Kundeninformation
"Was ist ein … IT-Sicherheitskonzept ?"

id newmedia KnowHow - für *Sie …*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen (KRITIS)
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

Steigt man in ein Auto, legt man den Sicherheitsgurt an.

Ist man nicht zu Hause, schließt man Türen und Fenster.

Über beides denken wir kaum noch nach, so selbstverständlich ist es für uns.

Aber warum gehen wir mit unseren digitalen Türen und Fenstern oft leichtsinnig um und riskieren damit, daß unser Unternehmen oder unsere Privatsphäre z. B. durch Unbefugte betreten oder beschädigt wird ?

Quelle und Bild : buerger-cert

 im Februar 2025

„To whom it may concern“

Ich habe nach 51 jähriger Berufserfahrung in der Elektronik und IT von 1974 bis 2025

– und insbesondere, seit ich dann von 2000 bis 2019
Leiter IT einer großen Gemeinde war –

die Erfahrung machen müssen, **daß Führungskräfte keine Zeit haben, umfangreiche Berichte durchzulesen**.

Insbesondere die, die sich mit dem Status der IT-Sicherheit einer Verwaltung oder eines Unternehmens befassen. Im Grunde genommen müßte die Führungsebene aber über bestehende und kommende Sicherheitsbelange im Bilde sein und wissen, welche Schlüsselereignisse ihre Aufmerksamkeit erfordert.

Regel Nummer Eins in diesem Zusammenhang mag sein, daß die meisten Chefs keine Überraschungen mögen.

Als Regel Nummer 2 sei das Ziel, in diesem Überblick zur IT-Sicherheit die Überraschungen für das Management auf ein Minimum zu reduzieren.

Deshalb faßt ein IT-Sicherheitskonzept eigentlich einfach nur all das zusammen, was wir alle schon wissen ☺ … sollten.

Germering, im Februar 2021

Ralf Kimmelmann
Informationselektroniker
ehem. Leiter IT/EDV

Präambel

"Bei mehr als jedem zweiten Unternehmen in Deutschland (63 Prozent) steht der Betrieb still, wenn es durch einen Cyberangriff zu einem IT-Ausfall kommt.

Jeder Fünfte könnte nur eine kurze Zeit ohne Datenzugang überbrücken, müßte dann aber auch wieder auf seine IT zugreifen können, um produktiv zu bleiben.

Gleichzeitig ist sich jedes vierte Unternehmen (26 Prozent) unsicher, daß sich alle unternehmensrelevanten Daten im Falle eines Hacks oder Datendiebstahl auch problemlos und zeitnah wiederherstellen lassen – ein weiterer Risikofaktor, der die Betriebsfähigkeit nachhaltig stören kann."

Das sind Ergebnisse einer Umfrage der internationalen Anwaltssozietät Bird & Bird in Zusammenarbeit mit dem Marktforschungsunternehmen YouGov Deutschland unter 250 Unternehmensentscheidern in Deutschland im Februar 2018.

Auch wenn Sie "nur" einen ebay-Shop betreiben sind Sie auf das Funktionieren Ihrer heimischen IT dringend angewiesen – gerade in COVID-19-Zeiten !

Wir starten dort, wo Ihre IT-Infrastruktur ggf. Sicherheitslücken aufweist und bei den Systemen, die dringend für wichtige Geschäftsprozesse benötigt werden.

Vergleichen Sie **Ihre** Geschäftsprozesse damit, um sich möglicher **Risiken** bewußt zu werden und angemessene **Entscheidungen treffen** zu können !

Der erforderliche Aufwand zur Absicherung kritischer Geschäftsprozesse ist maßgeblich davon abhängig, wie lange man auf diese verzichten kann, ohne daß ein existenzgefährdender Schaden eintritt.

Im nächsten Schritt sollte eine spezielle Prüfung stattfinden, inwiefern die IT-Systeme, von denen Ihre Geschäftsprozesse abhängig sind, ausreichend gegen Angriffe durch Dritte und vor Datenverlust geschützt sind.

Es gibt eine **Vielzahl wirksamer Maßnahmen** zur Steigerung der IT-Sicherheit – die passenden werden jedoch selten genutzt.

Externe Angreifer bedienen sich vorrangig an den Früchten,
die am niedrigsten am Baum hängen !

Leiten Sie daher zunächst Sicherheitsmaßnahmen ein, die verhindern, daß Ihr Unternehmen von außen als leichtes Angriffsziel erscheint. Womit wir zum eigentlichen Fahrplan für eine sichere IT-Infrastruktur kommen – dem IT-Sicherheitskonzept, **auch für kleinste Unternehmen.**

Was ist ein IT-Sicherheitskonzept ?
Ein Sicherheitskonzept ist erst einmal eine Sammlung von Erkenntnissen.

Gleichzeitig ist es eine Bestandsaufnahme von Stärken und Schwächen einer geschäftlichen oder heimischen IT-Infrastruktur, die man dadurch kennenlernt.

Ein IT-Sicherheitskonzept sollte folgende Bereiche beleuchten :

Teil 01 orange markiert

Betriebs- und Standzeiten der vorhandenen IT
- Systemverfügbarkeit

Risikoanalyse Gebäude & Haustechnik
- Stromausfall
- Brand / Feuer / Rauch (ergänzt 20190226 um Brandschutzbeauftragten/-helfer
- Explosion
- Wasser
- Naturkatastrophen
- Sabotage
- Gefahrstoffe

Warneinrichtungen Gebäude & Haustechnik
- Alarmanlage mit Polizei-Aufschaltung
- Panikanlage ohne Polizei-Aufschaltung
- Brandmeldeanlage mit ILS-Aufschaltung
- Hausnotruf ohne ILS-Aufschaltung
- Rauchwarnmelder
- Giftgaswarnmelder
- Optische Alarmmeldung
- Akustische Alarmmeldung
- Videoüberwachung mit Echtzeit
- Videoüberwachung mit Datenspeicher/Datenvorhaltung/Standort Zentrale
- EIB/KNX-Haustechnik/Standorte
- Klimaüberwachung
  - Normwerte
  - Grenzwerte
- Unterbrechungsfreie Stromversorgungen
- Klimaanlage

Notfallmanagement Gebäude & Haustechnik

Teil 02 blau markiert

Risikoanalyse Datentechnik

- Ausfall der Internetverbindung
- Ausfall Klimaanlage
- Datenverlust
- Angriff auf die Systeme
  - von extern
  - von intern

Warneinrichtungen und Meldesysteme IT/EDV

Sicherheits- und Schutzmaßnahmen

- Server
- Datensicherung
- Programmsicherung
- Netzwerktechnik
- Security Appliances
- Rechenzentrumsdienstleistungen
- Outsourcing & Cloud
- DSGVO
- Social Engineering
- Schwachstellenmanagement
- Bring-Your-Own-Device (BYOD)
- Home Office / Telearbeitsplatz

BSI Notfall- und Störungsmanagement

Informationen für Geschäftsleitungen

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. der Energie - Versorgungsunternehmen (EVU).

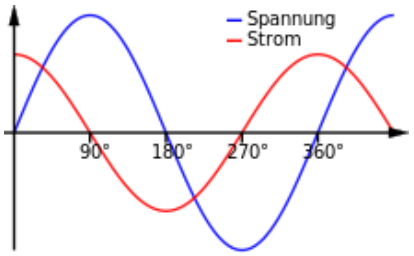


Diagramm : id-newmedia

Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, daß der Mensch sie nicht bemerkt.

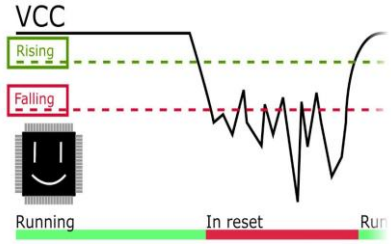


Diagramm : id-newmedia

Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Neben Störungen im Versorgungsnetz können jedoch auch Abschaltungen bei nicht angekündigten Arbeiten oder Kabelbeschädigungen bei Tiefbauarbeiten dazu führen, daß die Stromversorgung ausfällt.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig.

Viele Infrastruktur-Einrichtungen sind heute vom Strom abhängig, z.B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen und Sprinkleranlagen.

Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druck-Erzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.

Bei längeren Stromausfällen kann der Ausfall der Infrastruktur-Einrichtungen dazu führen, daß keinerlei Tätigkeiten mehr in den betroffenen Räumlichkeiten durchgeführt werden können.

Neben Ausfällen können auch andere Störungen der Stromversorgung den Betrieb beeinträchtigen. Überspannung kann beispielsweise zu Fehlfunktionen oder sogar zu Beschädigungen von elektrischen Geräten führen.

Zu beachten ist außerdem, daß durch Ausfälle oder Störungen der Stromversorgung in der Nachbarschaft unter Umständen auch die eigenen Geschäftsprozesse betroffen sein können, beispielsweise wenn Zufahrtswege blockiert werden.

Literatur

Stromausfall - KRITISwww.kritis.bund.de › Ratgeber › Stromausfalll › Strom...

EN 62040: Unterbrechungsfreie Stromversorgungssysteme (USV)

Feuer bei Cloud-Anbieter

Großbrand in Datenzentrum sorgt für Ausfall von Websites

Das Unternehmen OVH zählt zu den größten Cloud-Anbietern Europas. In Straßburg beschädigte am Mittwoch ein Feuer eines der Firmengebäude schwer. Die Folgen betrafen mehrere Websites und Dienste. OVH hat nach eigenen Angaben rund 1,5 Millionen Kunden weltweit und betreibt unter anderem 15 Rechenzentren in Europa.

10.03.2021, 17.22 Uhr

hpp/dpa

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Neben direkt durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können.

Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen.

Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, auch wenn sie in einem vom Brandort weit entfernten Teil des Gebäudes stehen.

Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT - Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brands kann unter anderem begünstigt werden durch : Aufhalten von Brandabschnittstüren durch Keile, unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier, Kopierpapier, Druckerpapier …), Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung, fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder), fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen), mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmaterialien zur Wärme- und Schallisolierung).

Brandschutzvokabular
DIN EN ISO 13943 Brandschutz – Vokabular, Ausgabedatum 2018-01

Brandschutzingenieurwesen
DIN 18009-1 Brandschutzingenieurwesen − Teil 1: Grundsätze und Regeln für die Anwendung, Ausgabedatum 2016-09

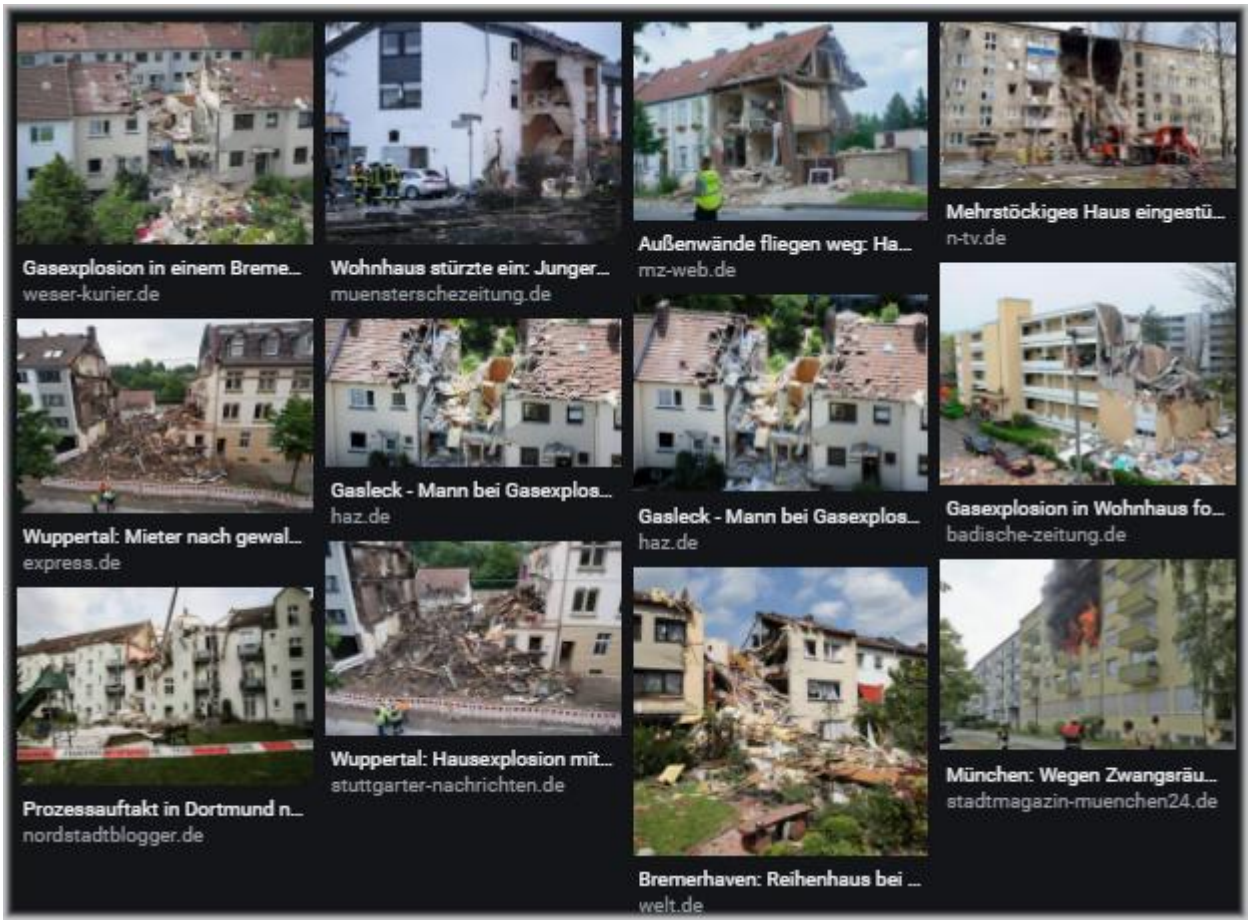
Normen zum baulichen Brandschutz
DIN 4102-xx ff.

https://de.wikipedia.org/wiki/Brandschutz

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Eine Behörde bzw. ein Unternehmen kann Schaden nehmen, wenn sich im Umfeld ein schwerer Unglücksfall ereignet, zum Beispiel ein Brand, eine Explosion, die Freisetzung giftiger Substanzen oder das Austreten gefährlicher Strahlung. Gefahr besteht dabei nicht nur durch das Ereignis selbst, sondern auch durch die häufig daraus resultierenden Aktivitäten, beispielsweise Sperrungen oder Rettungsmaßnahmen. Die Liegenschaften einer Institution können verschiedenen Gefährdungen aus dem Umfeld ausgesetzt sein, unter anderem durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetriebe oder Wohngebiete (z.B. wenn ein Wohnhaus durch eine Gasexplosion zerstört wird).



Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Solche Maßnahmen können auch dazu führen, daß Mitarbeiter ihre Arbeitsplätze nicht erreichen können oder Personal evakuiert werden muß.

Literatur

Henry Portz: Brand- und Explosionsschutz von A-Z - Begriffserläuterungen und brandschutztechnische Kennwerte. Springer-Verlag, 2015, ISBN 978-3-322-80197-5

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

Informationen für Geschäftsleitungen

Durch einen Anschlag kann eine Institution, bestimmte Bereiche der Institution oder einzelne Personen bedroht werden.

Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig : geworfene Ziegelsteine, Explosion durch Sprengstoff, Schußwaffengebrauch, Brandstiftung.

Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab.

Literatur

Peter Waldmann: Terrorismus und Bürgerkrieg. Der Staat in Bedrängnis. Gerling Akademie, München 2003, ISBN 3-932425-57-X

Sascha Lobo Unsere Sicherheit ist eine Inszenierung Blog 31/05/2017

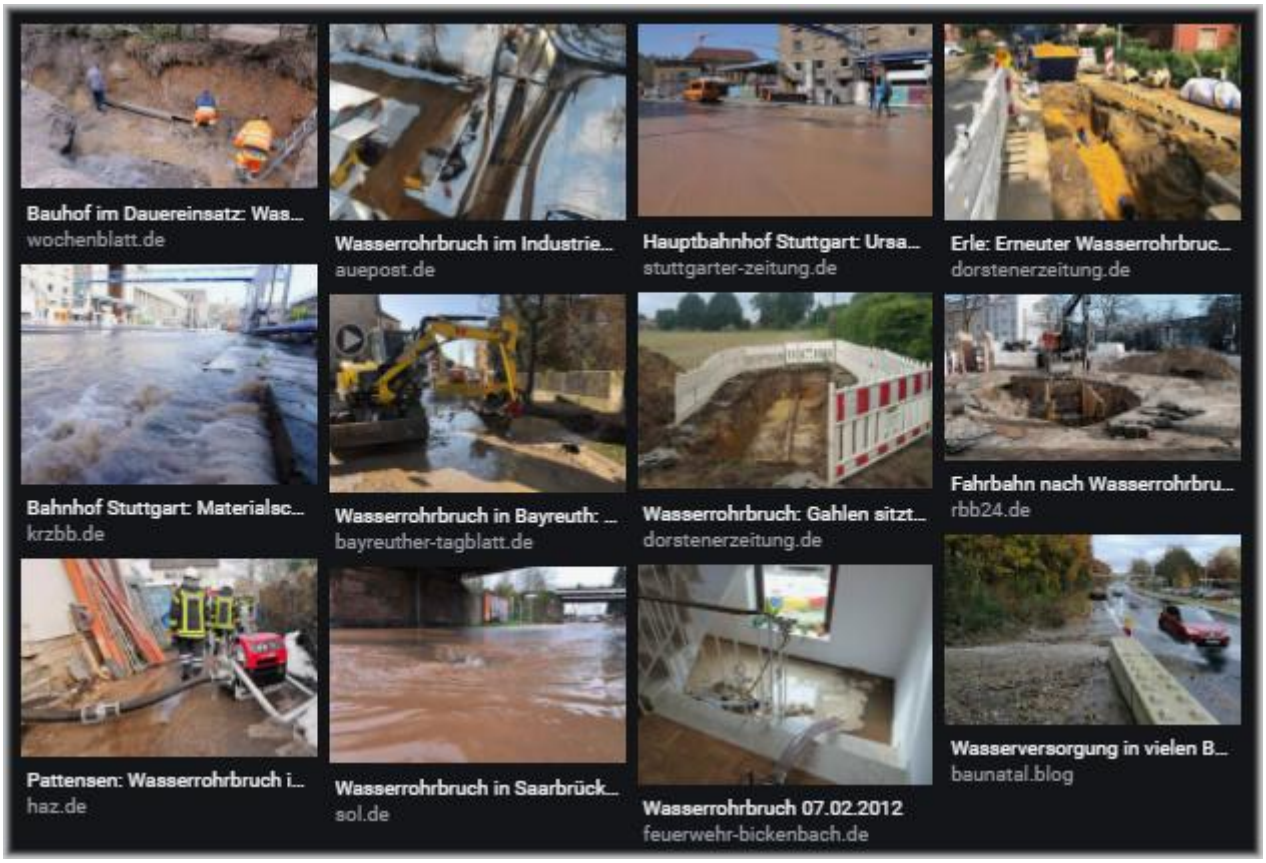
Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Durch Wasser kann die Integrität und Verfügbarkeit von Informationen beeinträchtigt werden, die auf analogen und digitalen Datenträgern gespeichert sind. Auch Informationen im Arbeitsspeicher von IT-Systemen sind gefährdet.

