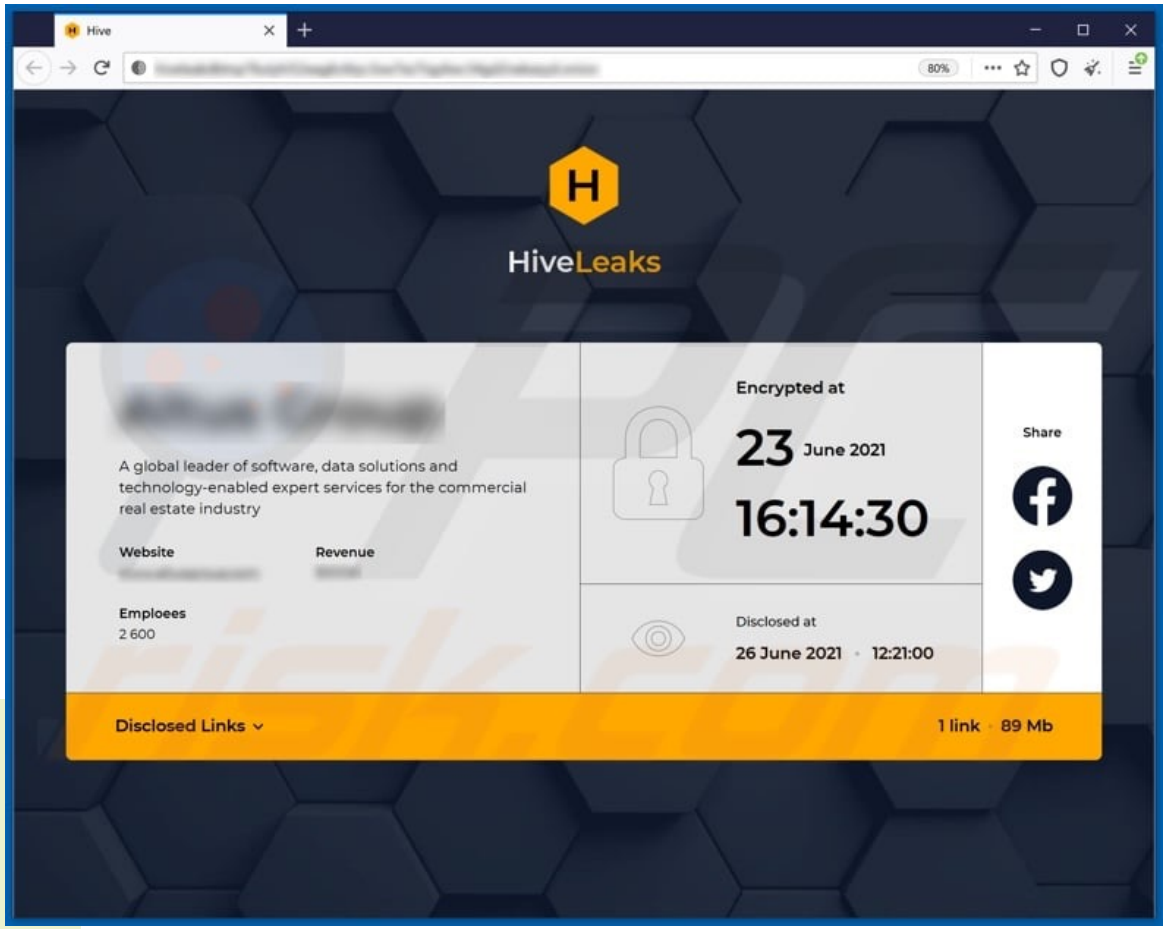
```
c:\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\outlooken.aspx
c:\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\outlookzh.aspx
c:\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\outlookus.aspx
c:\inetpub\wwwroot\aspnet_client\system_web\4_0_30319\err0r.aspx
c:\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\error.aspx
c:\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\front.aspx
```

Szenario 1: Einen Tag zu spät



Szenario 1: Was tun?

