Blackout:
Stromausfälle und ihre Folgen

iQSol
Security made in Austria.

Blackout: Stromausfälle und ihre Folgen

Gefahren und Lösungen für Unternehmen mit kritischen Infrastrukturen

Whitepaper

I. Einleitung

Blackouts – plötzliche, überregionale und länger andauernde Strom- und Infrastrukturausfälle – sind für Unternehmen echte Horrorszenarien, die nicht nur am Image kratzen, sondern schnell existenzbedrohend werden können. Aber auch lokale, kleinregionale Stromausfälle können rasch Daten und viel Geld kosten. Was geschieht dabei genau? Nun, es fällt zum Beispiel ein Strommast unter einer Schneelast zusammen, ein Hacker kappt die Stromversorgung bei den Elektrizitätswerken, ein Kurzschluss sorgt dafür, dass die Unterbrechungsfreie Stromversorgung (USV) mit begrenzter Laufzeit einsetzt.

In der Folge werden IT-Systeme nicht mehr mit Strom versorgt – und mit ihnen ganze Maschinenanlagen oder andere Kritische Infrastrukturen, wie man sie in Krankenhäusern oder bei Energieversorgern vorfindet. Dadurch werden Anlagen zerstört, Unternehmen sind nicht in der Lage, ihre Produktion oder Dienstleistungen fortzuführen, Daten werden gelöscht, fehlerhaft oder abgegriffen – das Ansehen in der Öffentlichkeit, bei Kunden und Partnern sinkt. Rechtsstreitigkeiten können folgen, Umsatzeinbußen folgen auf jeden Fall.

Das vorliegende Whitepaper verdeutlicht anhand verschiedener Beispiele, wie real die Bedrohung eines Blackouts ist. Zudem werden Lösungswege aufgezeigt, wie die eigene IT vor einem Zusammenbruch geschützt werden kann, ganz gleich ob Mittelstand oder Konzern, ob Krankenhaus, IT-Dienstleister oder Industrie. Jürgen Kolb und Alexander Graf, Gründer der iQSol GmbH, erörtern Aspekte und Möglichkeiten, wie man Business-Continuity-Management auf höchstem Niveau der Technik abbilden kann.

Die Verbindung von Theorie (Notfallhandbuch) mit der Praxis (Software-Tools im Verbund) muss strukturiert hergestellt werden. Prozessoptimierung und die Erfüllung aller Standards weit über die abstrakten Vorgaben hinaus sorgen dafür, dass, vom IT-Security-Management kommend, die Krisenkommunikation genauso integriert wird wie der ultimative USV-Shutdown und -Restart. Natürlich schließt dieser Ansatz heute alle verfügbaren Technologien beginnend bei Umweltsensoren über (virtuelle) Applikationen und Datenbanken bis hin zu bestehenden Management-Lösungen ein.

Vorab: Was ist eine Kritische Infrastruktur?

Kritische Infrastrukturen (KRITIS) sind Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. „Kritisch“ sind sie deshalb, weil bei einem Ausfall oder einer Störung zum Beispiel Versorgungsengpässe für die Bevölkerung entstehen. Die meisten Kritischen Infrastrukturen sind heute wechselseitig voneinander abhängig, was Risiken und Kaskadeneffekte begünstigt.

Das deutsche Bundesministerium des Inneren hat folgende Sektoren und Branchen zu Kritischen Infrastrukturen erklärt[1]:

Sektor	Branche
Energie	Elektrizität, Gas, Mineralöl
IT und Telekommunikation	IT und Telekommunikation
Transport und Verkehr	Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
Gesundheit	Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
Wasser	Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung
Ernährung	Ernährungswirtschaft, Lebensmittelhandel
Finanz- und Versicherungswesen	Banken, Börsen, Versicherungen, Finanzdienstleister
Staat und Verwaltung	Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich Katastrophenschutz
Medien und Kultur	Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke

[1] Bundesministerium des Innern (BMI), „Definition ‚Kritische Infrastrukturen'", 2009; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile

II. Die Theorie

A) Wie real sind Blackouts wirklich?

Ein kurzer Stromausfall, wo soll hier das Problem liegen? Es stimmt, nicht jeder Stromausfall ist ein Blackout und bedeutet deswegen, dass der schlimmste aller Fälle eintreten muss. Aber wenn der Strom doch mal länger als fünf Minuten wegbleibt, kann es im Einzelfall bereits kritisch werden. Man stelle sich etwa vor, welche Auswirkungen ein Bandstillstand in der Automobilproduktion nach sich ziehen kann – wo es doch auf Sekunden ankommt.

Beispiele aus der Praxis zeigen, dass dies nicht nur Fantasieschlösser sind:

Volkswagen, 2014
2014 lag Wolfsburg kurzzeitig im Dunkeln. Bei Volkswagen hatte es einen Fehler im eigenen Kraftwerk gegeben. Der rächte sich, denn an diesem Samstag waren nicht nur das Werk des Autobauers, sondern auch seine internationale Website, der E-Mail-Verkehr der Führungskräfte und sogar benachbarte Stadtteile offline. Ganze fünf Stunden hielt dieser Zustand laut Medienberichten[2] an. Die Arbeiter der Sonderschicht wurden zwischenzeitlich nach Hause geschickt, die Produktion stand still.