Der unkontrollierte Eintritt von Wasser in Gebäude oder Räume kann beispielsweise bedingt sein durch :

- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung
- Defekte der Heizungsanlage / Defekte an Klimaanlagen mit Wasseranschluß
- Defekte in Sprinkleranlagen
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.



Literatur

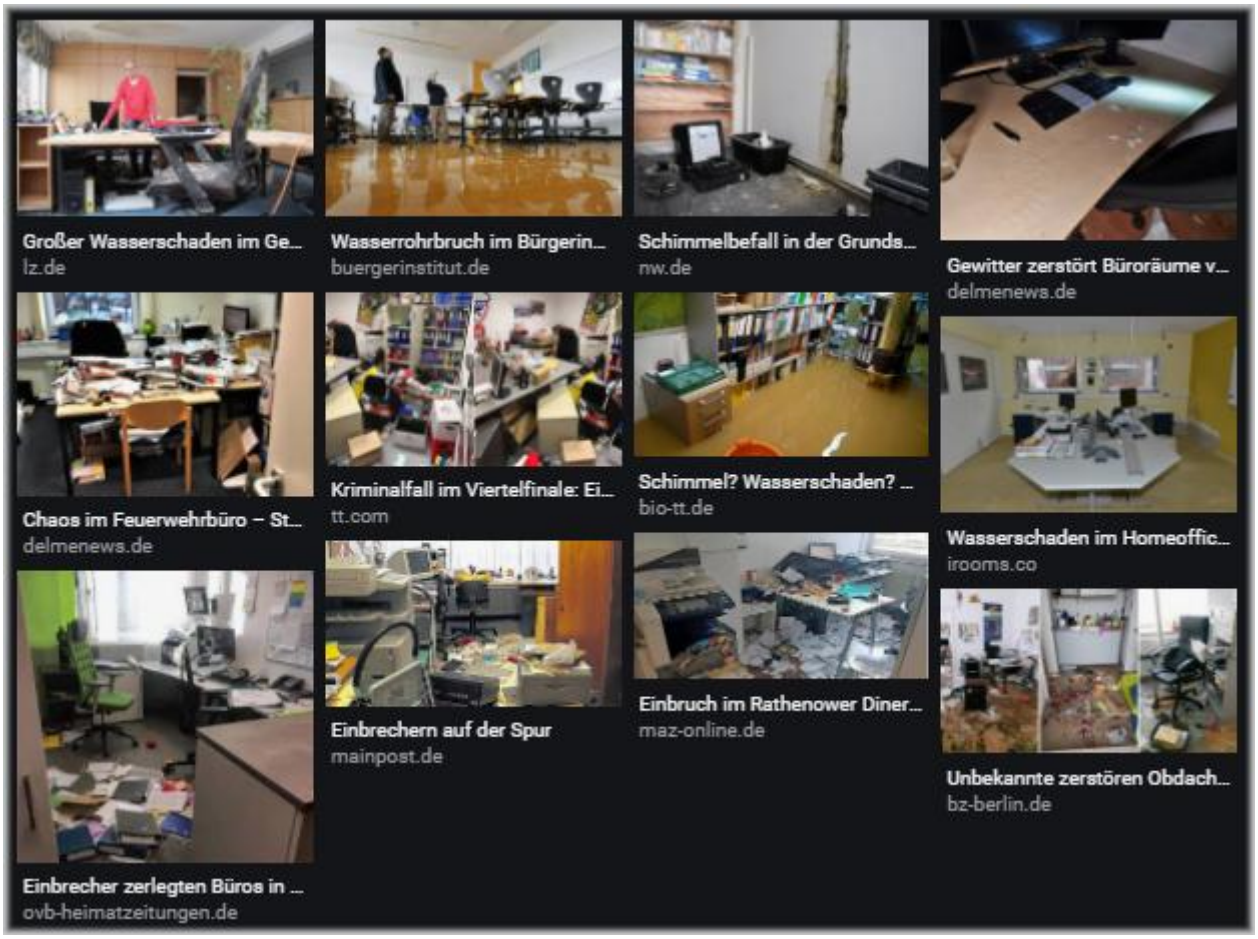
www.kritis.bund.de › Publikationen › Sektorspezifisch

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, daß Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluß, mechanische Beschädigung, Rost etc.).

Besonders wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.



Probleme können außerdem durch Frost entstehen. Beispielsweise können Rohre in frostgefährdeten Bereichen undicht werden, wenn darin Wasser bei anhaltendem Frost stillsteht. Auch eine vorhandene Wärmedämmung wird mit der Zeit vom Frost überwunden.

Technische Voraussetzungen

DIN 2460 Stahlrohre und Formstücke für Wasserleitungen – zu den Anforderungen an Wasserrohre aus Stahl (Haustechnik)
EN 1916 Stahlbetonrohr, EN 1917 Schachtringe und Konen, in deren nationalen Übernahmen und spezifischen Ergänzungen – zu den Anforderungen an die Haltbarkeit von Wasserleitungen aus Betonfertigteilen (Hauptwasserleitungen)

Informationen für Geschäftsleitungen

Piktogramm : animationfactory

Unter Naturkatastrophen werden natürliche Veränderungen verstanden, die verheerende Auswirkungen auf Menschen und Infrastrukturen haben.

Ursachen für eine Naturkatastrophe können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Starkregen, Hagel, Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone. Je nach Standort der Institution ist diese den Risiken durch die verschiedenen Arten von Naturkatastrophen unterschiedlich stark ausgesetzt.

Unabhängig von der Art der Naturkatastrophe besteht auch in nicht unmittelbar betroffenen Gebieten die Gefahr, daß Versorgungseinrichtungen, Kommunikationsverbindungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden.

Besonders der Ausfall zentraler Einrichtungen der Gebäudeversorgung, wie z. B. Hauptverteiler für Strom, Telefon oder Daten kann sehr hohe Schäden nach sich ziehen.

Betriebs- und Service-Personal kann aufgrund von großflächig eingerichteten Sperrbereichen der Zutritt zur Infrastruktur verwehrt werden.

Literatur

Internationale Forschungsgesellschaft Interpraevent (Hrsg.): Alpine Naturkatastrophen – Lawinen, Muren, Felsstürze, Hochwasser. Leopold Stocker, Graz 2009 (online)
Nicolai Hannig: Kalkulierte Gefahren. Naturkatastrophen und Vorsorge seit 1800. Wallstein, Göttingen 2019.
Gerrit Jasper Schenk (Hrsg.): Katastrophen. Vom Untergang Pompejis bis zum Klimawandel. Thorbecke, Ostfildern 2009.
Trevor Day: Faszination Naturkräfte. Eine eindrucksvolle Reise um die Erde. Dorling Kindersley Verlag, München 2002, ISBN 3-8310-0268-1.
Michael Matheus, Gabriella Piccinni, Giuliano Pinto, Gian Maria Varanini (Hrsg.): Le calamità ambientali nel tardo medioevo europeo: realtà, percezioni, reazioni, Atti del XII convegno del Centro di Studi sulla civiltà del tardo medioevo, S. Miniato 31 maggio – 2 giugno 2008. (Collana di Studi e Ricerche 12), Florenz 2010.
Lee Davis: Das große Lexikon der Naturkatastrophen. Verlag für Sammler, Graz 2003, ISBN 978-3-85365-199-5.

Informationen für Geschäftsleitungen

Bild : animationfactory

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen mit dem Ziel, dem Opfer dadurch Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter, punktuell manipuliert werden, um Betriebsstörungen hervorzurufen.

Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

Im Folgenden werden die vorhandenen Schutz- und Abhilfemaßnahmen haustechnischer Natur gegen Sabotage durch Nicht-Hausangehörige beschrieben.

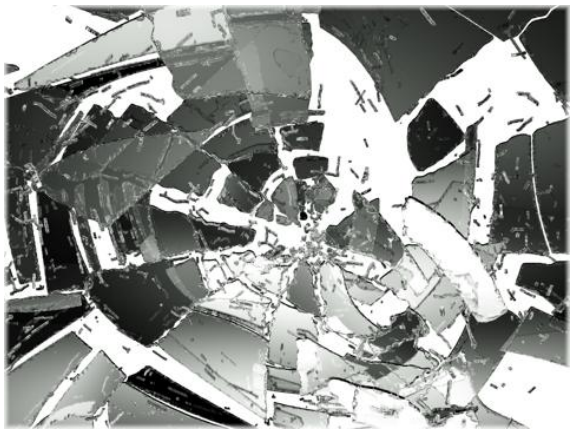


Bild : animationfactory

Sabotage der Datentechnik

→siehe Abschnitt „Risikoanalyse Datentechnik → Angriffe auf die Systeme von extern“

Sabotage via Mitarbeiter / Social Engineering

→siehe Abschnitt „Risikoanalyse Datentechnik → Angriffe auf die Systeme von intern“

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Aus wirtschaftlichen Gründen ist es oftmals ratsam, statt einen Serverraum oder ein Rechenzentrum neu zu bauen, die bestehenden Fläche der vorhandenen IT-Räume durch die Integration benachbarter Flächen zu erweitern. Solche Flächenerweiterungen haben oftmals erhebliche Eingriffe in die bestehende Bauwerksstruktur zur Folge, weil Wände verändert, entfernt oder auch neu gebaut werden müssen. Weiterhin sind die Erweiterungsflächen mit der entsprechenden Infrastruktur (Doppelboden, Elektroversorgung, Klimatisierung, Sicherheitstechnik, etc.) auszustatten, so daß auch hier Arbeiten massiven Ausmaßes anfallen können.

Neben dem Staubschutz ist bei Umbaumaßnahmen sicherzustellen, daß die weiterbetriebene IT ausreichend gekühlt wird. Bei Luftkühlung ist die zusätzliche Staubbelastung durch die Umbaumaßnahmen zu berücksichtigen.

Um die Geschäftstätigkeit der Institution nicht einzuschränken, ist es häufig notwendig, die bestehende IT-Infrastruktur während der Bauarbeiten weiter zu betreiben. Gleichzeitig sollen die Baumaßnahmen durch den laufenden IT-Betrieb möglichst nicht eingeschränkt oder Auflagen unterworfen werden, damit sich die Kosten nicht über das erforderliche Maß hinaus erhöhen.

Zunächst ist planerisch und durch vorbereitende Änderungen der Infrastruktur sicher zu stellen, daß die unterstützende Technik wie beispielsweise Stromversorgung, Klimatechnik, überwachende und alarmierende Technik, durch die Baumaßnahmen nicht beeinträchtigt wird und weiter funktionsfähig bleibt.

Anschließend ist der betroffene Bereich, in dem die IT betrieben wird, vor Verunreinigung, aber auch vor unbefugtem Zutritt zu bewahren. Gleichzeitig sollte die Baustelle nicht unnötig behindert werden.

Die Einhaltung von geltenden Vorschriften wie beispielsweise die Berufsgenossenschaftliche Regel für Sicherheit und Gesundheit bei der Arbeit BGR 217 "Umgang mit mineralischem Staub" oder die Technische Regel für Gefahrstoffe TRGS 500 "Schutzmaßnahmen Mindeststandards" sollte regelmäßig vom Auftraggeber oder dem von ihm eingesetzten Sicherheits- und Gesundheitsschutzkoordinator kontrolliert werden.

Zum Abschluß der Bauarbeiten ist eine Bau-Feinreinigung durchzuführen. Falls die nicht durch eigene Arbeitskräfte durchgeführt wird, ist sie explizit in die Ausschreibung aufzunehmen, da sie über die in der VOB (Vergabe- und Vertragsordnung für Bauleistungen) definierte Baureinigung durch Auftragnehmer hinausgeht.

Informationen für Geschäftsleitungen

Bild : animationfactory

Einbruchmeldeanlagen (EMA) sind Gefahrenmeldeanlagen (GMA), die dem automatischen Überwachen von Gegenständen auf unbefugte Wegnahme sowie von Flächen und Räumen auf unbefugtes Eindringen dienen. Nach VDE 0833 werden Einbruchmeldeanlagen (EMA) und Überfallmeldeanlagen (ÜMA) zusammen betrachtet. Das ist praxisorientiert, denn selbst kleine EMA haben auch die Überfallmeldelinien angeschlossen.

Die Größenklassen sind aufgeteilt in

- kleine EMA mit ca. 4 Meldelinien
- mittlere EMA mit 4 - 12 Meldelinien und
- große EMA mit 100 und mehr Meldelinien.

"Einbruchmeldesysteme mit einer Fernalarmierung direkt zur Polizei sind am erfolgreichsten in der Täterüberführung."

Das ist das Ergebnis der Auswertung einer Statistik des Landeskriminalamtes Bayern.

In 67,6 % der Fälle mit unbemerkbaren Fernalarmsystemen („Stiller Alarm“) konnten die Täter festgenommen werden.

Im Gegensatz dazu wirkt das zusätzliche Installieren eines akustischen oder optischen Alarmsignals auf 56,8 % der Täter abschreckend.

Systeme, die nur örtlich Alarm geben ließen die Festnahmen auf 18,3 % zurückgehen.

Bei der Planung, Projektierung, Installation und Wartung sind insbesondere zu beachten

DIN EN 50131-1; VDE 0830-2-1:2010-02 Alarmanlagen – Einbruch- und Überfallmeldeanlagen[4]
DIN VDE 0833-1 Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 1: Allgemeine Festlegungen
DIN VDE 0833-3 Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 3: Festlegungen für Einbruch- und Überfallmeldeanlagen
VdS 2311 Einbruchmeldeanlagen, Planung und EinbauÜEA-Richtlinie bei Anlagen mit Anschluss an die Polizei

Literatur

Hans-Joachim Geist: Die erfolgreiche Montage einer Einbruch-Melde-Anlage, Elektor-Verlag 1999, ISBN 3895760803
Adam Merschbacher: Sicherheitsanalyse für Haushalte, VdS-Verlag 2002, ISBN 3936050031
Gilles Vernet: Alarmanlagen. Konzeption und Aufbau mit handelsüblichen Komponenten, Elektor-Verlag 2002, ISBN 3895760137
Bodo Wollny: Alarmanlagen, Pflaum 2003, ISBN 3790507776
Hans-Joachim Geist: Bei Einbruch ALARM. Per Kabel, Funk und Satellit, Elektor-Verlag 2003, ISBN 3895761338
Hans-Werner Bastian: Sicherheits-Check für Haus und Wohnung. Schutz für Einbruch, Brand und Wasserschaden, Eccomedia 2003, ISBN 393678213X
Adam Merschbacher: Sicherheitsanalyse für Gewerbebetriebe, VdS-Verlag 2003, ISBN 393605004X
Bodo Wollny: Alarmanlagen. Planung, Komponenten, Installation., Pflaum 2003, ISBN 3790509035
Jascha Schmitz: Ihr-sicheres.Haus – Der Ratgeber zu Alarmsystemen, Brandschutz und Zugangssicherung, kostenloses eBook (38 Seiten)
Hans-Joachim Geist: *Die erfolgreiche Montage einer Einbruch-Melde-Anlage*, Elektor-Verlag 1999, ISBN 3895760803

Informationen für Geschäftsleitungen

Bild : animationfactory

Der Kundenkontakt und die Arbeit mit Ratsuchenden und Leistungsberechtigten in Behörden wird immer häufiger durch Konflikte belastet. Die Auswertung von Unfallmeldungen des Bundes verwiesen auf teilweise extreme Formen von Übergriffen, bis hin zu Bedrohungen mit Messern, Äxten und Schußwaffen.

"Übergriffe von Kunden auf Beschäftigte in Behörden nehmen seit Jahren zu. So stieg die Zahl der meldepflichtigen Arbeitsunfälle aufgrund aggressiver Übergriffe in den vergangenen Jahren kontinuierlich an. Im Jahr 2010 wurden 7.228 meldepflichtige Arbeitsunfälle durch Gewalt betriebsfremder Personen verursacht."
(Quelle : DGUV).

Diese Gewalt am Arbeitsplatz umfaßt verbale, physische oder psychische Angriffe auf Beschäftigte in Situationen, die in Bezug zu ihrer Arbeit stehen und die als Folge ihre Gesundheit, ihre Sicherheit oder ihr Wohlbefinden beeinträchtigen.

Die Formen der Gewalt sind vielfältig :
- bewußt unhöfliches oder unangepaßtes Verhalten
- verbalisierte Gewalt (auch Einschüchtern oder Beleidigen)
- Gewalt gegen Sachen (absichtliches Verschmutzen, Beschädigen oder Randalieren)
- indirekte Gewalt (Drohung/Nötigung)
- körperliche Übergriffe

Risikofaktoren in der Person des Gegenübers können beispielhaft sein :
- generelle Konfliktbereitschaft oder Aggressivität
- Gewalt als gelerntes Muster zur Lösung von Konflikten (z.B. EU-Osterweiterung)
- Mißverständnisse oder Kommunikationsprobleme/Sprachbarrieren
- mangelnde Konfliktfähigkeit oder geringe Frustrationstoleranz
- wirtschaftliche oder familiäre Probleme bzw. Existenzängste
- falsche Erwartungen bzw. Fehleinschätzungen bezüglich der Dienstleistung
- psychische Erkrankungen
- Alkohol- bzw. Drogeneinfluß
- keine Angst vor Repressionen oder Konsequenzen
- Einstellungen und Werte (kulturelle Hintergründe)
- gruppendynamische Zwänge

Literatur

Britta Bannenberg: AMOK Ursachen erkennen – Warnsignale verstehen – Katastrophen verhindern. Gütersloher Verlagshaus, 2010, ISBN 978-3-579-06873-2

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Eine Brandmeldeanlage (**BMA**) ist eine Gefahrenmeldeanlage aus dem Bereich des vorbeugenden Brandschutzes, die Ereignisse von verschiedenen Brandmeldern empfängt, auswertet und dann reagiert.

