|  |
| --- |
| [organization/department/business unit] |
| IT-Notfallwiederherstellungsplan (IT DRP) |
|  |
| **Buechel, Stephanie** |
| **Zuletzt getestet & getestet - [Wählen Sie das Datum]** |

# **Über diese Vorlage**

Über diese Vorlage

Diese Vorlage soll Unternehmen dabei helfen, sich mit den Bausteinen eines IT-Disaster-Recovery-Plans (IT-DRP) vertraut zu machen und sich Gedanken darüber zu machen, was nötig wäre, um den normalen Betrieb wieder aufzunehmen, wenn ihre Daten und ihre Infrastruktur von einem schweren IT-Vorfall betroffen wären.

Da jedes Unternehmen die IT anders nutzt, gibt es keinen einheitlichen Business-Continuity- oder Disaster-Recovery-Plan, der für alle passt. Die meisten erfolgreichen IT-DRP-Strategien folgen einem ähnlichen Rahmen und legen die folgenden Punkte fest:

- Was ist wichtig, um die Leistung zu erbringen/zu liefern?

- Wovon sind wir abhängig, um diesen Plan zu ermöglichen?

- Sind unsere IT-Systeme robust genug?

- Wie reagieren wir, wenn Systeme ausfallen?

Um die Planungsarbeit zu vereinfachen, müssen Sie für jede "Ebene" planen, z. B. die Bedürfnisse und Abhängigkeiten auf der Ebene des Unternehmens, des IT-Dienstes und des Serverraums klären. Diese Vorlage konzentriert sich auf Unternehmen, die die ersten Schritte in diesem Bereich unternehmen, und andere, detailliertere Vorlagen können verwendet werden, wenn sie mit dem Kontext dieser Vorlage vertraut sind. Bitte kontaktieren Sie Ihren lokalen Ontrack-Vertreter, wenn Sie zusätzliche Informationen benötigen.

#

# **Einleitung**

# Dieses Dokument beschreibt die Richtlinien und Verfahren von [Organisation/Abteilung/Geschäftseinheit] für den Fall einer Unterbrechung kritischer IT-Dienste oder einer Beschädigung von IT-Ausrüstung oder Daten. Mit diesen Verfahren wird sichergestellt, dass diese Vermögenswerte im richtigen Umfang und innerhalb des richtigen Zeitrahmens wiederhergestellt werden können, um eine Rückkehr zum normalen Betrieb mit minimalen Auswirkungen auf das Geschäft zu ermöglichen.

# Unsere Aufgabe ist es, die Betriebszeit von Informationssystemen, die Datenintegrität und -verfügbarkeit sowie die Geschäftskontinuität zu gewährleisten.

# **Grundsatzerklärung**

# Die Unternehmensleitung hat die folgende Grundsatzerklärung genehmigt:

# Das Unternehmen muss eine entsprechende Kontinuitäts- und Wiederherstellungsplanung durchführen.

# Alle Kontinuitäts- und Wiederherstellungspläne sollten wesentliche und kritische Infrastrukturelemente, Systeme und Netzwerke abdecken, indem sie sich an den wichtigsten Geschäftsaktivitäten orientieren.

# Die Pläne sollten regelmäßig in einer simulierten Umgebung getestet werden, um sicherzustellen, dass sie in Notfallsituationen umgesetzt werden können und dass die Geschäftsleitung und das Personal verstehen, wie sie ausgeführt werden sollen.

# Alle Mitarbeiter müssen mit den Plänen und ihren jeweiligen Aufgaben vertraut gemacht werden.

# Die Kontinuitäts- und Wiederherstellungspläne müssen auf dem neuesten Stand gehalten werden, um veränderten Umständen Rechnung zu tragen.

**Business Impact Analyse**

Im Folgenden finden Sie eine vereinfachte Analyse, die bei der ersten Planung von Arbeiten verwendet werden soll.

