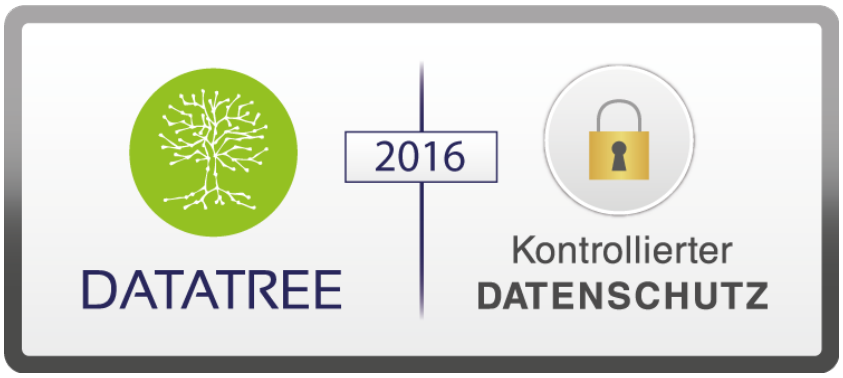
NOVOTERGUM

GESUNDHEITSDIENSTLEISTUNGEN

Datenschutz-Leitlinie



Datenschutzbeauftragter

In allen Fragen zum Datenschutz wenden Sie sich bitte an unseren Datenschutzbeauftragten:

Prof. Dr. Thomas Jäschke, Datatree AG
Mail: dsb@datatree.eu

DATATREE AG - Märkische Straße 212-218 - 44141 Dortmund
T +49 231 54380300 - office@datatree.ag

In der Wahrnehmung seiner Aufgaben wird er im Hause NOVOTERGUM unterstützt von

Herrn Stephan Kretschmer
Telefon +49 2054 9385620
Mail: s.kretschmer@novotergum.de

Bitte richten Sie Ihr Anliegen -wenn möglich- immer an Herrn Kretschmer. Sie haben aber jederzeit auch die Möglichkeit, sich persönlich direkt an den betrieblichen Datenschutzbeauftragten (bDSB) zu wenden. In seiner Tätigkeit ist der Datenschutzbeauftragte (bDSB) weisungsfrei und unterliegt gemäß §203 StGB der Schweigepflicht.

INHALTSVERZEICHNIS

A. Sensibilisierung

1 Einleitung

Dieses Datensicherungskonzept basiert auf dem IT – Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik und wurde den Besonderheiten und den Geschäftsprozessen der NOVOTERGUM angepasst.

1.1 Gefährdungslage

Der Verlust von Daten kann für die NOVOTERGUM erhebliche Auswirkungen auf die Geschäftstätigkeit haben. Sind Anwendungsdaten oder Kundenstammdaten verloren oder verfälscht, kann dies für unser Unternehmen Existenz bedrohend sein.

Darüber hinaus existieren gesetzlich verpflichtende Regelungen, die einzuhalten sind.

Die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein, wie z. B.:

- Zerstörung von Datenträgern durch höhere Gewalt wie z. B. Feuer, Wasser und mechanische Einwirkungen
- versehentliches Löschen oder Überschreiben von Dateien
- fehlerhafte Datenträger
- unkontrollierte Veränderungen gespeicherter Daten
- Datenzerstörung durch Computer-Viren
- Diebstahl der Daten

1.2 Zielsetzung

Ein kompletter Ausschluss der Risiken ist nahezu unmöglich, so dass die NOVOTERGUM Maßnahmen ergriffen hat, die die Folgen eines Datenverlusts mindern. Die Datensicherung gewährleistet, dass durch einen redundanten Datenbestand der IT-Betrieb nach einer Störung kurzfristig wiederaufgenommen werden kann.

Die NOVOTERGUM unterscheidet zwischen der Datensicherung und der Archivierung von Daten. Die Archivierung ist in einem separaten Archivierungskonzept beschrieben.

Darüber hinaus gilt das Notfallvorsorgekonzept der NOVOTERGUM, in dem Verhaltensregeln für den Notfall zusammengestellt sind.

1.3 Begriffliche Definitionen

1.3.1 Daten

Nachfolgend werden die verschiedenen Datenarten kurz dargestellt, die zu sichern sind.

Anwendungsdaten

Anwendungsdaten sind Dateien mit geschäftsbezogenen Inhalten (Textdateien, E-Mails, Datenbanken etc.).

Systemdaten

Systemdaten sind Dateien, die vom Betriebssystem oder Anwendungsprogrammen aus technischen Gründen verwaltet werden.

Protokolldaten

Aktionen von IT-Benutzern oder IT-Systemen werden teilweise zur besseren Nachvollziehbarkeit protokolliert. Daten aus der Protokollierung der Netz- und Zugriffsaktivitäten sind in der Regel auf den Servern hinterlegt.

Software

Hierbei handelt es sich neben System und systemnaher Software auch um Anwendungssoftware.

1.3.2 Datensicherungsarten

Die Wahl der Datensicherungsart ist abhängig von verschiedenen in Kapitel 2 dargestellten Einflussfaktoren.

Datenspiegelung

Die Daten werden redundant und zeitgleich auf verschiedenen Datenträgern gespeichert.

Diese Art der Datensicherung ist nur für die Systeme zu wählen, bei denen der Speicherausfall ohne Zeitverlust kompensiert werden soll, da durch die doppelte Auslegung der Datenträger (z. B. Festplatten) und durch die notwendige Steuerungssoftware hohe Kosten entstehen.

Zu beachten gilt, dass dies keine vollwertige Datensicherung darstellt, sondern lediglich einen Schutz gegen den Datenverlust durch Hardwaredefekte. Dem Datenverlust z. B. durch versehentliches Löschen oder dem Integritätsverlust durch unkontrollierte Datenänderungen kann dadurch nicht begegnet werden, da der Schaden auf beiden Speichermedien gleichermaßen auftritt.

Volldatensicherung

Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf zusätzlichen Datenträgern gespeichert.

Der Zeitraum zwischen zwei Sicherungen sollte nicht zu lang gewählt werden. Eine Volldatensicherung hat zwar einen hohen Speicherbedarf, ermöglicht aber ein schnelles und einfaches Wiedereinspielen (Rekonstruktion) der Dateien.

1.3.3 Datensicherungsmedium

Auch die Wahl des Datensicherungsmediums ist abhängig von verschiedenen in Kapitel 2 dargestellten Einflussfaktoren. Hierbei ist insbesondere das zu erwartende Datenvolumen von Bedeutung. Nachfolgend werden die Datenträger aufgezeigt, welche bei der NOVOTERGUM zur Datensicherung zum Einsatz kommen.

Wechseldatenträger

Optische Datenträger

Hierunter fallen CD und DVD. Diese eignen sich insbesondere für die Sicherung ganzer Festplatteninhalte, wenngleich selbst bei Datenkompression mehrere Datenträger zur Sicherung einer Festplatte notwendig sein können. Des Weiteren eignet sich dieses Medium zur Sicherung von Software. Vorteilhaft sind die geringen Kosten des Mediums und der geringe Platzbedarf zur Lagerung.

Diese werden bei der NOVOTERGUM nur sehr selten eingesetzt, um z.B. Anwenderdaten einzelner User zu sichern.

Bänder / Streamer Tapes

Vorteilhaft an Magnetbändern/Streamer Tapes ist die höhere Speicherkapazität gegenüber CD oder DVD bei gleichzeitig geringeren Kosten gegenüber Festplatten. Nachteilig ist die geringe Datensicherungsgeschwindigkeit und der nicht wahlfreie Zugriff auf die Daten. Magnetbänder/Streamer Tapes haben eine sehr hohe Lebensdauer.

