infopulse

eBook

Business Continuity und Disaster Recovery:

So schützen Sie Ihr Unternehmen_

Inhaltsverzeichnis

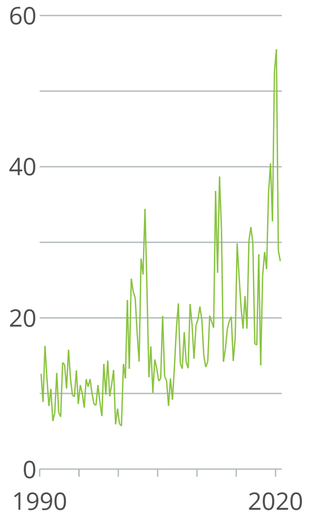
Egal, ob es sich um Lieferketten oder Informationsflüsse handelt, die Unternehmen sind heute stärker miteinander vernetzt als noch vor zehn Jahren.

Durch die stärkere Vernetzung wurde jedoch auch der Risikoradar der Unternehmen erweitert. Ein vorübergehender Stromausfall in einer Region kann Hunderte von Unternehmen lahmlegen. Wenn sich weitere negative Ereignisse ereignen - von sozialer Instabilität bis hin zu Naturkatastrophen und Cyberangriffen -, können ihre Auswirkungen branchenübergreifend zu Störungen führen.

Die meisten Unternehmen ziehen es heute vernünftigerweise vor, für den Fall einer Unterbrechung vorauszuplanen - anstatt darauf zu warten, dass die Unterbrechung eintritt - und Pläne für die Kontinuität des Geschäftsbetriebs und die Reaktion auf Katastrophen zu erstellen.

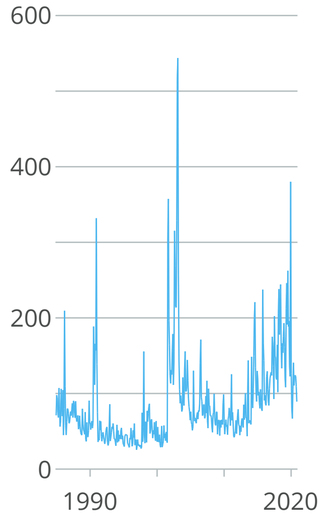
Unterbrechungen werden immer häufiger und gravierender

IMF World Uncertainty Index*, Tausend



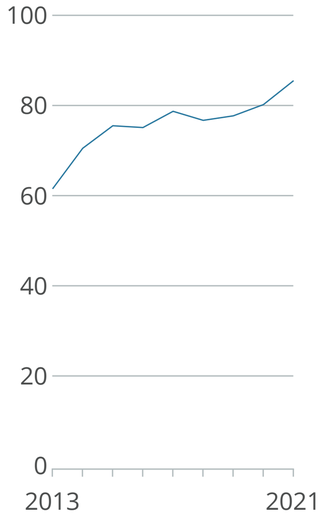
Die globale Unsicherheit hat seit 2000 um ein Vielfaches zugenommen

Federal Reserve Board, Geopolitischer Risikoindex**



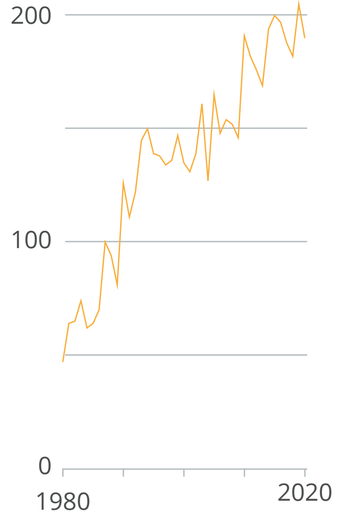
Das geopolitische Risiko ist so hoch wie seit 2003 nicht mehr

Unternehmen, die pro Jahr von einem Cyberangriff betroffen sind, %



Cyber-Vorfälle haben seit 2013 um 24 Prozentpunkte zugenommen

Naturkatastrophen pro Jahr, Anzahl



Die Häufigkeit von Naturkatastrophen nimmt zu

* Basierend auf dem prozentualen Anteil des Wortes "unsicher" (oder seiner Variante) in den Länderberichten der Economist Intelligence Unit.

** Automatisierte Textsuchergebnisse aus den elektronischen Archiven von 11 Zeitungen: Boston Globe, Chicago Tribune, Daily Telegraph, Financial Times, GLOBE and Mail, Guardian, Los Angeles Times, New York Times, Wall Street Journal und Washington Post. Der Index wurde berechnet, indem die Anzahl der Artikel zum Thema geopolitisches Risiko in jeder Zeitung für jeden Monat gezählt wurde (als Anteil an der Gesamtzahl der Nachrichtenartikel).

Quelle: CyberEdge: Swiss Re

Quelle

infopulse

Was ist Business Continuity (BC)?_

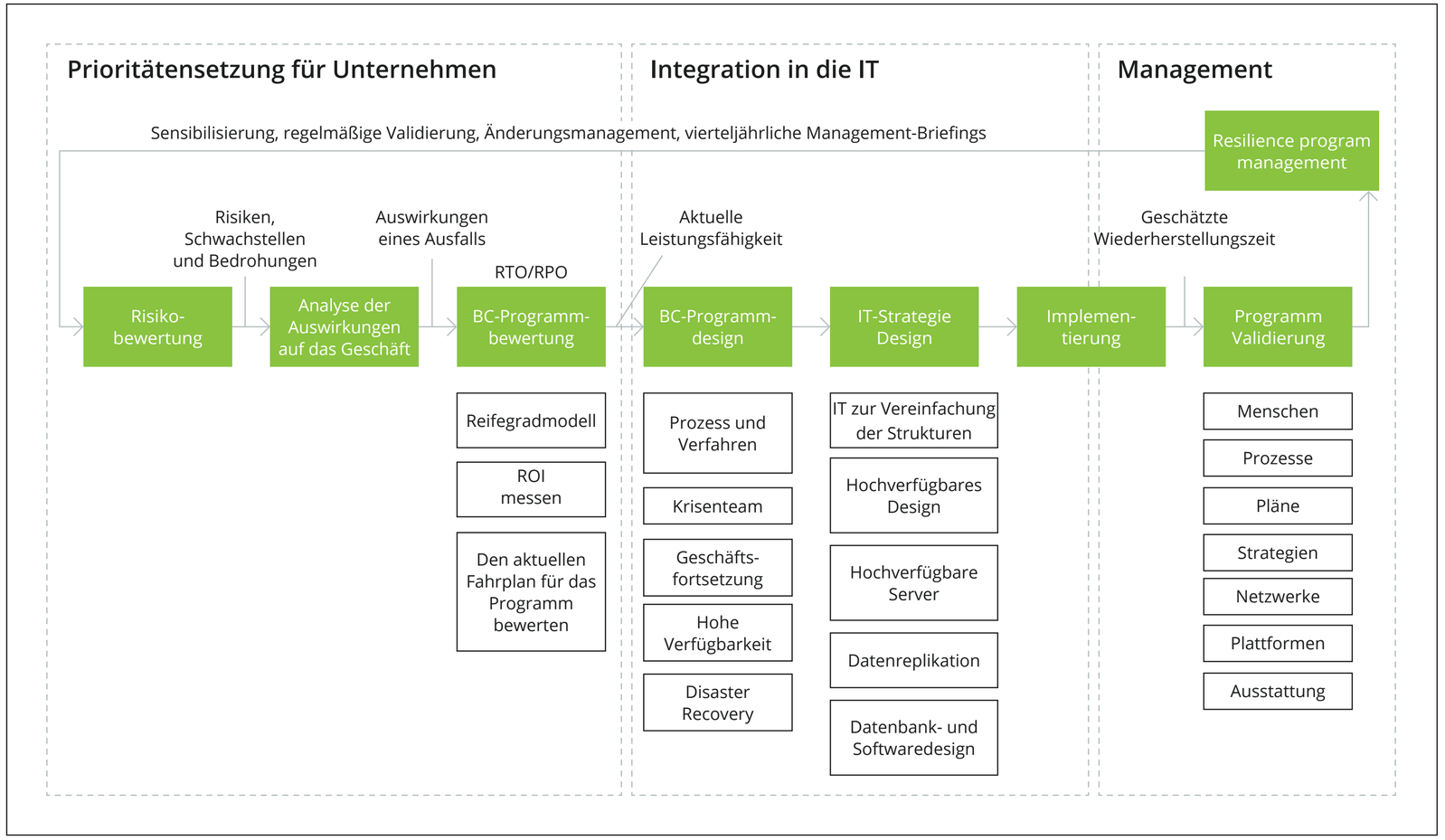
Business Continuity (BC) ist die Fähigkeit einer Organisation, den Betrieb nach einem Ereignis höherer Gewalt (z. B. einem Cyberangriff, einer Datenverletzung, einer Naturkatastrophe usw.) fortzusetzen.

