



ICT-Notfallkonzept

achermann ict-services ag
Geschäftshaus Pilatushof
Grabenhofstrasse 4
6010 Kriens

Version 1.0
20.08.2024

Inhaltsverzeichnis

1	ICT-Notfall-Management	3
1.1	Incident Management	3
1.2	Scope	3
1.3	Definition Notfall	4
1.4	Priorisierung	4
1.5	Kriseneskalation	4
2	ICT-Notfall-Organisation	5
2.1	Aufgaben Major-Incident Manager (MIM)	5
2.2	Kompetenzen Major-Incident Manager	5
2.3	Verantwortung Major-Incident Manager	5
2.4	Kontakte	5
2.4.1	Kontakte intern	5
2.4.2	Kontakte extern	5
3	ICT-Notfall Prozess	6
3.1	Auslöser ICT-Notfall Prozess	6
3.2	Kommunikation	7
3.2.1	Interne Kommunikation	7
3.2.2	Externe Kommunikation	7
3.3	Kommunikationsmedien	7
4	ICT-Notfall Debriefing	7
4.1	Intern	7
4.2	Extern	7
5	ICT-Notfallvorsorge und Planung	7
5.1	Change-Management	7
5.2	Backup Konzept	7
5.3	Notfallvorsorge	8
5.4	Notfallplanung	8
5.4.1	ICT-Notfallprozess	8
5.4.2	Systemdokumentation	8
5.4.3	Kundenliste	8
5.4.4	Kundenkontakte	8
5.4.5	Kundenverträge	8

Abbildungsverzeichnis

Abbildung 1	Incident Management	3
Abbildung 2	Major-Incident Management	6

1 ICT-Notfall-Management

1.1 Incident Management

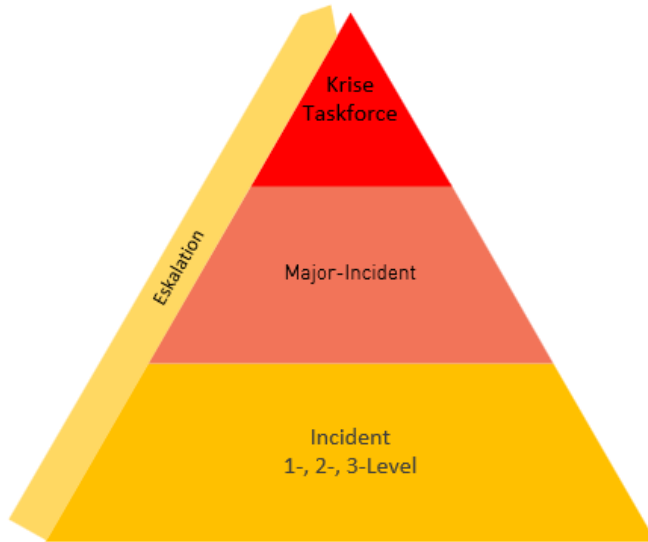


Abbildung 1 Incident Management

Der ICT-Notfallprozess beginnt mit dem Incident Management, welches in drei Ebenen unterteilt ist:

- Incident:
 - 1st Level Support: Zuständig für die Annahme und Erstbearbeitung von Vorfällen. Einfache Probleme werden direkt gelöst, komplexere werden weitergeleitet.
 - 2nd Level Support: Übernimmt die Bearbeitung von schwierigeren Vorfällen und führt tiefere Analysen durch. Bei Bedarf erfolgt eine Eskalation an den 3rd Level.
 - 3rd Level Support: Beschäftigt sich mit hochkomplexen technischen Problemen und arbeitet eng mit Herstellern und Entwicklern zusammen, um Lösungen zu finden.
- Major-Incident:
 - Ein Vorfall, der erhebliche Auswirkungen auf das Geschäft hat und eine sofortige Eskalation erfordert. Ein spezielles Team wird koordiniert, um eine schnelle Lösung herbeizuführen.
- Krise & Taskforce:
 - Wenn ein Major-Incident eskaliert und eine Bedrohung für das gesamte Unternehmen darstellt, wird eine Taskforce gebildet, um strategische Entscheidungen zu treffen und die Krise zu bewältigen.

1.2 Scope

Das Notfallkonzept umfasst alle Services, die von achermann im Datacenter Luzern bereitgestellt werden.