Daher sollen Streamer Tapes insbesondere bei der Speicherung großer Datenvolumen und bei der Speicherung von Daten über einen langen Zeitraum eingesetzt werden.

Diese werden bei der NOVOTERGUM in einem speziellen Safe aufbewahrt.

Cloudsicherung

Die Cloudsicherung hat gegenüber der herkömmlichen Datensicherung und Archivierung eine Vielzahl von Vorteilen. Hier sind insbesondere die nahezu unbegrenzte Speicherkapazität als auch die hohe Wirtschaftlichkeit zu nennen. Auch sind die heutigen Sicherheitsstandards als sehr hoch zu beurteilen.

Festplatte

Festplatten haben eine hohe Datenkapazität. Nachteilig ist die Gefahr eines Hardware-/ Festplattendefekts und die vergleichsweise geringe Lebensdauer.

Festplatten eignen sich für Sicherungen mit großen Datenvolumen und sind bei der Notwendigkeit einer schnellen Datenrekonstruierung zu nutzen.

Externe Festplatten werden bei der NOVOTERGUM nur für nicht unternehmenskritische Daten wie z.B. Installationsimages benutzt.

2 Einflussfaktoren

Zur Festlegung der Verfahrensweise zur Datensicherung hat die NOVOTERGUM eine Verfahrensanweisung erstellt, in der nachfolgende Angaben aufgeführt sind. Anhand dieser sind für die einzelnen IT-Systeme Datensicherungspläne erstellt worden, in denen die entsprechenden Verantwortlichen für die IT-Systeme und die darauf betriebenen Anwendungen einbezogen wurden.

(a) Spezifikation der zu sichernden Daten

Anwendungs- und Betriebssoftware, Systemdaten, Anwendungsdaten und Protokolldaten.

(b) *Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten*

(Wie lange kann die Fachaufgabe ohne diese Daten weitergeführt werden, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss.

(c) *Rekonstruktionsaufwand der Daten ohne Datensicherung*

(Können und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden, wenn eine Datensicherung nicht zur Verfügung steht.

(d) *Datenvolumen*

(e) *Änderungsvolumen*

Das Änderungsvolumen ist sehr entscheidend für die Wahl des Datensicherungsverfahrens und der Datensicherungshäufigkeit. Daher ist zu prüfen, in welchem Umfang die verschiedenen Daten sich innerhalb eines festgelegten Zeitraums ändern. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

(f) *Änderungszeitpunkte der Daten*

(Sicherungszeitpunkte für die verschiedenen Daten. Intervalle oder anlassbezogene Datensicherungszeitpunkte)

(g) *Fristen*

(Gesetzliche Aufbewahrungs- und Löschfristen)

(h) *Vertraulichkeitsbedarf der Daten*

B. Allgemeine Regelungen

3 Verpflichtung der Benutzer auf Datensicherung

Alle NOVOTERGUM Mitarbeiter sind zur Einhaltung dieses Datensicherungskonzepts verpflichtet und aufgefordert, an seiner stetigen Verbesserung mitzuarbeiten.

4 Regelung der Verantwortlichkeiten

Alle Informationseigentümer bzw. Vorgesetzte oder Projektleiter entscheiden für ihren Verantwortungsbereich über Regeln zur Dateiablage auf den NOVOTERGUM Servern.

Für die Durchführung der Datensicherung ist die IT verantwortlich. Es gibt folgende Verantwortlichkeitsgruppen:

1. IT-Benutzer bzw. Informationseigentümer selbst,
2. IT-Administratoren

Es ist nur den NOVOTERGUM Administratoren der Zugriff auf die Datensicherungen erlaubt.

Bei der Festlegung der Verantwortlichkeit hat die NOVOTERGUM insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen IT-Mitarbeiter berücksichtigt. Es muss durch den Leiter IT sichergestellt werden, dass der Verantwortliche IT-Administrator im Notfall erreichbar und ein Vertreter benannt und eingearbeitet ist.

B. Allgemeine Regelungen

5 Allgemeine Grundsätze

Die NOVOTERGUM strebt eine zentrale Datenhaltung an, so dass Daten automatisch über das Netz gesichert werden können. Ausnahmen für mobil eingesetzte IT-Systeme oder IT-Systeme, mit denen geheime Daten verarbeitet werden, sind zugelassen.

Die komplexen NOVOTERGUM Systeme sind durch entsprechend kompetente Mitarbeiter gesichert. IT-Benutzer müssen Daten nur selbst sichern, wenn die Sicherung durch einen ausgebildeten Administrator nicht möglich ist. (z. B. mobile Nutzung des IT-Systems, Smartphones).

Die Datensicherung bei der NOVOTERGUM läuft in der Regel automatisiert ab, um Fehler zu vermeiden.

Wird die Datensicherung nicht von den IT-Benutzern selbst durchgeführt, sind die Verantwortlichen IT Mitarbeiter durch die NOVOTERGUM zur Verschwiegenheit bezüglich der Dateninhalte verpflichtet.

Bei der Rekonstruktion von Daten ist die NOVOTERGUM IT angehalten größte Vorsicht walten zu lassen, um nicht versehentlich Daten zu überschreiben oder Abläufe zu stören.

6 Kontrolle der Datensicherung

Der Verantwortliche IT-Administrator überprüft täglich, ob die Datensicherung tatsächlich korrekt durchgeführt wurde.

7 Schulung und Information der Mitarbeiter

Die NOVOTERGUM Mitarbeiter werden hinsichtlich der Bedeutung der Datensicherung durch Schulungen und Anweisungen / Merkblätter, sensibilisiert.

Alle IT-Benutzer werden anhand des NOVOTERGUM QM-Systems über sie betreffende Regelungen, Aufbewahrungszeiten und Fristen informiert. Hierzu zählen:

- korrekte Wahl und Nutzung der Datensicherungs-Datenträger
- Zugriffsberechtigungen auf Datensicherung bei Datensicherung und Datenrekonstruktion
- korrekte Nutzung der Programme zur Datensicherung
- korrekte Aufbewahrung und Dokumentation der Datenträger zur Datensicherung.

8 Übungen zur Datenrekonstruktion

Für die Rekonstruktion eines Datenbestandes überprüft die NOVOTERGUM IT regelmäßig, ob mit den vorhandenen Sicherungskopien der Daten eine Rücksicherung durchgeführt werden kann. Somit werden technische Defekte, falsche Parametrisierung, eine unzureichende Datenträgerverwaltung o. ä. ausgeschlossen.

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen wird in regelmäßigen Abständen, getestet. Hierbei stellt die NOVOTERGUM IT sicher, dass eine vollständige Datenrekonstruktion möglich ist.

Auf diese Weise wird zuverlässig ermittelt ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion wird auch berücksichtigt, dass

- die Daten auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

9 Revision

Die Erkenntnisse aus den Übungen werden dazu verwendet, das Datensicherungskonzept zu verbessern. Dabei wird auf die Abstimmung mit dem Notfallvorsorgekonzept geachtet.

C. Detailregelungen

10 Durchführung von Datensicherungen

10.1 Transportmodalitäten

Bei der Durchführung einer Datensicherung werden Daten über ein Netz oder eine Leitung übertragen oder Datenträger zum Datenträgerarchiv transportiert.

Bei der Auswahl des Datenübertragungsmediums bzw. des Datenträger-Transportweges hat die NOVOTERGUM so weit wie möglich die Verfügbarkeitsanforderungen berücksichtigt. Für die Datenrekonstruierung über ein Netz wurde die Übertragungskapazität des Netzes und das Datenvolumen beachtet.