Die weltweite Pandemie hat die Unternehmen auf eine harte Probe gestellt, aber auch gezeigt, dass viele ihre Bereitschaft für Störungen stark überschätzt hatten. Im März 2020 berichtete Gartner, dass 12% der Unternehmen sich als sehr gut auf Covid-19 vorbereitet sahen und 56% sich als einigermaßen vorbereitet einstuften[1]. Mitte August 2020 mussten jedoch 80% der Vorstandsmitglieder zugeben, dass ihre Unternehmen auf ein Negativereignis wie die globale Pandemie nicht gut vorbereitet waren[2].

Der Stimmungsumschwung ist kaum überraschend, wenn man sich die zugrunde liegenden Fakten ansieht. Weltweit verfügten nur 53% der Unternehmen über einen formellen Business Continuity-Plan (BCP), bevor Covid-19 einschlug[3].

Ein **Business Continuity-Plan (BCP)** ist eine formale Zusammenstellung von Maßnahmen, Praktiken und Verfahren, die die schnelle Wiederaufnahme wesentlicher Geschäftsfunktionen nach einer ungeplanten Unterbrechung gewährleisten sollen.

Business-Continuity-Planungsprozess



Quelle

[1] Gartner Business Continuity Survey Shows Just 12 Percent of Organizations Are Highly Prepared for Coronavirus. Gartner. Abruf am 15. August 2022

[2] Nearly 80% of Board Members Felt Unprepared for a Major Risk Event Like COVID-19: EY survey. EY. Abruf am 15. August 2022.

[3] A global survey of enterprises: Managing the business disruptions of COVID-19. International Labour Organization. Abruf am 15. August 2022.

Ein BCP hat drei Hauptziele:

1. Sicherstellung einer hohen Ressourcenverfügbarkeit

Trotz der Unterbrechung kann ein Unternehmen den Zugang zu geschäftskritischen Systemen, Anwendungen und Daten aufrechterhalten, um seinen Betrieb fortzusetzen. Der Plan enthält Abhilfemaßnahmen und alternative Betriebsverfahren für den Fall, dass es zu einem Ausfall der physischen Anlagen, der IT-Infrastruktur oder der Geschäftsprozesse kommt.

2. Aufrechterhaltung eines störungsfreien Betriebs

Dank der im Voraus geplanten Schritte, Checklisten und Verfahren zur Schadensbegrenzung kann das Unternehmen wie gewohnt weiterarbeiten.

3. Disaster Recovery

Im Falle einer technischen Störung kann das Unternehmen sein Rechenzentrum und seine Geschäftsanwendungen von einem alternativen Standort aus wiederherstellen, ohne dass es zu Datenverlusten kommt.

Bestandteile eines Business Continuity-Plans

- Operative Strategie
- Organisatorische Pläne
- Optimierung von Prozessen
- Anlagenmanagement
- Verfügbarkeit von Anwendungen und Daten
- BC- und DR-Technologien

infopulse

Was ist Disaster Recovery (DR)?_

Disaster Recovery (DR) ist ein standardisiertes Verfahren zur Wiederherstellung des Zugriffs auf die IT-Infrastruktur nach einem Störfall. Es umfasst sowohl betriebliche Maßnahmen als auch technische Methoden zur Wiederherstellung des normalen IT-Betriebs.

Die IT-Infrastruktur, welche heutzutage Hardware vor Ort, öffentliche und private Clouds, Unternehmensnetzwerke, Geschäftsanwendungen und Rechenzentren umfasst, ist zu einem entscheidenden Faktor für die Geschäftskontinuität geworden. Doch aufgrund der grundlegenden Rolle der Technologie für den Unternehmensbetrieb ist die IT-Infrastruktur auch eine Schwachstelle.

Menschliche Fehler, Stromausfälle oder raffinierte Cyberangriffe können Unternehmen völlig lahmlegen. Letztes Jahr fielen Facebook, Instagram und WhatsApp wegen eines Fehlers in der DNS-Konfiguration stundenlang gleichzeitig aus. Oder ein früherer Fall von Vodafone, die nach einer schlecht durchgeführten CRM-Systemmigration, die nicht rückgängig gemacht werden konnte, eine Geldstrafe in Höhe von 4,6 Millionen Pfund erhielten[4].

Katastrophen kleineren Ausmaßes ereignen sich jeden zweiten Tag. Allerdings verfügten nur 54% der Unternehmen über eine dokumentierte unternehmensweite Disaster Recovery-Strategie. Obwohl 73% der Befragten schon einmal einen technischen Ausfall erlebt haben[5]. Gleichzeitig haben Unternehmen, die bereits über DR-Pläne verfügen, immer noch kein volles Vertrauen in ihre derzeitige Einrichtung. IDC berichtet, dass nur 13% der Unternehmen volles Vertrauen in die Fähigkeit ihres Backup-Systems haben, Daten wiederherzustellen, und gerade mal 20% vollständig auf ihre DR-Lösung vertrauen[6].

Disaster-Recovery-Pläne (DRP) umfassen alle Praktiken, Richtlinien und Technologien, die ein Unternehmen einsetzt, um die schnelle Wiederherstellung von IT-Systemen, Services, Anwendungen und Daten zu gewährleisten.

Nur 54% der Unternehmen verfügen über eine dokumentierte unternehmensweite Disaster Recovery-Strategie

[4] Vodafone's £4.6m CRM fine - when IT projects attack. Diginomica. Abruf am 15. August 2022.

[5] Only 54% of organizations have a company-wide disaster recovery plan in place. Security Magazine. Abruf am 15. August 2022.

[6] The State of Data Protection and Disaster Recovery Readiness: 2021. IDC. Abruf am 15. August 2022.

Ein DRP hat drei Hauptziele:

1. Den Kernbetrieb so wenig wie möglich unterbrechen	2. Konsistente und schnelle Wiederherstellung von IT-Services	3. Begrenzung der Auswirkungen und Schäden von Störungen
DRP dokumentiert eine Reihe von Prozessen und technischen Aspekten zur Sicherstellung alternativer Betriebsmittel im Voraus.	dank dokumentierter Verfahren und vorimplementierter Ausfallsicherung für Dienste, Datenredundanz und Sicherungsmechanismen für Systeme.	durch einen schnellen Wiederherstellungsprozess, proaktives Risikomanagement und Strategien zur Minimierung der Auswirkungen.

Bestandteile eines Disaster Recovery-Plans

- Verfahren für IT-Backups und externe Speicherung
- Matrix zur Bewertung von Risiken und Auswirkungen
- Checkliste für Notfallmaßnahmen
- Startverfahren für die Wiederherstellung
- Rollen- und Verantwortungsmatrix
- DR-Plan-Schulungs- und Testverfahren

infopulse

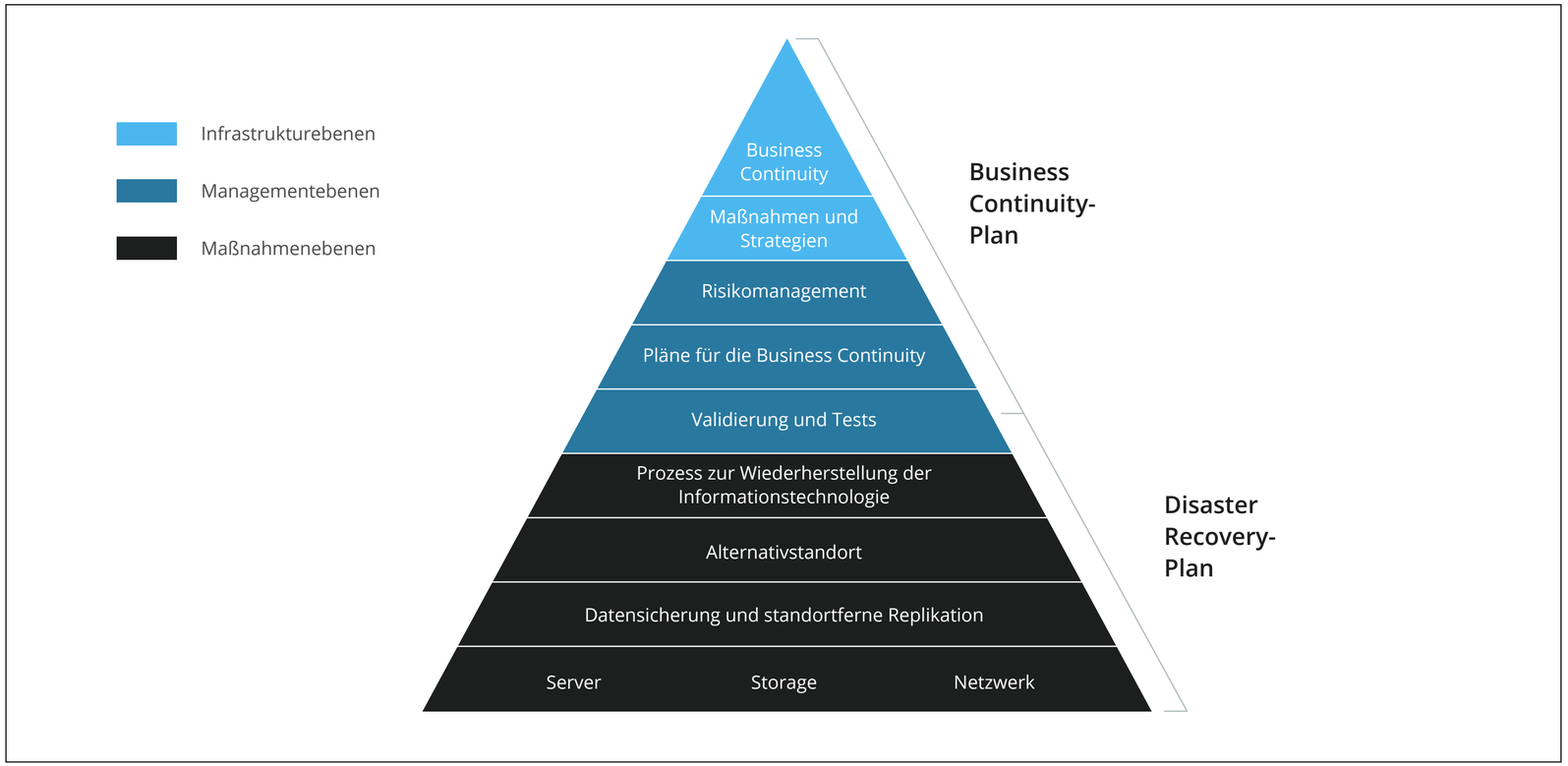
Was ist BCDR?