Im ersten Abschnitt geht es darum, wichtige IT-Services zu identifizieren, die für das Unternehmen benötigt werden, einschließlich der geschäftlichen Auswirkungen bei Unterbrechungen. Der zweite Abschnitt hilft bei der Identifizierung der Geschäftsanforderungen in Bezug auf Verfügbarkeit, Wiederherstellungszeiten, Backup, Datenintegrität und Datenvertraulichkeit.

|  |  |  |
| --- | --- | --- |
| **Geschäftsbereich** | **Unterstützung des IT-Service** | **Auswirkungen bei Unterbrechung, inkl. Zeit, in der sie inakzeptabel werden** |
| *Produktion* | *IT-system A* | *Montagelinien werden sofort gestoppt, inakzeptabel nach 4 Stunden.* |
|  |  |  |
| *Finanzen* | *IT-system B* | *Wird die Rechnungsstellung und Berichterstattung sofort einstellen, inakzeptabel nach 24 Stunden.* |
|  |  |  |
| *HR* | *IT-system C**IT-system B* | *Wird*  die *Verwendung von vorbereiteten manuellen Verfahren bedeuten, inakzeptabel nach 48 Stunden.*  |
|  |  |  |
| *Alle Geschäftsmitarbeiter* | *E-Mail-System* | *Wird sich sofort auf die Produktivität auswirken, inakzeptabel nach 4 Stunden.* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IT-Service** | **Geschäftliche Anforderungen von:** |  |  |  |  |
|  | **Verfügbarkeit** | **RTO** | **RPO** | **Datenintegrität** | **Vertraulichkeit der Daten** |
| *IT-system A* | *99,7%* | *4 A.m* | *10 Minuten* | *Sehr hoch* | *Niedrig* |
| *IT-system B* | *99,5%* | *24 Stunden* | *24 Stunden* | *Sehr hoch* | *Hoch* |
| *IT-system C* | *99,5%* | *48 Stunden* | *24 Stunden* | *Sehr hoch* | *Sehr hoch* |
| *E-Mail-System* | *99,9%* | *4 A.m* | *12 S.m.* | *Sehr hoch* | *Mittel* |
|  |  |  |  |  |  |

**Recovery Time Objective (RTO)** ist die maximal akzeptable Verzögerung zwischen der Unterbrechung und der Wiederherstellung des Service. Damit wird festgelegt, was als akzeptables Zeitfenster gilt, wenn der Service nicht verfügbar ist.

Der Wiederherstellungszeitpunkt (RPO) wird von der Organisation definiert. RPO

**Recovery Point Objective (RPO)** ist die maximal zulässige Zeitspanne seit dem letzten Wiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Service-Unterbrechung gilt.

**Datenintegrität** ist die Anforderung, dass Informationen intakt bleiben und nicht absichtlich oder unabsichtlich geändert werden.

**Datenvertraulichkeit** ist die Anforderung, die sicherstellt, dass Informationen nicht (absichtlich oder unabsichtlich) anderen zur Verfügung gestellt oder offengelegt werden.

**Belastbarkeitsanalyse**

Wenn der Bedarf des Unternehmens an wichtigen IT-Ressourcen festgestellt wird, ist eine Analyse erforderlich, um sicherzustellen, dass Sie über das richtige Maß an Robustheit zur Unterstützung Ihres Unternehmens verfügen. Bitte beachten Sie, dass dies auch bedeutet, ob Sie zu wenig (ein Risiko) oder zu viel (Kosten) haben.