Als Reaktion können verschiedene technische Einrichtungen angesteuert werden, z. B. :

- Weiterleitung einer Brandmeldung an die ständig besetzte Leitstelle zur Alarmierung der örtlichen Feuerwehr;
- Auslösung einer internen Alarmierung, um vor der Weiterleitung zur Feuerwehr kontrollieren zu können, ob ein Täusch- oder Fehlalarm vorliegt;
- Auslösung einer Alarmierung zur Räumung eines Objektes;
- Öffnen von Rauchableitungseinrichtungen;
- Ansteuerung von Aufzügen;
- Schließen von Feuerschutzabschlüssen;
- Auslösung einer Objektlöschanlage, z. B. CO2-Löschanlage.

Es gelten die folgenden verbindlichen Richtlinien :

- VDE 0800 : Bestimmungen für Fernmeldeanlagen*
- DIN 57833, VDE 0833 : Gefahrenmeldeanlagen*
  Teil 1 Allgemeine Festlegung
  Teil 2 Festlegungen für Brandmeldeanlagen (BMA)
- DIN EN 54 : Brandmeldeanlagen (Europanorm)*
- DIN 14675 : Brandmeldeanlagen; Aufbau*
- DIN 14661 : Feuerwehr-Bedienfeld für Brandmeldeanlagen*
- DIN 14662 : Feuerwehr-Anzeige-Tableau*
- DIN 4066 : Hinweisschilder für die Feuerwehr*
- DIN 33 404-3 : Gefahrensignale für Arbeitsstätten*
- VdS-Richtlinie 2095 : Planung und Einbau von Brandmeldeanlagen*
- VdS-Richtlinie 2105 : Feuerwehr-Schlüssel-Depot (FSD)*
- Richtlinie über brandschutztechnische Anforderungen an Leitungsanlagen*

* in der jeweils gültigen Fassung

Brandmeldeanlagen müssen durch eine ausreichende Instandhaltung betriebssicher gehalten werden. Entsprechende schriftliche Bestätigungen (Wartungsvertrag, Errichterbestätigung der BMZ und des Leitungsnetzes nach DIN 14675 und VDE 0833) müssen spätestens bei der Abnahme der → Integrierten Leitstelle Fürstenfeldbruck (ILS) über den Betreiber vorgelegt werden.

Literatur

Frieder Kircher, Rainer Sonntag: Die Roten Hefte, Heft 25 – Vorbeugender Brandschutz. 1. Auflage. Kohlhammer, Stuttgart 2014, ISBN 978-3-17-016996-8.

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Der Begriff „Hausalarmanlage“ hat sich unter Fachleuten inzwischen zu einem Reizwort entwickelt.

Das Problem besteht darin, daß Hausalarmanlagen gerne dort gefordert werden, wo man ein bißchen Brandüberwachung und eine halbwegs brauchbare Alarmierung von Personen haben möchte, den Einbau einer Brandmeldeanlage aber scheut

Unter **Hausalarm** versteht man akustische und optische Signale *innerhalb* eines Gebäudes, die einen Alarm anzeigen. Als akustische Signalgeber werden Sirenen, Glocken und Signalhupen eingesetzt.

Falls bereits akustische Signalgeber im Gebäude verbaut sind, so werden diese häufig für den Hausalarm mitverwendet. Das Alarmsignal muß sich hierbei von dem normalen Signal deutlich unterscheiden.

Ein Beispiel sind optische Signalgeber wie Blitzleuchten, Blinklichter und Rundumlichter zum Einsatz.

Literatur

DIN 14675 – Norm für den fachgerechten Aufbau und Betrieb einer Brandmeldeanlage, die eine direkte Alarmierung der Feuerwehr auslöst

Einsatzalarm – Alarm, der direkt zur Alarmierung von Einsatzkräften führt

Siegfried Volz: Die Roten Hefte, Heft 62 – Brandschutzerziehung in Schulen. 2., überarb. Auflage. Kohlhammer, Stuttgart 1997, ISBN 3-17-014539-8.

Informationen für Geschäftsleitungen

Piktogramm : wikipedia

Als Brandmelder werden technische Geräte oder Anlagen zum Auslösen eines Alarms im Falle eines Brandes in Wohnungen, öffentlichen Einrichtungen, Verkehrsmitteln oder Industrieanlagen bezeichnet.

Dabei wird unterschieden zwischen automatischen Brandmeldern, die den Brand anhand physikalischer Eigenschaften erkennen, und nicht-automatischen Brandmeldern, die von Hand betätigt werden müssen.

Sinn des Brandalarms ist das Warnen von Personen innerhalb eines Gebäudes, das Einleiten von Maßnahmen zur Brandbekämpfung und zum Sach- und Personenschutz meist die Alarmierung von zuständigem Sicherheitspersonal oder der Feuerwehr.

Rauchwarnmelder haben eine Sirene und ggf. zusätzliche Signalgeräte eingebaut. Die harmonisierte Europäische Norm EN 14604, in Deutschland beispielsweise als DIN-Norm DIN EN 14604 veröffentlicht, legt Anforderungen, Prüfverfahren und Montagetechniken für Rauchwarnmelder fest.

In Deutschland gilt ergänzend die DIN 14676, die im Unterschied zur EN 14604 nicht auf die Montage, aber beispielsweise auf die Kopplung mehrerer Rauchwarnmelder eingeht.

Gemäß dieser Produktnorm müssen Rauchwarnmelder einige Mindestleistungsmerkmale vorweisen :

- die Schalldruckpegel eines Rauchwarnmelders muß mindestens 85 dB(A) in 3 m Entfernung betragen. Es wird auf die Möglichkeit etwaiger Hörschäden hingewiesen.
- das Warnsignal muß mindestens 30 Tage vorher wiederkehrend darauf hinweisen, daß die Batterie ausgetauscht werden muß;
- eine Funktionsüberprüfung des Melders muß möglich sein, beispielsweise mittels eines Testknopfes;
- Rauch muß von allen Seiten in die Rauchmeßkammer eindringen können, die Einlaßöffnungen der Rauchkammer dürfen nicht größer als 1,3 mm sein und müssen einen Schutz vor Insekten und Verschmutzung vorweisen.

Zusätzlich dürfen in der EU nur Rauchwarnmelder verkauft werden, die das Symbol für die CE-Kennzeichnung sowie die Nummer der EU-Konformitätserklärung angegeben.

Literatur

Wolfgang J. Friedl (Hrsg.): *Fehlalarme minimieren – Brand- und Einbruchmeldeanlagen – Brandlöschsysteme*. VDE Verlag, Berlin 1994, ISBN 3-8007-1938-X.

Informationen für Geschäftsleitungen

Piktogramme : wikipedia

Kohlenmonoxid - kurz CO - ist ein besonders giftiges Gas.

Kohlenstoffmonoxid ist ein farb-, geruch- und geschmackloses sowie toxisches Gas. Es entsteht unter anderem bei der unvollständigen Verbrennung von kohlenstoffhaltigen Stoffen bei unzureichender Sauerstoffzufuhr.

Das Gas ist giftig, da es viel stärker an Hämoglobin bindet als Sauerstoff und so den Sauerstofftransport durch das Blut unterbindet.

Die Kohlenstoffmonoxidintoxikation ist häufig ein Teilvorgang der →Rauchgasvergiftung

Es entsteht also überall dort, wo etwas verbrannt wird. Solange ein Abzug der Gase gewährleistet ist, besteht keine Gefahr.

Können die Brandgase nicht richtig entweichen – etwa, weil ein Schwellbrand in einem **Drucker** oder **Kopiergerät** in einem schlecht gelüfteten oder geschlossenen Raum Kunststoff schmilzt und / oder verkohlt - wird es allerdings schnell und im schlimmsten Fall nachhaltig gefährlich.

Betritt ein Mitarbeiter den Raum können schon wenige Atemzüge tödlich sein !

Damit dieser Fall nicht eintritt, sollen CO-Warngeräte Alarm schlagen.

Sie melden sich, sobald die Menge an Verbrennungsgasen - insbesondere Kohlenmonoxid - in der Raumluft über einen festen Grenzwert steigt oder Phenole aus Kunststoffen ausgasen.

Informationen für Geschäftsleitungen

Bewegungsüberwachung mit optischen Bewegungsmeldern (nicht-video-basiert) ist die Überwachung von Orten durch optisch-elektronische (IrDA, PIR, Ultraschall Bewegungsmelder).

Videoüberwachung mit optischen Bewegungsmeldern ist die Beobachtung von Orten durch optisch-elektronische Einrichtungen bzw. optischen Raumüberwachungsanlagen (Videoüberwachungsanlage) mit einem Auswertesystem (Fangzonen-Detektion, siehe unten).

Optische Meldesysteme sind Monitore (Echtzeit) die durch einen eingewiesenen Benutzer „live“ beobachtet und ausgewertet werden.

Optische Meldesysteme sind auch Blitzleuchten oder Signallampen (z. B. im Ampelprinzip) die dazu dienen Zustände an Geräten, Räumen oder Maschinen zu signalisieren.

Häufig steht diese Form der Überwachung in Verbindung mit der Aufzeichnung und Analyse der gewonnenen audiovisuellen Daten. Die Daten werden häufig digital gespeichert und die Bilder können durch Software analysiert werden.

BayDSG Art. 21a

Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist :

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder

2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen. Es dürfen keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

(1) Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(2) Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

Informationen für Geschäftsleitungen

Akustische Alarmmeldungen und -geräte dienen in der Regel zur Unterstützung visueller Alarme bzw. zur Verständigung größerer Benutzergruppen.

Es ist zu differenzieren zwischen **lokalen** akustischen Alarmen die von Geräten in einzelnen Räumen abgegeben werden und globalen Alarmen wie z. B. Rauch- und Brandwarnmeldern.

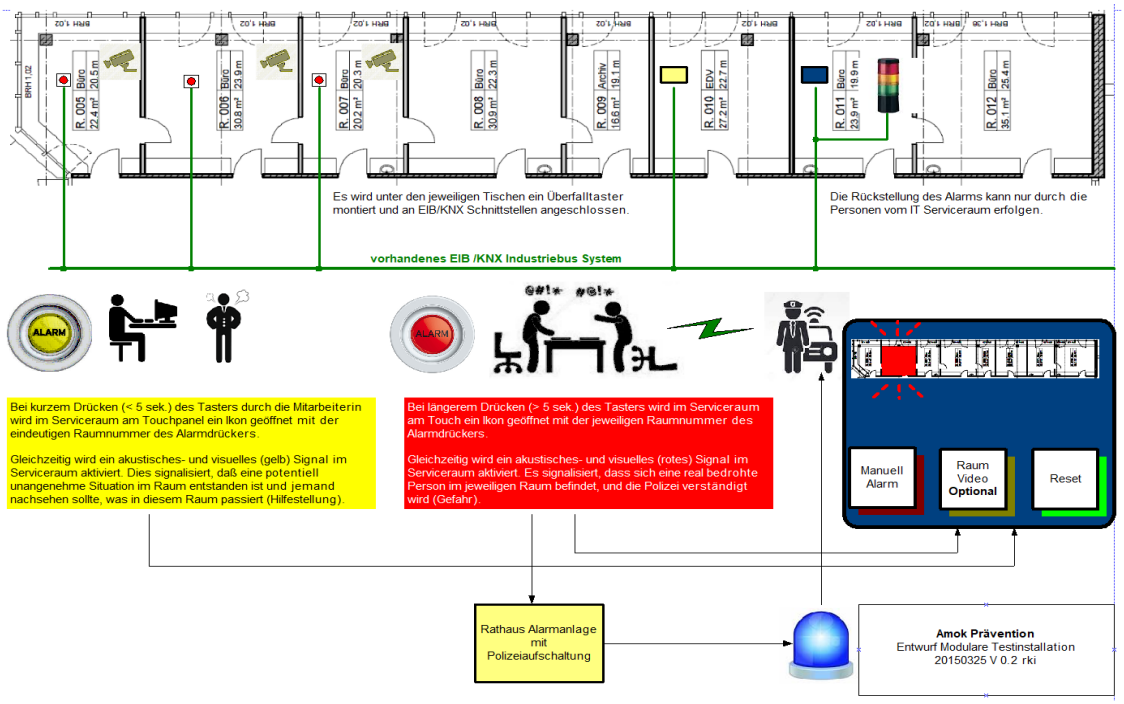
Lokale akustische Alarme, die **von einzelnen Geräten** abgegeben werden, erfordern einen Eingriff durch den jeweiligen Benutzer.

Dieser muß über die entsprechende Ursache informiert und in die darauf zu erfolgende Reaktion / Abhilfemaßnahmen eingewiesen sein.

Lokale akustische Alarme, die in einem **Raum** von einem Warnmeldesystem abgegeben werden (Rauchwarnmelder, Giftgasmelder, Wasserstandsmelder) erfordern eine Reaktion von den Verantwortlichen für diesen Raum.

Die passende Notfall-Meldekette muß angestoßen werden.

Globale akustische Alarme (Sirene) erfordern einen Notfallplan Fachbereiche und alle davon betroffenen Personen müssen über die daraus abzuleitenden Maßnahmen informiert sein. Das folgende Bild zeigt eine durch id-newmedia realisierte Notfall-Meldeanlage :



Informationen für Geschäftsleitungen

Videoüberwachung ist die Beobachtung von Orten durch optisch-elektronische Einrichtungen bzw. optischen Raumüberwachungsanlagen (Videoüberwachungsanlage) die durch einen eingewiesenen Benutzer „live“ beobachtet und ausgewertet werden.

WEB-Cams sind Videobeobachtungseinrichtungen die es einem freigegebenen, größeren Benutzerkreis erlauben die Darstellung des Beobachtungsraumes zu verfolgen.

Warneinrichtungen Gebäude & Haustechnik
Videoüberwachung mit Aufzeichnung

Informationen für Geschäftsleitungen

Grundsätzlich muß bei der **Videoüberwachung mit Aufzeichnung** zwischen der Überwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Bereichen (§ 6b Bundesdatenschutzgesetz BDSG), Videoüberwachungen von Beschäftigten nach § 32 Abs. 1 BDSG und der sonstigen Videoüberwachung in nicht-öffentlich zugänglichen Räumen gemäß § 28 BDSG unterschieden werden.

BayDSG Art. 21a

(1)Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist :

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder

2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen. Es dürfen keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

(2)Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3)Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

Informationen für Geschäftsleitungen

Hintergrund

KNX ist ein Feldbus zur Gebäudeautomation. Technisch ist KNX eine Weiterentwicklung des EIB durch Erweiterung um Konfigurationsmechanismen und Übertragungsmedien. KNX ist mit EIB kompatibel.

In herkömmlichen Elektroinstallationen sind die Steuerfunktionen mit der Energieverteilung fest verbunden und erfolgen mittels Parallel- oder Reihenschaltung.

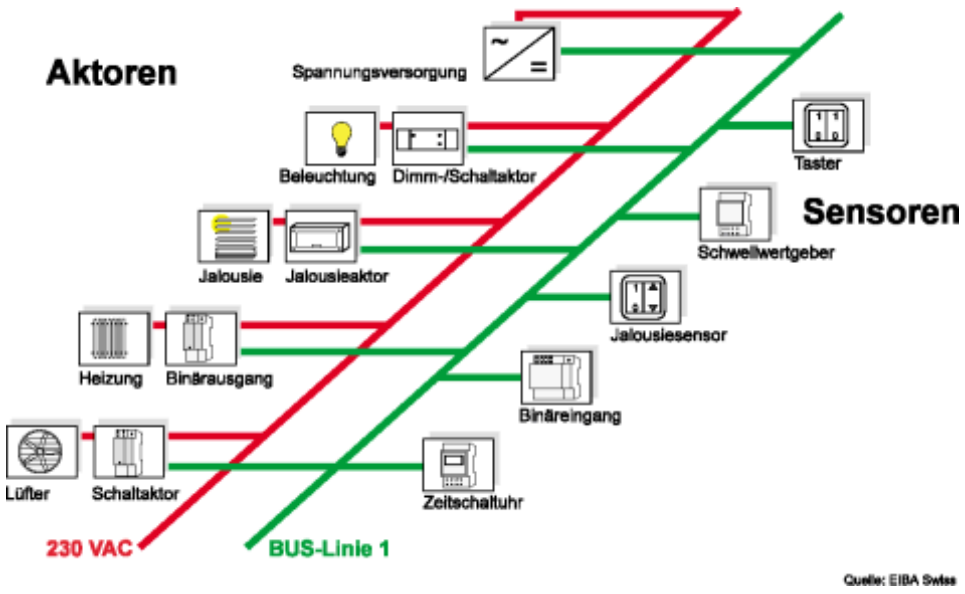
Nachträgliche Schaltungsänderungen sind daher schwierig umzusetzen. Auch übergeordnete Steuerfunktionen wie ein zentrales Schalten aller Beleuchtungsstromkreise in einem Gebäude können nur mit hohem Aufwand realisiert werden.

Arbeitsweise

Zwischen dem Verbraucher (zum Beispiel Elektrogerät, Lampe, Fensteröffner) und der Netzspannung wird ein Steuerungsgerät, „**Aktor**“ genannt, eingebaut. Der Aktor ist an den KNX-Bus angeschlossen und erhält von diesem Daten in Form von Telegrammen.

Diese Telegramme stammen entweder direkt von einem **Sensor** (zum Beispiel Schalter, Helligkeits-, Temperatur- oder CO2-Konzentrations-Sensor) oder aber indirekt von einem Computer, welcher etwa zeitgesteuerte Schaltungen regelt und sonstige Auswertungen von Sensordaten je nach Programmierung übernimmt und Aktoren entsprechend ansteuert.

Erhält ein Aktor den Befehl, dem Verbraucher Spannung zuzuführen, so schaltet er die Netzspannung an das Gerät durch.



Informationen für Geschäftsleitungen

Verantwortliche Stelle

Haustechnik

Art der Absicherung / Bereich

Ausgewiesene Bereiche

Wetterstation, z. B. auf dem Dach

Beleuchtung im den Gängen und Foyers

Hausalarm (z.B. in allen Fluren) / Ansteuerung von Blitzlichtern und Sirenen

Rauch- und Gassensoren (z.B. Steigschächte)

Wasserstandsmelder (z.B. Untergeschosse, Datensicherungsräume …)

Panikmelder, z. B. in den Büros

zukünftige Anwendungen

Literatur

Stefan Heinle: Heimautomation mit KNX, DALI, 1-Wire und Co. - Das umfassende Handbuch. Rheinwerk Verlag, Bonn 2015, ISBN 978-3-8362-3461-0.
Frank Völkel: Smart Home mit KNX, selbst planen und installieren. Franzis, München 2011, ISBN 978-3-7723-4387-2.
Rainer Scherg: EIB/KNX-Anlagen - planen, installieren und visualisieren. Vogel, Würzburg 2008, ISBN 978-3-8343-3125-0.
Willy Meyer: KNX/EIB Engineering Tool Software. Hüthig & Pflaum, München & Heidelberg 2007, ISBN 978-3-8101-0266-9.
Karlheinz Frank: EIB/KNX Grundlagen Gebäudesystemtechnik. Huss, Berlin 2008, ISBN 978-3-341-01540-7.