Disaster Recovery ist zu einem integralen Bestandteil der Business Continuity-Pläne geworden, da die Abhängigkeit der Menschen von Technologien ein noch nie dagewesenes Ausmaß erreicht hat.

Da ein kontinuierlicher Unternehmensbetrieb fast gleichbedeutend mit einer stabilen Leistung der IT-Infrastruktur geworden ist, wurden BC- und DR-Aktivitäten zu einem konsolidierten Business-Continuity-Disaster-Recovery-Plan (BCDR) zusammengefasst.

Als solcher umfasst er die technologischen, betrieblichen und grundsätzlichen Verfahren, die für eine effektive Rückkehr zum normalen Geschäftsbetrieb vorhanden sein müssen.

Business Continuity- und Disaster Recovery-Planung



> Der Grund, warum die ukrainische Regierung und viele kritische Infrastrukturen weiterhin sehr widerstandsfähig funktionieren, ist die Cloud-Infrastruktur. Wir konnten sogar mit der ukrainischen Regierung zusammenarbeiten, ihre Systeme migrieren und in gewisser Weise Kontinuität gewährleisten. Die Cloud wird also mehr und mehr allgegenwärtig. Ein weiteres gutes Beispiel [..] ist die NASA mit ihrer Internationalen Raumstation, sie müssen die Integrität der Anzüge sehr hoch halten. [...] Es darf keine Fehlfunktionen geben. Die Berechnungen finden jetzt in der Raumstation statt, weil die Latenzzeit zu hoch ist. Die Infrastruktur selbst breitet sich also dank 5G, dank des Weltraums, wirklich überall aus...

Satya Nadella

CEO von Microsoft

infopulse

Die Notwendigkeit des BCDR im Zeitalter von Digital-First und Post-COVID_

Seit Anfang 2022 wurden weltweit über 2,8 Milliarden Malware-Angriffe registriert

Die Pandemie hat das Vertrauen vieler Unternehmensleiter in ihre betriebliche Widerstandsfähigkeit gestärkt. In der Tat haben Unternehmen weltweit bewundernswerte Kreativität, Hartnäckigkeit und Ausdauer bewiesen, wenn es darum ging, den Geschäftsbetrieb aufrechtzuerhalten oder schnell auf neue Betriebsmodelle umzustellen.

Viele haben inzwischen die “temporären” Praktiken der “Remote-Arbeit” und des “Cloud-first-Denkens” zu einem festen Bestandteil ihrer Unternehmen gemacht. Nahezu jede Branche ist in Sachen Digitalisierung innerhalb weniger Monate um fünf Jahre vorangekommen[7].

Die Kehrseite der rasanten Digitalisierung (die viele Vorteile mit sich brachte) ist jedoch die zunehmende Abhängigkeit von unterbrechungsfreier Konnektivität, Datenübertragungen mit geringer Latenz und Datenredundanz. Die Raffinesse und die Verbreitung von Cyberangriffen stellen auch eine Belastung für den Schutz der Unternehmen dar. **Seit Anfang 2022 wurden weltweit über 2,8 Milliarden Malware-Angriffe registriert** - und die Ransomware-Raten in Europa stiegen um 63%[8].

Dennoch sind menschliches Versagen und Hardwarefehler die Gründe für fast 55% der Datenverluste[9]. Im Gegensatz zur Cybersecurity (die oft ein separater Verantwortungsbereich ist, der von SOC-Teams abgedeckt wird), werden diese beiden Fälle von den Unternehmen oft unterschätzt.

[7] Global surveys of consumer sentiment during the coronavirus crisis. McKinsey. Abruf am 15. August 2022.

[8] 2022 SonicWall Cyber Threat Report. SonicWall. Abruf am 15. August 2022.

[9] Data Health Check 2021. Databarracks. Abruf am 15. August 2022.

Im April 2022 kam es bei Atlassian zu einem zweiwöchigen Ausfall, von dem über 775 Kunden betroffen waren, die vollständig von ihren Konten ausgesperrt wurden. Die nachträgliche Analyse ergab, dass die Techniker im Rahmen der geplanten Wartung ein Skript zum Entfernen von Altdaten ausführten. Ein Fehler im Skript führte jedoch zu einer umfassenderen Datenlöschung, die ohne die umfangreichen Sicherungs- und Wiederherstellungssysteme von Atlassian schlimmere Folgen hätte haben können. Es gingen keine Kundendaten verloren und alle Services wurden normal wiederhergestellt[10].

Das zunehmende Verkehrsaufkommen belastet auch die alternde lokale Infrastruktur stärker. Die Häufigkeit von Serverausfällen stieg von 5% im ersten Jahr auf 18% im siebten Jahr[11]. Viele Unternehmen haben es jedoch nicht eilig, ihre alte Infrastruktur zu ersetzen oder aufzurüsten - ein Faktor, der auch die Betriebsrisiken erhöht.

> Die **Aufgabe von BCDR** besteht darin, die Chancen und Auswirkungen möglicher Unterbrechungen des Geschäftsbetriebs zu minimieren, unabhängig davon, ob diese technologischer, menschlicher oder physischer Natur sind.

[10] Post-Incident Review on the Atlassian April 2022 outage. Atlassian. Abruf am 15. August 2022.

[11] Frequency of server failure based on the age of the server. Statista. Abruf am 15. August 2022.

infopulse

BCDR-Geschäftsszenarien_

Durch die Implementierung von BCDR-Praktiken kann sich ein Unternehmen nach einem Zwischenfall schnell wieder erholen, das Risiko von Datenverlusten, Rufschädigung und Geldstrafen für die Nicht-Einhaltung von Vorschriften minimieren und auch in unsicheren Zeiten eine hohe betriebliche Widerstandsfähigkeit aufrechterhalten.

In diesem Abschnitt werden verschiedene Geschäftsszenarien für die Implementierung von BCDR-Technologien für kleine, mittelgroße und große Unternehmen in verschiedenen Branchen diskutiert.

Kleine und mittlere Unternehmen (KMUs)

Statistisch gesehen haben kleine und mittlere Unternehmen eine eher laxe Einstellung zu BCDR: 43% geben zu, dass sie keinen aktuellen BCP-Plan haben und auch nicht beabsichtigen, einen zu erstellen[12]. In den meisten Fällen erweist sich dies als ein großes Versäumnis.

Im Durchschnitt sind die Mitarbeitenden eines kleinen Unternehmens (weniger als 100 Personen) 350% mehr Social-Engineering-Angriffen ausgesetzt als die Mitarbeitenden eines größeren Unternehmens. **Infolgedessen wurde bei einem von fünf Unternehmen im vergangenen Jahr mindestens ein Konto kompromittiert[13].** Unabhängig davon gaben 56% der Beschäftigten zu, dass sie versehentlich Cloud-Datensätze gelöscht haben, wobei 43% von ihnen diese Tatsache ihren Vorgesetzten gegenüber nicht offenlegten[14].