Beziffert wurden die Umsatzeinbußen nicht, aber mehrere hundert nicht produzierte Fahrzeuge, Gehalt für nicht erbrachte Arbeit und mehr lassen erahnen, was der Stromausfall bei VW gekostet hat.

Google, 2015
Im August 2015 gingen im belgischen Rechenzentrum des Google-Konzerns die Lichter aus. Zahlreiche Blitzeinschläge im Laufe mehrerer Tage hatten zwar sämtliche Notstrom-Vorkehrungen gestartet, dennoch konnten einige Server nicht standhalten und fielen aus. Wie viele Kundendaten verloren gegangen sind, ist nicht überliefert[3].

Helios Kliniken Schwerin, 2013
Wenn in Krankenhäusern der Strom ausfällt, geht es nicht mehr um Zahlen, sondern um Menschenleben. In Schwerin kam es 2013 zu einem tragischen Unglück[4]: Aus ungeklärten Gründen kam es zu einem Stromausfall in den renommierten Helios Kliniken. Der durch Notstromaggregate erzeugte Ersatzstrom sprang zwar umgehend an, wurde aber nicht auf die Intensivstation weitergeleitet. Weil damit auch die Beatmungsgeräte nicht mehr funktionierten, kam ein 29-jähriger Patient ums Leben.

Stromausfälle in Kliniken sind kein Einzelfall: In Frechen bei Köln war 2010 ein Kurzschluss schuld an der unterbrochenen Energieversorgung, 2011 kam es in Freising aufgrund einer Berührung von nackter Stromleitung und Erde zum Ausfall, zwei Jahre später, 2013, waren Kliniken in Bad Waldsee und Lörrach betroffen, 2015 wurde das Sindelfinger Krankenhaus Opfer eines durchtrennten Stromkabels.

[2] wirtschaftswoche.de, „Bei Volkswagen: Folgen von Stromausfall gravierender als gedacht“, 10.03.2014;
http://www.wiwo.de/unternehmen/auto/bei-volkswagen-folgen-von-stromausfall-gravierender-als-gedacht-/9594976.html
[3] ZDNet.de, „Blitzeinschlag: Google verliert in belgischem Rechenzentrum Kundendaten“, 20.08.2015;
http://www.zdnet.de/88244502/blitzeinschlag-google-verliert-in-belgischem-rechenzentrum-kundendaten/
[4] FAZ.de, „Patient stirbt nach Stromausfall in Klinik“, 30.10.2013;
http://www.faz.net/aktuell/gesellschaft/gesundheit/ermittlungen-in-schwerin-patient-stirbt-nach-stromausfall-in-klinik-12640847.html

Als weitere Beispiele können der Stromausfall in einer Klinik in Leipzig[5], der Ausfall im Rechenzentrum[6], der zur Nichtverfügbarkeit von Seiten wie Spiegel Online führte, oder der Ausfall in der Universität Bochum[7] mit noch nicht absehbaren Schäden angeführt werden.

B) Was sagt die Wissenschaft?

Stromausfälle sind häufiger, als man annehmen möchte – auch in Deutschland, wo die Netze gemeinhin als sicher gelten.

Die Aufzeichnungen der Netzbetreiber zeigen, dass sich bei 49,6 Mio. Verbrauchern und 884 Netzen im Jahr 2014 in Deutschland insgesamt 147.800 Unterbrechungen bei Niederspannung, bei Mittelspannung 26.000 Aussetzer ereignet haben. Der von der Bundesnetzagentur angesetzte SAIDI[8] (System Average Interruption Duration Index)-Wert, also der bemessene Durchschnitt aller von den heute 883 Stromnetzbetreibern[9] eingereichten Werte, ergibt so: Im Jahr 2014 war der Strom im Niederspannungsbereich durchschnittlich 2,19 Minuten unterbrochen, im Mittelspannungsbereich ganze 10,09 Minuten. Allerdings: In ihrer Statistik erfasst die Bundesnetzagentur nur Ausfälle, die länger als drei Minuten dauern. Wie oft es vielleicht also auch nur wenige Sekunden zu einer Unterbrechung kommt, bleibt im Dunkeln. Diese sogenannten „Netzwischer" treten allerdings häufiger auf als bekannt – und verursachen enormen Schaden![10]

Viele mögliche Auslöseereignisse

Es gibt eine ganze Reihe möglicher Auslöseereignisse, die zu einem Blackout führen können (etwa technische Störungen und Fehler, menschliches Versagen, Naturereignisse, Sonnenstürme, Cyber-Angriffe, Terroranschläge etc.). Wie bisherige Ereignisse auf anderen Kontinenten gezeigt haben, führt in der Regel eine Verkettung von an und für sich beherrschbaren Störungen zum Dominoeffekt, was heute innerhalb weniger Sekunden zum Ausfall der Stromversorgung in weiten Teilen Europas führen kann.