Informationen für Geschäftsleitungen

Hintergrund

Zur optimalen Steuerung und Regelung einer Klimaanlage werden verläßliche Daten über die klimatischen Verhältnisse im Innenraum der IT/EDV Fachräume benötigt :

- Übertemperatur
- Netzausfall oder USV Defekte
- Schmorbrände und Feuer
- Wasserleckagen
- Einbruch und Diebstahl
- Menschliches Fehlverhalten

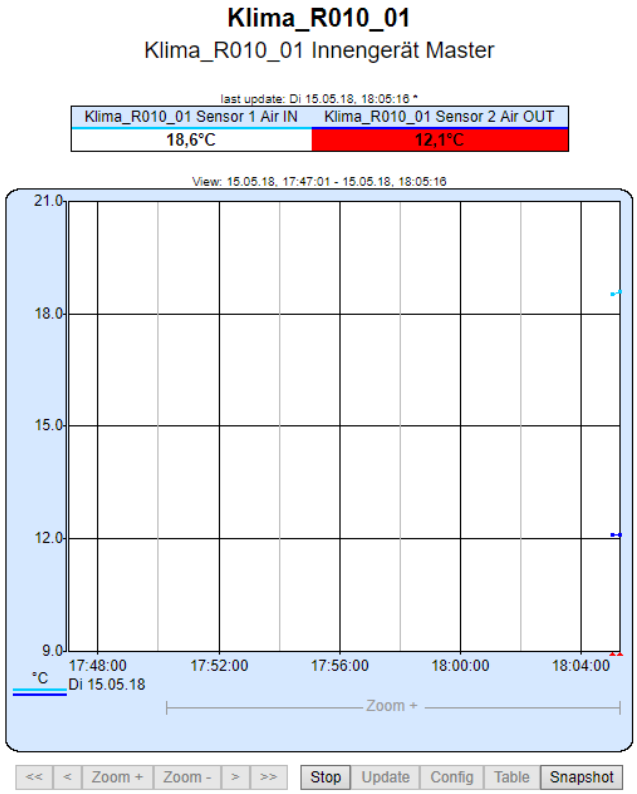


Diagramm : id-newmedia

Bild : animationfactory

Informationen für Geschäftsleitungen

Hintergrund

Eine unterbrechungsfreie Stromversorgung (USV), englisch Uninterruptible Power Supply (UPS), wird eingesetzt, um bei Störungen im Stromnetz die Versorgung kritischer elektrischer Lasten sicherzustellen.

USV-Geräte finden daher vor allem in allen empfindlichen Bereichen wie Krankenhäusern, Leitstellen, modernen Eisenbahn-Stellwerken und Rechenzentren Verwendung, mittlerweile aber ebenso in kleinen Büros (SoHo) oder zu Hause. Sie werden in die Stromzuleitung der zu sichernden Anlagen oder Geräte eingefügt.

Entgegen dem genauen Wortlaut der Bezeichnung kann bei einfachen Ausführungen der USV die Stromversorgung für einen kurzen Zeitraum unterbrochen werden, der von den angeschlossenen Verbrauchern ohne Funktionseinbußen toleriert wird. Normalerweise beträgt dieser Zeitraum aber nur wenige Millisekunden.

Eine batteriegestützte USV besteht aus Akkumulatoren, bei Arbeitsplatz-USV aus Blei-Vlies-Batterien (AGM) oder Blei-Gel-Batterien, bei Leistungs-USVs aus Bleiakkumulatoren (Rechenzentrum Rathaus), Stromrichtern und einer elektronischen Regelung.

Computer in einem Rechenzentrum werden bei einem Stromausfall automatisch heruntergefahren, bevor die Überbrückungszeit abgelaufen ist. Geöffnete Dateien, zum Beispiel sensible Datenbanken, werden so kontrolliert geschlossen, um Datenverlust zu verhindern.

Server und USV kommunizieren zu diesem Zweck standardmäßig über Ethernet bzw. SNMP, vereinzelt aber auch über die Schnittstelle RS-232 oder auch über USB. Über diese Verbindung kann die USV auch überwacht, gesteuert und eingestellt werden.

Identification

UPS Model	9155-10-N-25
UPS Firmware version	INV: 2.56 IFC: 1.20
VA Rating	10000 VA
User-Assigned Name	EATON-R010-USV01
Card's IP Address	172.25.2.20
Firmware Revision	ConnectUPS Web/SNMP Card V4.38

Current Status — Status@aGlance RSS

Overall Status	SYSTEM NORMAL
External Contact #1 Status	Disabled
External Contact #2 Status	Disabled
Remote Temperature *(Degrees C)*	19
Remote Humidity *(%)*	46
Runtime *(minutes)*	105
Last Battery Test Status	2007-05-31 13:44:46 - Passed
Last Logged Events	2018-04-16 08:53:30 ConnectUPS Cold Boot 2018-04-16 08:54:00 Communication with UPS restored 2018-05-13 20:42:49 UPS bypass unavailable

Input

Voltage (L to N) *(VAC)*	222 220 222
Current (L) *(AC Amps)*	5.5 7.1 6.10
Frequency *(Hertz)*	50.0

Output

Voltage Out *(VAC)*	229
Current Out *(AC Amps)*	22.1
Frequency *(Hertz)*	50.0
True Power *(Watts)*	4267
UPS Load *(%)*	51

Bypass

Bypass Status	Normal
Voltage (L to N) *(VAC)*	222

Battery

Die Grundfunktionen von großen USVs umfassen in der Regel alle 24 Stunden einen automatischen Belastungstest, bei dem die Akkumulatoren im laufenden Betrieb mit der angeschlossenen Last entladen werden.

Bei 10-Jahres-Batterien sollten die Akkus spätestens nach acht Jahren, bei 5-Jahres-Batterien sollten die Akkus nach spätestens vier Jahren komplett ausgetauscht werden, um einem Ausfall der USV-Anlage durch eine defekte Batterieanlage vorzubeugen.

Informationen für Geschäftsleitungen

Hintergrund und Beispiel

Die Gemeinde G. betreibt ein Rechenzentrum für die Verwaltung, den Bauhof, das Bürgerbüro im Ortsteil S., die Sozialstation I. sowie vier Grundschulstandorte, einen Realschulzweckverband, ein Regionalmanagement sowie fünf (5) Feuerwehren.

Dieses Rechenzentrum hat eine energetische Leistungsaufnahme (je nach Auslastung) zwischen 6 und 10 kWh.

Dabei entstehen (je nach Auslastung) zwischen 6 und 8 kWh Wärmelasten die abzuführen sind. Diese Abwärme ist vergleichbar mit der Heizleistung die für drei (3) Einfamilienhäuser benötigt würde. Bis 2017 wurde diese Abwärme Sommer wie Winter ins Frei abgeleitet.

Bereits mit der vorhergehenden Generation 2008-2017 trug sich das Rechenzentrum mit dem Gedanken die entstehende Abwärme in das Gebäude rückzuführen und über die Brauchwasseraufheizung im Wärmekreislauf zu nutzen. Die damals in Auftrag gegebene Ingenieurstudie zeigte (bezogen auf die damaligen Primär-Energiekosten) eine Amortisation des Invest nach frühestens zwölf (12) Jahren.

Auf Grund der Notwendigkeit die Klimaanlage im Jahre 2017 völlig neu zu konzipieren wurde der Gedanke der Wärme-Rückführung wieder aufgegriffen und in Planung und Realisierung einbezogen.

Sinnbild Arbeitsweise

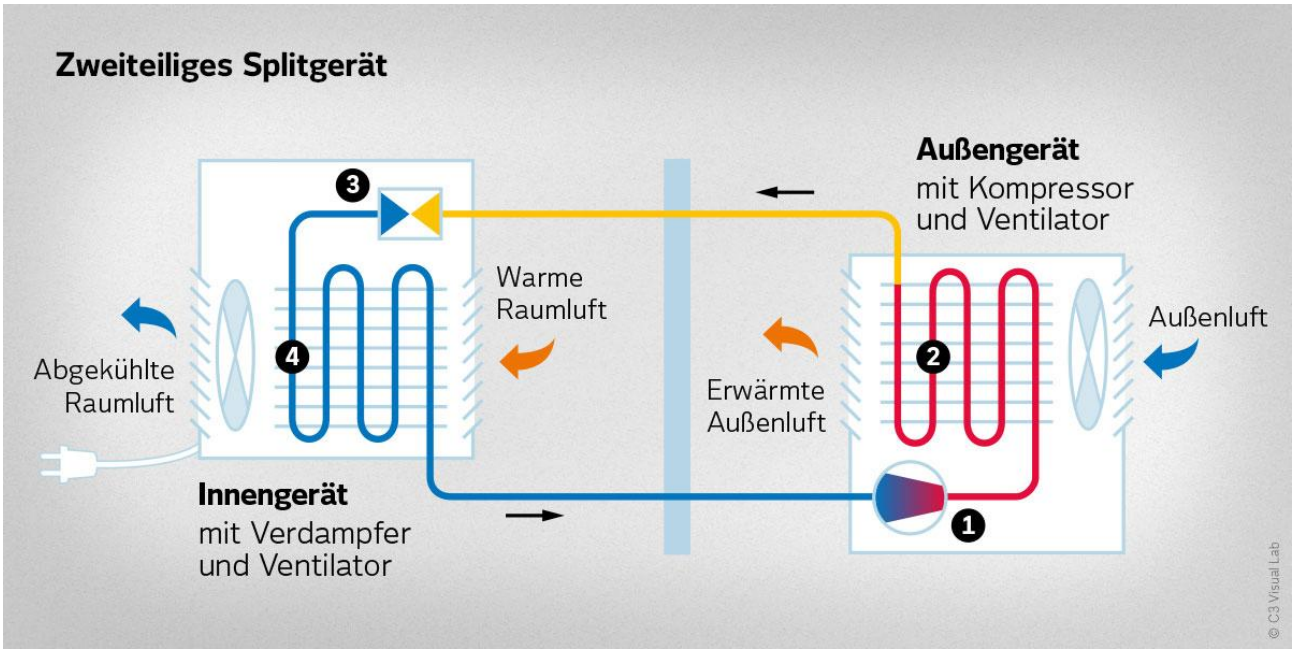
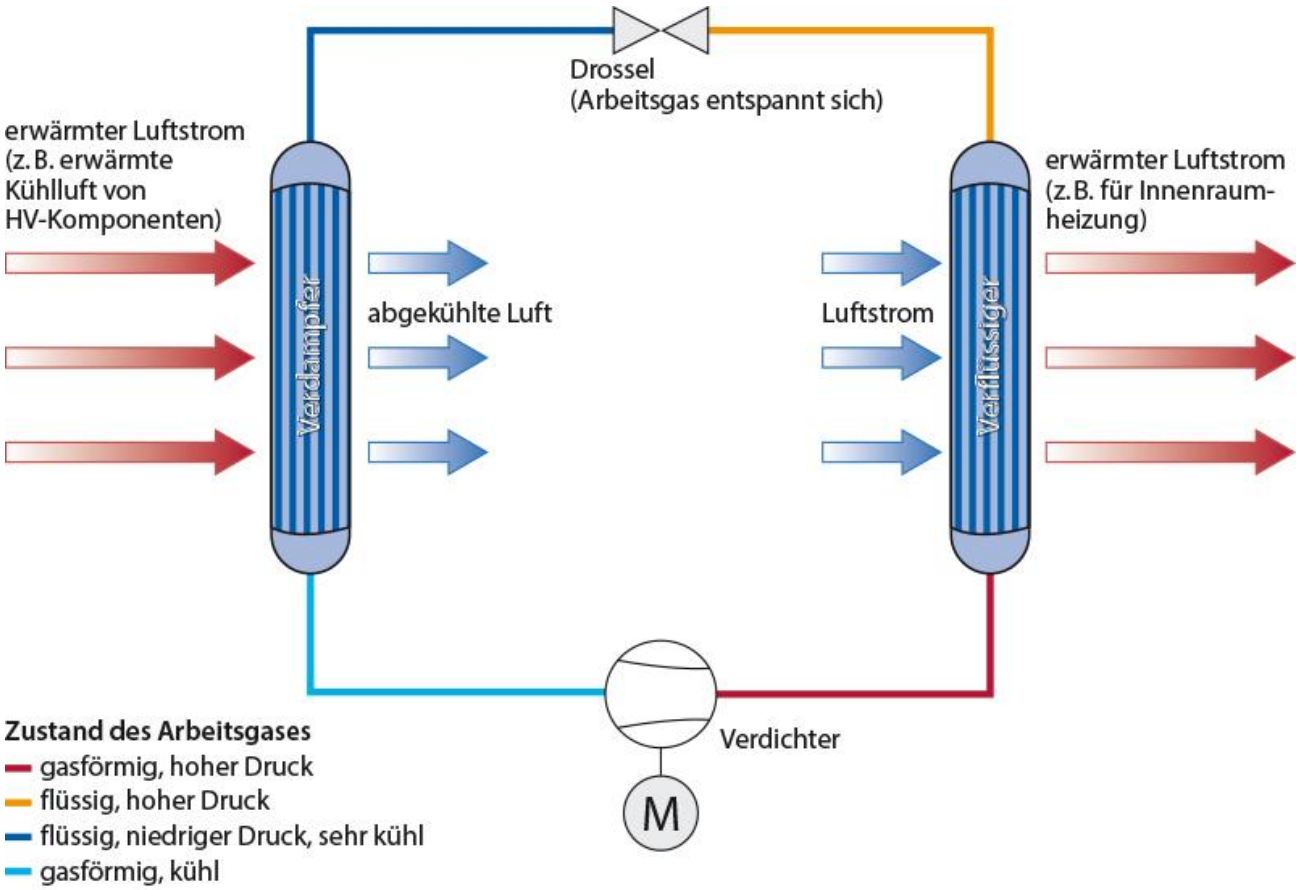


Bild : elife.vattenfall.de

Informationen für Geschäftsleitungen

Generation	(2018 –)	Klimaanlage **mit** Wärmetauscher
Nennleistung	Kühlen 22,4 kW	
	Heizen 25,0 kW	
Betriebswert typisch	8 kW/h	
Abwärme Ableitung	6 kW/h	

Sinnbild Arbeitsweise



Vorteile gegenüber Konzepten vor 2018

- Betrieb in einem günstigen Kennlinienbereich bei typisch < 50% und damit erheblich verbesserter Wirkungsgrad
- dadurch Einsparung an elektrischer Primärenergie
- dadurch ca. 25 kg CO_2 pro Tag vermieden
- dadurch niedriger Eigenenergieverbrauch / Eigenabwärme
- Abwärme wird im Winter zur Beheizung des Gebäudes verwendet
- Ausgleich des schlechten Heizenergiekoeffizienten des Gebäudes
- Leistungsreserven für kommende „heiße“ Sommer

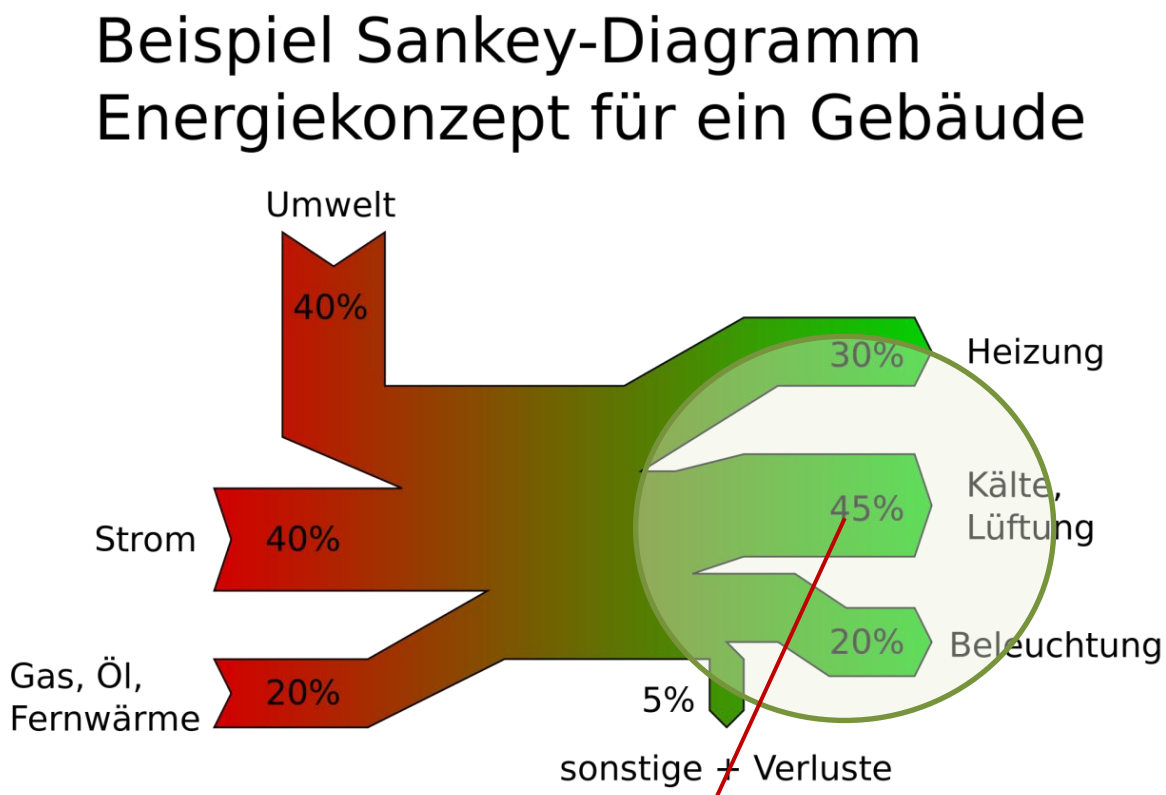
Nachteile

Anschaffungskosten ca. 40% höher wie klassische Kältelösungen

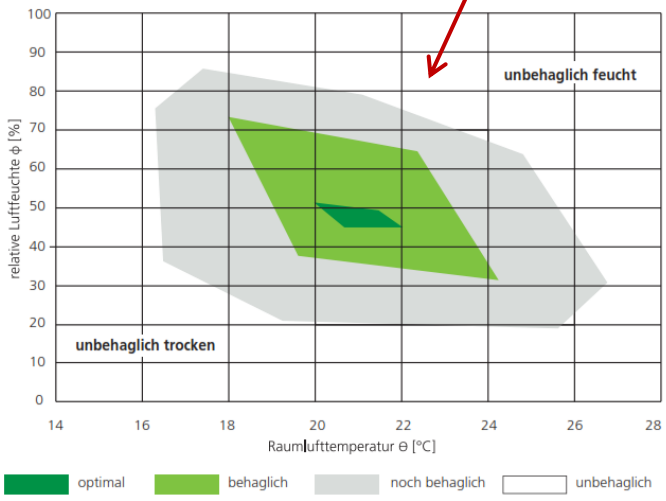
Informationen für Geschäftsleitungen

Wirksamwerden der Verbesserungen durch neue Wärmetauscher-Konzepte

Diagramm



Bilder / Diagramme : org.wikipedia



Informationen für Geschäftsleitungen

Bestandteile des Notfallmanagements sind präventive Maßnahmen zur Notfallvorsorge und Pläne zur Bewältigung von Notfällen und zur Wiederherstellung von Geschäftsprozessen.