1.3 Definition Notfall

Ein Notfall wird definiert als jede Situation, die eine erhebliche Störung der ICT-Dienste verursacht und eine schnelle Wiederherstellung erfordert. Wie zum Beispiel:

- **Technische Ausfälle:** Hardware- oder Software-Defekte, Netzwerkunterbrechungen, Datenbankkorruption oder andere technische Probleme, die den Betrieb kritischer Systeme unterbrechen.
- **Cyber-Angriffe:** Angriffe wie Hacking, Ransomware, DDoS-Attacken oder andere bösartige Aktivitäten, die die Integrität, Verfügbarkeit oder Vertraulichkeit von Daten und Systemen gefährden.
- **Umweltkatastrophen:** Naturkatastrophen wie Feuer, Überschwemmungen, Erdbeben oder extreme Wetterereignisse, die physische Schäden an IC-Infrastruktur verursachen und den Betrieb behindern.
- **Menschliches Versagen:** Fehler, die durch unsachgemäße Bedienung, Konfigurationsfehler, unbeabsichtigte Datenlöschung oder andere menschliche Handlungen verursacht werden, die den Betrieb von ICT-Systemen stören.
- **Externe Ereignisse:** Stromausfälle, Unterbrechungen der WAN-Kommunikation oder andere externe Störungen, die die Verfügbarkeit der ICT-Services beeinträchtigen.

1.4 Priorisierung

Die Priorisierung von Notfällen erfolgt nach den vereinbarten Service Level Agreements (SLAs) und richtet sich nach der Bedeutung der betroffenen Systeme und Services:

Nach SLA:

1. Platin Kunden
2. Gold Kunden
3. Silber Kunden

Key Systeme

- Datacenter Infrastruktur (Gebäude, Strom, Kühlung)
- Basis System Host, Storage
- Core-Netzwerk Infrastruktur
- Core-Services
- Kunden-Services

1.5 Kriseneskalation

Bei Eskalation eines Major-Incidents, der eine kritische Bedrohung für das Unternehmen resp. Kunden darstellt, wird eine Taskforce gebildet.

Die folgenden Umstände können eine Kriseneskalation auslösen:

- **Unfähigkeit zur Arbeitsfortführung für mehrere Kunden und/oder Mitarbeiter eines Kunden:** Wenn es mehreren Kunden und/oder Mitarbeiter nicht möglich ist, ihre Arbeit fortzusetzen und eine schnelle Lösung nicht in Aussicht steht.
- **Notwendigkeit von Entscheidungen ausserhalb der üblichen Kompetenzen:** Wenn Entscheidungen erforderlich sind, die die Befugnisse der derzeit involvierten Personen übersteigen.
- **Gefährdung des Datacenter durch externe Einflüsse:** Wenn das Datacenter durch externe Faktoren bedroht ist oder bereits in seiner Funktionalität beeinträchtigt wurde.
- **Erforderliche erhebliche finanzielle Ressourcen:** Wenn zur Bewältigung des Major-Incident erhebliche finanzielle Mittel benötigt werden, die über das übliche Mass hinausgehen.

2 ICT-Notfall-Organisation

2.1 Aufgaben Major-Incident Manager (MIM)

- Bildung der Taskforce
- Bestimmt einen Stellvertreter und hält diesen auf dem Laufenden
- Sorgt für eine adäquate interne und externe Kommunikation
- Organisiert und leitet Taskforce-Meetings
- Bestimmt die Mitglieder der Taskforce
- Koordiniert Pendenzen, sammelt und bereitet die erarbeiteten Lösungen auf
- Der MIM kümmert sich primär um das Funktionieren des Prozesses und arbeitet fachlich nur methodisch unterstützend mit

2.2 Kompetenzen Major-Incident Manager

- Entscheidet über den Abschlusszeitpunkt des Störfalls.
- Stellt im Notfall nach eigenem Ermessen ein Notfall-Team zusammen.
- Kann bei Ressourcenknappheit Mitarbeiter anderer Teams aus dem täglichen Geschäft abziehen und der Bearbeitung des Notfalls zuteilen.
- Entscheidet über Eskalation oder Deeskalation eines Notfalls.