Die NOVOTERGUM verhindert durch ein VPN, Firewall, Verschlussboxen und weitere Sicherheitseinrichtungen, dass die Daten während der Übertragung bzw. auf dem Transport unbefugt gelesen, kopiert oder manipuliert werden. Der Transport von Datenträgern erfolgt in der Weise, dass eine Beschädigung der Datenträger möglichst ausgeschlossen ist.

Es ist für die einzelnen Anwendungsdaten festgelegt, wie schnell diese rekonstruiert zur Verfügung stehen müssen. Die Zeit für die Rekonstruierung ist kleiner als die maximal tolerierbare Ausfallzeit.

10.2 Datensicherungsarchiv

Der Zugriff auf Datensicherungsdatenträger ist im erforderlichen Umfang und in angemessener Zeit gewährleistet. Auch nach einem Katastrophen-Fall sind die Datensicherungen verfügbar bzw. zugänglich da die Datensicherungsträger außerhalb der NOVOTERGUM, in einer Cloud bzw. in einem externen Rechenzentrum gelagert werden.

Backup-Datenträger, die im Rahmen der der mobilen Nutzung eines IT-Systems durch die IT-Benutzer angefertigt werden, müssen auch im häuslichen Bereich verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der IT-Benutzer selber (bzw. sein Vertreter) darauf Zugriff hat.

Die Aufbewahrung erfordert angemessene Sicherheitsmaßnahmen. Diese haben sicherzustellen, dass niemand unbefugt auf die Datenträger zugreifen kann. Der Schutzbedarf der Schränke und Räume kann variieren und richtet sich nach dem Schutzbedarf der gelagerten Daten. Es sind durch den IT Benutzer folgende Maßnahmen zu ergreifen:

- Es ist durch entsprechende Maßnahmen die sachgemäße Lagerung sicherzustellen. Darunter fällt u. a. die magnetfeld-/staubgeschützte und klimagerechte Aufbewahrung der Datenträger. Hierzu sind die Angaben der Hersteller zu beachten.
- Es sind Maßnahmen zur Verhinderung des unbefugten Zutritts und Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

10.3 Anforderungen an Datensicherungsmedien

Die NOVOTERGUM hält ausreichend Datensicherungsmedien vor. Hierbei wurde der Verschleiß und der Alterung der verschiedenen Datensicherungsmedien Rechnung getragen. Wiederbeschreibbare Datenträger werden regelmäßig entsorgen und durch neue ersetzt. Hierbei beachtet die NOVOTERGUM die entsprechenden Herstellerangaben.

Die Entsorgung ist so sicher gestaltet, so dass eine Rekonstruktion durch einen unbefugten Dritten nicht möglich ist.

Für die Sicherstellung von etwaigen Aufbewahrungsfristen ist das Archivierungskonzept zu beachten.

11 Datensicherungspläne

Bei der NOVOTERGUM sind die Datensicherungspläne so aufgebaut, dass ein sachverständiger Dritter in der Lage ist, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten, in angemessener Zeit beschaffen und zu installieren.

Hierbei wird eine Unterscheidung zwischen den einzelnen Datenarten vorgenommen, da diese unterschiedlichen Vertraulichkeits-, Verfügbarkeits- und Integritätsanforderungen unterliegen.

Folgende Punkte sind im Datensicherungsplan enthalten:

C. Detailregelungen

- Art der Daten
- zuständig für Sicherung bzw. Rekonstruktion
- Art der Datensicherung (z. B. inkrementell, voll, komprimiert, verschlüsselt)
- Hinweise zur Rekonstruktion
- Häufigkeit und Zeitpunkt der Datensicherung
- Datensicherungsmedium
- Aufbewahrungszeit

11.1 Sicherung von Anwendungsdaten

Die Anwendungsdaten bei der NOVOTERGUM unterliegen stark unterschiedlichen Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen. Daher sind die Schutzanforderungen individuell festzulegen.

Anwendungsdateien dürfen nur auf den entsprechenden NOVOTERGUM Servern gespeichert werden. Bei nicht vernetzten Rechnern sind lokale Datensicherungen vorzunehmen.

Art der Datensicherung

Die NOVOTERGUM IT stellt sicher, dass alle Anwendungsdaten der Server-Festplatte, die älter als 24 Stunden sind, rekonstruiert werden können.

Bei Daten mit sehr hohen Verfügbarkeitsanforderungen (z. B. Kundendatenbank) werden die Daten gespiegelt auf einer zweiten Festplatte gesichert.

Alternativ werden bei der NOVOTERGUM Datensicherungen automatisiert durch spezielle Programme erstellt.

Darüber hinaus werden bei der NOVOTERGUM die von Anwendungsprogrammen angebotenen automatischen Datensicherungsmöglichkeiten genutzt (z. B. das von Textverarbeitungsprogrammen angebotene automatische Erstellen einer Sicherheitskopie).

Häufigkeit und Zeitpunkt der Datensicherung

Die Anwendungsdaten werden einer täglichen Sicherung unterzogen.

Sofern es möglich ist, IT-Systeme im mobilen Einsatz (z. B. Laptops) regelmäßig an ein Netz anzuschließen, hat die Sicherung der lokalen Daten über eine gesicherte (VPN) Netzanbindung zu erfolgen. Dies sollte mindestens wöchentlich durchgeführt werden. Alternativ sind zur Sicherung externe Datensicherungsmedien wie CDs zu nutzen. Datensicherung ist zu kontrollieren.

Die Datensicherung orientiert sich an den arbeitsüblichen Begebenheiten.

Datensicherungsmedium

11.2 Sicherung von Systemdaten

Unter Systemdaten sind systeminterne Einstellungen zu verstehen, die sowohl auf den Servern als auch lokal auf den Endgeräten existieren. Auf den Servern sind z. B. die Rechtestruktur oder Passwörter hinterlegt, auf den Endgeräten zumeist Initialisierungsdateien von Textverarbeitungs- oder Datenbank-Software (*.INI und *.BNK), Makrodefinitionen sowie Textbausteine etc.

Diese Dateien haben unterschiedliche Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen. Systemdaten auf den Servern weisen höhere Anforderungen als angeschlossene (vernetzte) Endgeräte auf.

Bei der NOVOTERGUM werden so wenige Systemdaten auf den Endgeräten gespeichert wie möglich.

Art der Datensicherung

Aufgrund des relativ geringen Daten- und Änderungsvolumens hat man sich bei der NOVOTERGUM auch hier für eine Volldatensicherung entschieden.

11.3 Sicherung von Protokolldaten

Protokolldaten (Login-Protokolle, Protokolle von Sicherheitsverletzungen, Datenübertragungsprotokolle etc.) liegen in der Regel auf dem Server vor.

C. Detailregelungen

Protokolldaten haben hohe Vertraulichkeits- und auch Integritätsanforderungen, was bei der Datensicherung berücksichtigt ist.

Art der Datensicherung

Protokolldaten werden in unserem Unternehmen mittels einer Vollsicherung gesichert. Hierbei werden betriebliche Notwendigkeiten berücksichtigt, wie z.B. Speicherkapazitäten.

11.4 Sicherung von Software

Hierbei handelt es sich neben System- und systemnaher auch um Anwendungssoftware.

Je nach Bedeutung der einzelnen Software für den Geschäftsablauf liegen entsprechend unterschiedliche Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen vor.

Urheberrecht und Copyright-Vereinbarungen werden beachtet.

Art der Datensicherung

Es werden von den Originaldatenträgern gekaufter Software sowie von Eigenentwicklungen und Downloads eine Sicherungskopie erstellt.