Szenario 1: Der Angreifer meldet sich

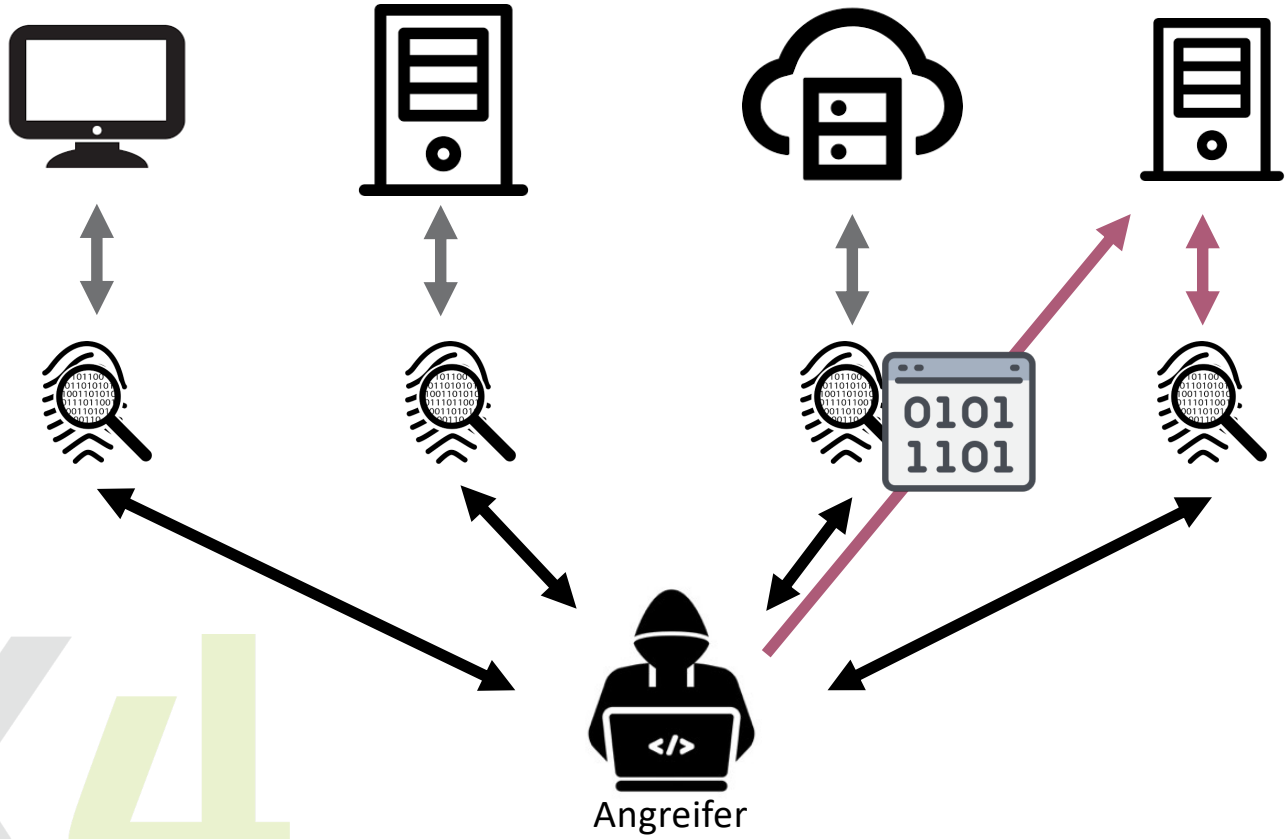


Szenario 1: Auflösung

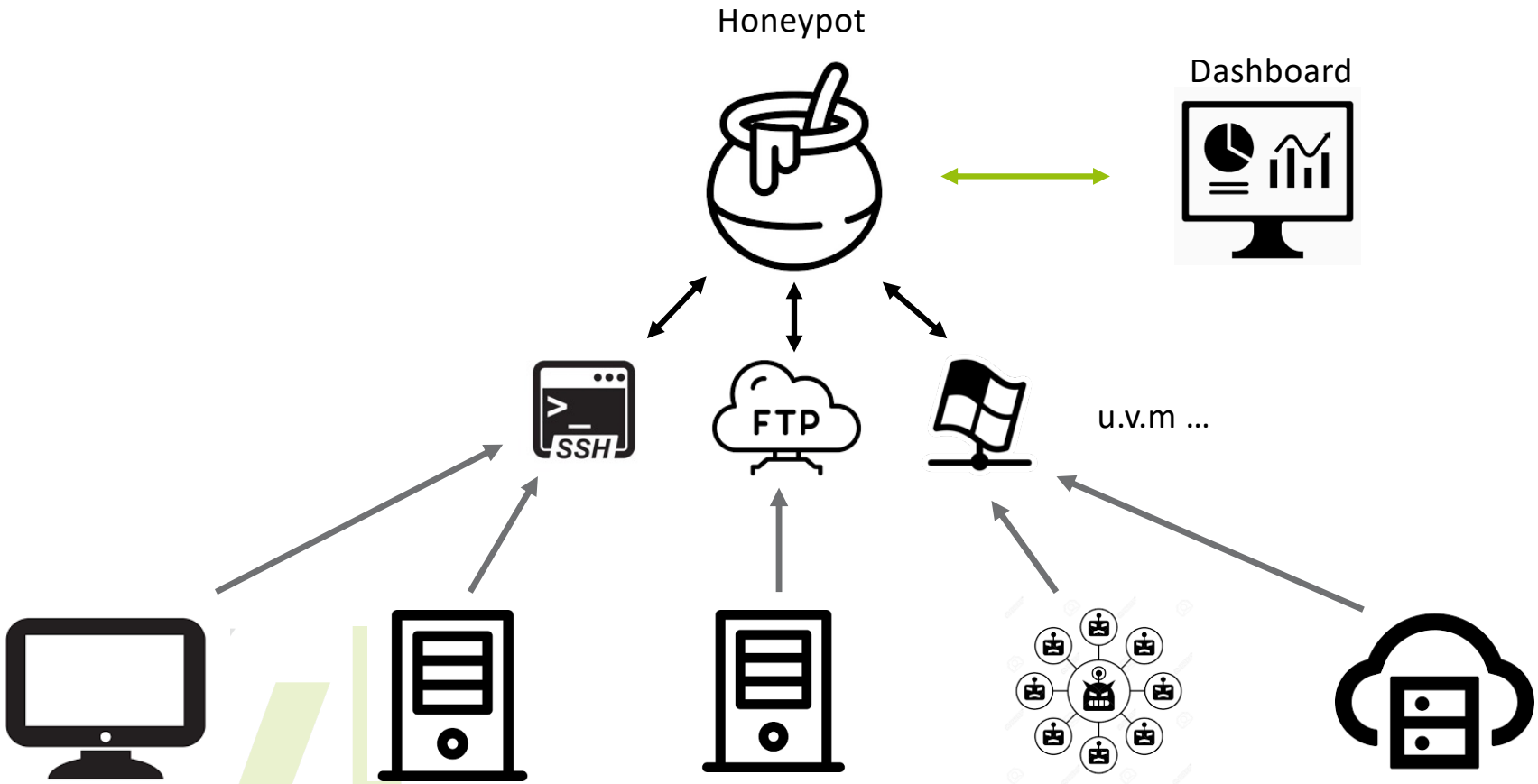
Post Mortem und Analyse

Szenario 1

Szenario 1: Massenangriffe



Szenario 1: Honeypot



Szenario 1: Honeypot Demo

Szenario 1: Lessons learned

- Internetverbundene Systeme schnellstmöglich patchen
  - Vor allem bei kritischen Sicherheitslücken!
- Angreifer: Masse statt Klasse
  - Kaum Expertise nötig um öffentliche Exploits anzuwenden
  - Kein gezielter Angriff
- Wenn ich zahlen muss:
  - Angreifer „vertrauenswürdig“
  - Woher bekomme ich Bitcoin?
  - Versicherungen?

