die ausfallsichere nullPC Cloud
Kosten halbiert - Verfügbarkeit verdoppelt

nullPC White Paper

nullPC als Baustein für das Notfallmanagement – Business Continuity

Gespiegelte virtuelle Server und Desktops
sowie effiziente Ersatzgeräte

Inhalt

1 Zusammenfassung

Die technische Entwicklung bringt für Behörden und Unternehmen eine stetig steigende Abhängigkeit von Systemen mit sich, deren Ausfall gar nicht oder nur kurze Zeit möglich ist, ohne dass die Organisation erheblichen Schaden erleidet. Umfangreiche und vorbeugende Maßnahmen sind daher unbedingt notwendig, um die Funktionsfähigkeit und damit das Überleben der Organisation zu sichern. Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** hat für das Notfallmanagement eine Richtline unter der Bezeichnung **BSI-Standard 100-4** herausgegeben, die auf ca.120 Seiten die notwendigen Maßnahmen und Anleitung zur Umsetzung beschreibt.

Das Notfallmanagement umfasst demzufolge eine Vielzahl an organisatorischen, personellen und technischen Vorkehrungen, die im Folgenden kurz und im Überblick betrachtet werden.

Besonders hervorgehoben wird die Möglichkeiten einer hochverfügbaren nullPC IT-Infrastruktur Lösung, die ad hoc zugängliche Telearbeitsplätze und äußerst einfach installierbare Ersatz-IT-Arbeitsplätze mit redundant ausgelegten Rechenzentren, in denen die gespiegelte Server- und Desktop-Systeme ausgeführt werden, verbindet.

2 Zweck eines Notfall Konzeptes

Das Notfallmanagement wird von der obersten Leitungsebene einer Organisation initiiert und kontrolliert. Entscheidend ist, dass dafür genügend personelle und technische Ressourcen auf allen untergeordneten Ebenen bereitgestellt werden.

Oftmals haben sehr grundlegende Entscheidungen großen Einfluss auf das Notfall-management. Dazu zählen die Standortplanung, der Grad an Zentralisierung und Dezentralisierung der Organisation usw.

Notfallmanagement ist eine Methode, mit die Chancen einer Organisation verbessert werden, Krisen oder Katastrophen zu überstehen, und gliedert sich in folgende Teilbereiche, die zeitlich abgestimmt ineinander greifen:

- Risikoanalyse und –steuerung dienen der Verhinderung von Krisen,
- Notfallplanung umfasst die Maßnahmen zur systematischen Krisenabwehr,
- Krisenmanagement geht darüber hinaus und fördert sachgemäßes Handeln auch in Stresssituationen.

Die Risikoanalyse besteht in einer Bestandsaufnahme von Gefahrenpotentialen in der Organisation, die Risikobewertung wählt im nächsten Schritt diejenigen Gefahren aus, die

- auf Grund der Kombination von Eintrittswahrscheinlichkeit und Schadenshöhe, oder
- wegen gesetzlicher Vorgaben

eine besondere Bedrohung darstellen.

Die daraus folgende Notfallplanung ist ein Prozess

- mit dem Ziel ein umfassendes und detailliertes Konzept in Form eines Notfallhandbuch zu erstellen,
- in den möglichst alle betroffenen Mitarbeiter, einschließlich wichtiger Lieferanten und Kunden, involviert sind,
- unter Einbeziehung externer Berater und **anerkannter Standards (z.B. BSI 100-4)**.

Ein wesentlicher Teilbereich beschäftigt sich mit Vorkehrungen für den Ausfall einer technischen Anlage, wie beispielsweise eines IT-Systems. Der entscheidende Parameter ist die maximale vertretbare Dauer eines ungeplanten Ausfalls, die als Zeitdauer oder häufig als Prozentzahl (z.B. ungeplante Ausfalldauer pro Jahr) angeben wird.

3 Grundsätze der technischen Notfallplanung

Die Notfallplanung muss vom Ausfall der größten Einheit, eines Standortes oder eines Gebäudes, ausgehen und herunter gebrochen werden bis auf die Stufe einzelner Geräte, einer Festplatte oder eines Druckers.

Robustheit und hohe Ausfallsicherheit bei technischen Geräten lässt sich durch drei grundsätzliche Prinzipien erreichen:

- Redundanz,
- Standardisierung,
- Einfachheit.

Die ohne Zweifel größte Bedeutung hat dabei auf allen hierarchischen Ebenen der Grundsatz der Redundanz, besser zwei Standorte als ein großer, besser zwei Rechenzentren als eines, besser ein RAID-Verbund als Einzelfestplatten, besser doppelt ausgelegte statt einfacher Netzwerkverbindungen (Teaming).