Viel häufiger kommt es jedoch zu lokalen Stromausfällen, egal ob diese durch Extremwetterlagen (Eis, Schnee, Hochwasser, Sturm, Hitze), einen Bagger oder technische Störungen ausgelöst werden. Auch diese können durchaus länger als nur ein paar Minuten dauern. Besonders hervorzuheben ist, dass die Zahl der Extremwettereignisse in den letzten Jahren angestiegen ist. Besonders in urbanen Räumen kam es bei Hitzewellen zu häufigeren Erdkabelfehlern. Gleichzeitig sind Erdkabel weniger anfällig gegenüber Eis-, Sturm- oder Schneeereignissen.

Hinzu kommt, dass durch die volatile Einspeisung aus erneuerbaren Energiequellen die Spannungs- und Frequenzqualität leidet. Während kurzfristige Störungen im Sekundenbereich im Haushalt nicht einmal wahrgenommen werden, verursachen diese in Produktionsanlagen und im Infrastrukturbereich regelmäßig Schäden und führen zum Ausfall wichtiger Komponenten.

---

[5] http://www.herbert.saurugg.net/2015/blog/stromversorgung/leipzig-stromausfall-im-krankenhaus
[6] http://www.herbert.saurugg.net/2015/blog/stromversorgung/stromausfall-legt-populaere-deutsche-websites-lahm
[7] http://www.herbert.saurugg.net/2015/blog/stromversorgung/schaeden-nach-stromausfall-an-uni-bochum-noch-nicht-absehbar
[8] Bundesnetzagentur, Versorgungsqualität/SAIDI-Werte 2006-2014;
http://www.bundesnetzagentur.de/cln_1412/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/Stromnetze/Versorgungsqualit%C3%A4t/Versorgungsqualit%C3%A4t-node.html
[9] Bundesnetzagentur, Übersicht aller Stromnetzbetreiber in Deutschland, Stand: 27.08.2015;
http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/DatenaustauschundMonitoring/UnternehmensStammdaten/UebersichtStromUndGasNetzbetreiber/UebersichtStromUndGasnetzbetreiber_node.html
[10] http://www.herbert.saurugg.net/2014/blog/stromversorgung/qualitaet-der-stromversorgung-in-deutschland

Auch die Forscher des Deutschen Zentrums für Luft- und Raumfahrt (DLR) und des Instituts für Energiewirtschaft und Rationelle Energieanwendung (IER) der Universität Stuttgart haben in einer für das Umweltministerium Baden-Württemberg durchgeführten Studie[11] festgehalten, dass es um die Versorgungssicherheit frühestens ab 2018, spätestens aber ab 2021 in Deutschland nicht mehr allzu gut bestellt sein wird und temporäre Ausfälle sich häufen werden.

Die Folgen sind „katastrophal"

Der schlimmste aller Fälle, nämlich dass in weiten Teilen Europas zeitgleich die Stromversorgung ausfällt, wird von unterschiedlichen Experten als gering eingestuft. Gleichzeitig gibt es aber auch glaubwürdige Experten, die genau vor einem solchen Ereignis warnen und dabei auf die zunehmende Komplexität des Gesamtsystems verweisen.[12] Bei der bisher größten Störung im europäischen Verbundsystem im Jahr 2006 wäre ein solcher Zusammenbruch beinahe passiert. Innerhalb von 19 Sekunden zerfiel das europäische Stromversorgungssystem in drei Frequenzbereiche, wobei in Westeuropa von Hamburg bis Südspanien rund 10 Millionen Kunden durch die hohe Unterfrequenz komplett ohne Strom waren.[13] Unter den heutigen Rahmenbedingungen geht niemand mehr davon aus, dass ein solches Ereignis so glimpflich ausgehen würde.

An der Universität Karlsruhe stellte ein Forscher-Team im Jahr 2011 fest, dass „massive Funktions- und Versorgungsstörungen, Gefährdungen der öffentlichen Ordnung sowie Schäden und Produktionsausfälle in Milliardenhöhe" bereits vorgekommen wären. Würde ein Stromausfall noch länger dauern und sich über weite Teile des Landes erstrecken, hätte dies noch dramatischere Konsequenzen.[14] Die Versorgung der Menschen, Produktionsanlagen, die Unterbrechung der Kommunikation, der Betrieb von Krankenhäusern – all das wäre in Gefahr. Im TA-Bericht[15] des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages wurde daher schon im April 2011 darauf hingewiesen, dass größere Anstrengungen unternommen werden müssten, um die beschriebenen Folgen zu verhindern und einen Blackout abzuwenden.

Deutschland ist nicht das einzige Land, das sich um Vorsorge für Blackouts bemüht. In Österreich zum Beispiel hat sich Herbert Saurugg, MSc und ehemaliger Berufsoffizier, dem Thema angenommen und die zivilgesellschaftliche Initiative „Plötzlich Blackout"[16] ins Leben gerufen. Und auch der niederösterreichische Zivilschutzverband hat einen Ratgeber[17] veröffentlicht, um nicht nur auf die Gefahr aufmerksam zu machen, sondern Bürgern konkrete Handlungsempfehlungen an die Hand zu geben. Mittlerweile überprüfen auch Rechnungshöfe der Länder die Resilienz der öffentlichen Verwaltungen und zeigen schonungslos Schwachstellen auf.