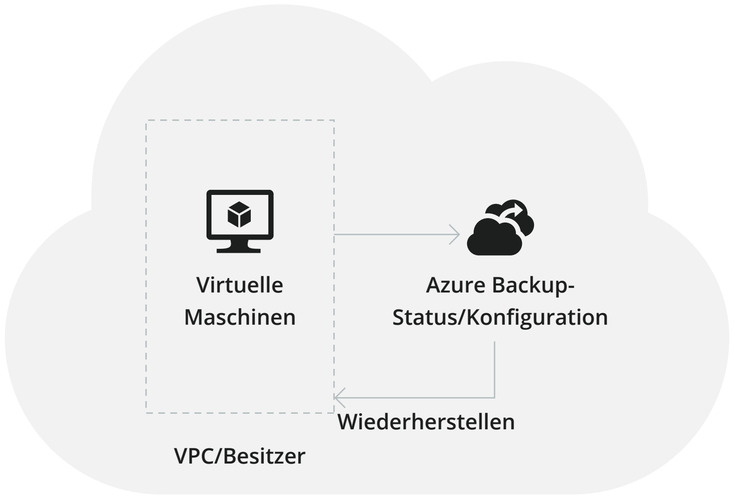
Für kleine und mittlere Unternehmen kann selbst die einfachste BCDR-Architektur als “Sicherheitsnetz” fungieren, das sie im Falle eines negativen Ereignisses vor erheblichen finanziellen und Imageverlusten schützt. Angesichts der durchschnittlichen Kosten einer Datenschutzverletzung für KMUs in Höhe von 108.000 US-Dollar zahlen sich Investitionen in BCDR um ein Vielfaches aus - und generieren auch später noch einen ROI.

[12] Data Health Check 2021. Databarracks. Abruf am 15. August 2022.
[13] Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies. Forbers. Abruf am 15. August 2022.
[14] Report: 56% of workers admit they’ve accidentally deleted cloud data. VentureBeat. Abruf am 15. August 2022.
[15] Security for your small or medium-sized business. Microsoft. Abruf am 15. August 2022.

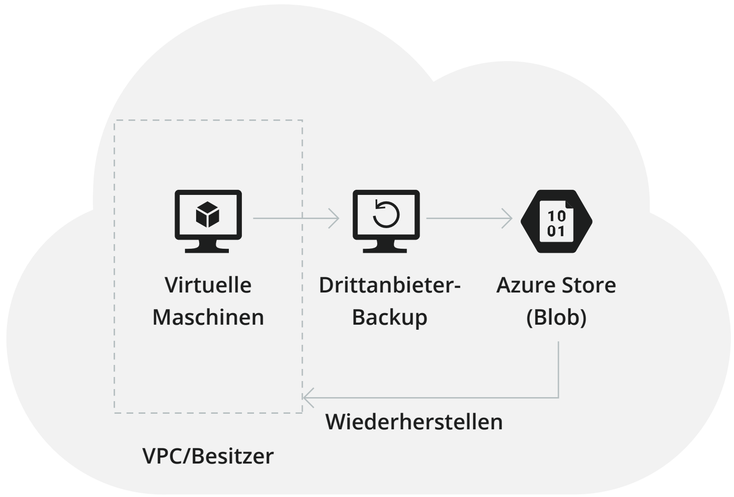
Szenario 1. Erstellung eines Cloud-Backups für wichtige Dienste_

Der ungestörte Zugang zu wichtigen Geschäftssystemen - von Anwendungen für den digitalen Arbeitsplatz bis hin zu Dokumentenverwaltungssystemen - ist für den normalen Betrieb unerlässlich. Lösungen für Disaster Recovery as a Service (DRaaS) wie Azure Backup ermöglichen es Ihnen, Anwendungen und Daten asynchron in der Cloud zu sichern. Im Falle eines Unfalls können Sie den Zugang zu wichtigen Systemen innerhalb weniger Stunden, wenn nicht sogar Minuten, wiederherstellen.

Hinweis: *In diesem Szenario sichern Sie nur bestimmte Geschäftsanwendungen und Daten, nicht aber Ihre gesamte IT-Infrastruktur. Das bedeutet, dass Sie im Falle eines großflächigen IT-Ausfalls oder eines Zwischenfalls in Ihrer physischen Anlage möglicherweise keinen Zugriff auf alle Ihre Ressourcen haben.*



Option 1 - Native Azure-Backup verwenden



Option 2 - Backup-Anwendungen von Drittanbietern verwenden

Architekturkomponenten

Azure Backup ist ein zentraler Daten-Backup-Service und eine Sammlung von unterstützenden Diensten zur Automatisierung von Backups von Infrastruktur, Datenbanken und Speicher-Workloads.

Damit können Sie eine umfassende Sammlung von Strategien für automatische Backups und Datensicherheit erstellen.

Unterstützt:

- Azure Virtual Machines
- Lokale Server
- SQL-Server
- SAP HANA auf Azure Virtual Machines
- Azure Files
- Azure Database für PostgreSQL.

Drittanbieter-Service + Azure Blob Storage. Alternativ können Sie auch eine Backup-Lösung eines Drittanbieters (z. B. Commvault) verwenden, um Datenbank- und Anwendungs-Backups in Azure Blob Storage einzurichten. Azure Blob Storage ist eine skalierbare Cloud-Datenplattform, die Multi-Protokoll-Zugriff, Geo-Replikation und erstklassige Sicherheit bietet. Blob Storage ist nach Bedarf skalierbar und kann als Hot-Backup-Site (für sofortige Datenverfügbarkeit) und als Cold-Site für weniger wichtige Anwendungen und Archivdaten-Backups eingesetzt werden.

Szenario 2. Einführung der empfohlenen DR-Infrastruktur_

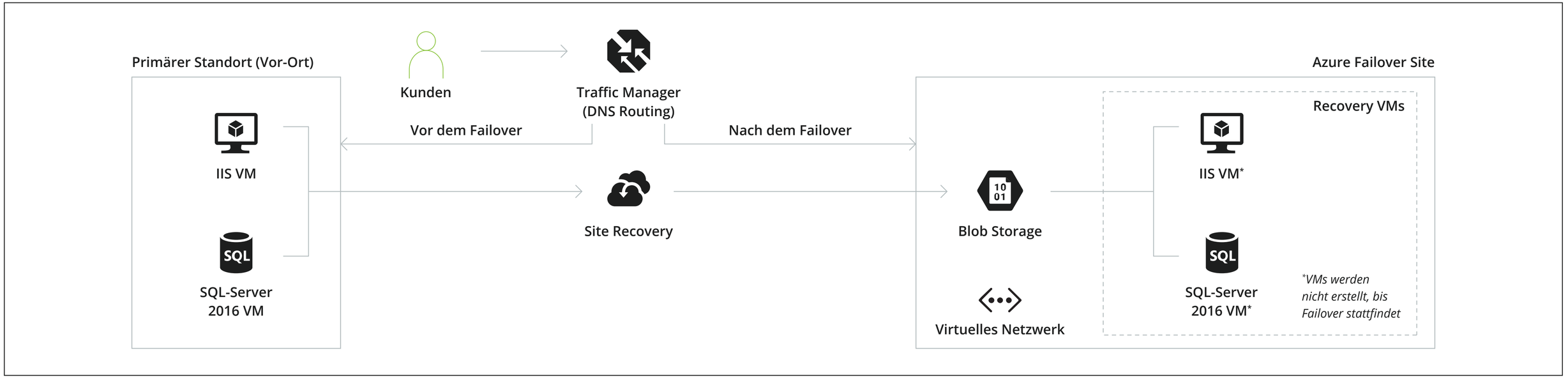
Für kritischere Geschäftsdaten und Anwendungen möchten Sie möglicherweise eine vollständige Systemredundanz erreichen (d. h. bis zu 99,999% Betriebszeit in einem bestimmten Zeitraum). Als Agrarhandelskonzern, zum Beispiel, benötigen möglicherweise hochentwickelte IT-Systeme für den gesamten Warenhandel und die Buchhaltung, da Sie sonst Gefahr laufen, unzureichende Entscheidungen zu treffen.

Ebenso ist die ständige Verfügbarkeit von IT-Systemen eine Selbstverständlichkeit für Anwendungen im Gesundheitswesen, AdTech-Lösungen oder Video-Streaming-Services, da die Endbenutzer dies standardmäßig erwarten. In solchen Fällen ist die Implementierung von Failover-Services der optimale Weg vorwärts.

> **Failover** ist ein Sicherungsvorgang, der automatisch auf eine Standby-Datenbank, einen Standby-Server oder ein Standby-Netzwerk umschaltet, wenn die primäre Datenbank ausfällt oder repariert werden muss.

Die Failover-Implementierung hilft Ihnen, Ihre Datenbanken während geplanter Wartungsarbeiten oder eines Systemausfalls zu schützen. Wenn beispielsweise ein Hardwarefehler im Hauptserver vor Ort auftritt, kann ein Cloud-Service sofort einspringen. Die automatisierte Umschaltung ermöglicht Ihnen auch die Durchführung geplanter Wartungsarbeiten ohne Beeinträchtigung der Anwendungsleistung und bietet einen wirksamen Schutz vor Cyberrisiken.

Azure bietet eine Vielzahl von Tools zur Implementierung verschiedener Failover-Szenarien für Cloud-, Hybrid- und Vor-Ort-Architekturen.



Architekturkomponenten

Der **Traffic Manager** ist eine DNS-basierte Lastenausgleichslösung für die Weiterleitung des Datenverkehrs zwischen verschiedenen Services. In einem DR-Szenario leitet der Traffic Manager eingehende DNS-Anfragen vom primären Standort innerhalb weniger Sekunden an den sekundären (Failover-)Standort um. Sie können entweder ein manuelles Failover implementieren (d. h., wenn ein technisches Team beschließt, Ihre Failover-Site zu aktivieren und dann den Datenverkehr umzuleiten) oder ein automatisches Failover programmieren.