Häufigkeit und Zeitpunkt der Datensicherung

Die Software wird dann gesichert, wenn diese erworben bzw. eingespielt wurde. Eine regelmäßige Sicherung ist nicht erforderlich, jedoch findet eine regelmäßige Überprüfung statt, ob Sicherheitskopien erstellt wurden.

12 Dokumentation

Bei der NOVOTERGUM werden bei jeder Datensicherung folgende Punkte dokumentiert.:

- Datum der Datensicherung,
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- Datenträger, auf dem die Daten gesichert wurden,
- Für Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- Bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus wird die Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes (z. B. erforderliche Hard- und Software, benötigte Parameter) beschrieben.

Des Weiteren verfügt die NOVOTERGUM über ein Bestandsverzeichnis. Dies ermöglicht einen schnellen und zielgerichteten Zugriff auf die Datensicherungsdatenträger. Im Bestandsverzeichnis sind folgenden Angaben enthalten:

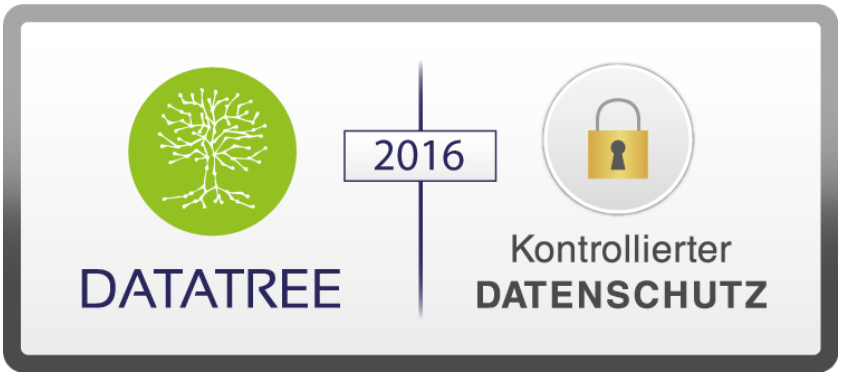
- Aufbewahrungsort
- Aufbewahrungsdauer
- berechtigte Empfänger

Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Hierbei verwendet die NOVOTERGUM eine festlegte Struktur von Kennzeichnungsmerkmalen. Hierbei wurde eine (sprechende) Bezeichnung gewählt, die sowohl das Datum der Datensicherung und die Art der Sicherung enthält. Dies erleichtert die Zuordnung in den Bestandsverzeichnissen.

NOVOTERGUM

GESUNDHEITSDIENSTLEISTUNGEN

Notfallvorsorgekonzept



Inhaltsverzeichnis

1 Einleitung: Was ist ein Notfallvorsorgekonzept?

1.1 Notfall-Definition

Der Ausfall des NOVOTERGUM IT-Systems kann unter Umständen einen großen Schaden nach sich ziehen. So kann der Ausfall eines zentralen NOVOTERGUM IT-Systems zu einem Ausfall des gesamten IT-Betriebs der NOVOTERGUM führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann zu Störungen des IT-Betriebs führen.

Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten (z. B. fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt (wie Feuer, Blitzschlag oder Hochwasser) können hohe Schäden eintreten.

Ein Sicherheitsvorfall stellt jedoch nicht zwangsläufig einen Notfall für die NOVOTERGUM dar. Für einen Notfall gilt die folgende Definition:

„Ein Notfall tritt ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit der NOVOTERGUM IT - Systeme nicht möglich ist und sich daraus ein untragbarer Schaden ergibt.“

1.2 Zielsetzung dieses Notfallvorsorgekonzepts

Um größere Schäden zu begrenzen bzw. diesen vorzusorgen, ist eine zügige und effiziente Behandlung von Sicherheitsvorfällen, die zum Ausfall von IT-Systemen führen, notwendig.

Dieses Notfallvorsorgekonzept hat zum Ziel, die Geschäftstätigkeit der NOVOTERGUM während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen (Business Continuity) sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen (Business Recovery).

Dabei wurden nicht nur die technischen Maßnahmen zum Wiederanlauf beachtet. Besonders wichtig war hier die Planung im Vorfeld, um Notfälle zu verhindern oder zumindest die Auswirkungen begrenzen zu können. Zur Vorbereitung gehörten die Dokumentation von Verfahren und Maßnahmen sowie organisatorische Regelungen. Im Notfall gibt es z. B. Verantwortliche mit klaren Kompetenzen.

Das NOVOTERGUM Notfallvorsorgekonzept beschreibt, welche Maßnahmen zur Vorbereitung auf Notfälle eingeleitet werden und was im Notfall zu tun ist.

2 Verantwortliche Personen

Der "Notfall" wird bei der NOVOTERGUM durch den IT-Sicherheitsbeauftragten, oder den Leiter IT ausgerufen, da schnelle Entscheidungen unabhängig von Hierarchieebenen erforderlich sein können und Mitarbeiter vielleicht außerhalb der normalen Arbeitszeit verständigt werden müssen. Auch könnten Maßnahmen, die vom normalen Arbeitsablauf abweichen und Sonderberechtigungen erfordern, notwendig werden. In Notfällen müssen unter Umständen Beschränkungen und Sicherheitsvorkehrungen außer Kraft gesetzt werden, um ein Problem schneller und unbürokratisch lösen zu können.

Im NOVOTERGUM Notfallplan ist daher festgelegt, welche Aufgaben einzelne Personen im Notfall übernehmen und welche Rechte sie haben. Die beteiligten Personen und Organisationseinheiten sind dann im Notfall befugt, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen.

3 Verhalten in Notfällen

3.1 Allgemeine Regeln für alle NOVOTERGUM Mitarbeiter

Folgende Verhaltensregeln gelten allgemein für alle NOVOTERGUM Mitarbeiter:

- Alle NOVOTERGUM Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzepts (z. B. Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.
- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall bei der NOVOTERGUM hindeuten, sind gemäß der ***Alarmierungspläne*** (siehe Kapitel 3.3) unverzüglich an den IT-Sicherheitsbeauftragten zu melden.
- Die **Handlungsanweisungen** für ausgewählte Schadensereignisse sind einzuhalten.
- Es sind die Anweisungen des IT-Sicherheitsbeauftragten zu beachten.
- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT-Sicherheitskonzepts zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.
- Nach einem Notfall ist der sichere Normalzustand wieder herzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.
- Das Notfallvorsorgekonzept ist stets aktuell zu halten und zu verbessern.

3.2 Sofortmaßnahmen

Derjenige, der einen Sicherheitsvorfall bemerkt, leitet umgehend erste Maßnahmen ein (z. B.: Alarmierung, Rechner ausschalten, den IT-Sicherheitsbeauftragten und andere Kollegen unterstützen...).

Welche Verhaltensregeln bei Vorfällen gelten, ist in den **Handlungsanweisungen** für ausgewählte Schadensereignisse beschrieben.

3.3 Alarmierung

Die verantwortlichen Stellen, die aktiv handeln oder Verantwortung übernehmen müssen, sind zu alarmieren (z. B. Feuerwehr, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter…). Sie übernehmen dann die weitere Untersuchung und Bewertung des Vorfalls und leiten geeignete Maßnahmen ein.

Im Vorfeld wurden Alarmierungspläne erstellt, die die Meldewege für ausgewählte Schadensereignisse beschreiben.

Im Anhang ist eine Adress- und Telefonliste in der alle relevanten Telefonnummern interner verantwortlichen und externer Dienstleister und Behörden aufgeführt sind.