Bild : animationfactory

Es sind im Rahmen des Notfallmanagements alle Aspekte der Prozesse zu betrachten, die für die Fortführung im Notfall erforderlich sind.

Notfallplanungen sind durch regelmäßige Übungen auf ihre Anwendbarkeit in der Praxis zu überprüfen.

Literatur

Peter Höbel, Thorsten Hofman: Krisen-Kommunikation. 2., völlig überarbeitete Auflage. Verlagsgesellschaft UVK Konstanz–München. (2014)

Jochen Zschau, Bruni Merz, Eric J. Plate, Johann G. Goldhammer: Vorhersage und Frühwarnung. In: Eric J. Plate, Bruno Merz (Hrsg.):

Naturkatastrophen Ursachen – Auswirkungen – Vorsorge. E. Schweizerbart'sche Verlagsbuchhandlung (Nägele u. Obermiller). Stuttgart. (2001)

Elke M. Green: Bevölkerungsverhalten und Möglichkeiten des Krisenmanagements und Katastrophenmanagements in multikulturellen Gesellschaften. In: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Forschung im Bevölkerungsschutz Band 11. (2010)

Ansgar Thießen (Hrsg.): Handbuch Krisenmanagement. 2. Auflage. Springer Fachmedien, Wiesbaden 2014, ISBN 978-3-658-04292-9.

Michael St. Pierre; Gesine Hofinger; Cornelius Buerschaper: Notfallmanagement, Human Factors und Patientensicherheit in der Akutmedizin. 2. aktualisierte und erweiterte Auflage. Springer-Verlag Heidelberg 2011, ISBN 978-3-642-16880-2

Informationen für Geschäftsleitungen

„Obwohl durch einen Kurzschluß oder unzureichend gekühlte Komponenten in Computerräumen in Sekunden ein Feuer ausbrechen kann, sind viele Serverräume mangelhaft gesichert.

Der einzige hundertprozentige Schutz vor Datenverlust, die redundante Sicherung an einem externen Standort, wird nur von gut zwei Drittel der IT - Unternehmen in Anspruch genommen.

Fast 60 Prozent der internationalen IT - Führungskräfte halten Feuer für die größte Bedrohung ihres Datenmaterials“

Quelle : Storage Index , eine halbjährlich Studie von Hitachi Data Systems

Bild : id-newmedia

Informationen für Geschäftsleitungen

Was der Ausfall eines Servers genau kostet, läßt sich nach einer recht einfachen Formel berechnen : Ausfallkosten = (To + Td) x (Rp + Lr)

Bild : animationfactory

To steht für die tatsächliche Dauer des Ausfalls in Zeiteinheiten.

Td bezeichnet die so genannte Delta Time. Darunter versteht man die seit dem letzten Backup verstrichenen Zeiteinheiten.

Rp Rate of Personel bildet Kosten ab, die durch die untätig herumsitzende Belegschaft entstehen. Dieser Wert errechnet sich aus den monatlichen Personalkosten des betroffenen Bereichs, geteilt durch die geleisteten Zeiteinheiten.

Lr Lost Revenue schließlich gibt den entgangenen Profit an. Hier nimmt man am besten einen Durchschnittswert aus mehreren Monaten und dividiert ihn wieder durch die betrachteten Zeiteinheiten.

Auf diese Weise läßt sich das Risiko kaufmännisch exakt berechnen, heruntergebrochen auf Tage, Stunden oder Minuten. Daß auf einem physischen Server mehrere virtuelle Maschinen angesiedelt sind, macht die Sache allerdings nicht gerade einfacher. Denn die einzelnen Workloads umfassen ja nicht selten verschiedene Teile des Unternehmens / der Verwaltung. Will man also das Risikopotenzial eines bestimmten Server errechnen, legt man zuerst nach der eben beschriebenen Formel die Ausfallkosten für jeden Workload fest und addiert diese dann.

Berechnung nach Workloads

Die nach Workloads getrennte Risikoabschätzung ist zwar mühsam, aber in mehrfacher Hinsicht hilfreich. Sollen Prozesse von einer physischen Maschine auf eine andere übertragen werden, läßt sich das neue Risikoprofil schnell aus den vorhandenen Modulen errechnen. Außerdem kann man so Konstellationen vermeiden, die eine unnötig hohe Risikoakkumulation auf einem physischen Server bedeuten würden. Addiert man wiederum die Ausfallkosten der einzelnen Server, kommt man schließlich das Gesamtrisiko für einen kompletten Standort.

Daß die Ausfallhäufigkeit in konsolidierten Rechenzentren aufgrund der geringeren Anzahl der in Betrieb befindlichen Komponenten abnimmt, spricht für die Virtualisierung. Für eine Kosten -Nutzen - Abschätzung bei der Anschaffung einer Hochverfügbarkeitslösung ist dieser Faktor aber leider nicht von Belang. Schließlich kann ja auch ein „statistisch sehr unwahrscheinlicher“ Ausfall bereits am nächsten Morgen eintreten.

Informationen für Geschäftsleitungen

Rolle von Datensicherungen („BackUp“)

Betrachtet man die Formel (To + Td) x (Rp + Lr) genauer, zeigt sich deutlich, daß die Art der Datensicherung einen ganz entscheidenden Einfluß auf die Ausfallzeit und die Ausfallkosten hat. So wurden bisher Band - Backups in der Regel einmal pro Nacht gezogen (Differentialsicherung bei Dokumenten und Bildern, Vollsicherung bei Datenbanken und email - Beständen).

Bild : animationfactory

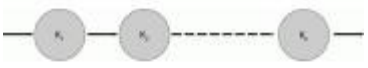
Fällt der Server dann am nächsten Tag um 17 :00 Uhr aus, beträgt der **Td** - Wert bereits mindestens acht Stunden – ein erheblicher Multiplikator, auch wenn ein schneller Support die tatsächliche Ausfallzeit (**To**) gering hält.

Der Personalkosten - Ausfallwert **Rp** wird stark durch moderne und vernetzte Arbeitsweise getrieben. So wird ein ausgefallener Mail - oder Internet - Server schnell die gesamte Belegschaft lahmlegen, insbesondere, wenn Verbindungen zu Außenstellen abreißen. Der entgangene Umsatz **Lr** hängt natürlich stark von der jeweiligen Applikation ab. Besonders teuer wird eine „Downtime“ bei unmittelbar am Verkauf / an finanziell honorierten Dienstleistungen beteiligten Prozessen wie etwa eShops, Warenwirtschaft - Systeme (LIMES) oder Verfahren wie OK.EWO oder H+H.

Auch wenn eine Risikoabschätzung nach dieser relativ einfachen Formel keine statistischen Parameter wie Varianz oder Standardabweichung mit einbezieht, sollten diese Ergebnisse Geschäftsleitung und Kämmerei wachrütteln. Zeigen sie doch, daß auch ein relativ kurzer Ausfall oft viel, viel teurer kommt als ein richtig dimensioniertes Hochverfügbarkeit - System.

Möchte man die Verfügbarkeit eines Gesamtsystems angeben, kennt aber nur die Verfügbarkeit der Einzelkomponenten, kann die Gesamtverfügbarkeit nach den Regeln der Serien- und Parallelschaltung berechnet werden. Abhängige und redundante Komponenten können hierbei in Ersatzschaltbildern dargestellt werden.

Eine **Serienschaltung** verschaltet abhängige Komponenten. Das System ist nur dann verfügbar, wenn alle Einzelkomponenten verfügbar sind. Ein Rechner ist beispielsweise nur dann verfügbar, wenn alle betriebsrelevanten Komponenten wie CPU, Speicher und Netzteil verfügbar sind. Das Ersatzschaltbild für eine Serienschaltung ist in der folgenden Abbildung dargestellt :



Die Gesamtverfügbarkeit eines Systems, das aus in Serienschaltung angeordneten Komponenten besteht, wird durch die Multiplikation der Einzelverfügbarkeiten berechnet.

$$V_{gesamt} = \prod_{i=1}^{n} V_i$$

Informationen für Geschäftsleitungen

Sind die Ausfallzeiten Ni der Komponenten darüber hinaus sehr klein, läßt sich die Gesamtausfallzeit auch als Summe der Ausfallzeiten der Einzelkomponenten angeben.

Die Ausfallrate ist dann die Summe der Ausfallraten der Einzelkomponenten.

Es gilt :

beziehungsweise
wobei (VKn) die Verfügbarkeit der Komponenten n beschreibt

$$V_{gesamt} = V(K_1) * V(K_2) * \ldots * V(K_n)$$

Für N << 1 gilt :

beziehungsweise

$$N_{gesamt} = N(K_1) + N(K_2) + \ldots + N(K_n)$$

wobei N(Kn) die Nichtverfügbarkeit der Komponenten n beschreibt.

Die Fehlerquote eines Systems, das aus mehreren Elementen besteht, steigt mit der Zahl der Elemente.

Betrachtet man hierfür nur die für die Sicherheit relevanten Elemente, so arbeitet ein solches System nur dann sicher, wenn alle Einzelelemente richtig arbeiten.

Damit sind Ausfallzeit und Ausfallwahrscheinlichkeit des Gesamtsystems wesentlich größer als jene einer Einzelkomponente.

Quelle : Andrea Held : Oracle 10g Hochverfügbarkeit - RAC, Data Guard und Flashback, Addison-Wesley, München (26. Oktober 2004)

Wahre Aussage eines Betriebsleiters :
"Was interessiert mich der BackUp, Hauptsache der Restore funktioniert …"

Informationen für Geschäftsleitungen

Bild : animationfactory

Für viele Geschäftsprozesse werden heutzutage zumindest zeitweise intakte Kommunikationsverbindungen benötigt, sei es über Telefon, Fax, E-Mail oder andere Dienste über Nah- oder Weitverkehrsnetze (z. B. Cloud-Betrieb).

Fallen einige oder mehrere dieser Kommunikationsverbindungen über einen längeren Zeitraum aus, kann dies beispielsweise dazu führen, daß Geschäftsprozesse nicht mehr weiterbearbeitet werden können, weil benötigte Informationen nicht abgerufen werden können, Kunden die Institution nicht mehr für Rückfragen erreichen können, Aufträge nicht abgegeben oder beendet werden können.

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorhanden sind.

Zu ähnlichen Problemen kann es kommen, wenn die benötigten Kommunikationsnetze gestört sind, ohne jedoch vollständig auszufallen.

Kommunikationsverbindungen können beispielsweise eine erhöhte Fehlerrate oder andere Qualitätsmängel aufweisen. Falsche Betriebsparameter können ebenfalls zu Beeinträchtigungen führen.

Störungen, Notfälle, Krisen und Katastrophen im Verständnis des BSI-Standards 100-4

Vorfallsart	Erläuterung	Behandlung
Einfache Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung
Notfall	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt	Da Krisen nicht breitflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt

Informationen für Geschäftsleitungen

Bild : animationfactory

Um IT-Geräte dauerhaft zuverlässig zu betreiben, muß sichergestellt werden, daß die Umgebungsbedingungen innerhalb der von den Herstellern genannten Grenzen gehalten werden.

Der in diesem Zusammenhang stets genutzte Begriff Klimatisierung umfaßt die folgenden vier Bereiche der Luftkonditionierung :

- Lufttemperatur
- Luftfeuchtigkeit
- Frischluftanteil
- Schwebstoffbelastung

Die größte Bedeutung kommt der Einhaltung der Temperaturgrenzwerte zu. Nahezu die gesamte, der IT zugeführten elektrische Energie muß in Form von Wärmeenergie wieder aus dem Bereich abgeführt werden. Reicht der normale Luft- und Wärmeaustausch eines Raumes nicht aus, wird der Einbau einer zusätzlichen Kühlung erforderlich.

Neben der Temperatur muß oft auch die Luftfeuchtigkeit innerhalb bestimmter Grenzen gehalten werden, um elektrostatische Aufladungen (bei zu geringer Luftfeuchtigkeit) oder Oxidation und Schimmelbildung (bei zu hoher Luftfeuchtigkeit) zu vermeiden.

Der Schwebstoffgehalt der Luft wird meist schon durch die normalen Filter in Klimaanlagen hinreichend niedrig gehalten.

Nur bei besonders stark belasteter Umgebungsluft oder spezieller Hardware ist hier eine weitergehende Filterung erforderlich. Um den erforderlichen Luftdurchsatz zu gewährleisten, müssen die Filter der Klimaanlage regelmäßig kontrolliert und rechtzeitig gewechselt werden.

Die vierte Komponente einer Klimatisierung, die Frischluftbeimischung, ist für den eigentlichen IT-Betrieb belanglos. In dem Umfang jedoch, in dem die klimatisierten Flächen als Arbeitsplatz ausgewiesen sind, muß entsprechend der einschlägigen Arbeitsstättenverordnungen eine Frischluftbeimischung erfolgen.

Um ihrem Hauptzweck dienen zu können, muß eine Klimatisierung ausreichen dimensioniert sein. Werden gewisse Ungleichmäßigkeiten im Energieverbrauch aller IT-Systeme berücksichtigt, kann in erster Näherung davon ausgegangen werden, daß jedes Kilo-Voltampere (kVA) elektrischer Energie mit 0,8 kW bis 1 kW Wärmelast zu Buche schlägt.

Informationen für Geschäftsleitungen

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen.

Bild : animationfactory

Eine Datensicherung soll gewährleisten, daß durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verlorengehen.

1. Definitionen

- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage zur Motivation

- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflußfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

4. Datensicherungsplan je IT-System

4.1 Festlegungen je Datenart

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

Informationen für Geschäftsleitungen

Die Ausübung der verfassungsrechtlich garantierten Aufgaben der judikativen, legislativen und exekutiven Staatsgewalten setzt einen sicheren und zuverlässigen Betrieb der Informationssysteme voraus.

Bild : animationfactory

Nur auf diese Weise sind eine lückenlose und gegen Manipulationen jeglicher Art geschützte Kommunikation und eine fälschungssichere Dokumentation des Verwaltungshandelns garantiert. Das Vertrauen der Bürger und Unternehmen in die Integrität des digitalen Staates wird erschüttert, wenn dieser seinen Aufgaben wegen funktionsunfähiger Informationssysteme nicht mehr nachkommen kann.

Die Informationssysteme in den Staatsgewalten sind dadurch zu kritischen Infrastrukturen für das Gemeinwesen geworden.

- Die Abwehr von Gefahren für die IT ist eine der Kernaufgaben der IT-Administration
- Wichtigste Sicherheitsmaßnahmen für ein Rechenzentrum sind eine durchgängig gesicherte Kommunikation und eine robuste, redundante Architektur. Darüber hinaus wird ein geregelter, vertrauensvoller Betrieb gewährleistet. Zudem wird die sicherheitstechnische Aufstellung der Netze permanent verbessert sowie auch eine enge Anbindung der Netze der Außenstellen realisiert.
- Für den bestmöglichen Schutz der Netze und IT-Systeme muß ein mehrstufiges Sicherheitssystem etabliert werden. Es besteht neben kommerziellen Schutzprodukten auch aus individuell angepaßten und entwickelten Maßnahmen. Sie werden kontinuierlich überprüft, weiterentwickelt und an die dynamische Bedrohungslage angepaßt. Durch die Kombination verschiedener Abwehrmaßnahmen entsteht ein gutes Bild über die IT-Sicherheitslage des Rechenzentrums

Abwehr von Schadprogrammen

Cyber-Angriffe auf die Netze von Unternehmen finden täglich statt. Neben ungezielten Massenangriffen sind die Netze auch gezielten Angriffskampagnen ausgesetzt. Dabei zählen emails mit Schadprogrammen zu den am häufigsten gezählten Angriffen auf die Verwaltung. Mittels automatisierter AntiVirus-Schutzmaßnahmen werden bei uns z. B. pro Monat durchschnittlich fast 5.000 solcher Mails in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichen.

Davon werden monatlich im Durchschnitt rund 1.000 schädliche emails nur aufgrund erstellter AntiVirus-Signaturen erfaßt. Der erneute Anstieg dieser Zahlen um 18 Prozent im Vergleich zum Vorjahresbericht ist vor allem auf die massenhafte Verbreitung von Ransomware seit 2016 zurückzuführen, der auch außerhalb usneres Rechenzentrums zu beobachten war.

Informationen für Geschäftsleitungen

Die Angreifer verwendeten dazu häufig email-Anhänge mit in Archiven gepacktem JavaScript oder Makrocode in **Office-Dokumenten**, um dann das eigentliche Schadprogramm aus dem Internet nachzuladen.

Bild : animationfactory

Seit Jahresbeginn hat sich die Lage diesbezüglich etwas entspannt. Im 1. Quartal 2021 wurden ohne erkennbare Einbußen in der Schutzwirkung nur noch halb so viele emails mit Schadsoftware abgefangen wie im 2. Halbjahr 2017.

Den automatisierten AntiVirus-Schutzmaßnahmen nachgelagert empfiehlt sich ein eigenes System zur Detektion von Schadprogrammen, das für das Unternehmen zusätzlichen Schutz bietet.

Gestaffelte Verteidigung
Die verschiedenen Schutzmaßnahmen an den Netzübergängen und auf den Client-Systemen können nicht immer alle Angriffsversuche zuverlässig abwehren.

Daher sollten auch weitere Maßnahmen zur Detektion und Reaktion eingesetzt werden, die in solchen Fällen greifen, diese Angriffe verhindern oder deren negativen Effekte minimieren (z. B. NetSpider). So werden u. A. im Rechenzentrum ausgehende Netzverbindungen auf Webseiten blockiert, die Schadprogramme verteilen.

Bild : animationfactory

Ebenso werden Verbindungsversuche von bereits aktiven Schadprogrammen zu Kontrollservern unterbunden, die für die Steuerung und den Datenfluß genutzt werden. Auf diese Weise können bereits infizierte Systeme erkannt und ein unberechtigter Datenfluß verhindert werden.