In der Schweiz fand 2014 die landesweite Sicherheitsverbundsübung 2014[18] zu den Szenarien „Pandemie, Blackout und Strommangellage" statt. Zudem werden auch im aktuellen Risikobericht 2015 der Schweiz wie auch bereits 2012 eine Strommangellage/Blackout und eine Pandemie als größte Risiken für die Schweiz eingestuft.[19]

---

[11] dlr.de, DLR-Studie zur Versorgungssituation in Süddeutschland bis 2025, 17.09.2014;
http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10081/151_read-11600/#/gallery/16481
[12] http://www.saurugg.net/Risikoeinschaetzungen-Blackout-Gefahr.pdf
[13] https://de.wikipedia.org/wiki/Stromausfall_in_Europa_im_November_2006
[14] medizin-und-technik.de, „Kein Strom? Das führt zur Katastrophe", 2011,
http://www.medizin-und-technik.de/undausserdem/-/article/27544623/32618234/Kein-Strom-Das-f%C3%BChrt-zur-Katastrophe!/art_co_INSTANCE_0000/maximized/
[15] Bundestag.de, „Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung", 27.04.2011;
http://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf
[16] ehemals: http://www.ploetzlichblackout.at/; heute: http://www.herbert.saurugg.net/strom-blackout
[17] noezsv.at, „Safety-Ratgeber Blackout";
http://www.noezsv.at/noe/media/0_Dokumente/Safety_Ratgeber_blackout.pdf
[18] http://www.vtg.admin.ch/internet/vtg/de/home/dokumentation/news/newsdetail.57427.nsb.html
[19] http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/dokumente/news/detail.57955.nsb.html

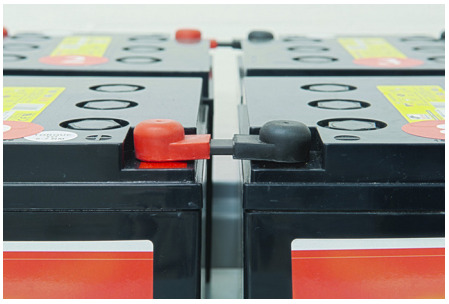
III. Die Praxis

A) Selbst für Business-Continuity-Management sorgen

Stromausfälle können weder von Privatpersonen noch von der Wirtschaft verhindert werden – und auch die Politik und die Energieversorger haben nur eine eingeschränkte Handhabe. Was aber jeder selber tun kann ist, einen Schutz zu errichten, um eine alternative Stromversorgung sicherzustellen oder wichtige Systeme so herunterzufahren, dass zumindest Schäden an der Hardware oder Datenverluste gering gehalten werden können.

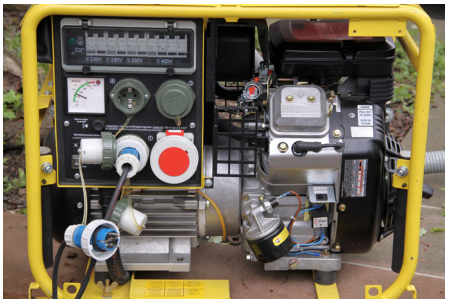
Klassische Schutzmechanismen außer Kraft

Die Überbrückung kurzzeitiger Aussetzer erfolgt in der Regel über Geräte (Appliances) wie eine Unterbrechungsfreie Stromversorgung (USV) oder über Notstromaggregate sowie -generatoren.



USV

Bei Stromausfällen und Spannungsabfällen, die oftmals nur wenige Millisekunden andauern, springen USVs ein und bieten eine zuverlässige Überbrückung. Sie sorgen dafür, dass PCs und Maschinen nicht sofort den Dienst versagen, sondern halten die Geräte noch einige Zeit am Laufen. So haben die Anwender Zeit, ihre Rechner und Server bei Bedarf in Eigenregie herunterzufahren – was bei großen Anlagen und Unternehmen allerdings kaum realistisch ist. Je nach Anwendungsfall können verschiedene USV-Typen mit unterschiedlichen Schutzstufen und Technologien ausgewählt und eingesetzt werden. Alleine die Dimensionierung der USV-Anlagen ist eine Wissenschaft für sich und eine lebende IT-Infrastruktur sorgt dafür, dass oft nach wenigen Monaten die ohnehin theoretischen Berechnungen obsolet werden.



Notstromaggregate

Durch Notstromaggregate sind Unternehmen unabhängig vom öffentlichen Stromnetz in der Lage, sich für einen gewissen Zeitraum selbst mit Energie zu versorgen. Dabei wird in der Regel ein Diesel- oder Benzinmotor mit einem Generator kombiniert. Grundsätzlich eine gute Einrichtung. Doch auch nur dann, wenn Unternehmen mit Notfallplänen arbeiten und diese regelmäßig überprüfen. Denn geht dem Aggregat der Sprit aus (was bei voller Ladung meist spätestens nach vier Tagen geschieht) ist die Stromversorgung unterbrochen und der Schaden tritt trotz aller Vorsichtsmaßnahmen ein. Und auch für mechanische Entlüftung, ausreichend Schmiermittel und einem eventuellen Ausfall dieser Systeme muss vorgesorgt sein.