- Vorstände
- Bereichsvorstände
- Leiter IT
- IT-Sicherheitsbeauftragter
- Datenschutzbeauftragter
- Feuerwehr
- Polizei
- Notarzt
- Wasser- und Stromversorger
- Telekommunikationsanbieter
- Versicherer

Untersuchung und Bewertung des Vorfalls:
Um einen Sicherheitsvorfall bei der NOVOTERGUM untersuchen und bewerten zu können, sind folgende Informationen notwendig:

- betroffene IT-Komponenten (IT-Systeme und IT-Anwendungen)
- betroffene Geschäftsprozesse
- Ansprechpartner (Technik und Fachabteilung)
- Verfügbarkeitsanforderungen der IT-Komponenten
- Schutzbedarf der IT-Komponenten und der damit verarbeiteten Informationen
- möglicher Schaden: Schadensart, Schadenshöhe, Geschädigte (z. B. Kunden oder Geschäftspartner)
- mögliche Folgeschäden
- Ursache des Vorfalls (technisches Versagen, Unachtsamkeit, gezielter Angriff)
- Maßnahmen zur Behebung des Vorfalls

Um alle Informationen schnell zur Hand zu haben wurden folgende Dokumentationen erstellt:

- Bestandsliste Hard- und Software inkl.
  - Schutzbedarfsfeststellung
  - Verfügbarkeitsanforderungen
- Netzwerkplan

3.4 Maßnahmen zur Problemlösung

3.4.1 Reihenfolge der Fehlerbehebung

Bei der Behebung von Schäden werden verschiedene Aspekte berücksichtigt, wenn unterschiedliche Vorfälle, mehrere IT-Komponenten oder verschiedene Geschäftsprozesse betroffen sind und eine Wiederanlaufreihenfolge festgelegt werden muss.

- Bedeutung einer ausgefallenen IT-Komponente oder des betroffenen Geschäftsprozesses
- Bewertung unterschiedlicher Schadensarten durch die Unternehmens- oder Behördenleitung
- Technische oder ablaufbedingte Abhängigkeiten der IT-Systeme und IT-Anwendungen voneinander.

Es besteht die Möglichkeit, dass bestimmte Prozesse erst dann wiederhergestellt werden können, wenn andere, die als Grundlage zu sehen sind, bereits wieder funktionsfähig sind.

3.4.2 Voraussetzungen für kurze Wiederanlaufzeiten

Um im Schadensfall Probleme möglichst schnell lösen zu können, wurden folgende Vorbereitungen getroffen:

- Erstellung von eigenen Dokumentationen
- Datensicherung (siehe Kapitel 6.1)
- Verträge mit externen Dienstleistern, Herstellern und Lieferanten (siehe Kapitel 6.2)
- Ersatzbeschaffungsplan für Hardware (siehe Anhang B 4.3)

3.4.3 Notbetrieb

Nicht immer kann jedes Problem in einer tolerierbaren Zeitspanne behoben werden (Beispiel: Reparatur eines IT-Systems dauert zu lange). In diesen Fällen ist es erforderlich, die wichtigsten Geschäftsprozesse provisorisch aufrecht zu erhalten. Für die NOVOTERGUM bedeutet dies:

- Einschränkung des IT-Betriebs Um bei einem eingeschränkten IT-Betrieb die geschäftskritischen Prozesse betreiben zu können, ist für IT-Anwendungen die zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren.
- manuelle Ersatzverfahren
- interne oder externe Ausweichmöglichkeiten

Die notwendigen Dokumentationen sowie Kontaktadressen von Dienstleistern, Herstellern und Lieferanten wurden im Vorfeld zusammengestellt.

3.5 Informationspolitik

Unter Umständen müssen betroffene interne und externe Stellen über den Vorfall informiert werden. Dies sind insbesondere diejenigen Stellen, die direkt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. In Einzelfällen kann es auch notwendig sein, die Medien zu informieren.

Über Art und Umfang der Information externer Stellen entscheidet ausschließlich der Vorstand der NOVOTERGUM.

3.6 Dokumentation

Eine Dokumentation des Notfalls ist notwendig, um für zukünftige Vorfälle zu lernen und Veränderungen an IT-Systemen und IT-Anwendungen nachvollziehen zu können. Dies ist besonders wichtig, wenn unter Zeitdruck gearbeitet wurde.

4 Nachbereitung von Notfällen

Eine Nachbereitung von Notfällen erfolgt bei der NOVOTERGUM aus zwei Gründen:

1. Verbesserungspotentiale erkennen

Dazu werden folgende Fragen versucht zu klären:

- Waren die Reaktionszeiten ausreichend?
- Hat die Alarmierung funktioniert oder gab es Probleme bei der Eskalation des Vorfalls?
- Wurde die Ursache des Vorfalls schnell gefunden und wurden die Auswirkungen richtig eingeschätzt?
- Waren alle Dokumentationen brauchbar und aktuell?
- Wenn es einen Täter gab: Was hat ihn motiviert?
- Was muss in Zukunft verbessert werden?

2. Wiederherstellung eines stabilen Normalzustandes

Nach einem Notfall wird dafür gesorgt, dass möglichst schnell der sichere Normalzustand wieder erreicht wird. Zur Behebung des Notfalls sind unter Umständen Anwendungen, IT-Systeme oder Konfigurationen verändert oder elektronische Abläufe durch manuelle ersetzt worden.

Es kann z. B. auch erforderlich sein, Passwörter neu zu vergeben.

5 Revision des Notfallvorsorgekonzepts

Das Managementsystem zur Behandlung von Sicherheitsvorfällen, und damit auch das Notfallvorsorgekonzept, wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft werden.

Alle Maßnahmen müssen regelmäßig daraufhin überprüft werden, ob sie

- wirksam und effektiv sind,
- den betroffenen NOVOTERGUM Mitarbeitern bekannt sind,
- unter Stress umsetzbar sind und
- in den NOVOTERGUM Betriebsablauf integrierbar sind.

6 Prävention und Vorbereitung

Die folgenden Maßnahmen sollten zur Notfallvorsorge ergriffen werden.

6.1 Datensicherungsplan

Datensicherungen sind zu erstellen, um Datenverlust vorzubeugen und Ersatz-Systeme schnell in Betrieb nehmen zu können.

Mit Hilfe eines Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können. Ein Datensicherungsplan muss Auskunft geben können über:

- Datum der Datensicherung
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert)
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind
- Datenträger, auf dem die Daten gesichert wurden
- für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.)
- Ort der Aufbewahrung

Es ist ein Datensicherungskonzept zu erstellen und zu beachten, in dem die Datensicherung explizit geregelt wird.

6.2 Outsourcing, Verträge mit Hersteller und Lieferanten

Notfallvorsorge muss Bestandteil von Verträgen mit externen Dienstleistern sein. Außerdem kann es erforderlich sein, bei Notfällen auf die Dienste von Spezialisten zurückzugreifen.

Die wichtigsten Vorgaben sind vertraglich zu vereinbaren, z. B:

- Zuständigkeiten, Ansprechpartner und Abläufe
- Datensicherung
- Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen
- regelmäßige Notfallübungen

Alle für eine Ersatzbeschaffung von IT-Systemen notwendigen Vereinbarungen mit Lieferanten (Servicezeiten, Lieferfristen etc.) sind zu treffen.

Bei der Auswahl von Software sind Support- und Serviceleistungen als Auswahlkriterium zu berücksichtigen. Bei Bedarf sind vertragliche Regelungen (Hotline, Antwortzeiten, individuelle Updates und Patches) mit den Herstellern abzuschließen.