Mittels Standardisierung lässt sich ebenfalls in gewissem Umfang dem Ausfall einzelner Geräte entgegen wirken, besser einheitliche und damit austauschbare Geräte, z.B. bei Druckern. Auch die Ersatzteilbevorratung und -beschaffung profitiert von einheitlichen ausgelegten Geräten, ganz abgesehen vom geringeren Know-How-Bedarf beim technischen Personal.

Damit verwandt, aber auch darüber hinausgehend, ist die Forderung nach Einfachheit, im Gegensatz zu Komplexität und Vielfalt, die oftmals historisch gewachsen ist oder den Sonderwünschen einzelner Abteilungen entspringt. Aus der Forderung nach Einfachheit lässt sich beispielsweise eine angemessene Form der Zentralisierung ableiten, ein zentraler Server ist einfacher redundant vorzuhalten als eine große Anzahl dezentraler PCs.

Das letzte Beispiel macht bereits deutlich, dass die genannten drei Prinzipien häufig mit einander kombiniert werden, und erst dadurch die gewünschte Robustheit des Gesamtsystems erreicht werden kann.

Aus all dem wird deutlich, dass die Notfallplanung bereits bei der Konzeption und Planung des Normalbetriebs beginnen muss.

Bei der Planung von Ersatzgeräten spielt darüber hinaus deren Wiederbeschaffungsdauer und -kosten bzw. deren Lagerfähigkeit eine entscheidende Rolle.

Das BSI-Notfallmanagement beschreibt dies eingehend im **Kapitel 5 Konzeption**.

4 Unterbrechungsfreies Rechenzentrum

Die Methoden zum Aufbau eines unterbrechungsfreien Rechenzentrums sind seit langem bekannt und basieren auf Redundanz und Spiegelung von Servern und Speichern. Um auch gegen katastrophale Ereignisse wie Brand eines ganzen Gebäudes oder eines Teilbereichs gewappnet zu sein, muss ein angemessener Abstand zwischen den beiden Rechenzentren eingehalten werden, mindestens in zwei unterschiedlichen Brandabschnitten eines Gebäudes, einem anderen Gebäude des gleichen Firmengeländes oder besser noch heutzutage, in Folge zunehmend verfügbarer, schneller Glasfaser-Verbindungen, in einer anderen Niederlassung oder einem Ersatzgebäude.

Die beiden Rechenzentren können auf zweierlei Weise betrieben werden:

- eines als primäres und im Normalfall einziges aktives System, das andere im passiven Standby-Betrieb oder,
- bei heute möglichen Übertragungsraten, im Normalfall beide im Aktiv-Aktiv-Betrieb.

Letztere Variante bietet die Möglichkeit zu erheblichen Einsparungen, vor allem wenn im Notfall ein eingeschränkter Systembetrieb, für nur einen Teil der Mitarbeiter, ausreichen sollte.

Sehr von Vorteil ist es dabei, wenn sämtliche Stufen der Kommunikation auf einem einheitlichen Protokoll, vorzugsweise TCP/IP, basieren:

- iSCSI als Protokoll für Standort übergreifenden Speicherzugriffe,
- für den Datenaustausch zwischen den verschiedenen Serversystemen
- sowie zwischen Servern und Endgeräten.

Weiterhin bietet heutzutage die ausgereifte und bereits weitverbreitete Technik der Virtualisierung von IT-Systemen beste Voraussetzungen für die Spiegelung kompletter Server- und Desktop-Systeme.

Ein Beispiel dafür stellt in besonders kompakter Weise ein nullPC Cluster dar, das bereits in der Grundausbaustufe mit zwei physischen Servern die gleichzeitige Spiegelung von Speicher, Servern und Desktops zulässt. Bei Bedarf lässt sich ein solches nullPC Cluster sehr einfach um zusätzliche physische Server erweitern.

Dabei handelt es sich um ein sogenanntes „shared nothing Cluster“, d.h. bei richtig konfigurierter Redundanz der Netzwerk-Verbindungen gibt es keinen „Single Point of Failure“. Damit kann dem Ausfall einzelner technischer Komponenten sowie dem ganzer Gebäude oder Gebäudeteile vorgebeugt werden.

Das BSI-Handbuch 100.4 erläutert diese Vorkehrungen ausführlich im **Anhang A.3 Informationstechnik** und **A.6 Externe Dienstleister und Lieferanten**.

5 Unterbrechungsfreier Zugriff durch effiziente Ersatz-Endgeräte

Um auch nach einem Gebäudeausfall den Geschäftsbetrieb möglich bald fortsetzen zu können, sind weitere umfangreiche Notfallplanungen erforderlich. Während die Spiegelung des Rechenzentrums und damit dessen unterbrechungsfreier Betrieb bei vielen Organisationen häufig bereits zum Standard gehören, stellt es nach wie vor eine große Herausforderung dar, Ersatz-Arbeitsplätze ähnlich schnell zur Verfügung zu stellen.