Idealerweise wird der Angriff bereits im Vorfeld verhindert, in dem zum Beispiel der Aufruf einer zur Schadprogrammverteilung oder zum Phishing genutzten Website verhindert werden kann.

Mit dieser Methode wurden bei einem Kunden täglich rund 500 Verbindungsversuche zu Schadcodeservern verhindert. Vereinzelt sind darunter auch lang laufende Watering-Hole-Angriffe, bei denen Täter mit Spionagehintergrund Schadcode auf Webseiten plazieren, die für Mitarbeiter relevant sind. Der Schadcode wird dabei im Abstand von mehreren Monaten durch neue Varianten ausgetauscht.

Informationen für Geschäftsleitungen

Angriffsvarianten

So vielfältig wie Netze sind, so vielfältig sind auch die Angriffsmöglichkeiten auf ein Netz. In vielen Fällen werden mehrere Angriffe kombiniert, um ein Ziel zu erreichen.

Bild : animationfactory

Angriffe auf Software(-implementierungen).

Da Kommunikationsnetze immer aus einer (großen) Menge von Systemen bestehen, werden sehr oft genau diese Systeme über das Kommunikationsnetz angegriffen.

Hierbei zielen viele …

… Angriffe auf Schwächen in Software(-implementierungen)

- Pufferüberlauf – vor allem in Programmen in der Programmiersprache C findet man häufig den Fehler, daß über einen Puffer hinausgeschrieben wird und hierbei andere Daten oder Kontrollinformationen überschrieben werden
- Stack Smashing – hierbei überschreibt z. B. ein Pufferüberlauf den Stack eines Programmes, hierdurch können Schadroutinen eingeschleust und ausgeführt werden (Exploit)
- Formatstring-Angriffe – Ausgaberoutinen, wie printf, nutzen einen Format-String um eine Ausgabe zu modifizieren. Durch die Nutzung sehr spezieller Formatierungsanweisung können hierbei Speicherbereiche überschrieben werden.

… Angriffe auf Netzwerkprotokolle

- Man-In-The-Middle-Angriff – falls keine gegenseitige Authentifizierung durchgeführt wird, täuscht ein Angreifer den Kommunikationspartnern jeweils den anderen vor (z. B. telnet, rlogin, SSH, GSM, Ciscos XAUTH)
- Unerlaubte Ressourcennutzung – falls keine sichere Authentifizierung bzw. sichere Autorisierung vorhanden (z. B. rlogin)
- Mitlesen von Daten und Kontrollinformationen – alle unverschlüsselten Protokolle, wie POP3, IMAP, SMTP, Telnet, rlogin, http
- Einschleusen von Daten oder Informationen – alle Protokolle ohne ausreichende Nachrichtenauthentifizierung, wie POP3, SMTP, Telnet, rlogin, http
- Tunnel können verwendet werden, um Datenverkehr in zugelassene Protokolle (z. B. Http) einzubetten. Dadurch können Firewallregeln unterlaufen werden.

  Beispiel : Der SSH-Client baut über Https und den Proxy eine Verbindung zu einem Server außerhalb des internen Netzes auf. Dadurch umgeht er die Regeln, die den SSH-Verkehr nach außen kontrollieren. Diese Verbindung kann auch umgedreht werden, wodurch eine Verbindung von außen in das interne Netz geschaltet wird.

  Die *Bekämpfung* erfordert entsprechende Regeln im Proxy, die eine Einschränkung der Methoden CONNECT bzw. POST bewirken. Der Url-Filter UfdbGuard ermöglicht es z. B. Https-Tunnel zu erkennen und zu blockieren.

Informationen für Geschäftsleitungen

Bild : animationfactory

Angriffsvarianten, Fortsetzung …

Angriffe auf die Netzstruktur

Die Überlastung von Diensten wird als Denial of Service-Angriff (DoS) bezeichnet. Besonders verteilte DoS-Angriffe werden auch als Distributed-Denial-of-Service-Angriffe (DDoS) bezeichnet.

Sehr effektiv sind Angriffe, die mit nur einem Paket auskommen, wie z. B. der TCP-SYN-Angriff, da hierbei die Absenderadresse und somit die Herkunft gefälscht werden kann.

Tarnung von Angriffen

- Fragmentierung von Paketen, vor allem bei überlappenden Fragmenten, kann genutzt werden um Angriffe vor Angriffserkennern zu verstecken
- Spoofing – das Fälschen von meist Absendeadressen zum Verschleiern der Herkunft von Paketen (siehe auch Firewall)

Verwandte Angriffe (werden durch die verteilte Struktur eher begünstigt)

- Social Engineering wird die Vorgehensweise genannt, soziale Aspekte auszunutzen, um bestimmte Ziele, z. B. das Umgehen einer Passwortabfrage, zu erreichen.
- Passwörter können erlangt werden, um Zugang zu Diensten zu erlangen. Geschieht dies durch Ausprobieren aller Möglichkeiten spricht man von einer Brute-Force-Attacke.
- Mangelhafte Installationen können einen Angriff mit Standard-Passwörtern erfolgreich machen.
- Aus der Außenwelt kommende Daten werden nicht auf ihre Validität überprüft, sondern als „korrekt“ hingenommen (Tainted Data oder Cross-Site Scripting und SQL Injection).
- Überflutung mit sinnlosen oder nicht angeforderten E-Mails wird als UBE („unsolicited bulk email“) und insbesondere, wenn es sich um Werbung handelt, als UCE („unsolicited commercial email“) bezeichnet.
- Würmer, Trojanische Pferde, Dialer oder Viren
- Leichtgläubigkeit und die leichte technische Möglichkeit zum Vorspiegeln falscher Webseiten können durch Phishing ausgenutzt werden.
- Leichtgläubigkeit läßt Anwender auch unbekannte Programme ausführen, die per Mail versandt wurden.

Literatur

BSI Grundschutzkatalog

Informationen für Geschäftsleitungen

Mangelndes Problembewußtsein der Führungskräfte zur Sicherheit

Studie des *Deutschland sicher im Netz e.V.* : *„… im Vergleich mit anderen Anforderungen (Kosten, Bequemlichkeit, große Funktionalität, etc. hat die IT-Sicherheit insgesamt einen zu geringen Stellenwert und wird eher als Kostenfaktor statt Gewinnfaktor angesehen. Im Rahmen von mehreren Workshops wurde Unternehmen und insbesondere dem Öffentlichen Dienst "ein Mangel an Aufmerksamkeit für das Thema Sicherheit im Umgang mit IT bescheinigt".*

Das *"unzureichende Problembewußtsein der Geschäftsleitungen"* und *"der Mangel an gefühlter Bedrohung"* verhindere das Verständnis der Notwendigkeit für IT-Sicherheitsmaßnamen. Da ist es wie mit COVID-19 … Die Gründe für einen geringen Stellenwert der IT-Sicherheit sind demnach neben der mangelnden Managementunterstützung die viel zu knappen Budgets, die in wirtschaftlich schwierigen Zeiten weiter begrenzt werden. Die IT-Sicherheit nimmt also … *„noch lange nicht den Stellenwert ein, der notwendig wäre, um ein effektives und für die jeweilige Institution zugeschnittenes* Sicherheitsmanagement zu etablieren bzw. aufrecht zu erhalten“.

Unwissenheit und mangelnde Schulung der Mitarbeiter

Nachlässigkeit und Unwissenheit von Mitarbeitern stellen die größten Risiken im IT/EDV-Umfeld dar, wenn es um zielgerichtete Attacken geht. Einer Studie zufolge sind 28 Prozent aller Cyberangriffe auf Phishing und Social Engineering zurückzuführen, weitere 30 Prozent entfallen auf Exploits und den Verlust von mobilen Endgeräten. Laut *Kaspersky* waren im vergangenen Jahr 46 Prozent aller Cybersecurity-Vorkommnisse auf uninformierte oder nachlässige Mitarbeiter zurückzuführen.

Verständnis der Mitarbeiter zur Sicherheit

Das Verhalten der Mitarbeiter ist oft besorgniserregend. *Application Intelligence Report (AIR), eine Studie von A10 Networks* : *„… fast ein Drittel der befragten Mitarbeiter nutzt wissentlich gesperrte Apps (30 Prozent). 10 Prozent geben an, daß sie nicht wissen, ob die verwendeten Apps zugelassen sind oder nicht …“.*

Von denjenigen, die gesperrte Apps verwenden, gibt über die Hälfte der Befragten (51 Prozent) an, daß „jeder das macht“, während über ein Drittel (36 Prozent) der Meinung ist, die IT-Abteilung hätte kein Recht darüber zu bestimmen, welche Apps sie nutzen dürfen.

Fast die Hälfte der befragten IT-Führungskräfte (48 Prozent) berichtet, daß die Mitarbeiter sich nicht für Sicherheitsvorgaben interessieren oder sich bereitwillig darüber hinwegsetzen. 59 Prozent der befragten IT-Verantwortlichen sind daher wenig optimistisch, daß sie Gefahren stoppen und ihr Unternehmen schützen können.

Bilder : animationfactory

Informationen für Fachbereiche, Fachbereichsleitungen …

Auflistung potentieller und real vorhandener Gefährdung durch Mitarbeiter

Organisatorische Mängel

- mangelndes Problembewußtsein durch Fehlen von Vorgaben/Konsequenzen
- unkritischer Umgang mit externen Speichermedien (Sticks, Mobiles, Kameras)
- unzureichende Kenntnis über Regelungen
- unerlaubte Ausübung von Rechten
- unzureichende Sensibilisierung für Informationssicherheit
- unzureichende Schulung der Mitarbeiter
- Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
- nicht erkannte/gemeldete Sicherheitsvorfälle
- unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern

Menschliche Fehlhandlungen

- mangelnde Systemkenntnisse (Fehlbedienung, z. B. Löschen, Verschieben statt Kopieren, etc.)
- mangelnde Interesse an aktuellen Bedrohungen
- Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
- Nichtbeachtung von Sicherheitsmaßnahmen
- Gefährdung durch Reinigungs- oder Fremdpersonal
- fehlerhafte Nutzung von IT-Systemen
- fehlerhafte Administration von IT-Systemen
- Sorglosigkeit im Umgang mit Informationen
- mangelhafte Akzeptanz von Informationssicherheit

Vorsätzliche Handlungen

- Manipulation oder Zerstörung von Geräten oder Zubehör
- Manipulation an Informationen oder Software
- unberechtigte IT-Nutzung
- Mißbrauch von Benutzerrechten
- Mißbrauch von Administratorrechten
- Social Engineering
- gezielte Sabotage
- gezieltes Ausspähen von Informationen

So vielfältig wie Netze sind, so vielfältig sind auch die Angriffsmöglichkeiten auf ein Netz.

In vielen Fällen werden mehrere Angriffe kombiniert, um ein Ziel zu erreichen.

Literatur

BSI Grundschutzkatalog

Informationen für Geschäftsleitungen

Warum (automatisierte) Warneinrichtungen ?

Beispiel
Im Jahre 2000 verfügte Unternehmen "X" über 60 Client-PCs und sieben (7) Server.

Im Jahre 2021 verfügt Unternehmen "X" über über 500 Client-PCs und ca. 70 Server an 18 Standorten, dazu ungezählte Peripheriegeräte.

Um einen 100% Überblick über die Funktionsbereitschaft der Systeme bei den zuständigen – in der Regel unterbesetzten - Administratoren zu behalten ist eine Automatisierung der Erfassung von Ereignissen unabdingbar.

Mehr als 700 Sensoren erfassen die Systemzustände im Unternehmen "X", in den meisten Außenstellen und im Dienstleistungsbereich (Hosting für Dritte).

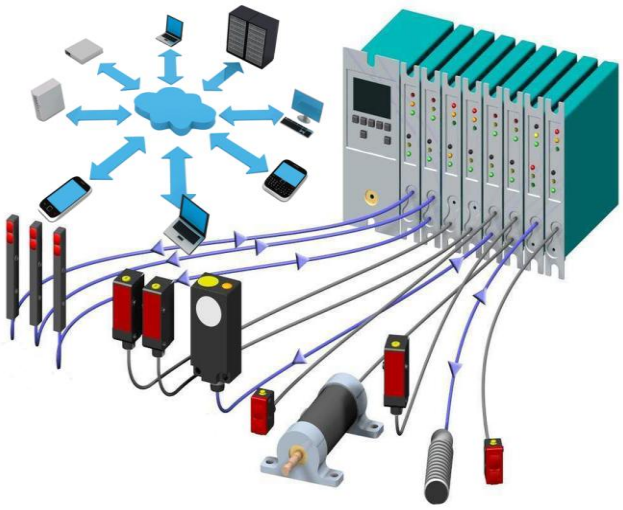


Bild : animationfactory

Erfaßt werden unter anderem :

- Server Verfügbarkeit und –speicherzustände
- gesamte Netzwerk-Infrastruktur
- alle Internet-Verbindungen werden minütlich gemonitored (verschiede Kontrollziele)
  Parameter wie Temperaturen, Luftfeuchte, Luftdruck, Stromaufnahme, Leistungsverluste, Klimaanlagen, Rauchwarnmelder, Giftgasmelder, Wasserstandsmelder, Alarmanlagen und vieles mehr …

Informationen für Geschäftsleitungen

Wichtigkeit des Schutzes

Nahezu alle Institutionen sind von einer funktionierenden Informationstechnik (IT) abhängig.

Dazu zählen nicht nur Arbeitsplatz-PCs, sondern insbesondere Server, die Basisdienste für das Rechnernetz bereitstellen, E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten.

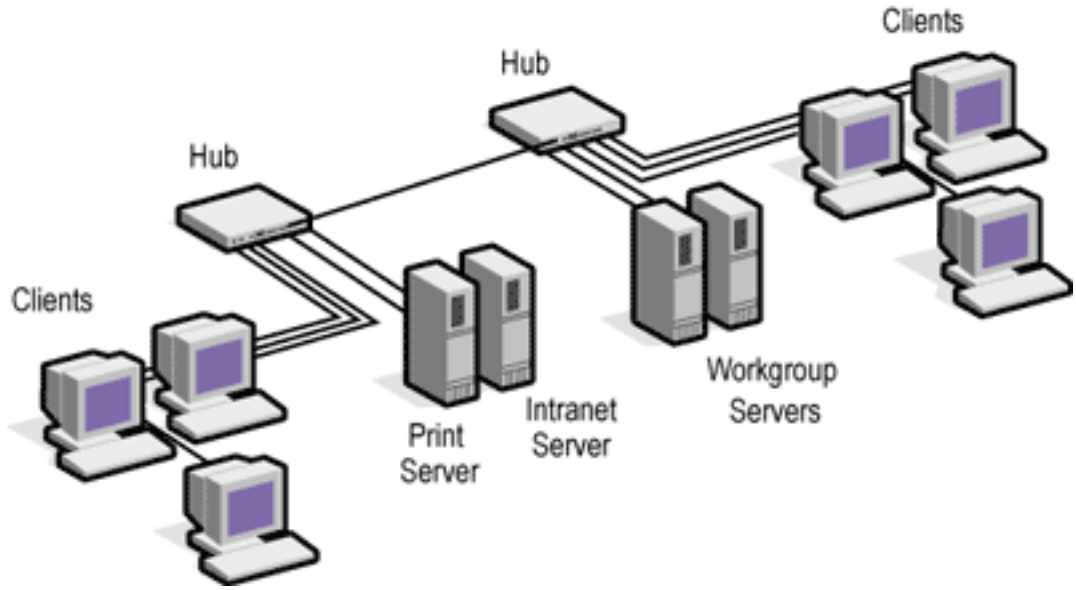


Bild : animationfactory

Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Organisation.

Angreifer können erheblichen Schaden anrichten, wenn sie es schaffen, in Server einzudringen, um dort Daten abzugreifen (Angriff auf die Vertraulichkeit), Daten zu manipulieren (Angriff auf die Integrität) oder Verfügbarkeit von Servern zu stören.

Die Verfügbarkeit von Servern kann auch durch technische Defekte bedroht sein, wie den Ausfall von Festplatten oder der Netzverbindung.

Um Server und deren Dienste vor Angriffen und Ausfällen zu schützen, ist die Absicherung sowohl des Betriebssystems als auch der darauf installierten Dienste von entscheidender Bedeutung.

Informationen für Geschäftsleitungen

Wichtigkeit des Schutzes

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen.

Das Thema Datensicherung betrifft keineswegs nur die Computer-Spezialisten, sondern hat absolute unternehmerische Relevanz. Unternehmen, die der IT-Sicherheit nur wenig Beachtung schenken, handeln grob fahrlässig und werden mittlerweile auch seitens der Gerichte als schlicht "blauäugig" bezeichnet.

So ist die Geschäftsleitung spätestens mit der DSGVO verpflichtet, ein System zur frühzeitigen Erkennung von den Fortbestand des Unternehmens bedrohenden Entwicklungen und Risiken zu implementieren.

Schenkt die Geschäftsleitung der Gefahr einer fehlenden Datensicherung keine Beachtung oder stellt nicht ausreichend finanzielle Mittel zur Verfügung, so ist in Anbetracht der zu erwartenden Schäden auch deren Verhalten als fahrlässig zu bezeichnen.

Bild : animationfactory

Eine Datensicherung soll gewährleisten, daß durch einen redundanten Datenbestand der gestörte IT - Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verlorengehen.