6.3 Versicherungsschutz

Verbleibende Restrisiken werden von der NOVOTERGUM unter Beachtung von Kosten- Nutzen-Aspekten durch Versicherungen abgedeckt. Beispiele sind:

- Sachversicherungen
- Feuerversicherung
- Einbruchdiebstahlversicherung
- Elektronik-Versicherung
- Betriebsunterbrechungs- Versicherung

6.4 Technische Maßnahmen

Um zu vermeiden, dass ein Sicherheitsvorfall zum Notfall wird, müssen Sicherheitsvorfälle bei der NOVOTERGUM durch technische Maßnahmen verhindert oder möglichst frühzeitig entdeckt werden.

6.4.1 Einsatz von technischen Detektionsmaßnahmen

Es gibt eine Reihe von Sicherheitsvorfällen, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Zu diesem wurden bei der NOVOTERGUM Detektionsmaßnahmen installiert.

Dies sind zum Beispiel:

- Gefahrenmeldeanlage
- Rauchmelder
- Fernanzeige von Störungen
- Computer-Viren-Schutzprogramme
- Intrusion Detection und Intrusion Response Systeme
- Kryptographische Checksummen und digitale Signaturen

Die technischen Detektionsmaßnahmen sind durch zusätzliche organisatorische Maßnahmen ergänzt, wie z. B. Meldewege, regelmäßige Aktualisierung und Überprüfungen.

Bei der Auswahl von Detektionsmaßnahmen wurden bei der NOVOTERGUM immer eine Kosten-Nutzen-Berechnung zugrunde gelegt und die Wirksamkeit kritisch hinterfragt.

6.5 Sichere Infrastruktur

Die Infrastruktur (Gebäude und Räume) ist durch geeignete Maßnahmen gesichert. Dazu gehören beispielsweise die Bereiche Zugangs- und Zutrittsschutz, Diebstahlschutz, Schutz vor Naturereignissen, Stromversorgung und Klimatisierung.

Durch eine unterbrechungsfreie Stromversorgung ist sichergestellt, dass für hochverfügbare IT-Systeme ein kurzzeitiger Stromausfall keinen Schaden verursacht.

6.6 Ausbildung und Training der Mitarbeiter

6.6.1 Notfallschulungen

Ein qualitativ hochwertiges Notfall- und Kontinuitätsmanagement greift nur dann optimal, wenn die Mitarbeiter zum einen für sicherheitsrelevante Vorfälle sensibilisiert sind und zum anderen bestmöglich für sicherheitsrelevante Vorfälle geschult werden.

Sämtliche Mitarbeiter, auch nicht unmittelbar mit dem IT-Betrieb befasste Personen, werden bei der NOVOTERGUM in der Anwendung des Notfallvorsorgekonzeptes geschult.

6.6.2 Notfallübungen

Es werden regelmäßig angekündigte und unangekündigte Übungen durchgeführt. Bei einer Notfallübung werden z. B. folgende Tätigkeiten durchgeführt:

- Durchspielen der Notfallsituation im Team
- Wiedereinspielen von Datensicherungen
- Wiederanlauf nach Ausfall eines ausgewählten IT-Systems
- Durchführung einer Alarmierung
- Funktionstests von Stromaggregaten
- Durchführung von Feuerübungen

Die Erkenntnisse aus den Übungen werden zur Verbesserung des Notfallvorsorgekonzepts genutzt.

A. Anhang: Verantwortliche Personen

1 Notfall-Verantwortlicher

Der Notfallverantwortliche der NOVOTERGUM ist der Leiter der IT Abteilung, Herr Alexander Hilsing.

Der Notfall-Verantwortliche hat folgende Aufgaben:

- Erstellung und Pflege des Notfallvorsorgekonzepts
- Bewertung von Sicherheitsvorfällen
- formale Ausrufung und Beendigung des Notfalls
- Koordination der Notfallmaßnahmen
- Dokumentation des Notfalls, Erstellung eines Abschlussberichts
- Unterrichtung der betroffenen Fachabteilungen sowie bei Bedarf der Leitungsebene.
- Zusammenstellung und Einberufung eines Notfall-Teams
- Organisation und Vorbereitung von Notfall-Schulungen und –Übungen

2 IT-Sicherheitsbeauftragter

Die NOVOTERGUM hat Herrn Bastian Fernges zum IT-Sicherheitsbeauftragten bestellt.

Der IT-Sicherheitsbeauftragte hat folgende Aufgaben:

- Entgegennahme von Meldungen über Sicherheitsvorfälle
- bei Bedarf, Information an den Notfall-Verantwortlichen
- Unterstützung bei der Behebung und Aufarbeitung eines Notfalls
- Überwachung ob alle IT-Sicherheitsmaßnahmen nach Beendigung des Vorfalls wieder in Kraft gesetzt wurden
- Überprüfung ob mit den Erkenntnissen aus dem Vorfall das IT-Sicherheitskonzept auf Schwächen und Verbesserungsmöglichkeiten hin angepasst wurde

3 IT-Benutzer

Alle NOVOTERGUM Mitarbeiter haben die Notfallvorsorge zu unterstützen. Das gilt besonders für die Fachabteilungen bei der Erstellung von spezifischen Notfallplänen und Dokumentationen sowie der Zusammenarbeit mit dem Notfall-Verantwortlichen.

Im Notfall gelten für alle die allgemeinen Verhaltensregeln, die in Kapitel 3.1 des Hauptdokuments zusammengefasst sind.

4 Brandschutzbeauftragter

Der Brandschutzbeauftragte der NOVOTERGUM ist Herr Stephan Kretschmer.

Der Brandschutzbeauftragte hat folgende Aufgaben:

- Einhaltung der Brandschutzvorschriften
- Brandschutzbegehungen
- Die Zusammenarbeit mit der Feuerwehr
- Aufstellung der Brandschutzordnung
- Kontrolle und Wartungsüberwachung der Brandmelde- und Löschvorrichtungen
- Durchführung von Übungen

Der Brandschutzbeauftragte und der IT-Sicherheitsbeauftragte arbeiten eng zusammen und sorgen dafür, dass bei den Brandschutzmaßnahmen die besonderen Belange der Informationssicherheit berücksichtigt werden.

A. Anhang: Verantwortliche Personen

5 Weitere Rollen

Unternehmensleitung

Der Vorstand der NOVOTERGUM trifft abschließende Entscheidungen zur Durchführung von Maßnahmen. Er schaltet die Polizei und Strafverfolgungsbehörden ein, wenn der Verdacht auf kriminelle Handlungen besteht und informiert bei Bedarf die Presse und andere Medienvertreter.

IT - Administratoren

NOVOTERGUM IT - Administratoren haben eine große Verantwortung. Sie überwachen ihre IT-Systeme und Anwendungen und sind die ersten Ansprechpartner von IT-Benutzern bei Problemen und Fragen. Sie werden daher oftmals die ersten sein, die erkennen, dass eine Unregelmäßigkeit sicherheitsrelevant ist. Sie müssen dann verantwortungsbewusst entscheiden, ob sie das Problem selbst beheben können oder ob sie den Vorfall eskalieren.

Justitiar, Datenschutzbeauftragter

Diese Positionen sind heranzuziehen, sofern ein Notfall juristische, datenschutzrechtliche oder mitbestimmungspflichtige Aspekte hat.

Ersthelfer

Bei der NOVOTERGUM sind Ersthelfer benannt und durch Aushänge bekannt.

.

B. Anhang: Dokumente

1 Vorgaben zur Priorisierung von Sicherheitsvorfällen

Ein Sicherheitsvorfall bei der NOVOTERGUM hätte in der Regel unterschiedliche Schäden zur Folge. Dies könne sein:

- Einen Verstoß gegen Gesetze
- finanzielle Auswirkungen
- Imageschäden

Der Vorstand der NOVOTERGUM hat Prioritäten für die Problembeseitigung vor dem ersten Vorfall festgelegt.