Setzen Sie sich mit den Verantwortlichen für die einzelnen IT-Services in Verbindung, die für die Planungsarbeiten in Frage kommen. Führen Sie eine ausführliche Diskussion über den geschäftlichen Bedarf und darüber, was heute durch den Dienst abgedeckt wird. Letztendlich ist es eine geschäftliche Entscheidung, was zur Verfügung stehen soll, einschließlich der Risiken, die das Unternehmen bereit ist einzugehen, wenn z. B. die Kosten für einen besseren IT-Service zu hoch sind. Beschreiben Sie die ermittelten Maßnahmen anhand der nachstehenden Tabelle.

|  |  |  |
| --- | --- | --- |
| **Aktion** | **Beschreibung** | **Umsetzungsplan** |
| *Ändern der Backup-Lösung* | *Identifizierung einer neuen Lösung für das IT-System A, um die geschäftlichen Anforderungen von Recovery Point Objective zu erfüllen* | *Analyse durchgeführt (Datum)* |
| *RTO-E-Mail-System* | *Besprechen Sie die Kosten für ein kürzeres Recovery Time Objective mit dem Lieferanten* | *Diskussion (Datum)* |
| *Sicheres Löschen von Festplatten beim Austausch* | *Besprechen Sie eine Lösung mit Ontrack, um alle Festplatten beim Austausch auf sichere Weise zu löschen (für alle Systeme mit hohen* *Vertraulichkeitsanforderungen*  | *Diskussion (Datum)* |

**Abschnitt Wiederherstellungsplanung**

Dieser Teil des Business-Continuity-Plans umfasst die Vorbereitungen zur effizienten Bewältigung von IT-Störungen und zur Verringerung der Auswirkungen auf das Unternehmen.

**Wichtige persönliche Kontaktdaten**

| **Name, Titel** | **Kontaktmöglichkeit** | **Kontaktnummer** |
| --- | --- | --- |
| **Name 1** | Arbeit |  |
| IT-System A | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Name 2** | Arbeit |  |
| IT-System B | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Name 3** | Arbeit |  |
| IT-System C | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Name 4** | Arbeit |  |
| Lokaler Serverraum | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |

# **Externe Kontakte**

| **Name, Titel** | **Kontakt option** | **Kontakt number** |
| --- | --- | --- |
| **Vermieter / Hausverwaltung**  |  |  |
| Account  |  |  |
|  | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Stromanbieter**  |  |  |
| Account | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Telefonanbieter**  |  |  |
| Account | Arbeit |  |
|  | Mobil |  |
|  | Fax |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Datenrettung - Ontrack** |  |  |
| Account | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | E-Mail |  |
|  |  |  |
| **Hardware Dienstleister 1** |  |  |
| Account | Arbeit |  |
|  | Mobil |  |
|  | Notfall-Reporting |  |
|  | E-Mail |  |
|  |  |  |
| **Server Dienstleister 1**  |  |  |
| Account | Arbeit  |  |
|  | Mobil |  |
|  | Fax |  |
|  | E-Mail  |  |
|  |  |  |
| **E-Mail Dienstleister**  |  |  |
| Account | Arbeit |  |
|  | Mobil |  |
|  | Privat |  |
|  | Senden Sie eine E-Mail an ein Kleid |  |
|  |  |  |

Vorbereitete Verfahren zur Datenrettung

## Je nach Vorfall können eines oder mehrere der folgenden Notfallwiederherstellungsverfahren aktiviert werden:

## Verfahren zur Datenrettung bei Ransomware

|  |  |
| --- | --- |
| **Szenario** | Ransomware auf einem oder mehreren Computern/Servern erkannt |
| **Mögliche Ursachen** | Malware |
| **Gefährdete IT-Services und Daten** | Speichersystemeund Laptops |
| **Auswirkung** | Verlorene oder beschädigte Daten |