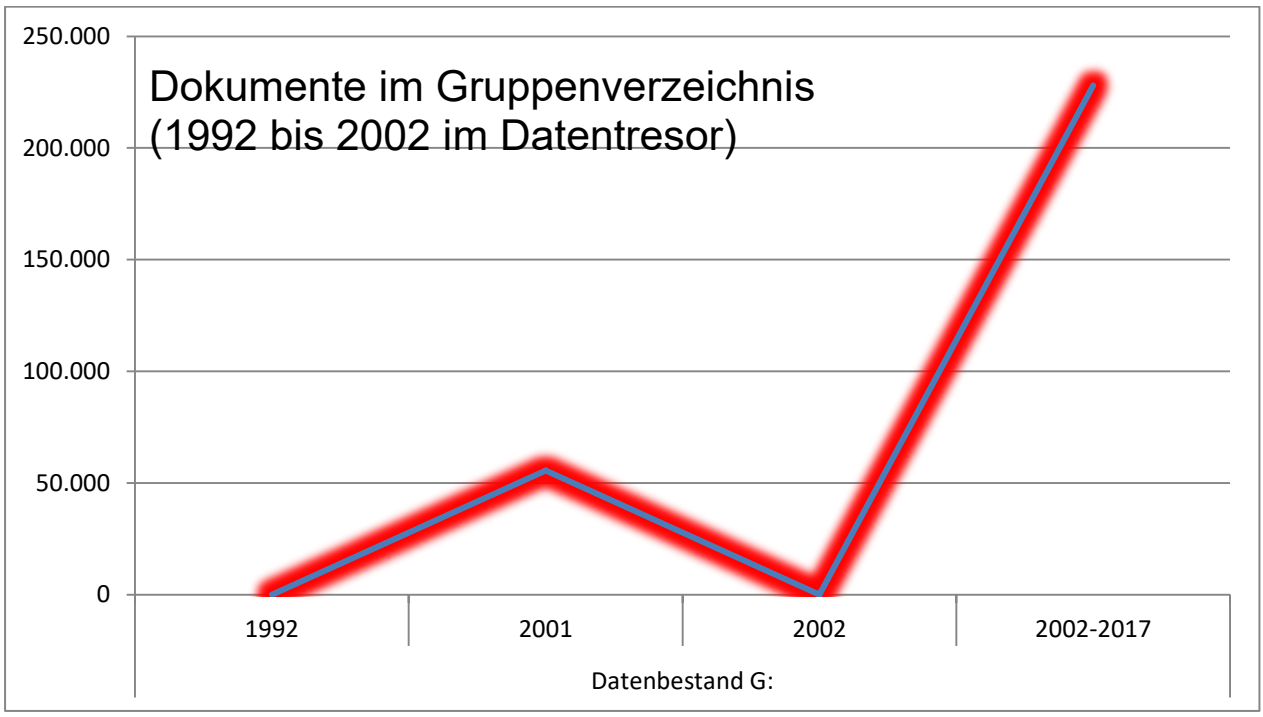
Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung bedarf aufgrund der Komplexität einer geordneten Vorgehensweise.

Im Grundschutzkatalog des BSI wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

Um eine effektive Datensicherung einzurichten, ist eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.33 „Entwicklung eines Datensicherungskonzepts“ beschrieben und werden durch die dort aufgeführten Einzel - Maßnahmen erläutert.

Informationen für Geschäftsleitungen

Beispiel : Unternehmen "X"



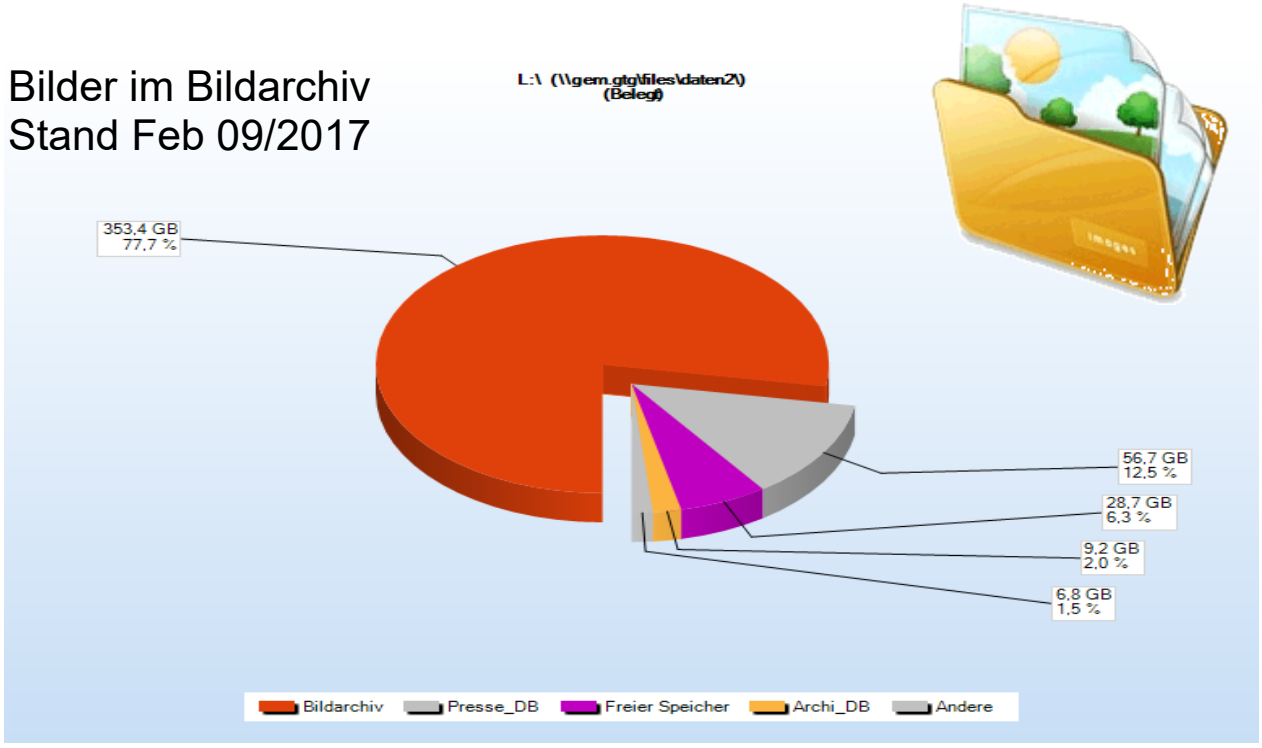


Diagramme / Bilder : id-newmedia

Informationen für Geschäftsleitungen

Bild : animationfactory

Clients (Arbeitsplatzrechner)
Auf Clients mittelgroßer Unternehmen ist überwiegend ein Corporate-Betriebssystem-Image (LTSB) installiert welches in der Regel von einem sog. „Golden Image“ abstammt.

Golden Images werden mit jedem bedeutenden Versionswechsel des Betriebssystems erstellt und regelmäßig z. B. via WSUS aktualisiert (Patch-Management).

Die Daten des Benutzers kommen aus einem „Profile“-Verzeichnis welches automatisch das Anmelden an jedem beliebigen PC erlaubt.

Zentral gepflegte „Global Policies“ steuern die betriebssystemspezifischen Rechte des Benutzers, die zugelassenen Programme und die gesamten Einstellungen des PCs.

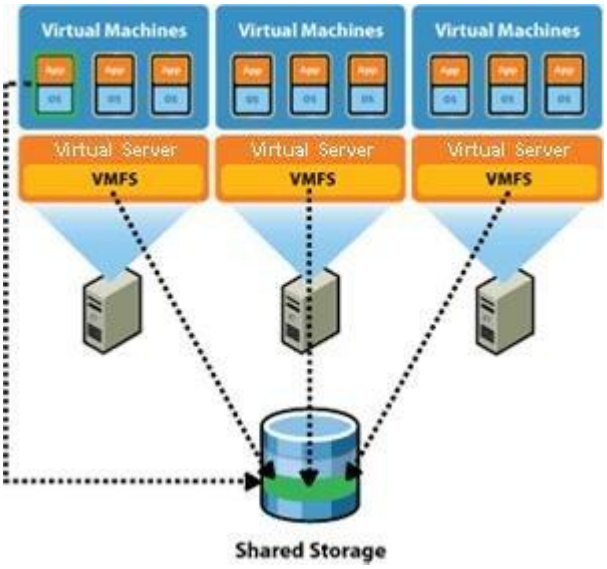
Eigene Programme aus einer Liste vorqualifizierter und lizensierter Programme dürfen nur durch Administratoren lokal installiert werden(1).

(1) Keine Programme und Datenhaltung auf lokalen PCs !

Alle „globalen Verfahren“ werden über gemappte Laufwerke (DFS) aufgerufen und sind vollständig Client-unabhängig.

Das heißt : wenn der PC (Client) eines Benutzers Schaden nimmt so kann er in wenigen Minuten mit einem Austauschgerät bedient werden und weiter arbeiten.

Server



Anwendungsserver sind alle zu virtualisieren und können dann über eine Image-Sicherung (typisch : 2 Stunden-Zyklus automatische Aktualisierung) „restored“ werden.

Alle Server sind z. B. via WSUS, die wichtigsten Anwendungsprogramme via ein gesondertes Patch-Management-System zu sichern.

Kritische Sicherheitsupdates werden bei den meisten Servern und allen Clients automatisch verteilt und installiert.

Bild : researchgate.net

Informationen für Geschäftsleitungen

LAN

Ein Local Area Network (LAN) ist ein Zusammenschluß von netzfähigen IT -Systemen, wie z. B. Clients, Server, Router oder Switches innerhalb eines räumlich begrenzten Gebiets.

Um die IT -Systeme zu vernetzen, können unterschiedliche Übertragungsmedien eingesetzt werden, wie beispielsweise verdrillte Kupferkabel oder Lichtwellenleiter.

Zunehmend werden die Daten auch drahtlos übertragen, z. B. per WLAN .

Neben den IT -Systemen und der Verkabelung sind die eingesetzten LAN -Techniken und insbesondere die zugrundeliegende Topologie wesentliche Bestandteile eines LAN.

Die Absicherung eines LAN s beginnt in der Planungsphase.

Der erste Schritt ist immer die Erhebung und daran anschließende Analyse der vorliegenden Netzsituation. Basierend auf den Ergebnissen der Analyse kann dann das LAN konzipiert und realisiert werden, um die vorher festgelegten Netz-Anforderungen zu erfüllen.

Besondere Aufmerksamkeit bei der Planung und Konzeption eines LAN s ist der Netz-Segmentierung zu widmen. Nur durch eine geeignete physische und gegebenenfalls logische Segmentierung kann verhindert werden, daß Angriffe auf ein Teilnetz die Funktionsfähigkeit anderer Teilnetze beeinträchtigen.

Außerdem muß eine Sicherheitsrichtlinie für das LAN erstellt werden, in der Regelungen und Hinweise zum sicheren Betrieb und zur sicheren Administration des LANs beschrieben sind.

Bild : animationfactory

Informationen für Geschäftsleitungen

Security Appliances („Firewall“, „Security Gateway“ oder auch **„Sicherheitsgateway“)**
Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP -Netze sicher zu koppeln.

Dazu wird die technisch mögliche auf die in einer Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation eingeschränkt. Sicherheit bei der Netzkopplung bedeutet hierbei die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen.

Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar.

Vielmehr können auch interne Netze unterschiedlich hohen Schutzbedarf besitzen, z. B. bei der Trennung des Verwaltungsnetzes vom Service-Netz der IT oder einem Schüler-/Lehrernetz.

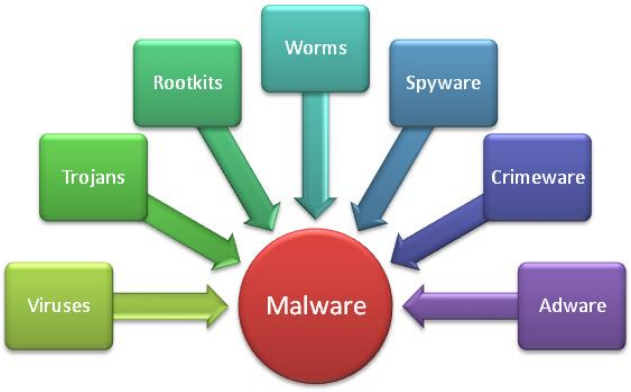


Bild : 13hitech.com.au

Die Verwendung des Begriffs Security Appliance = Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs "Firewall" soll verdeutlichen, daß zur Absicherung von Netzübergängen heute oft nicht mehr ein einzelnes Gerät verwendet wird, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs ("Intrusion Detection").

Die wichtigsten Komponenten eines Sicherheitsgateways sollten redundant ausgelegt werden.

Dies sind vor allem diejenigen Komponenten, die zum Übertragen von Informationen genutzt werden. In diese Kategorie fallen in der Regel Router, Paketfilter, Application-Level-Gateway und eventuell VPN -Komponenten. Bei anderen Komponenten (z. B. Virenscanner oder Intrusion Detection Systeme) muß die Bedeutung für die Sicherheit des zu schützenden Netzes im Einzelfall betrachtet werden.

Nicht nur die internen Netzwerke sollten vollständig überwacht, auch alle Außenstellen (Home Office) mit eigenen Firewalls sollten verbunden werden. Verbindungen von und zu Heimarbeitsplätzen werden ausschließlich über ausgegebene Security Appliances (Remote Ethernet Devices) angebunden. Diese wiederum lassen nur Terminal Server Verbindungen bzw. VPN zu.

Informationen für Geschäftsleitungen

Rechenzentrumsdienstleistungen
Ein Rechenzentrum führt Dienstleistungen („Managed Hosting“) z. B. für Schulen und Drittunternehmen durch.

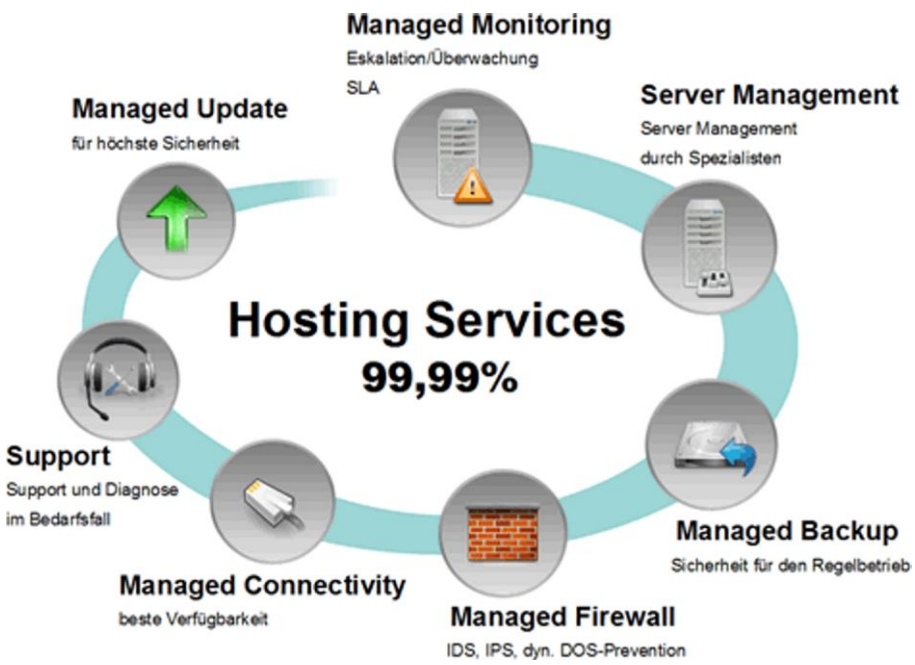


Bild : intares.net

Es wird keine Auftragsdatenverarbeitung durchgeführt !

Unter Hosting versteht man das physikalische Bereitstellen von sicheren Räumlichkeiten mit Servern (Host) und der dafür benötigten Infrastruktur (Unterbrechungsfreie Stromversorgungen, Klimaanlagen, Alarmanlagen).

Dabei werden die Hosts als „BlackBox“ – Systeme geführt, Zugang auf die darauf gehosteten Daten haben nur die Systembetreuer des Host-Nehmers sowie die autorisierten Systembetreuer des Hosting-Gebers.

Informationen für Geschäftsleitungen

Cloud-Computing

Die Verantwortung für die Risiken bleibt weiterhin beim KRITIS-Betreiber und kann nur im rechtlich zulässigen Rahmen auf den Cloudanbieter übertragen werden.

Chancen

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

- Skalierbar und flexibel
- Nur Nutzungskosten werden bezahlt
- geringere Investitionskosten im Vergleich zur lokalen Bereitstellung
- keine Infrastruktur-Vorhaltekosten
- Sicherheitsmaßnahmen sind günstiger
- Sicherheitsmaßnahmen bei Hauptanbietern i. d. R. besser / professioneller als On Premise
- Mehrere Standorte können Geo-Redundanzen ermöglichen
- seriöse Cloudanbieter verfügen i. d. R. über mehr Spezialisten
- Standardisierung von Plattformen und Software

Risiken

Bundesamt für Sicherheit in der Informationstechnik

- Tatsächliche Verfügbarkeit entspricht nicht den Anforderungen des KRITIS-Betreibers
- Konfigurationsmöglichkeiten nicht flexibel genug, um kurzfristige Änderungen der Anforderung umzusetzen
- Abhängigkeit steigt (Internet, Lieferant)
- Vertrauenswürdigkeit des Anbieters
- Sachkosten steigen
- Verlust der direkten Steuerung von Daten / Prozessen und Sicherheitsmaßnahmen bei verbleibender Verantwortung beim KRITIS-Betreiber
- Verstoß gegen rechtliche Vorgaben
- Verlust von IT-Expertise beim KRITIS-Betreiber
- große Anbieter sind attraktives Angriffsziel
- Daten werden nach außen (außerhalb des Unternehmens) transportiert und übertragen, ggf. auch grenzübergreifend und somit in andere Rechtsräume
- Management Verschlüsselungszertifikate problematisch
- Bei Public Cloud-Services = potentielle Datenexposition
- Migrationen von einem Anbieter zum nächsten erzeugt Abhängigkeiten
- Kostendruck auf Cloudanbieter führt zum Einsatz weniger geschulten Personals
- Ungeplante Einstellung der Leistungserbringung des Cloud-Dienstes
- Finanzielle Planungsunsicherheit über die initiale Vertragslaufzeit hinaus
- Durch die internetbasierte Verbindung zur Cloud entstehen Laufzeiten, welche ggf. mit der bislang eingesetzten Lösung nicht kompatibel sind.
- Der KRITIS-Betreiber könnte fälschlich seine Ressourcen für die Informationssicherheit reduzieren, da er das Risiko nur noch beim Cloud-Betreiber sieht.

Informationen für Geschäftsleitungen

DSGVO

Die Datenschutz-Grundverordnung (DSGVO), englisch General Data Protection Regulation (GDPR), ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden.

Bild : id-newmedia

Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Die Verordnung ersetzt die aus dem Jahre 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Im Gegensatz zur Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden mußte, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018.

Die Mitgliedstaaten bringen jedoch durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang (Art. 88 der Verordnung).

Für diese und andere Rechtsvorschriften ist die Datenschutz-Grundverordnung bereits seit ihrem Inkrafttreten am 24. Mai 2016 maßgeblich.

Sehen Sie hierzu auch unsere folgenden Kundeninformationen :

- pr_dsgvo.pdf
- pr_dsgvo_datenpanne.pdf
- pr_dsgvo_email_impressum_signatur.pdf
- pr_dsgvo_email_verschluesselung.pdf
- pr_dsgvo_toms.pdf
- pr_dsgvo_verarbeitungsverzeichnis.pdf

Informationen für Geschäftsleitungen

Social Engineering
Die Abwehr von Social Engineering ist nicht einfach zu bewerkstelligen, da der Angreifer im Grunde positive menschliche Eigenschaften ausnutzt : den Wunsch etwa, in Notsituationen unbürokratisch zu helfen oder auf Hilfe mit Gegenhilfe zu reagieren.