Diese Prioritäten haben Einfluss auf die Reihenfolge, in der die Probleme angegangen werden und wie der Wiederanlauf geschehen soll.

2 Handlungsanweisungen für ausgewählte Schadensereignisse

2.1 Schadensszenarien und Handlungspläne

Bei Sicherheitsvorfällen und in Notfällen ist es entscheidend, dass alle Mitarbeiter wissen, was zu tun ist. Aus diesem Grund wurden bei der NOVOTERGUM für die wichtigsten Schadensereignisse Handlungsanweisungen und Verhaltensregeln aufgestellt. Die Fachverantwortlichen bei der NOVOTERGUM haben entschieden, für welche Geschäftsprozesse, Abläufe und Szenarien derartige Handlungspläne sinnvoll und notwendig sind:

Schäden durch höhere Gewalt, die Auswirkungen auf die Verfügbarkeit der Informationsverarbeitung haben:

- Brand
- Stromausfall
- Hochwasser
- Hardware-Ausfall aufgrund technischer Defekte
- Ausfall der Datenübertragungseinrichtungen wie DFÜ
- Virenbefall
- Vandalismus, Sabotage, Einbruch
- Rechenzentrum nicht zugänglich

IT-Sicherheitsvorfälle, die zu Notfällen werden können:

- Ausfall einzelner IT-Systeme
- Ausfall einzelner Anwendungen
- Ausfall eines Netzes

2.2 Inhalt der Dokumentation

Für jedes Szenario wurden folgende Aspekte beschrieben:

- **Sofortmaßnahmen** (siehe Kapitel 3.2)

  Wie muss derjenige, der einen Vorfall bemerkt, umgehend reagieren?

- **Alarmierungsplan** (siehe Kapitel 3.3)

  Welche verantwortlichen Stellen müssen zuerst benachrichtigt werden?

- **Maßnahmen zur Schadensbegrenzung**
- **Maßnahmen zur Behebung des Vorfalls**

B. Anhang: Dokumente

- **Informationspolitik** (siehe Kapitel 3.5)

  Welche internen und externen Stellen sind zusätzlich zu informieren?

3 Eskalationsstrategie

Bei der NOVOTERGUM wird die Meldung über einen Sicherheitsvorfall oder eine darauf hindeutende Unregelmäßigkeit zunächst dahingehend geprüft, welches Ausmaß und welche Bedeutung der Vorfall bzw. die Unregelmäßigkeit hat, um dann entsprechende Maßnahmen zu ergreifen. Innerhalb der NOVOTERGUM Eskalationsstrategie werden Personen, Zeitpunkte und Medien der Eskalation definiert.

Entscheidungshilfe für Eskalation

Die NOVOTERGUM hat für folgende Sicherheitsvorfälle und Notfallszenarien festgelegt, in denen eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen erforderlich ist:

- Die (Vermutete) Schadenshöhe übertrifft den Verantwortungsbereich
- Die Kosten und Ressourcen für die erforderlichen Maßnahmen übertreffen den Kompetenzbereich
- Die Komplexität des Sicherheitsvorfalls übersteigt Kompetenz- bzw. den Zuständigkeitsbereich

Eskalationswege

Die NOVOTERGUM hat definiert, wer an wen eine Meldung weitergibt. Dabei wurden sowohl die regulären Eskalationswege als auch der Vertretungsfall berücksichtigt.

Die notwendigen Adress- und Telefonlisten sind im NOVOTERGUM QM – System eingebunden.

4 Dokumentation der Informationstechnik

4.1 Beschreibung und Bestand der Hard- und Software

Die Notfallvorsorge des IT-Einsatzes basiert bei der NOVOTERGUM auf einer aktuellen Dokumentation der vorhandenen IT-Anwendungen und IT-Systeme.

Die NOVOTERGUM hat erfasst, welche IT-Systeme betrieben werden und mit welcher Hard- und Software diese ausgestattet sind. Ein Bestandsverzeichnis der Systemsoftware sowie der zu dem IT-System gehörenden Systemdaten wird geführt.

Hier sind die wichtigsten IT-Anwendungen beschreiben und ihre Abhängigkeit von den IT-Systemen dargestellt.

Alle Dokumentationen werden regelmäßig aktualisiert und sind so aufbewahrt,

dass sie im Bedarfsfall jederzeit verfügbar, aber trotzdem nur zuständigen Personen zugänglich sind.

4.2 Schutzbedarf und Verfügbarkeitsanforderungen

Die NOVOTERGUM hat festgelegt, welche Geschäftsprozesse von hoher Relevanz für die Geschäftstätigkeit sind und daher ein Verlust oder die Nicht-Verfügbarkeit einen hohen Schaden für die NOVOTERGUM bedeutet.

4.3 Ersatzbeschaffungsplan

Wenn die Reparatur eines ausgefallenen IT-Systems nicht möglich ist oder zu lange dauert, kann eine Ersatzbeschaffung notwendig werden. Zur Vorbereitung hat die NOVOTERGUM einen Ersatzbeschaffungsplan mit folgenden Angaben erstellt:

- Bezeichnung der IT-Komponente

B. Anhang: Dokumente

- Hersteller / Lieferant
- Dauer der Re-Installation

Der Ersatzbeschaffungsplan erfordert eine regelmäßige Überarbeitung.

4.4 Wiederanlaufreihenfolge

Technische oder ablaufbedingte Abhängigkeiten der NOVOTERGUM IT-Systeme und NOVOTERGUM IT-Anwendungen sowie deren Wichtigkeit, beeinflussen die Wiederanlaufreihenfolge nach einem Ausfall eines NOVOTERGUM IT-Systems oder dem Abbruch einer Anwendung. Entsprechende Zusammenhänge sind wurden hier berücksichtigt

5 Beschreibung der Infrastruktureinrichtungen

Bei der NOVOTERGUM existieren alle notwendigen Raum- und Fluchtwegpläne.

6 Ersatzverfahren und Ausweichmöglichkeiten

6.1 Manuelle Ersatzverfahren

In den NOVOTERGUM – Einrichtungen sind manuelle Ersatzverfahren für IT-Prozesse zeit- und arbeitsaufwendig, helfen aber kurzzeitig den Ausfall von IT-Anwendungen oder IT-Systemen zu kompensieren. Alle Fachverantwortlichen kennen die für ihren Verantwortungsbereich manuellen Ersatzverfahren für den Notfall. Die erforderlichen Hilfsmittel (Faxgeräte, Formulare, Papierlisten, etc.) werden in den NOVOTERGUM - Einrichtungen bereitgehalten.

6.2 Ausweichmöglichkeiten

6.2.1 Interne Ausweichmöglichkeiten

Alle Fachverantwortlichen überprüfen regelmäßig, ob bei Problemen mit den standardmäßig genutzten IT-Systemen ein Ausweichen auf andere IT-Systeme möglich ist (z. B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Dies geschieht in Enger Abstimmung mit dem Leiter IT der NOVOTERGUM.

6.2.2 Externe Ausweichmöglichkeiten

Bei der NOVOTERGUM werden externe Ausweichmöglichkeiten dann herangezogen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können. Ausweichmöglichkeiten für nicht IT-spezifische Komponenten werden hierbei auch berücksichtigt.