|  |  |
| --- | --- |
| **Prävention** | * Identifizieren Sie potenzielle Schwachstellen Ihrer Netzwerk- und IT-Umgebung.
* Implementieren Sie die use von VPN-Verbindungen für alle mobilen Mitarbeiter.
* Beschäftigte, die servicekritische IT-Dienste benötigen, sollten den maximalen Zugang haben, der erforderlich ist, um ihre Arbeit erledigen zu können.
* Implementieren Sie einen Backup- und Recovery-Plan für alle wichtigen Daten mit der 3-2-1-Strategie:
	+ 3 - Bewahren Sie mindestens drei Kopien der Daten auf. 2 - Speichern Sie Daten auf zwei verschiedenen Arten von Medien. 1 - Sichern Sie eine Kopie Ihrer Backups extern.
* Testen Sie Backups regelmäßig, um eine ordnungsgemäße Konfiguration sicherzustellen, wodurch die Auswirkungen einer Datenschutzverletzung begrenzt und der Wiederherstellungsprozess beschleunigt wird.
* Isolieren Sie kritische Backups aus dem Netzwerk (Air Gap) für maximalen Schutz.
* Implementieren Sie Copy-on-Write-Dateisysteme (NetApp WAFL – Linux ZFS) oder WORM-Funktionen in NAS-Systemen oder Appliances.
* Patchen Sie kritische Betriebssysteme, Virenschutz-, Sicherheits- und Backup-Software so schnell wie möglich.
* Richten Sie fortlaufende Cybersicherheitsschulungen für Benutzer und Administratoren ein, um Phishing-E-Mails zu identifizieren.
 |

|  |  |
| --- | --- |
| **Aktionsplan** | * Trennen Sie alle von Ransomware betroffenen Systeme vom Netzwerk.
* Zahlen Sie niemals das Lösegeld! Die Bezahlung der Kriminellen garantiert nicht, dass Sie Ihre Daten zurückbekommen. In vielen Fällen (und auf jeden Fall, wenn es sich um einen "Ranscam" oder eine Wischer-Malware handelt) erhalten Sie Ihre Daten nicht zurück, so dass Sie keine Daten haben.
* Versuchen Sie nicht, die Daten selbst zu entschlüsseln. Wenden Sie sich an Ontrack, um sich beraten zu lassen.
* Überprüfen Sie IhreBackups. Selbst wenn Ihr Backup nach einem Ransomware-Angriff fehlt, sollten Sie die Möglichkeit einer Wiederherstellung niemals ausschließen. Mögliche Lösungen hängen von der Art des Mediums oder Speichersystems und der Art der Ransomware ab.
* Identifizieren Sie das Problem und koordinieren Sie eine erste Reaktion.
* Lassen Sie sich sofort beraten, indem Sie sich an Ontrack wenden.
* Folgen Sie den Anweisungen im Detail.
 |

|  |  |
| --- | --- |
| **Wichtige Ansprechpartner** | * XXXX (IT-Systemadministrator)
* XXXX (Ontrack-Kontakt)
* XXXX (FAcilities Manager)
 |

##

## Verfahren zur Datenrettung bei virtuellen Systemen

|  |  |
| --- | --- |
| **Szenario** | Datenverlustsituationen in virtuellen Systemen |
| **Mögliche Ursachen** | * Zeitmangel: Jedem zweiten IT-Mitarbeiter fehlt die Zeit, Abläufe und Prozesse regelmäßig zu dokumentieren.
* Fortsetzen der Arbeit an einem betroffenen System nach einer Datenlöschung.
* Laufwerksausfälle und Probleme mit dem RAID-Betriebssystem.
* Gelöschte oder fehlende virtuelle Maschine/VMDK.
* Beschädigte VMFS-Metadaten oder nicht zugänglicher Datenspeicher.
* Beschädigung im Gastbetriebssystem.
* Die Datensicherungsprozesse sind veraltet.
 |
| **Gefährdete IT-Services und Daten** | STorage-Systemes, die virtuelle Maschinen unterstützen |
| **Auswirkungen** | Verlorene oder beschädigte Daten |