2.3 Verantwortung Major-Incident Manager

- Übernimmt die Verantwortung über den gesamten Prozess.
- Ist für die Erarbeitung von Zwischen- und Schlussberichten verantwortlich.
- Dient als Eskalationsstelle für die Mitglieder der Taskforce und ist erste Anlaufstelle bei Fragen und Inputs zum laufenden Störfall.

2.4 Kontakte

2.4.1 Kontakte intern

Die technischen Produkt- und Serviceverantwortlichen sind intern in der Produktverantwortungsmatrix (PV-Matrix) definiert und dokumentiert. Zusätzlich sind alle weiteren Know-how-Träger in der Matrix für jedes Produkt bzw. jeden Service kategorisiert und nach stellvertretenden Produktbeauftragter (SPB), 1st, 2nd und 3rd Level eingestuft.

2.4.2 Kontakte extern

Externe Notfallkontakte sind im ERP unter Kontakte mittels Flag «Notfallkontakt» gekennzeichnet.

3 ICT-Notfall Prozess

Major-Incident Prozess Beschreibung:

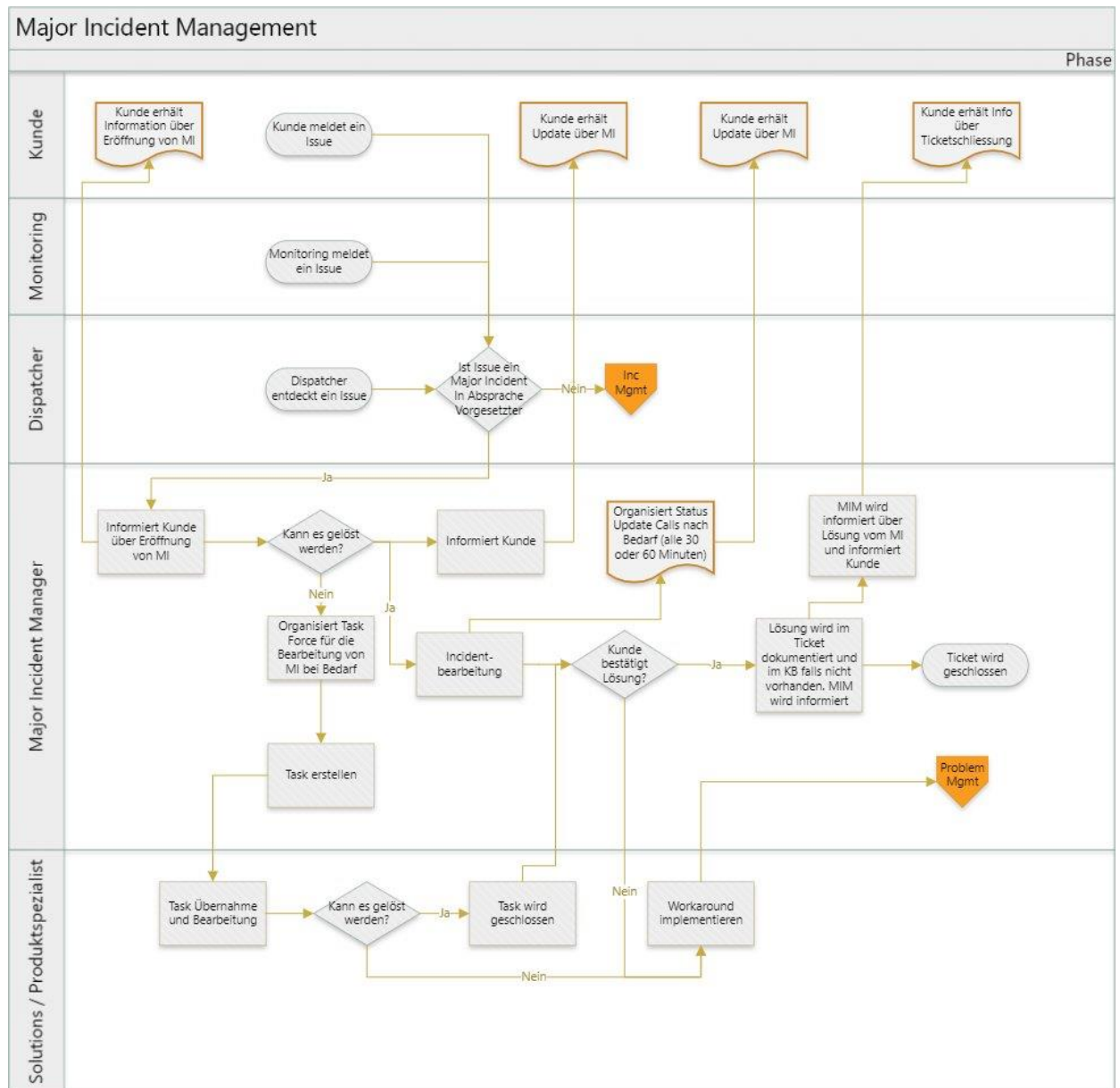


Abbildung 2 Major-Incident Management

3.1 Auslöser ICT-Notfall Prozess

Der ICT-Notfall Prozess wird durch das Eintreten eines Major-Incidents ausgelöst, die erheblichen Auswirkungen auf die Geschäftsprozesse hat und eine Eskalation erfordert.

3.2 Kommunikation

3.2.1 Interne Kommunikation

- **Benachrichtigung des ICT-Service Desk und ICT-Service Teams:**
Der ICT-ServiceDesk sowie das Service Management Team werden umgehend über den eingetretenen ICT-Notfall informiert.
- **Information der betroffenen Teamleiter:**
Alle Teamleiter, deren Mitarbeiter in den ICT-Notfall involviert sind, werden unverzüglich benachrichtigt.
- **Zusätzliche Information des Accountmanagers:** Der zuständige Accountmanager wird ebenfalls über den Notfall informiert.

3.2.2 Externe Kommunikation

- **Kundenkommunikation erfolgt durch den Major-Incident Manager:**
Der Major-Incident Manager initiiert stets die Information der Kunden und trägt die Verantwortung für den Inhalt der Mitteilungen.
- **Benachrichtigung der Kunden durch den ICT-ServiceDesk:**