6.2.3 Ausweichlösungen für DFÜ-Versorgung

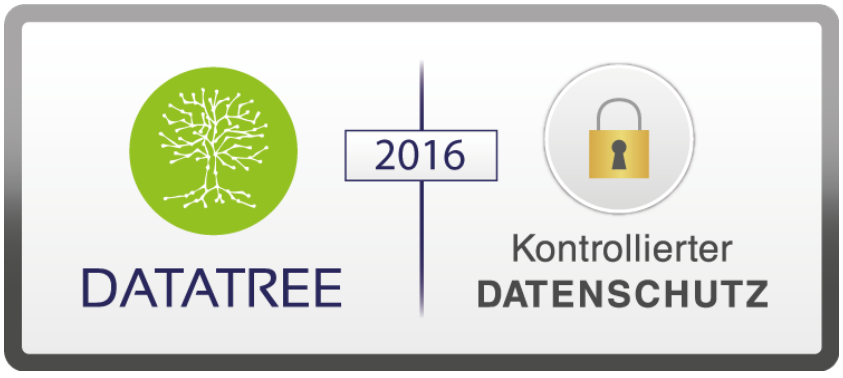
Aufgrund der oftmals hohen Verfügbarkeitsanforderungen bei der NOVOTERGUM, sind für die DFÜ-Verbindungen folgende Ausweichlösungen definiert:

- Ersatz der Datenübertragung durch Austausch von Datenträgern oder Druckerzeugnissen per Kurier
- Datenübertragung über andere DFÜ-Einrichtungen
- Einsatz mobiler Kommunikationseinrichtungen

NOVOTERGUM

GESUNDHEITSDIENSTLEISTUNGEN

Informationssicherheitsleitlinie



Präambel

Die Verarbeitung von Informationen spielt bei der NOVOTERGUM eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch die Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Geschäft nicht auf Grund eines Ausfalls der Systeme zusammenbrechen.

Da unser know how und unsere Kernkompetenz in der Entwicklung und Erbringung innovativer Produkte und Dienstleistungen liegt, ist der Schutz dieser Informationen und Konzepte vor unberechtigtem Zugriff und vor unerlaubter Manipulation von existenzieller Bedeutung.

Geltungsbereich

Die Informationssicherheitsleitlinie gilt für den gesamten Tätigkeitsbereich der NOVOTERGUM. Sie enthält Vorgaben zur Datensicherheit, zum Datenschutz und die zugehörige Sicherheitsstrategie. Werden Dritte mit der Erbringung von Leistungen beauftragt, ist durch vertragliche Vereinbarungen sicher zu stellen, dass die Informationssicherheitsleitlinie in den Leistungsbeziehungen berücksichtigt wird.

Übergreifende Ziele

Unsere Daten und unsere IT-Systeme werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten toleriert werden können. Hierzu wurde ein, auf die NOVOTERGUM Prozesse abgestimmtes Datensicherungs- und Archivierungskonzept erstellt.

Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau. Für den Umgang mit Kennzahlen, Betriebsgeheimnissen und insbesondere Patientendaten gelten bei der NOVOTERGUM maximale Anforderungen an die Vertraulichkeit.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze wie z.B. Strafgesetzbuch, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz und vertraglichen Regelungen wie z.B. die Verschwiegenheitsverpflichtung und die Verpflichtung auf das Datengeheimnis ein. Negative finanzielle und immaterielle Folgen für die NOVOTERGUM sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit IT-Systemen und beim Umgang mit sensiblen Daten bewusst und unterstützen die Sicherheitsstrategie der NOVOTERGUM nach besten Kräften.

Detailziele

Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen für die NOVOTERGUM und ihre Mitarbeiter nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten, insbesondere Kennzahlen, wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit aller Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher mit dem bei der NOVOTERGUM höchst möglichen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Patienten, Kunden und Geschäftspartner.

Für die Operative ist die Aufrechterhaltung der Kommunikation zur Zentrale, zu den Kunden und Geschäftspartnern und der Zugriff auf die eingesetzten Softwaresysteme, insbesondere auf das CRM und NOVOBASE elementar. Die Behandlung von Patienten und die Betreuung unserer Partner darf nicht unverhältnismäßig verzögert oder gar fahrlässig gefährdet werden. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Umsatzminderungen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Operative hat einen besonders hohen Schutzbedarf.

Kennzahlen, Betriebsgeheimnisse Mitarbeiter- und Patientendaten haben bei der NOVOTERGUM sehr hohe Vertraulichkeitsanforderungen. Durch deren Verlust oder Diebstahl können Wettbewerbsnachteile entstehen.

Durch technische und organisatorische Maßnahmen sowie eine hohe Aufmerksamkeit aller Mitarbeiter wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt. Hierzu erarbeitet der Datenschutzbeauftragte der NOVOTERGUM ein umfassendes Datenschutzkonzept nach den Vorgaben der DSGVO.

Innerhalb der IT-Abteilung werden die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Ausfallzeiten sind nur in einem sehr geringen Maße akzeptabel, da diese direkt, aber auch indirekt beispielsweise durch negative Auswirkungen auf nachfolgende Prozesse, zu Umsatzminderungen führen können.

Die Nutzung von Intranet und Internet zur Informationsbeschaffung und zur Kommunikation ist für die NOVOTERGUM selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen und Regelungen stellt die NOVOTERGUM sicher, dass die Risiken der Internetnutzung möglichst gering bleiben.

Informationssicherheitsmanagement

Zur Erreichung der Datenschutzsicherheitsziele hat die oberste Leitung einen Datenschutzbeauftragten öffentlich bestellt. Der Datenschutzbeauftragte berichtet in seiner Funktion direkt an den Vorstand. Des Weiteren wurde ein IT-Sicherheitsbeauftragter, zur Erreichung der Datensicherheitsziele benannt, welcher ebenfalls direkt an den Vorstand berichtet. Der Datenschutzbeauftragte und der IT - Sicherheitsbeauftragte haben ein ausreichend bemessenes Zeitbudget für die Erfüllung ihrer Pflichten zur Verfügung. Beide sind angehalten, sich regelmäßig weiterzubilden.

Dem Datenschutz- und IT-Sicherheitsbeauftragter werden von der obersten Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

Der IT- Sicherheitsbeauftragte und der Datenschutzbeauftragte sind durch die IT-Benutzer ausreichend in ihrer Arbeit zu unterstützen.

Der Datenschutzbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheits- und datenschutzrelevante Aspekte zu berücksichtigen.

Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des Datenschutzbeauftragten und des IT- Sicherheitsbeauftragten zu halten.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme bestimmt die NOVOTERGUM den jeweiligen Schutzbedarf und legt die Zugriffsberechtigungen fest.

In den Stellenbeschreibungen sind die Vertretungen zu regeln. Es muss durch Unterweisungen und ausreichende Dokumentationen (Einarbeitungspläne, Schulungsnachweise) sichergestellt werden, dass die Vertreter ihre Aufgaben erfüllen können.

NOVOTERGUM Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen NOVOTERGUM IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen an Daten verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den Datenschutzbeauftragten der NOVOTERGUM.

Auch bei der NOVOTERGUM können Datenverluste nie vollkommen ausgeschlossen werden. Durch ein umfassendes Datensicherungs- und Archivierungskonzept wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.
Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Für Ausgelagerte IT-Dienstleistungen an externe Stellen, wie z.B. Webhosting oder E-Mail, werden von der NOVOTERGUM konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Hier wird auch das Recht auf Kontrolle der Umsetzung der Sicherheitsmaßnahmen festgelegt.

IT-Benutzer nehmen an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die NOVOTERGUM unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Sicherheit

Das Qualitätsmanagementsystem für die Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die oberste Leitung unterstützt die ständige Verbesserung des NOVOTERGUM Sicherheitsniveaus. Alle Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den Datenschutzbeauftragten weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau bei der NOVOTERGUM sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.