Manuelles Failover ist ein häufigeres Szenario bei kleinen und mittleren Unternehmen, da es geringere Kosten für die DR-Infrastruktur verursacht. In diesem Fall halten Sie Ihren sekundären Standort im Cold-Standby-Modus, d. h. Ihre Infrastruktur ist erst dann aktiv, wenn ein Failover erforderlich ist. Dann zahlen Sie für die in Auftrag gegebenen Speicher- und Rechenressourcen nur dann, wenn der zweite Standort aktiv ist.

Für Systeme, die eine minimale Latenzzeit und hohe Verfügbarkeit erfordern (z. B. vernetzte Anwendungen im Gesundheitswesen oder im Finanzbereich), kann eine automatische Ausfallsicherung jedoch empfehlenswert sein.

In diesem Fall sendet Traffic Manager den gesamten Datenverkehr standardmäßig an den primären Standort, aber wenn die Leistung des Endpunkts nachlässt, schaltet Traffic Manager den Datenverkehr automatisch auf einen anderen Endpunkt um. Dieses Szenario erfordert jedoch einen Warm-Standby-Standort, d. h. der Standby-Standort verfügt über maximale Konfigurationen und die automatische Skalierung der Instanzen ist aktiviert. Der Unterhalt eines solchen Standorts ist zwar teurer, doch die Vorteile liegen in einer nahezu zeitnahen Wiederherstellungspunkt- (Recovery Point Objective, RPO) und Wiederherstellungszeit-Zielsetzung (Recovery Time Objective, RTO).

Azure Site Recovery ist ein Microsoft-eigener Disaster Recovery as a Service (DRaaS). Als solcher bietet er eine umfassende Sammlung von DR-Lösungen für optimierte Replikation, Failover und Systemwiederherstellung.

Der Site Recovery Service repliziert physische und virtuelle Maschinen-Workloads vom primären auf einen sekundären Standort. Tritt ein Zwischenfall ein, werden alle Arbeitslasten an den vorgesehenen Standort verlagert und Sie können von dort aus auf alle Systeme zugreifen. Sobald der primäre Standort wieder in Betrieb ist, wird der Verkehr dorthin umgeleitet.

Unterstützt:

- Azure-VMs-Replikation zwischen Azure-Regionen
- Replikation von lokalen VMs, Azure Stack VMs und physischen Servern in die Cloud.

Der **Azure Virtual Network Service** hilft bei der Konfiguration einer privaten Netzwerkinfrastruktur in der Cloud als Ihre Failover-Standort.

Der **Blob Storage** enthält die Replikat-Images aller Maschinen, die durch Site Recovery geschützt sind. Wenn ein Ausfallereignis eintritt, initiiert Site Recovery die Erzeugung einer Failover-Site aus den verfügbaren Snapshots.

Konzerne_

Konzerne haben größere Datenbestände und mehr kritische Anwendungen zu speichern und zu sichern. Die Messlatte für die Verfügbarkeit von IT-Systemen liegt ebenfalls höher, da selbst kurzfristige Ausfälle und Service-Latenzzeiten zu Verlusten in Millionenhöhe führen können.

Im Jahr 2018 erlebte Amazon einen der schlimmsten Serviceausfälle während des Prime Day. Die Server des Unternehmens konnten die Spitzenlast des Datenverkehrs nicht bewältigen und lösten eine Kaskade von Ausfällen aus. Berichten zufolge verlor Amazon dadurch 1,2 Millionen Dollar pro Minute an Umsatz[16].

Störungen können auch durch Ereignisse vor Ort verursacht werden, von Naturkatastrophen bis hin zu bösartigen Angriffen. Da viele Unternehmen weiterhin Rechenzentren vor Ort unterhalten, sollten diese Faktoren nicht außer Acht gelassen werden. Im Jahr 2011 kam es bei Vodafone zu einer größeren Serviceunterbrechung, nachdem Kriminelle in das Rechenzentrum in Basingstoke eingebrochen waren und dort Geräte im Wert von 4 Millionen Dollar gestohlen hatten[17].

Um sowohl auf physische als auch auf digitale Bedrohungen vorbereitet zu sein, sollten die BCDR-Pläne von Unternehmen ein sekundäres Cloud-basiertes Rechenzentrum vorsehen.

[16] What Amazon lost (and made) on Amazon Prime Day. TechCrunch. Abruf am 15. August 2022.

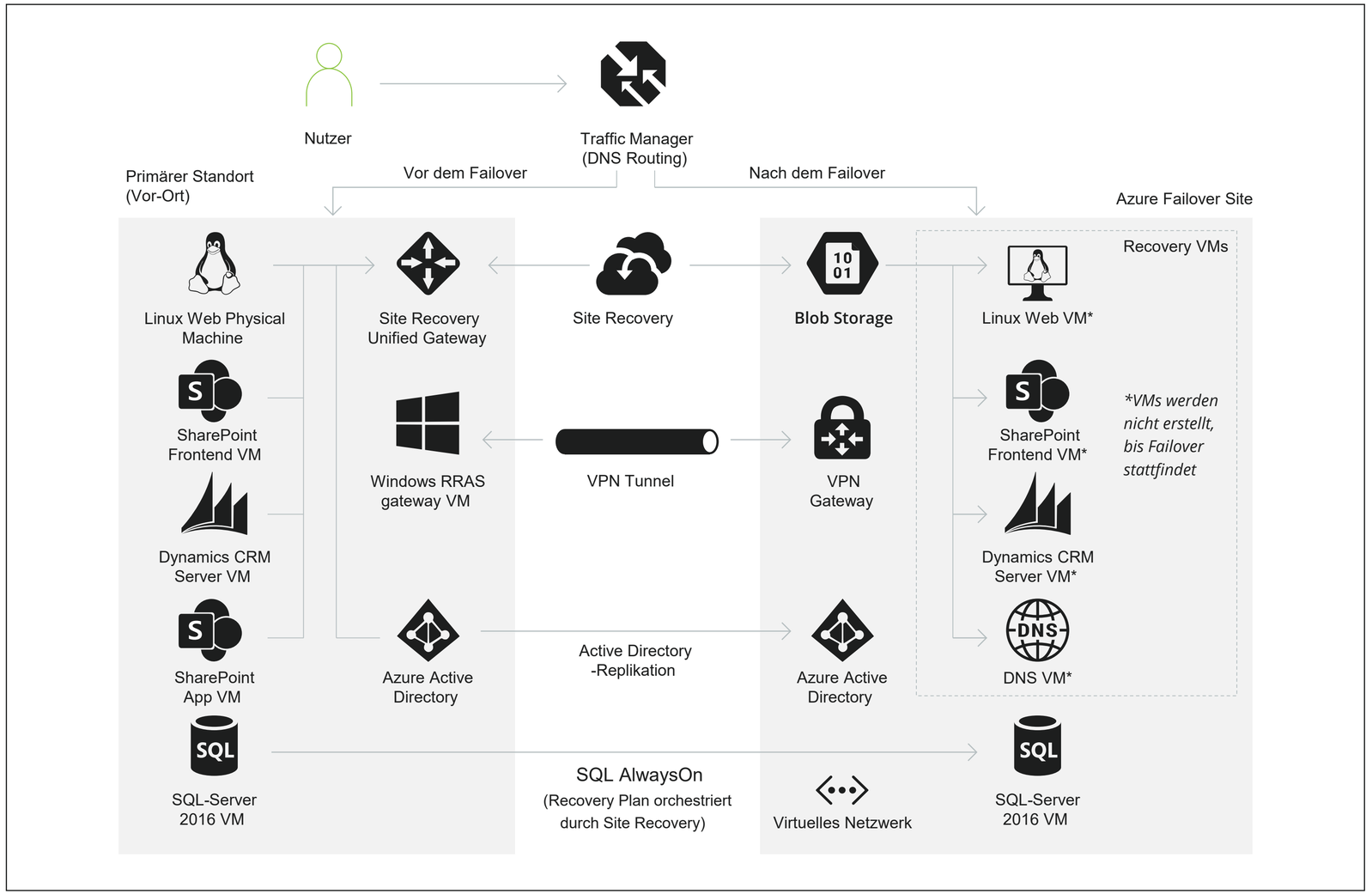
[17] Data centre security: It's time to get physical. Teledata. Abruf am 15. August 2022.

Szenario: Einrichtung eines sekundären Rechenzentrums_

Die Einrichtung eines sekundären Datenzentrums hilft sowohl bei der Wiederherstellung als auch bei der Vermeidung von Katastrophen (entscheidend für die Geschäftskontinuität). Cloud-basierte DR-Standorte in einer zweiten Verfügbarkeitszone oder bei einem zweiten Cloud-Anbieter (Multi-Cloud) dienen nicht nur als Failover-Standort für den Fall, dass es zu einem Störfall in der Hauptstelle kommt, sondern können auch die kritische Geschäftskontinuität bei regionalen Ausfällen sicherstellen.