Für eine kurzzeitige Überbrückung eines Energieab- oder -ausfalls sind beide Lösungen sinnvoll und notwendig. Bleibt der Strom jedoch länger aus, werden auch sie den Dienst versagen und Maschinen und Systeme wie gehabt abstürzen. Es tritt also wieder der Fall ein, dass durch unvorhergesehene Abstürze der PCs oder Anlagen wichtige Daten verloren gehen, in Krankenhäusern sogar lebenserhaltende Maschinen nicht mehr arbeiten und Schäden an der gesamten IT vorherzusehen sind.

B) Verlässliche Alternative: Desaster Recovery

Ein wichtiger Punkt beim Schutz seiner Systeme ist daher das Business-Continuity-Management, das bei Vorfällen dafür sorgt, dass Unternehmen handlungsfähig bleiben. Und auch die sogenannte „Desaster Recovery", also die Wiederherstellung nach dem Vorfall, muss bedacht werden.

Eine Reihe diesbezüglicher Standards finden sich übrigens in der ISO-Norm 27002[20]. Ein ganzes Kapitel (14) behandelt hier nicht nur Verfügbarkeitsanforderungen eines IT-Systems, sondern definiert auch im Detail die Bestellung eines im Notfall Verantwortlichen, die Erstellung eines Notfallhandbuchs bis hin zu einem Alarmierungsplan. Ausführungen zur redundanten Leitungsführung und der redundanten Auslegung von Netzkomponenten finden sich ebenfalls. Zudem sind ein Wiederanlaufplan und regelmäßige Desaster-Recovery-Übungen sowie Tests zur Datenrekonstruktion vorgesehen. Bei Letzterem etwa wird ausdrücklich darauf hingewiesen, dass Daten gegebenenfalls auf einem Ausweich-IT-System installiert werden müssen. Sicherzustellen ist ebenfalls, dass auch sachverständige Dritte die Datenrestaurierung anhand der vorhandenen Dokumentation durchführen können.

Nicht minder wichtig ist der BSI-Standard 100-4[21] des Bundesamts für Sicherheit und Informationstechnik, der sich auf 117 Seiten dem Notfall-Management widmet. Er liefert eine Anleitung, wie das Notfall-Management in Einklang mit dem IT-Grundschutz eingeführt und aufrechterhalten werden kann.

C) Maßnahmen für eine erfolgreiche Desaster Recovery

Nach all dem bisher Gesagten: Was genau können Unternehmen, Organisationen und Behörden tun, um sich vor den Folgen eines Stromausfalls zu schützen? Einen Ansatz bietet das Power-Management.

Notfallhandbuch

Damit Desaster Recovery gelingt, ist zunächst wichtig, klar zu definieren, welche Prozesse unbedingt aufrechterhalten werden müssen und welche Maßnahmen dies erfordert. Hier kommt das Notfallhandbuch ins Spiel.

Ein Notfallplan bzw. Notfallhandbuch definiert, wo sich Backups wie zum Beispiel extern gelagerte bzw. in der Cloud gespeicherte Daten befinden, wie diese nach einem Crash wieder eingespielt werden können, welche Systeme welche Passwörter erfordern, wo eventuell benötigte Ersatzcomputer stehen und dergleichen mehr. Auch die einzelnen zu ergreifenden Schritte sind klar definiert. Wichtig ist in diesem Zusammenhang

[20] Iso.org, „ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls"; http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533
[21] BSI.de, „BSI-Standard 100-4, Notfallmanagement Version 1.0", 2008; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile&v=1

eine regelmäßige inhaltliche Pflege: Ändert sich auch nur ein Switch im Netzwerk, sollte dies entsprechend festgehalten werden. Auch, wenn andere neue Hard- oder Software im Unternehmen zum Einsatz kommt, wenn Mitarbeiter, die komplexe Skripte geschrieben haben, nicht mehr im Unternehmen tätig sind, wenn sich Zugriffsberechtigungen ebenso wie Software-Lizenzen geändert haben, erfordert dies einen Eintrag im Notfallplan. Auch sollten Übungen durchgeführt werden, damit im Notfall keine Überraschungen auf das Team zukommt.

Software zum Power-Management

„Wiederherstellung nach der Katastrophe". Das bedeutet der Begriff Desaster Recovery wörtlich. Man kann es als Art Versicherung, die im Notfall die Ressourcen eines IT-Systems schützt, bezeichnen. Redundante Server, Replikations- und Backup-Systeme, womöglich ein Ausfallrechenzentrum, Firewalls, Anti-Viren-Software und ähnliches sind dafür die Basis.