Szenario 2

Fährtenleser

Szenario 2: Fährtenleser

PM **An:** Peter Michely

Intern

Nicht Öffentlich

Hallo zusammen,

leider müssen wir euch informieren, dass unser Unternehmen Opfer eines Hackerangriffs geworden ist.
Der genaue Ablauf wird noch recherchiert, allerdings können wir schon jetzt sagen, dass alle unsere Systeme mit Ransomware infiziert wurden.

Weiterhin besteht die Möglichkeit, dass Daten aus unserem Unternehmen abgeflossen sind.
Darunter können auch Kunden- und Projektdaten sein, die wir ausgetauscht haben.

Wir würden euch, zu eurer eigenen Sicherheit, bitten, unsere Accounts auf euren Systemen so schnell wie möglich zu sperren.
Aktuell untersuchen wir den Vorfall und melden uns, sobald mehr über den Angriff herausgefunden wurde!

Mit freundlichen Grüßen

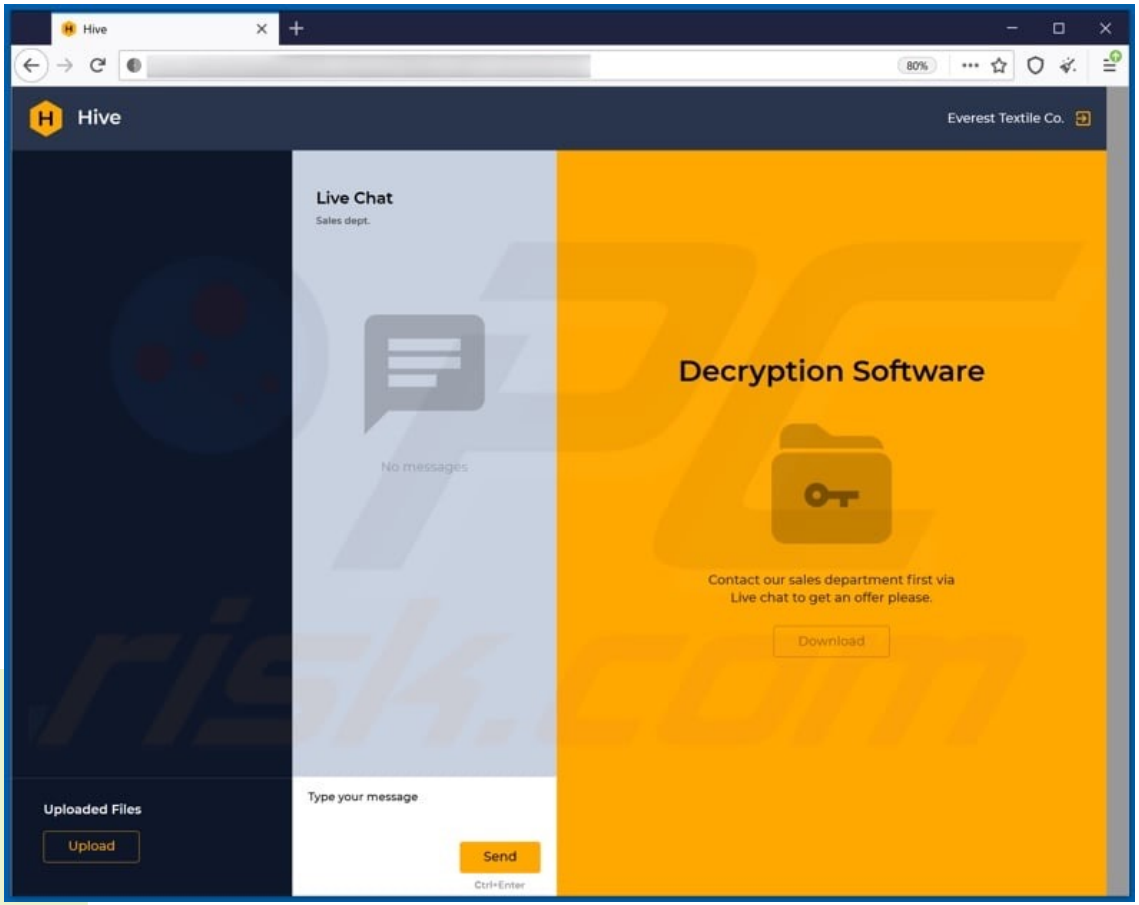
Szenario 2: Was tun?