|  |  |
| --- | --- |
| **Aktionsplan** | * Verwalten Sie eine ordnungsgemäße Sicherung für alle Systeme, die virtuelle Maschinen enthalten.
* Arbeiten Sie niemals auf einem betroffenen System, auf dem eineversehentliche Datenlöschung stattgefunden hat.
* Stellen Sie sicher, dass alle Backup-Prozesse auf dem neuesten Stand sind und über einen Notfall-Datenwiederherstellungsplan verfügen.
* Stellen Sie verlorene Daten auf einem sekundären System wieder her, um sich vor weiterem Datenverlust zu schützen.
* Führen Sie keine FSCK- oder CHKDSK-Dateisystemreparaturtools auf einem virtuellen Laufwerk aus, es sei denn, Backups wurden durch Wiederherstellung auf einem sekundären Gerät getestet.
* Stellen Sie sicher, dass Sie über einenaktualisierten Notfallplan mit den besten Praktikenfür die Datenwiederherstellung und Kontaktdaten zu vertrauenswürdigen Experten verfügen.
 |

|  |  |
| --- | --- |
| **Wichtige Ansprechpartner** | * XXXX (IT-Systemadministrator).
* XXXX (Ontrack-Kontakt).
* XXXX (FAcilities Manager).
 |

#

## Verfahren zur Datenrettung bei RAID-Systemen

|  |  |
| --- | --- |
| **Szenario** | Datenverlustsituationen von RAID-Systemen  |
| **Mögliche Ursachen** | * Menschliches Versagen
	+ Ob versehentlich oder mit böswilliger Absicht durchgeführt, Datenverluste durch Neuformatierung, Neuinstallation oder Überschreiben von Volumes können in der Regel von erfahrenen Datenwiederherstellungsingenieuren überwunden werden.
* Probleme mit der Stromversorgung
	+ RAID-Systeme können von einem Stromausfall, Stromausfällen und Stromstößen betroffen sein, was zu einem Datenverlust führt. RAIDs, die in einem verschlechterten Zustand ausgeführt werden, sind besonders anfällig, da Stromprobleme dazu führen können, dass nicht synchronisierte Laufwerke wieder in das Array integriert werden.
* Mechanische Probleme und fehlgeschlagene Umbauten
	+ RAID-Systeme sind so konzipiert, dass sie einzelnen Laufwerksfehlern standhalten, aber sobald ein RAID in einem verschlechterten Zustand ausgeführt wird, steigt die Arbeitslast der verbleibenden Laufwerke und damit auch das Risiko von sekundären Laufwerksausfällen. Zusätzliche Laufwerksausfälle können zu einem vollständigen Ausfall des RAID führen.
* Naturkatastrophen
	+ Feuer, Wasser, Schmutz und andere Verunreinigungen durch Naturkatastrophen können Festplatten im Handumdrehen zerstören.
 |
| **Gefährdete IT-Services und Daten** |  RAID-Systeme |
| **Auswirkungen** | Verlorene oder beschädigte Daten |

|  |  |
| --- | --- |
| **Aktionsplan** | * Führen Sie CHKDSK nicht aus.
	+ Während CHKDSK auf Einzellaufwerkssystemen mit leichter Beschädigung nützlich sein kann, um Dateisysteme in einen konstanten Zustand zu zwingen, sind in den meisten Fällen Inkonsistenzen in einem auf RAID-Speicher gespeicherten Volume das Ergebnis von Problemen auf RAID-Ebene (z. B. nicht synchronisierte Laufwerke, fehlerhafte Neuerstellungen usw.). Das Ausführen von CHKDSK in diesen Szenarien kann zu irreversiblen schädlichen Änderungen an den Dateisystemstrukturen führen.
* Ersetzen Sie niemals ein ausgefallenes Laufwerk durch ein Laufwerk, das Teil eines früheren RAID-Systems war.
	+ Einlways Null aus dem Ersatzlaufwerk vor der Verwendung.
* Wenn ein Laufwerk ungewöhnliche mechanische Geräusche macht, schalten Sie es sofort aus.
	+ Ein mechanisch ausfallendes Laufwerk, das noch verwendet wird, kann die Schwere des Datenverlusts erhöhen und die Chancen auf eine vollständige Wiederherstellung verringern.
* V Sicherungskopien von Daten zu erstellen, bevor Hardware- oder Softwareänderungen vorgenommen werden.
* Beschriften Sie die Laufwerke mit ihrer Position in einem RAID-Array, bevor Sie sie aus Ihrem System entfernen.
* Wenn ein RAID-System mitten in einem Neuerstellungsprozeß ausfällt, führen Sie keine weiteren Wiederherstellungsversuche durch.
* Wenn das Dateisystem bei einem Stromausfall mit einem RAID-Array verdächtig aussieht, nicht eingehängt werden kann oder auf die Daten nach der Wiederherstellung der Stromversorgung nicht zugegriffen werden kann, führen Sie keineVolume-Reparaturprogramme aus.
 |