Alleine jedoch liefert diese noch keine Hochverfügbarkeit, die eine Ausfallsicherheit der Firmen-IT und die perfekte Datenwiederherstellung gewährleistet. Es sind einzelne, aber keine gesamtheitlichen, zentral gesteuerten Schutzmaßnahmen.

IT nach Plan herunterfahren

Fällt der Strom aus und fahren Server, Systeme, Applikationen unkoordiniert herunter, ist das Chaos perfekt. Ein geordnetes Herunterfahren der IT, gesteuert nach bestimmten Prioritäten, die Wichtiges von Unwichtigem trennen, ist entscheidend. Wie im umgekehrten Fall: Ist der Strom wieder da, muss das System geordnet wieder hochfahren. So etwas lässt sich schwer „händisch" bewerkstelligen. Im Notfall, etwa bei einem längerem Stromausfall und womöglich kurzer USV-Überbrückungszeit, werden sich selbst die besten IT-Verantwortlichen schwer tun, einen Shutdown für hunderte Server manuell zu steuern. Ganz abgesehen davon, dass das Personal auch verfügbar sein muss. Denn solche Ereignisse treten nicht nur in der Bürozeit ein. Eine einfache Lösung ist ein zentrales Power-Management-System mit einer Software-Applikation, die physikalische Kontakte, Sensoren sowie USV-Geräte zusammenfasst und koordiniert. Ein logikbasierter Failover-Ablauf ist dabei zentraler Bestandteil für die Ausfallfallsicherheit, da bei einem Ausfall auf einen anderen Netzwerkdienst umgeleitet wird. Die Anwendung selbst ist entsprechend abgesichert: Sie ist die letzte, die herunter-, und die erste, die wieder hochfährt.

Um die oft bestehenden Abhängigkeiten unterschiedlicher Server-Systeme zueinander berücksichtigen zu können, bedarf es eines ausgeklügelten Shutdown-Procederes. Eine instabile Stromversorgung erfordert in einem Betrieb etwa den Einsatz der USV-Anlage. Nach einigen Stunden muss jedoch alles heruntergefahren werden. Ist die Stromversorgung wieder kontinuierlich verfügbar, sollen die IT-Systeme automatisch in der umgekehrten Reihenfolge des Shutdowns hochgefahren werden.

Beispiel einer Power-Management-Lösung
Die **„PowerApp“** der **iQSol GmbH** bietet den beschriebenen Server-Shutdown und -Restart per Knopfdruck. Im Notfall ist zudem eine Live-Migration ganzer virtueller Systeme möglich. Darüber hinaus können mit der Appliance Shutdown-Szenarien geprobt werden.

Das integrative Shutdown-Konzept erlaubt es, auch Außenstellen einzubeziehen. Mit dem Feature „PowerNode“ lässt sich ein Procedere mit autonom arbeitenden Anwendungen, die zentral konfiguriert und periodisch synchronisiert werden, von der Zentrale aus in den jeweiligen Niederlassungen und deren lokalen Servern steuern. Für den generellen Überblick werden die jeweiligen Logs an die Zentrale übermittelt.

Kombiniert mit einem modernen **„Security Information & Event Management“ (SIEM)** gibt es neben der damit erfolgenden automatischen Auswertung und Analyse aller Log-Dateien im IT-Netz weitere Monitoring- und Schutzfunktionen. Die Ergebnisse werden an das zentrale Log-Management geschickt, das entsprechende sicherheitsrelevante Alarme auslöst. Unabhängig vom periodischen Scan ermöglicht eine solche Applikation ebenfalls einen Alarm an den Administrator, wird etwas (unbefugt) am File-System geändert. Exemplarisch sei hier die **„LogApp“** von **iQSol** mit weiteren Modulen und Erweiterungsmöglichkeiten erwähnt.

Business-Continuity-Management vollendet: Alerting & Notification

Das fehlende Glied in einem vollständigen BCM-Prozess ist die automatisierte Alarmierung und die Abbildung der internen Kommunikation („Enterprise-Notification-System“). Physikalische Sensoren von Klimaanlagen oder Brandmeldern können ebenso Alarme generieren wie überschrittene Schwellwerte aus gängigen Netzwerk- oder System-Management-Lösungen. Um relevante Alarme und schwere Vorfälle zur richtigen Zeit an die richtigen Personen weiterzureichen, ist eine Alarmierungs- und Eskalationslogik notwendig, die via E-Mail sowie über moderne mobile Geräte im Sprachmodus oder per SMS angewendet werden kann. Umfassende Dokumentationsaufgaben, vordefinierte Verantwortlichkeiten und vor allem rasches Zugreifen auf Informationen und freie Handlungsoptionen sind im Krisenfall unumgänglich. Der **„Alert Messaging Server“ (AMS)** von **iQSol** zum Beispiel ist auf die Anforderungen einer **modernen Alerting-Lösung** abgestimmt und seit zehn Jahren erfolgreich am Markt etabliert.