Szenario 2: Fährtenleser

```
-----------------------------------------------
Initializing SharpHound at 20:41 on 20/02/2020
-----------------------------------------------

Resolved Collection Methods: Group, Trusts, ACL, ObjectProps, Container, GPOLocalGroup, DCOnly

[+] Creating Schema map for domain [redacted] using path CN=Schema,CN=Configuration,DC=[redacted]
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 23 MB RAM
Status: 2060 objects finished (+2060 68,66666)/s -- Using 84 MB RAM
Status: 5356 objects finished (+3296 89,26667)/s -- Using 89 MB RAM
Status: 8248 objects finished (+2892 91,64445)/s -- Using 102 MB RAM
Status: 13808 objects finished (+5560 115,0667)/s -- Using 89 MB RAM
Status: 22365 objects finished (+8557 149,1)/s -- Using 116 MB RAM
Status: 29469 objects finished (+7104 163,7167)/s -- Using 115 MB RAM
Status: 38997 objects finished (+9528 185,7)/s -- Using 119 MB RAM
Status: 47652 objects finished (+8655 198,55)/s -- Using 143 MB RAM
Status: 57706 objects finished (+10046 212,9373)/s -- Using 166 MB RAM
Status: 66979 objects finished (+9225 222,5216)/s -- Using 165 MB RAM
Status: 75874 objects finished (+8887 229,2266)/s -- Using 169 MB RAM
Status: 82305 objects finished (+6429 227,9917)/s -- Using 207 MB RAM
Status: 85162 objects finished (+2857 230,1676)/s -- Using 211 MB RAM
Enumeration finished in 00:06:10.2613620
Compressing data to .\20200220204118_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 20:47 on 20/02/2020! Happy Graphing!
```

Szenario 2: Was tun?

Szenario 2: Ransomware



Szenario 2: Was tun?