|  |  |
| --- | --- |
| **Wichtige Ansprechpartner** | * XXXX (IT-Systemadministrator)
* XXXX (Ontrack-Kontakt)
* XXXX (FAcilities Manager)
 |

## Verfahren zur Datenrettung bei Einzelfestplatten und SSDs

|  |  |
| --- | --- |
| **Szenario** | Datenverlustsituationen einzelner Laufwerke |
| **Mögliche Ursachen** | * Mechanische Ausfälle
	+ Wenn Ihre Festplatte nicht funktioniert oder Klick- und/oder Schleifgeräusche macht, liegt wahrscheinlich ein mechanischer Ausfall vor.
* Logische Fehler
	+ Wenn Ihre Festplatte funktioniert, Sie aber nicht auf einige Dateien zugreifen können, liegt ein logisches Problem vor. Dies kann auf eine verlorene Partition oder eine versehentliche Neuformatierung des Laufwerks zurückzuführen sein.
 |
| **Gefährdete IT-Services und Daten** | Benutzerdaten, die lokal auf einem einzigen Laufwerk gespeichert sind |
| **Auswirkungen** | Verlorene Daten |

|  |  |
| --- | --- |
| **Aktionsplan** | * Ausschalten
	+ Schalten Sie den Computer oder das Speichergerät aus, um weitere Schäden zu vermeiden.
* Wasserschaden
	+ TROCKNEN SIE ES NICHT AUS. Korrosion auf die Medien beginnt mit der Trocknung und erhöht den Datenverlust. Legen Sie die Festplatte in eine luftdichte Ziplock-Tasche und senden Sie sie so schnell wie möglich an ein Ontrack-Büro für Festplatten-Datenwiederherstellungsdienste.
* Seltsame Geräusche
	+ Schalten Sie das Gerät aus. Wenn Ihre Festplatte seltsame Klick- oder Schleifgeräusche macht, könnte dies ein Zeichen dafür sein, dass Ihr Laufwerk möglicherweise einen Kopfabsturz erlebt hat und die Daten nicht richtig liest. Ein Kopfabsturz kann zu dauerhaften, nicht behebbaren Schäden an Ihren Dateien führen, wenn das Laufwerk weiter läuft.
* Fehlende , neu formatierte oder gelöschte Dateien
	+ Egal, ob es sich um eine versehentliche Löschung handelte oder ob Ihre Dateien verloren gegangen sind, die Datenwiederherstellungssoftware von Ontrack könnte Ihre Antwort sein. Laden Sie eine kostenlose Testversion der Ontrack EasyRecovery-Software herunter, um eine Liste der wiederherstellbaren Dateien anzuzeigen. Simplizieren Sie, die Volllizenz zu erwerben, um die Daten wiederherzustellen.
 |

|  |  |
| --- | --- |
| **Wichtige Ansprechpartner** | * XXXX (IT-Systemadministrator)
* XXXX (Ontrack-Kontakt)
* XXXX (FAcilities Manager)
 |

## Revisionshistorie

|  |  |  |
| --- | --- | --- |
| **Version** | **Datum** | **Details zur Revision** |
|  |  |  |