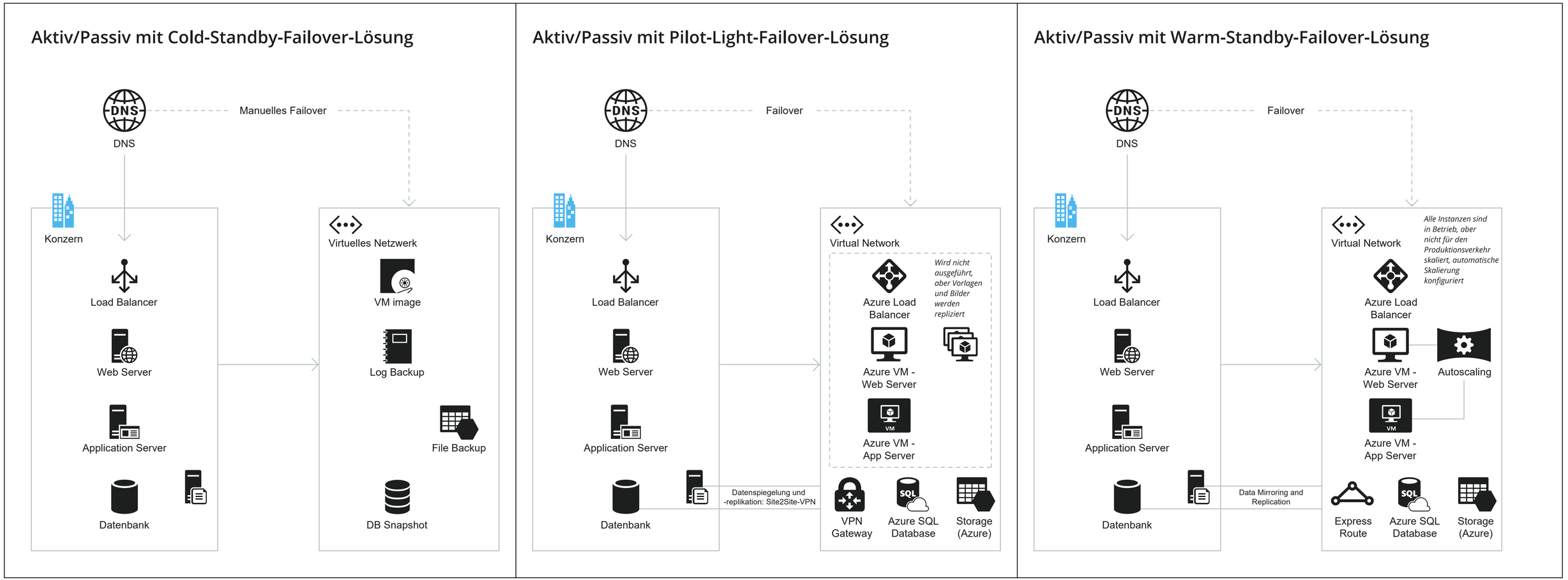
Herkömmliche DR-Standorte (z. B. NAS-Speicher) erfordern meist eine manuelle Aktivierung, Datenreplikation und Migration der Benutzer. Cloud-basierte Lösungen ermöglichen eine automatisierte, durchgängige Service-Wiederherstellung, deren Aktivierung oft nur Minuten dauert. Cloud-Lösungen bieten außerdem unbegrenzte Kapazitäten, d. h. Sie können die Größe Ihres Rechenzentrums schrittweise erweitern, ohne langwierige Hardware-Beschaffungszyklen oder überhöhte Kosten für bestehende ungenutzte Kapazitäten in Kauf nehmen zu müssen.

Die Einrichtung eines sekundären Rechenzentrums mit Failover auf die Azure-Infrastruktur ist eine kluge Entscheidung für Unternehmen, die kritische Daten hosten, sowie für Unternehmen, die Wert auf die Einhaltung hoher Endkunden-SLAs legen.



Architekturkomponenten

Der **Traffic Manager** leitet den DNS-Verkehr, auf der Grundlage der kodifizierten Richtlinien, von einem Standort zum anderen weiter. Je nach Bedarf können Sie manuelles oder automatisches Failover für verschiedene Disaster-Recovery-Szenarien implementieren.



Azure Site Recovery DRaaS orchestriert den Replikationsprozess und verwaltet die Konfiguration der Failback-Verfahren.

Vorteile von Site Recovery für Unternehmen:

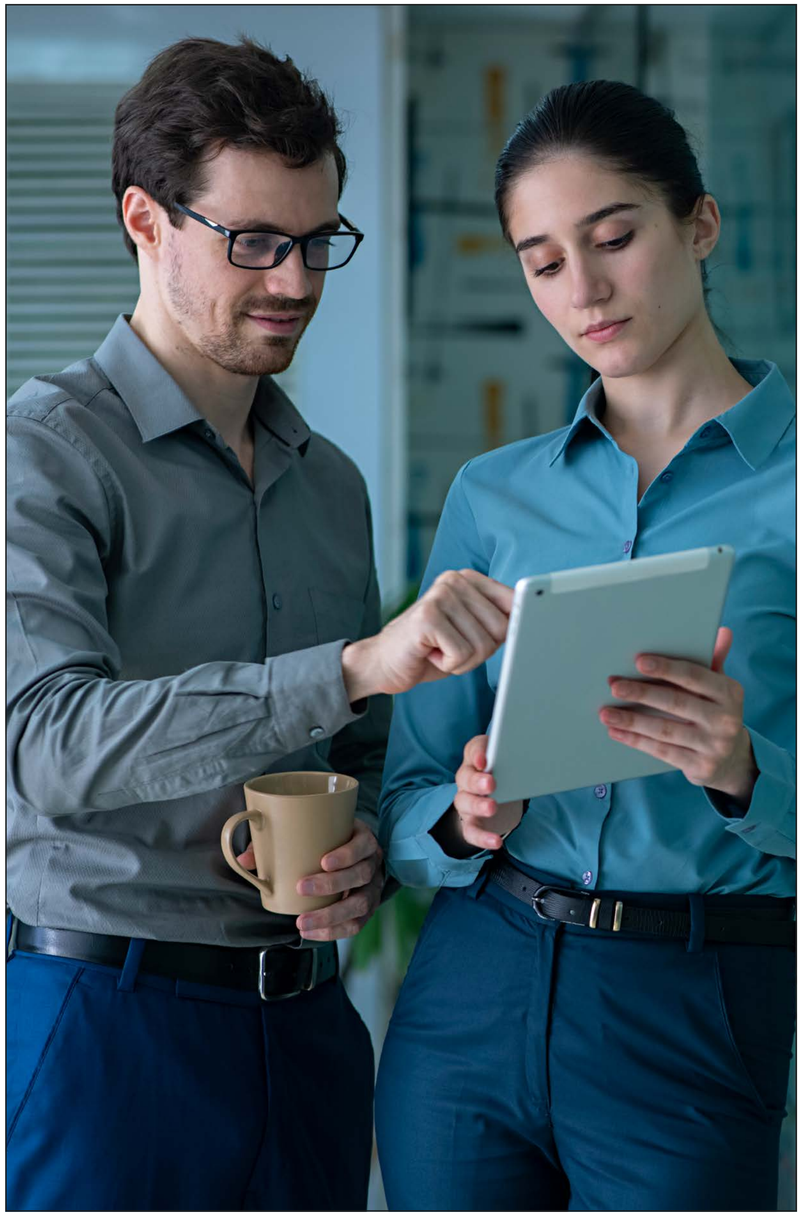
- Die Daten werden automatisch in Azure Elastic Storage gespeichert. Azure VMs werden auf der Grundlage der replizierten Daten erstellt.
- Bietet eine kontinuierliche Replikation für Azure VMs und VMware VMs mit einer Replikationsfrequenz von nur 30 Sekunden.
- Erstellen Sie anwendungskonsistente Snapshots, die Festplattendaten, alle Daten im Speicher und alle laufenden Transaktionen für Anwendungen erfassen.
- Erstellen Sie individuelle Wiederherstellungspläne und Failover-Sequenzen für mehrschichtige Anwendungen, die auf mehreren virtuellen Maschinen ausgeführt werden.
- Integrieren Sie andere BCDR-Technologien, um ein breiteres Spektrum an Anwendungen, Datenbanken und Arbeitslasten abzudecken.

Alle von Site Recovery erstellten Replika-Bilder werden im **Blob Storage** gespeichert - einer skalierbaren, sicheren Cloud-Speicherlösung mit reservierten und auf Abruf verfügbaren Instanzen.

Um eine angemessene Sicherheits- und Zugriffsverwaltung zu gewährleisten, werden die lokalen **Azure Active Directory**-Konfigurationen automatisch auf den Failover-Standort repliziert. Auf diese Weise können die Benutzer die richtigen Berechtigungen und Zugänge zu allen Cloud-Anwendungen erhalten.

Der **VPN Gateway-Service** hilft bei der Einrichtung eines privaten Kommunikationstunnels zwischen den Standorten vor Ort und der Cloud für die Datenreplikation und nachfolgende Zugriffe. Sie können einen Point-to-Site-VPN-Zugang von überall aus mit einer Betriebszeit von 99,9% einrichten. Die Konnektivität wird durch die Protokolle Internet Protocol Security (IPsec) und Internet Key Exchange (IKE) gesichert.