IV. Fazit

„Solange nichts passiert, ist alles gut“. Das Bewusstsein, dass diese Aussage nicht stimmt, steigt zwar, auch angesichts der steigenden Terrorgefahr oder wegen der zunehmenden Extremwetterereignisse bzw. Komplexität von Systemen. Notfalltests in der realen Umgebung sind hingegen noch selten zu finden. Wirtschaftsprüfer und auch staatliche Stellen verlangen jedoch immer häufiger Informationen über nachvollziehbare Vorsorgemaßnahmen, Redundanzen und die Abläufe im Schadens- oder Katastrophenfall.

Im Krisenfall, ohne Strom und ganz sicher unter massivem Stress, ist es sinnvoll, alles parat zu haben und auf das Ereignis eingehen zu können – und nicht erst suchen zu müssen, wer zuständig ist oder wie lange der Ausfall maximal dauern darf, bis der Worst Case eintritt. Eine geplante Vorgangsweise mit automatisierter Software erleichtert die Entscheidungen, erfüllt die Compliance-Vorgaben und dokumentiert für die Zukunft auch, wo Fehler unterlaufen sind und wer diese womöglich zu verantworten hat.

V. Fragen und Antworten

Ist mein Unternehmen auf längere Stromausfälle vorbereitet? IT-Verantwortliche befassen sich immer häufiger mit dieser Frage und stellen diese auch der iQSol GmbH. Im Folgenden sollen einige Antworten auf die häufigsten Fragestellungen gegeben werden.

A) Wir haben uns selbst ein Skript gebaut und können die Server runterfahren. Warum sollte ich weitere finanzielle Mittel investieren?

Wie alt ist dieses Skript und ist der Programmierer noch in der Firma tätig? Wird das Skript auf Verlässlichkeit und Aktualität getestet? Kann dieses Skript immer angestoßen werden, hinsichtlich Redundanz, und kann auch sichergestellt werden, dass nichts vergessen wurde? Erkennt der Auditor oder externe Prüfer die Qualität und Verlässlichkeit des Skripts an? Selbst dann verzichten Unternehmen auf weitere Features wie automatisiertes Hochfahren der Server und Applikationen, Simulationen und eine Einbindung virtueller Systeme, Live-Migration und vieles mehr wie die Einbindung von Dieselaggregaten und weiterer Sensoren.

B) Meine USV reicht für 10 bis 15 Minuten bei etwa 500 Servern. Wie könnte mir eine Lösung wie die „PowerApp“ helfen?

Unternehmen mit dieser Ausgangssituation haben keine Chance, bei einem Aussetzen der USV manuell einzugreifen. Im ersten Schritt einer Analyse würde man die wichtigsten Systeme berücksichtigen und die robustesten bzw. anfälligsten Hardware-Geräte identifizieren. Beim Einsatz einer Lösung wie der „PowerApp“ würde man Cluster bilden und somit Gruppen anlegen und auf mehrere „PowerApp“-Geräte (auch „PowerNodes“) verteilen, um mit dieser Anforderung fertigzuwerden. Die Reihenfolge ist entscheidend, um die USV-Akkus zu entlasten und ein rasches Hochfahren dann wieder zu ermöglichen. Die Entscheidung, alles herunterzufahren, müsste sehr rasch erfolgen, somit wird das Hochfahren umso wichtiger. „PowerApp“ ist hier die einzige Möglichkeit, jede Sekunde optimal zu nutzen und auf Ereignisse zu reagieren. Immerhin wäre es auch möglich, den Shutdown zu stoppen, wenn der Strom wieder verfügbar wird.

C) Einmal im Jahr müssen wir einen Desaster-Test durchführen. Geht das mit „PowerApp“ effizienter und effektiver?

Dieses Szenario ist mit „PowerApp“ mit weniger Stress und zudem geplanter durchzuführen. Das System ist „up to date“ mit der aktuellen IT-Landschaft und ermöglicht einen Testlauf. Unternehmen lösen den Shutdown aus und erhalten die notwendigen Informationen (Restlaufzeiten, Statusmeldungen, Fehlermeldungen etc.). Sie beobachten die Vorgänge und wissen genau, wann welche Systeme ruhend sind oder ob welche abstürzten und warum (falsch gepatched usw). Sie sind im Bilde darüber, wie USV-Auslastungen besser verteilt werden können, ob noch Daten migriert, aktualisiert oder gespeichert werden können, da es die verfügbare Zeit zulässt. Viele Variable werden feststellbar und jeder Test in jedem Jahr erhöht die Verfügbarkeit, die Erfahrungen und Lerneffekte um ein Vielfaches.

D) Wir beginnen ein Business-Continuity-Projekt – wie kann uns iQSol helfen?

Im ersten Schritt wird ein Notfall- bzw. Betriebsführungshandbuch erstellt. In weiterer Folge werden die Prozesse definiert, die IT-Landschaft analysiert und die Vorgaben festgestellt. Bei Bedarf ist auch ein umfassender Security-Check, Pen-Test oder simulierter Hacker-Angriff möglich – bis hin zum Probealarm („Stecker ziehen") oder Social-Engineering. Mit den Lösungen „PowerApp", „Alert Messaging Server" und „LogApp" ist ein komplettes Log-Management-/SIEM-Projekt sowie Alarmierungs- und Notfall-Management implementiert, wahlweise auch als Managed-Security-Service direkt oder über Partner.