Ersatz für Büroraum und -einrichtung lassen auf unterschiedliche Weise organisieren:

- Telearbeitsplätze, z.B. im Home-Office mit dem privaten PC und einer ausreichend schnellen Internet-Anbindung,
- in den Räumen einer anderen Filiale derselben Organisation,
- in angemieteten Ersatzbüros oder Containern.

Im ersten Fall genügt die ad hoc eingerichtete Remote-Verbindung zum Ersatzrechen-zentrum für eine sehr schnelle Wiederherstellung der Einsatzbereitschaft, wie dies beispielsweise mit einem nullPC Remote-USB-Stick möglich ist. Auf Basis von Voice-over-IP lässt sich damit der Anschluss ans Telefonsystem der Organisation ebenso leicht wiederherstellen.

In den beiden andern Fällen geht es darum, binnen Kurzem das notwendige Mobiliar sowie Bürogeräte, u.a. PC-Arbeitsplätze, zu beschaffen. Auch dazu bietet eine nullPC-Lösung mit ihrem minimalen, von jedermann installierbaren Zero-Client beste Voraussetzung.

Zero Clients, ohne bewegliche Teile wie Festplatten oder Lüfter, können darüber hinaus wegen ihrer Kompaktheit und Robustheit so effizient gelagert werden, wie dies bei normalen PCs niemals möglich wäre. Auch bei schnellster Bestellung und Lieferung dauert es mindestens 1 bis 2 Tage bis Ersatzsysteme zur Verfügung stehen, die im Anschluss daran erst noch von Fachleuten konfiguriert und installiert werden müssen. Somit vergehen etliche Tage, bevor die Mitarbeiter wieder Zugang zu ihren Anwendungen und Daten erhalten.

Das BSI-Handbuch betrachtet diese Vorkehrungen im **Anhang A.2 Arbeitsplätze** und **A.4 Komponentenausfälle.**

6 Längere Notfallstromversorgung durch geringeren Energieverbrauch

Die Reduzierung des Stromverbrauchs ist eine wichtige gesamtgesellschaftliche Herausforderung. Die Anstrengungen im Bereich der IT werden EU-weit unter dem Begriff GreenIT zusammengefasst und beziehen sich vorzugsweise auf den Normalbetrieb von IT-Systemen.

Für die Notfallplanung ergeben sich allerdings weitere wesentliche Aspekte, die von einem geringerem Stromverbrauch deutlich profitieren würden. Dabei sollen Krisen von regionalem oder nationalem Ausmaß, die das Stromangebot insgesamt drastisch reduzieren würden, hier gar nicht betrachtet werden, da diesen den Zuständigkeitsbereich einzelner Organisationen und damit deren Notfallplanung überschreiten würden.

Kurze Stromschwankungen und -ausfälle dagegen werden typischer Weise durch batteriegespeiste USV-Anlagen überbrückt. Der Einsatz stromsparender Endgeräte lässt die überbrückbare Zeitspanne entsprechend verlängern. Vergleichbares gilt bei länger anhaltenden Ausfällen, wenn ein eigener Generator zur Verfügung steht und dieser nach wenigen Minuten die Notstromversorgung übernehmen kann.

7 Risiko-Übertragung und -verteilung

Üblicherweise wird eine Organisation versuchen, ihr Risiko durch den Abschluss einer entsprechenden Versicherung zu vermindern, durch Absicherung der Wiederbeschaffungskosten für die vernichteten Sachwerte sowie häufig auch eine Betriebsausfallversicherung, die für entgangenen Erlöse während der Zeit des Betriebsausfalls aufkommt.

In jedem Fall sind ausschließlich direkte finanzielle Schäden versicherbar, nicht dagegen weitergehende Einbußen, wie Imageschäden oder Verletzung gesetzlicher Verpflichtungen zur Leistungserbringung, bei der Verwaltung, Feuerwehr oder im Krankenhaus.

Somit ist es in solchen Fällen nahezu unumgänglich, alle oben genannten Möglichkeiten zu nutzen, um innerhalb kürzester Zeit eine zumindest eingeschränkte Betriebsbereitschaft wiederherzustellen.

Oftmals wird es in diesen Fällen zweckmäßig sein, wenn mehrere Organisationen sich zusammenschließen und die Notfallvorsorge gemeinsam organisieren. Damit ließe sich auch die Lagerhaltung für Mobiliar und Geräte von der Anzahl und damit den Kosten her deutlich reduzieren.

Autor

Harro von Wardenburg, Dipl. Math.
Geschäftsführer und Miteigentümer der nullPC GmbH, einem Unternehmen, das sich ganz der Entwicklung ausfallsicherer Cluster-Lösungen für Speicher, Server und Desktops verschrieben hat. Er besitzt langjährige Erfahrungen in diesem Bereich, die noch auf das legendäre OpenVMS-Cluster von HP, ehemals DEC, zurückgehen.