Die **Azure Virtual Network**-Lösung erleichtert die Einrichtung einer privaten Netzwerkinfrastruktur in der Cloud für Ihren Failover-Standort. Auf diese Weise können Sie Ihre Website zusätzlich mit VPNs oder dem Azure ExpressRoute-Service absichern. Sie können auch isolierte und hochsichere Umgebungen für Ihre wichtigsten Datenbanken mithilfe von Firewalls und Netzwerksicherheitsgruppen (Network Security Groups, NSGs) einrichten. Aktivieren Sie dann den Zugriff der Benutzer auf diese Dateien mit entsprechender Berechtigung.



infopulse

BCDR bei Infopulse_

Im Jahr 2016 begann Infopulse mit der Vorbereitung und Einführung eines unternehmensweiten BCDR-Plans. Im Januar 2022 erreichten wir bei allen 46 Produkt-IT-Systemen ein Testergebnis von 100%.

Im Jahr 2019 konnten wir erfolgreich ein zweites Rechenzentrum in der EU einrichten. Aufgrund der geopolitischen Ereignisse in der Ukraine haben wir uns jedoch entschlossen, ihn in einen primären Standort umzuwandeln und den Großteil des Betriebs erfolgreich in die Cloud zu verlagern. Im Rahmen dieser massiven Umstellung haben wir unser E-Mail-System vollständig auf Exchange Online migriert, die internen SharePoint-Lösungen (das Intranet und die Abteilungsseiten von Infopulse) auf SharePoint Online migriert und RMS (Rights Management Center) neben anderen Teilprojekten auf Azure Information Protection übertragen.

Dank der Proaktivität des BCP-Teams, zahlreicher Maßnahmen, die in den letzten sechs Jahren ergriffen wurden, und der Umsetzung bewährter Praktiken im Bereich der Geschäftskontinuität konnten unsere Ingenieure alle möglichen Ad-hoc-Szenarien bewältigen, die viele Unternehmen während der ersten beiden Kriegsmonate (Februar-März 2022) in der Ukraine erschütterten. Infopulse verfügt jetzt über eine hybride Infrastruktur, die wie ein Uhrwerk läuft.

infopulse

So integrieren Sie die Sicherheit in Ihre BCDR-Planung_

78%

der Führungskräfte in Unternehmen[18]

Geben zu, nicht zu wissen, wie oder wann sich ein Cybervorfall auf ihr Unternehmen auswirken wird.

44%

der Führungskräfte[19]

Sagen, dass sie durch die zunehmende Nutzung von Partnern und Zulieferern erheblichen Risiken im Bereich der Cybersecurity ausgesetzt sind.

270

cyber attacks[20]

Geschehen pro Unternehmen pro Jahr. Davon sind 29 erfolgreich. Das ist ein Anstieg von 31% im Vergleich zu 2020.

Unternehmen müssen heute ein breiteres Verteidigungsperimeter einrichten, das Cloud-, lokale und hybride Infrastrukturen abdeckt. Dies erweist sich als die nächste Sicherheitsherausforderung.

Vorfälle im Bereich der Cybersecurity, die jetzt immer häufiger auftreten, stellen eine weitere Reihe von Störungen dar, die in BCDR-Plänen berücksichtigt werden sollten. Nahezu jede Art von Unternehmen scheint heute ein attraktives Ziel für Cyberkriminelle zu sein.

Der Grund dafür ist einfach: Daten. Das gesamte globale Datenvolumen betrug im Jahr 2020 “nur” 64 Zetabyte und stieg auf 97 Zetabyte im Jahr 2022[21]. Dazu gehören Finanzdaten, personenbezogene Daten der Bürger (Private Identifiable Information, PII), medizinische Daten und Anmeldedaten für Websites - alles wertvolle Ziele für Cyberangreifer.

Wenn Hacker in den Besitz von Unternehmensdaten gelangen, können sie entweder die Kontrolle über zentrale Geschäftssysteme erlangen (wie im Fall des SolarWinds-Hacks) oder sensible Geschäftsdaten stehlen/verschlüsseln, um Ransomware zu fordern (wie im Fall von Cognizant im Jahr 2020). In jedem Fall entsteht dem betroffenen Unternehmen nicht nur ein direkter Schaden in Form von Umsatzeinbußen und Bußgeldern, sondern es erleidet auch einen erheblichen Imageschaden. Die britische Telefongesellschaft TalkTalk hat durch einen schwerwiegenden Datenschutzverstoß über 280.000 Kunden und einen Wert von fast 1,4 Milliarden Dollar verloren[22].

Ein umfassender BCDR-Plan muss daher Cyber-Risiken berücksichtigen und Maßnahmen zur effektiven Bewältigung von Cyber-Ereignissen und - was noch wichtiger ist - zu deren Vermeidung enthalten.

[18] State of Cybersecurity Resilience 2021. Accenture. Abruf am 15. August 2022.

[19] Many security executives say they’re unprepared for the threats that lie ahead. TechRepublic. Abruf am 15. August 2022.

[20] Businesses Suffered 50% More Cyberattack Attempts per Week in 2021. DarkReading. Abruf am 15. August 2022.

[21] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. Statista. Abruf am 15. August 2022.

[22] 250,000 People Leave Telco TalkTalk After Hack in October 2015. Business Insider. Abruf am 15. August 2022.

Disaster Recovery: Minimierung von Ausfallzeiten aufgrund eines Cybersecurity-Vorfalls_

Die Planung der Disaster Recovery beginnt mit einer Risikokartierung und einer Analyse der Auswirkungen. Ihr Ziel ist es, zwei Hauptmetriken aus allen Geschäftssystemen zu ermitteln:

- **Recovery Time Objective (RTO)** - maximal akzeptable Ausfallzeit für Ihre Anwendung.
- **Recovery Point Objective (RPO)** - maximaler Zeitraum, in dem Daten aus Ihrer Anwendung verloren gehen können.

Für einen Zahlungsabwickler beispielsweise kann ein RPO von mehreren Minuten zu erheblichen Problemen bei der Einhaltung der Vorschriften führen. Im Gegensatz dazu kann ein RPO von mehreren Stunden für einige archivierte Datenbanken in Ordnung sein.

Auf der Grundlage der oben genannten Metriken sollten Sie eine optimale Datensicherungsstrategie für verschiedene Systeme entwickeln. Wie bereits erwähnt, bedeutet dies die Implementierung von Cloud-Backups der verschiedenen Dienste und Daten. Implementieren Sie dann geeignete Mechanismen zur Ausfallsicherung von Services an sekundären Standorten. Nebenstandorte sollten genauso gesichert und penetrationsgetestet werden wie Ihre Hauptstandorte, da Eindringlinge sie aufspüren und einen zweiten Angriffsvektor nutzen können. Stellen Sie sicher, dass einheitliche Sicherheitsrichtlinien auf alle Standorte angewendet werden, indem Sie Referenzvorlagen erstellen und anhand dieser Vorlagen testen.

Größere Unternehmen werden auch geografische Redundanz anstreben (d. h. zweite Standorte in verschiedenen Regionen einrichten, um sich vor lokalen Katastrophen zu schützen). Überprüfen Sie dann routinemäßig die Ausführung Ihres Backup-Plans. Stellen Sie sicher, dass alle Backups wie geplant durchgeführt werden, sich in einem brauchbaren Zustand befinden, vollständig gesichert und für ein Failover bereit sind.

Ihr nächster Schritt ist die Einführung einer intelligenten Prozessautomatisierung. Wenn ein Cybervorfall eintritt, ist eine schnelle Reaktion erforderlich. Dennoch scheint alles Priorität zu haben und Ihre Mitarbeiter müssen schnell handeln, was Raum für Fehler lässt. Um Fehler und Verzögerungen zu minimieren, sollten Sie mit Lösungen wie Azure Site Recovery ein gewisses Maß an Automatisierung in DR-Workflows einführen.

Business Continuity: Sicherstellung eines unterbrechungsfreien Geschäftsbetriebs_

Sobald die Infrastruktur wiederhergestellt (oder vor Cyberangriffen geschützt) wurde, besteht Ihr nächstes Ziel darin, die Geschäftskontinuität zu gewährleisten.

Während die vorherigen Maßnahmen auf die *Wiederherstellung* ausgerichtet waren, konzentriert sich die Planung der Geschäftskontinuität mehr auf die Prävention. In diesem Sinne ist der BCP eng mit der allgemeinen Cybersecurity-Leistung Ihres Unternehmens verbunden. Schließlich können Sie den normalen Betrieb nicht aufrechterhalten, wenn Ihre Unternehmenssysteme manipuliert wurden, Daten missbraucht oder vertrauliche Informationen an unbefugte Dritte weitergegeben wurden.

Daher bewerten wir im Rahmen von BCDR stets die aktuelle Sicherheitslage unserer Kunden und schlagen zusätzliche Cybersecurity-Lösungen vor, um bestehende Lücken in der Identitätsverwaltung, den Zugangskontrollen, dem Schutz von Vermögenswerten, der Überwachung von Bedrohungen und der Bedrohungsabwehr zu schließen.