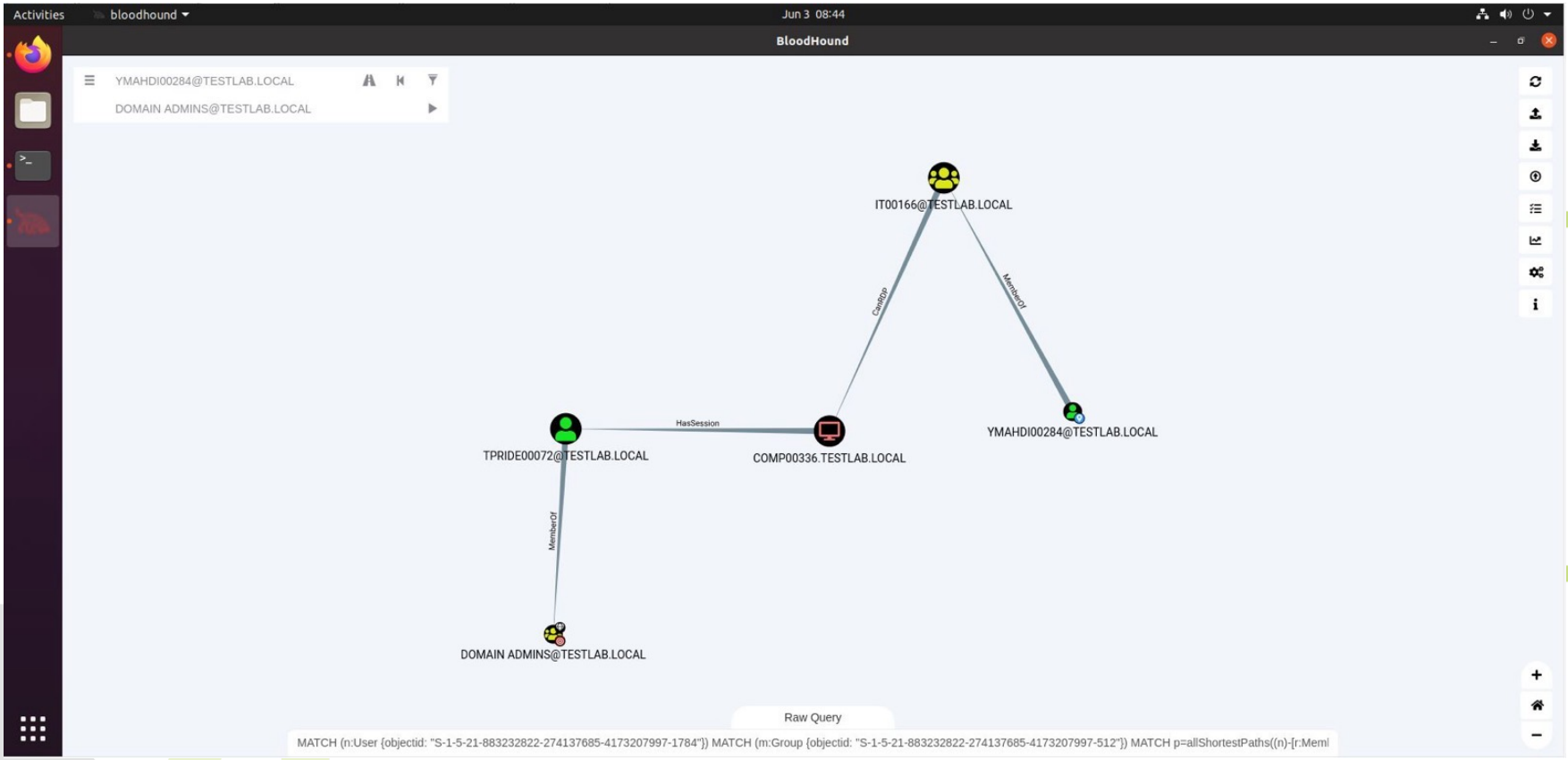
Post Mortem und Analyse

Szenario 2

Szenario 2: Auflösung

Szenario 2: AD Security mit BloodHound

Szenario 2: AD Security mit BloodHound



Szenario 2: Lessons learned

- Supply Chain Angriffe sind ein Problem
- Active Directory so restriktiv wie möglich konfigurieren
- Bei Verlust von Login-Daten:
  - Accounts sperren
  - Aktivitäten überprüfen (auch in der Vergangenheit)
  - Weitere ungewöhnliche Vorgänge prüfen
    - Viele Anfragen an AD
    - Logins auf Domain Controller
    - Viele Sessions
    - …

Fazit

- Angriffsszenarien können sehr unterschiedlich sein
- Anfangs unübersichtlich
  - viele Infos in kurzer Zeit
  - Lage ändert sich ständig
- Richtige Vorgehensweise sehr situationsabhängig
- Vorbereitet sein!

Für Fragen und Informationen:

K4 DIGITAL GmbH
Alfred-Nobel-Allee 38
66793 Saarwellingen

+49 (0)6831 6879-0
info@k4.digital
https://k4.digital