E) Wir haben Filialen im Ausland und dort sind wir öfter von Stromausfällen und Störungen betroffen. Vor Ort ist jedoch niemand mit IT-Know-how, lediglich eine kleine USV-Anlage. Die Server und Geräte stehen auch etwas exponiert und werden nicht extra gekühlt oder vor Umwelteinflüssen geschützt. Hohe Investitionen rentieren sich natürlich auch nicht und Cloud-Lösungen wollen wir nicht.

In der Zentrale kann die „PowerApp" das Management übernehmen, während vor Ort eine „PowerNode"-Appliance (pro Filiale) für das Management sorgt, sprich für das Herunterfahren und Hochfahren im Notfall. Dies kann autonom erfolgen, also nach einem beliebigen Zeitintervall nach Inbetriebnahme der USV oder auch manuell von der Zentrale aus (z. B. aufgrund eines laufenden Hacker-Angriffes) gesteuert werden. Wahlweise wird der Befehl durch einen Sensor ausgelöst (Hitzesensor im Raum oder Wassereintrittsfühler), der an die „PowerNode" angeschlossen und auf Wunsch mitgeliefert wird.

F) In einem Krisenszenario sind wir gezwungen, auf Knopfdruck alles hinunterzufahren – und zwar so schnell wie möglich. Ist die „PowerApp" dazu das richtige Tool und hilft es auch beim Restart, sprich dem optimalen und schnellstmöglichen Wiederanlauf?

Genau für diese Zwecke wurde „PowerApp" entwickelt und wird dahingehend permanent ausgebaut, um auch USV-Desaster-Tests zu ermöglichen oder um Daten auch virtueller Systeme einzubinden. iQSol geht darüber hinaus auf individuelle Wünsche ein, wenn dies sinnvoll erscheint. Zudem bringt jedes Update weitere Erkenntnisse anderer User ein.

VI. Weiterführende Informationen

	Links
iQSol GmbH	www.iqsol.biz
Musterbeispiel eines Notfallhandbuchs	www.notfallhandbuch.at/musterhandbuch/
Antares NetlogiX	www.netlogix.ws
Vernetzung & Komplexität	www.herbert.saurugg.net

Die Autoren

DI Alexander Graf ist der technische Kopf der iQSol GmbH. Nach abgeschlossenem Informatikstudium arbeitete er zunächst im Internet-Provider-Umfeld, bevor er anschließend österreichweit im Netzwerkbereich als Consultant für GECITS aktiv wurde. Seit dem Jahr 2000 zeichnet Alexander als geschäftsführender Gesellschafter bei der Antares NetlogiX Netzwerkberatung GmbH für die Leitung der Technik verantwortlich.

Seit 2010 ist er außerdem Managing Partner der iQSol GmbH, wo er nicht nur für die Entwicklung neuer Lösungen, sondern auch für den Aufbau der internationalen Partnerlandschaften verantwortlich zeichnet.

Jürgen Kolb ist Managing Partner der österreichischen iQSol GmbH. Nach verschiedenen beruflichen Stationen in der öffentlichen Verwaltung sowie in der freien Wirtschaft gründete er als (fast fertig studierter) Wirtschaftswissenschaftler das Unternehmen gemeinsam mit seinem Partner aufgrund vorangegangener Erfahrung aus verschiedenen IT-Projekten und -Audits.

Heute verantwortet Jürgen bei der iQSol GmbH den Bereich Sales, PR & Marketing und treibt das IT-Security-Business gemeinsam mit seinem Team voran. iQSol ist seine zweite erfolgreiche Unternehmensgründung, denn auch am Aufbau der Antares NetlogiX Netzwerkberatung GmbH ist er schon seit Beginn im Jahr 2001 beteiligt.

Bildnachweise

Seite 2: Mediterranean Sea - Night © Guillaume Le Bloas / fotolia.com
Seite 4: Young electrician © bernardbodo / fotolia.com, Montage Basisstation © Kara / fotolia.com, Modern city traffic road at night. Transport junction. © denyshutter / fotolia.com, OP Saal ohne Team © jenshagen / fotolia.com, Hydrant, Standrohr, Löschwasser © mitifoto / fotolia.com, / Einkaufswagen in einem Supermarkt © Gina Sanders / fotolia.com, justice © izzetugutmen / fotolia.com, Bulle und Bär © Klaus Eppele / fotolia.com, Pile of old newspapers, selective focus © mitrija / fotolia.com
Seite 8: USV Batterien - UPS batteries © Andreas Schindl / fotolia.com, Stromaggregat © Klaus Eppele / fotolia.com
Seite 9: Disaster Recovery Plan, DRP © Olivier Le Moal / fotolia.com
Seite 10: drp disaster recovery plan crisis strategy backup redundancy © bakhtiarzein / fotolia.com
Seite 11: touchscreen smartphone with security alarm on the screen © georgejmclittle / fotolia.com

iQSol GmbH
Oed 119
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz
W: www.iqsol.biz