Im Rahmen der BCP sollten Sie über die notwendigen Lösungen verfügen, um die Auswirkungen gängiger Cybersecurity-Ereignisse auf Ihren Betrieb zu minimieren (oder ganz zu eliminieren). Dazu gehört auch der Schutz Ihrer Anwendungen vor häufigen DDoS-Angriffen. Zum Vergleich: Das Volumen der DDoS-Angriffe auf der HTTP-Ebene stieg im Vergleich zum Vorjahr um 164%[23].

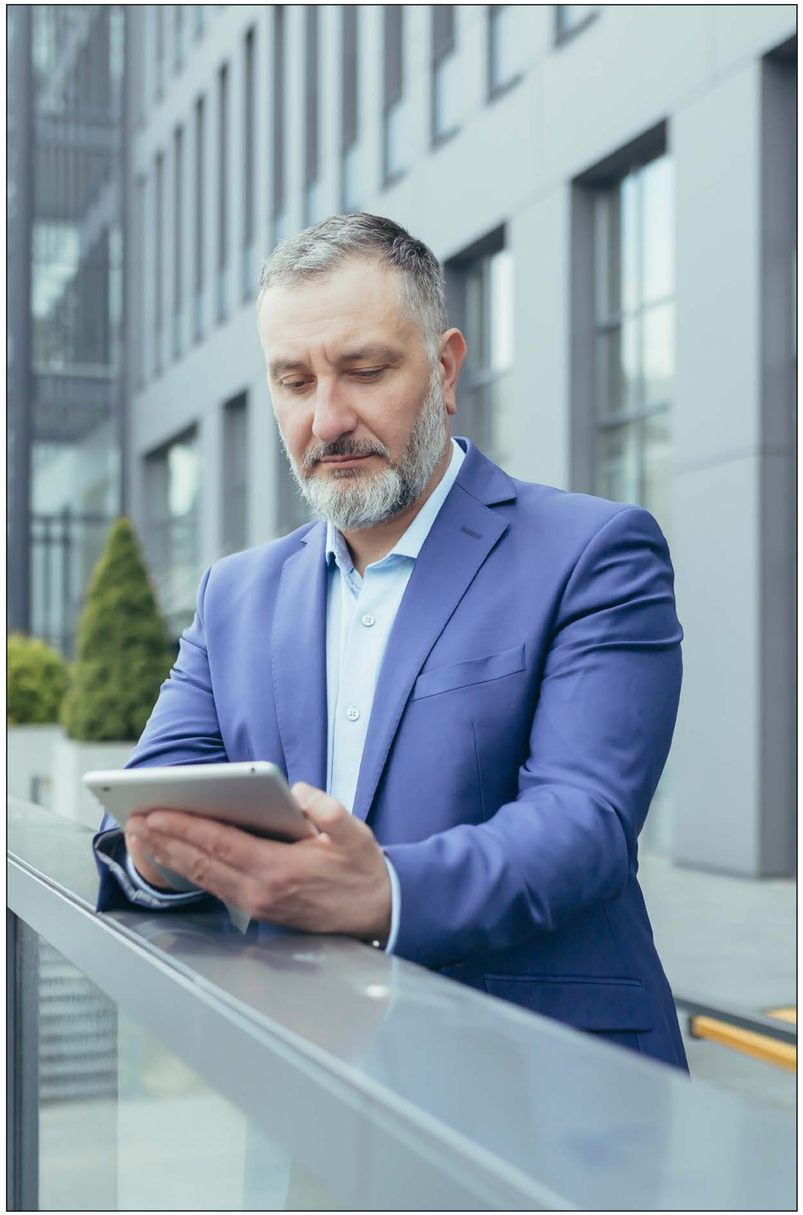
> Hier finden Sie eine detaillierte Referenzarchitektur für Cybersecurity von Microsoft - einer der Ansätze, auf denen unsere Empfehlungen basieren.

Ebenso sollten Sie geeignete Mechanismen zum Schutz der Benutzeridentität und E-Mail-Sicherheitslösungen implementieren, um das Risiko eines unbefugten Zugriffs und eines Datenverlusts zu minimieren. Azure AD und Microsoft Defender für Office 365 sind die beiden Tools für diese Aufgabe. Beide Tools tragen dazu bei, Risiken im Zusammenhang mit gestohlenen Zugangsdaten, der Verbreitung von Malware und Phishing-Angriffen zu vermeiden.

Auf Infrastrukturebene sollten Sie optimale Firewall-Konfigurationen einsetzen, um Ihre Webanwendung vor gängigen Cyberangriffen wie SQL-Injections, Cross-Site-Scripting und der Einbindung lokaler Dateien zu schützen. Azure Web Application Firewall (WAF) ist eine robuste, Cloud-native Lösung, die wir für diesen Zweck empfehlen.

Und schließlich sollten Sie sich auf den erweiterten Endpunktschutz konzentrieren. Schaffen Sie einen konsolidierten Prozess für die Erfassung von Sicherheits-Telemetrie aus verschiedenen Unternehmenstools und die Umwandlung von Rohdaten in Bedrohungsdaten. Ihr Ziel ist es, nach und nach die verschiedenen Systeme und Umgebungen - Netzwerke, Cloud-Workloads, lokale Services, E-Mail, Geschäftsanwendungen und mehr - *miteinander zu verbinden*, um zu verstehen, wo Risiken und Schwachstellen auftreten können und diese schnell zu erkennen. Cloud SIEM- und SOAR-Tools wie Azure Sentinel bieten Ihren Sicherheitsteams die Abdeckung, Skalierbarkeit und Automatisierungsmöglichkeiten, die sie benötigen.

[23] DDoS Attack Trends for 2022 Q1.Cloudflare. Abruf am 15. August.



Fragebogen zur Cybersecurity für BCDR_

In dem Bemühen, eine praktikable BCDR-Lösung zu schaffen, werden leicht einige Aspekte ausgelassen, die sich später als wesentlich erweisen. Um Ihnen dabei zu helfen, jedes einzelne Element des Sicherheitsdesigns abzudecken, haben wir diesen Fragebogen erstellt, der sich in jeder Phase Ihrer BCDR-Reise als hilfreich erweist.

1. Wie gewährleistet Ihre Infrastruktur die hohe Verfügbarkeit der Services?
2. Wie führen Sie den Sicherungsprozess durch? Was ist der Backup-Plan? Wie stellen Sie die Kohärenz sicher? Für welchen Zeitraum können Daten verloren gehen? Erfüllt Ihr Backup-Plan diese Anforderungen?
3. Wie können Sie sicherstellen, dass die Backups rechtzeitig erstellt werden und nicht ausfallen?
4. Wie betreiben Sie Ihre Backup-/Sekundärstandorte?
5. Gibt es Unterschiede bei den Lösungen, der Leistung oder den Modellen?
6. Wie verteilen Sie die Konfigurationen zwischen den Standorten?
7. Wie testen Sie die Sicherheit der gleichen Services an verschiedenen Standorten?
8. Ist Ihr Sicherheitsteam in der Lage, Haupt- und Neben-/Backup-Standorte mit demselben Maß an Transparenz zu überwachen?
9. Erfassen Ihre Erkennungssysteme alle Standorte und entdecken sie auch Bedrohungen an sekundären Standorten/Backups?
10. Wie schützen/isolieren Sie Ihr(e) Backup-System/Lösung?
11. Wie können Sie Ihre Management-Ebenen von den Hauptnetzen isolieren?

infopulse

Einführung von BCDR mit Infopulse_

Verankern Sie Resilienz in Ihrer Unternehmens-DNA mit den Technologieberatungs- und Security Assessment Services von Infopulse. Unsere Berater können eine gründliche Prüfung Ihrer aktuellen Systeme durchführen, den Risikoradar abbilden und die Auswirkungen verschiedener Risiken auf unterschiedliche Geschäftssysteme, Arbeitsabläufe und Abläufe im Allgemeinen miteinander in Beziehung setzen. Mit einem starken Fokus auf Sicherheit hilft unser Team sowohl KMUs als auch multinationalen Konzernen bei der Implementierung von robusten Disaster Recovery- und Disaster Mitigation-Kontrollen, um einen kontinuierlichen Betrieb unter allen Bedingungen zu gewährleisten.

Mehr Informationen über unsere Beratungsdienste im Bereich Technologie und Sicherheit.

Über Infopulse

Infopulse, Teil des führenden nordischen, digitalen Dienstleistungs-Unternehmens Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune 100 Unternehmen auf der ganzen Welt. Das in 1991 gegründete Unternehmen verfügt über ein Team von über 2.300 Fachleuten und ist weltweit in 7 Ländern - in Europa sowie in Nord-, Mittel- und Südamerika - vertreten.

Infopulse genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und vieler anderer.

Für weitere Informationen besuchen Sie bitte **www.infopulse.com/de**

Kontaktieren sie uns:

PL +48 (663) 248-737

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com