Der ICT-ServiceDesk informiert die Kunden gemäss der aktuellen Kundenliste.

3.3 Kommunikationsmedien

Grundsätzlich via E-Mail, bei Bedarf auch telefonisch oder durch andere geeignete Mittel.

4 ICT-Notfall Debriefing

4.1 Intern

Nach Abschluss des Notfalls findet ein Debriefing statt, um den Vorfall zu analysieren und Verbesserungen zu identifizieren.

4.2 Extern

Es wird ein Bericht erstellt und an die betroffenen Parteien weitergeleitet.

5 ICT-Notfallvorsorge und Planung

5.1 Change-Management

Alle Änderungen im Rahmen des Change-Management-Prozesses müssen dokumentiert und auf potenzielle Auswirkungen auf die Notfallbereitschaft überprüft werden.

5.2 Backup Konzept

Das Backup-Konzept wird gemäss den festgelegten Richtlinien durchgeführt, um eine schnelle Wiederherstellung im Notfall zu gewährleisten.

5.3 Notfallvorsorge

Im Rahmen des Business Continuity Managements (BCM) werden regelmässige Tests und Überprüfungen durchgeführt. Das BCM ist Bestandteil der ISO27001 und wird jährlich auditiert.

5.4 Notfallplanung

5.4.1 ICT-Notfallprozess

Der Prozessverantwortliche ist für die kontinuierliche Aktualisierung und Pflege des ICT-Notfallprozess verantwortlich.

5.4.2 Systemdokumentation

Jeder, der Veränderungen am System vornimmt, ist für die Aktualisierung der Systemdokumentation verantwortlich.

5.4.3 Kundenliste

Bei Kunden, die vertraglich einen Service Manager zugesichert bekommen haben, wird die Kundenliste gepflegt und stets auf dem aktuellen Stand gehalten. In allen anderen Fällen übernimmt der Account Manager diese Aufgabe.

5.4.4 Kundenkontakte

Bei Kunden, die vertraglich einen Service Manager zugesichert bekommen haben, werden die Kundenkontakte gepflegt und stets auf dem aktuellen Stand gehalten. In allen anderen Fällen übernimmt der Account Manager diese Aufgabe.

5.4.5 Kundenverträge

Der Accountmanager und Service Manager stellen sicher, dass alle Verträge aktuell und vollständig sind.