Bild : internetx.com

Generelles Mißtrauen zu schüren, würde auch die Effektivität und die vertrauensvolle Zusammenarbeit in Organisationen negativ beeinflussen.

Den wichtigsten Beitrag zur Bekämpfung von Social Engineering liefert deshalb im konkreten Fall das Opfer selbst, indem es Identität und Berechtigung eines Ansprechenden zweifellos sicherstellt, bevor es weitere Handlungen vornimmt. Bereits die Rückfrage nach Name und Telefonnummer des Anrufers oder dem Befinden eines nicht existierenden Kollegen kann schlecht informierte Angreifer enttarnen. Höflich um Geduld zu bitten, wenn eine heikle Anfrage auch noch so dringend vorgetragen wird, sollte deshalb gezielt trainiert werden.

Auch scheinbar geringfügige und nutzlose Informationen sollten Unbekannten nicht offengelegt werden, denn sie könnten in folgenden Kontaktaufnahmen zum Aushorchen anderer mißbraucht werden oder zusammen mit vielen anderen für sich genommen nutzlosen Angaben zum Abgrenzen eines größeren Sachverhalts dienen.

Ist die Identität des Absenders einer email nicht sicher, sollte man stets mißtrauisch sein.
Bei Anrufen sollten auch scheinbar unwichtige Daten nicht sorglos an Unbekannte weitergegeben werden, da diese die so erhaltenen Informationen für weitere Angriffe nutzen können.

Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder finanzielle Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
Keine Links aus E-Mails verwenden, die persönliche Daten als Eingabe verlangen. Statt dessen die URL selbst im Browser eingeben.

Bei Unklarheit über die Echtheit des Absenders diesen nochmals telefonisch kontaktieren, um die Authentizität der E-Mail zu überprüfen.

Informationen für Geschäftsleitungen

Schwachstellenmanagement
Eine Schwachstellen-Scanning und -Management Plattform ermöglicht sowohl interne als auch externe Gefahren zu erkennen und zu verwalten, Risiken zu melden, und bestehende / kommende gesetzliche Anforderungen zu erfüllen (PCI, GDPR, etc.).

Es macht Shadow-IT /"Schatten-IT") sichtbar um die volle Angriffsfläche aufzuzeigen und auf alle kritischen Schwachstellen reagieren zu können.

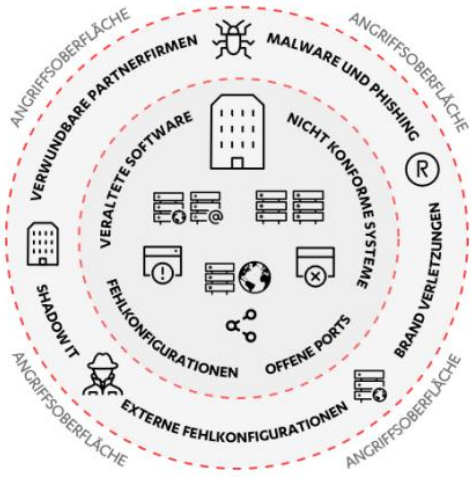


Bild : id-newmedia

Es gibt viele Möglichkeiten, die Abwehrschilde eines Unternehmens zu durchbrechen, aber **Webanwendungen** sind die durch Angriffe am stärksten gefährdeten Teile eines Netzwerks.

Durch die steigende Zahl dieser Webanwendungen steigt die Gefährdung der Datenintegrität im Rathaus-Rechenzentrum überproportional an.

Schwachstellen lassen sich nur durch kontinuierliches Scannen und unbestechliche Kontrolle aufspüren, bevor andere sie finden können.

*"Das **IT-Sicherheitsgesetz** nimmt sog. "Kleinstunternehmen" von den Anforderungen ausdrücklich aus. Dies betrifft Unternehmen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Millionen Euro erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Millionen Euro beläuft.*

Es ist allerdings für Unternehmen verfehlt zu glauben, sich mit den Anforderungen dieser Normen nicht beschäftigen zu müssen.

Den Unternehmen, die nicht Adressat dieses Gesetzes sind, ist sogar ausdrücklich zu empfehlen, sich mit den Anforderungen zu befassen. Zum einen zählt "IT-Sicherheit" zu den elementaren Bestandteilen der Compliance in Unternehmen. Wer die IT-Sicherheit vernachlässigt, riskiert nicht nur wirtschaftliche und immaterielle Schäden. Er riskiert u. a. auch, in Zukunft von Ausschreibungen, Angeboten und Vertragsverhandlungen ausgeschlossen zu werden."

Quelle
Dr. Philipp Herrmann in https://www.informatik-aktuell.de/management-und-recht/it-recht/cloud-und-das-it-sicherheitsgesetz-herausforderungen-und-auswirkungen-fuer-unternehmen.html

Informationen für Geschäftsleitungen

BYOD

Bring-Your-Own-Device (BYOD) ist die Bezeichnung für private mobile Endgeräte wie Speicher-Sticks, Kameras, Smart-Watches, Laptops, Tablets oder Smartphones in die Netzwerke von Behörden, Unternehmen oder Schulen, Universitäten, Bibliotheken und anderen Institutionen zu integrieren. Darunter verstanden werden auch Organisationsrichtlinien, die regeln sollen, auf welche Art und Weise der Zugriff auf Netzwerkdienste und das Verarbeiten und Speichern organisations- oder unternehmensinterner Daten stattfinden darf.

BYOD soll den Nutzern eine größere Wahlfreiheit bringen und der Organisation eine bessere Orientierung an persönlichen Bedürfnissen ermöglichen.

Im Bildungsbereich bietet BYOD ökonomische und ökologische Potentiale.

Statt daß Schulen und Hochschulen mit finanziellem Aufwand schuleigene Geräte beschaffen müssen, sollen die zunehmend privat bereits verfügbaren Geräte der Lernenden auch für schulische Zwecke genutzt werden können.

Bild : animationfactory

Ein anderer Ansatz ist das Konzept Corporate Owned, Personally Enabled (COPE), bei dem Mitarbeitern ein konzerneigenes Gerät auch zur privaten Nutzung überlassen wird (Telearbeitsplätze → siehe dort).

Verloren oder gestohlen ?

Laut einer 2013 von Ernst und Young durchgeführten Studie zu BYOD gehen etwa 22% aller produzierten mobilen Geräte im Laufe ihres Lebens verloren oder werden gestohlen und etwa 50% aller verlorengegangenen oder gestohlenen Geräte tauchen niemals wieder auf. Obwohl die Mehrheit dieser Geräte wegen des Werts des Gerätes selbst gestohlen wird wächst auch die Anzahl der verlorengegangenen oder gestohlenen Geräte, auf deren Daten zugegriffen wurde. Und wenn personenbezogene Daten mit vertraulichen Firmendaten in einem Gerät vermischt werden, ist das Risiko, daß diese Informationen im Falle eines Diebstahls an die Öffentlichkeit gelangen, inzwischen eine beängstigende Möglichkeit.

Kein bzw. unzureichender Passwortschutz

Viele Benutzer schützen ihre persönlichen Geräte oder die Anwendungen auf ihren Geräten nicht wirklich mit Passwörtern. Oder, wenn sie es tun, neigen sie dazu, aus Bequemlichkeit einfache Passwörter zu wählen. Diese Geräte sind bei Diebstahl oder Hacking leicht zu kompromittieren.

Informationen für Geschäftsleitungen

Datenschutzverletzung über Mobile Apps
Es gibt unzählige schädliche Apps, deren Ziel es ist, nicht nur die Gerätesoftware zu beschädigen, sondern auch private Daten auf dem Gerät zu hacken und darauf zuzugreifen. Und wenn personenbezogene und Behördendaten auf gleiche Weise behandelt werden, laufen beide in Gefahr, skrupellosen Gruppen oder Personen in die Hände zu fallen.

Bild : animationfactory

Abgesehen davon können auch Apps, die vom Unternehmen selbst bereitgestellt werden, ein Problem darstellen.

Selbst wenn eine App vom Unternehmen bereitgestellt wird, ist sie, wenn keine Sicherheitsvorkehrungen in der App enthalten sind, immer noch anfällig für Angriffe.

Nicht verschlüsselte Daten und Verbindungen
Stellen Sie sich vor, Ihre Daten, einschließlich Sprachnachrichten, gehen ohne Schutz oder Sicherheitsvorkehrungen durch das öffentliche Internet. Sie können während der Übertragung oder im gespeicherten Zustand einfach und jederzeit abgefangen werden.

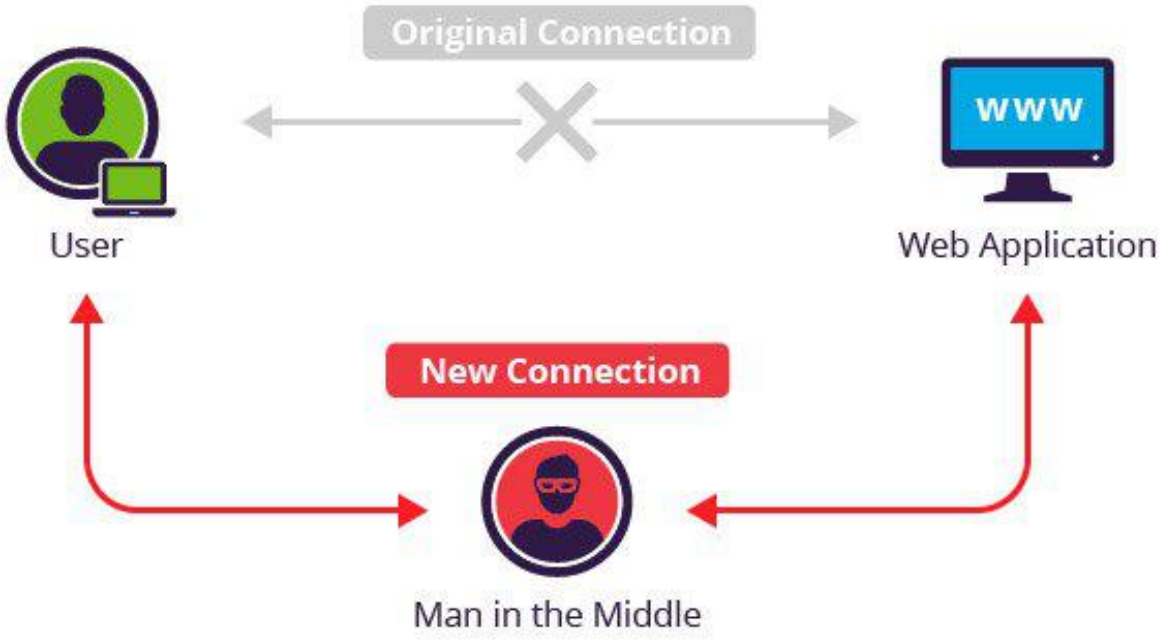


Bild : cloudflare.com

Informationen für Geschäftsleitungen

Telearbeitsplatz - Definition
Telearbeit ist jede auf Informations- und Kommunikationstechnik gestützte Tätigkeit, die ausschließlich oder zeitweise an einem außerhalb der zentralen Betriebsstätte liegenden Arbeitsplatz verrichtet wird. Dieser Arbeitsplatz ist mit der zentralen Betriebsstätte durch elektronische Kommunikationsmittel verbunden.

Telearbeit ausschließlich zu Hause
Bei dieser Tätigkeitsform steht dem Telearbeiter kein Arbeitsplatz beim Arbeitgeber zur Verfügung. Statt dessen erfolgt die Arbeitsverrichtung ausschließlich in der Wohnung des Mitarbeiters.

Alternierende Telearbeit
Bei dieser Form der Telearbeit arbeitet der Arbeitnehmer sowohl an seinem Arbeitsplatz beim Arbeitgeber als auch in seiner Wohnung, wobei er zwischen diesen wechselt.

Mobile Telearbeit
Mobile Telearbeit bezeichnet das ortsunabhängige Arbeiten mit mobiler Kommunikationstechnik (z. B. auch Bauamt, Bauhof, Öffentlichkeitsarbeit unterwegs).

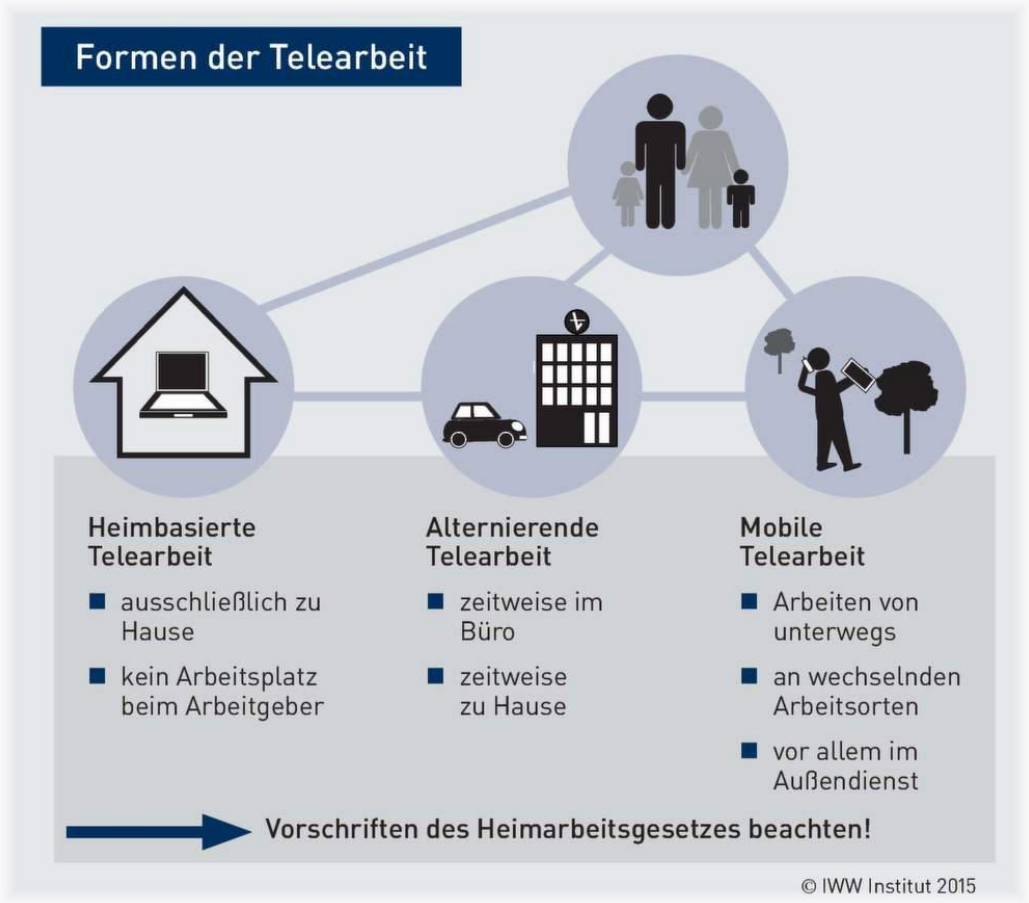


Bild : IWW Institut

BSI Grundschutzkatalog Anforderungen

Höhere Gewalt
G 1.1 Personalausfall

Organisatorische Mängel
G 2.1 Fehlende oder unzureichende Regelungen
G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen
G 2.7 Unerlaubte Ausübung von Rechten
G 2.22 Fehlende oder unzureichende Auswertung von Protokolldaten
G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter
G 2.50 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
G 2.51 Mangelhafte Einbindung des Telearbeiters in den Informationsfluß
G 2.53 Unzureichende Vertretungsregelungen für Telearbeit

Menschliche Fehlhandlungen
G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
G 3.9 Fehlerhafte Administration von IT-Systemen
G 3.13 Weitergabe falscher oder interner Informationen
G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.30 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Technisches Versagen
G 4.13 Verlust gespeicherter Daten

Vorsätzliche Handlungen
G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör
G 5.2 Manipulation an Informationen oder Software
G 5.9 Unberechtigte IT-Nutzung
G 5.10 Mißbrauch von Fernwartungszugängen
G 5.18 Systematisches Ausprobieren von Passwörtern
G 5.19 Mißbrauch von Benutzerrechten
G 5.20 Mißbrauch von Administratorrechten
G 5.21 Trojanische Pferde
G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Jeder Mitarbeiter muß für das FB15 eine Belehrung zum BSI-konformen Maßnahmenkatalog zur Sicherheit am Arbeitsplatz zeichnen.

Alle Komponenten des Heimarbeitsplatzes werden vorkonfiguriert gestellt. Der Zugriff erfolgt ausschließlich über VPN-Tunnel und Terminalserver.

Quelle : BSI Grundschutzkatalog

Bildquellen

Bilder, soweit nicht gesondert erwähnt, lizenziert von :

- animationfactory.com / - Vital Imagery Ltd. / - wikimedia.org / - id-newmedia

Textquellen

AWV - Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. [Hrsg.] :
Sicherheit, Haltbarkeit und Beschaffenheit optischer Speichermedien. 2. vollst. überarb. und erw. Auflage 2003.

Grundschutzkatalog Bundesamt für die Sicherheit in der Informationstechnik (BSI)

Brandner, R.; Pordesch, U.; Rossnagel, A.; Schachermeyer, J. (2002) : Langzeitsicherung qualifizierter elektronischer Signaturen. Datenschutz und Datensicherheit 26 (2), 97 - 103.

Bredow, Felix von; Kampffmeyer, Dr. Ulrich (2003) : Verfahrensdokumentation, Rechtsfragen.
http ://www.project-consult.net/ Files/ Download_Verfahrensdokumentation_20020523.pdf

Bundesministerium des Innern [Hrsg.] (2003) : SAGA : Standards und Architekturen für E-Government-Anwendungen, Version 2.0, 2003 In : Schriftenreihe der KBSt, Bd.59. Bundesministerium des Innern [Hrsg.] (1998) : Konzept zur Aussonderung elektronischer Akten. In : Schriftenreihe der KBSt, Bd.40.

Dollar, Charles (2000) : Authentic Electronic Records. Strategies for Long-Term Access, Chicago, S. 57 f.

Quelle : Andrea Held : Oracle 10g Hochverfügbarkeit - RAC, Data Guard und Flashback, Addison-Wesley, München (26. Oktober 2004)

Härder, Theo ; Bühmann, Andreas (2004) : Datenbank-Caching – Eine systematische Analyse möglicher Verfahren.Technische Universität Kaiserslautern.

Henstorf, Karl-Georg ; Kampffmeyer, Dr. Ulrich ; Prochnow, Jan (1999) : Grundsätze der Verfahrensdokumentation nach GoBS „Code of Practice“ zur revisionssicheren Archivierung, In : VOI-Schriftenreihe Kompendium Band 4.

Kampffmeyer, Dr. Ulrich (1996) : Restart, Recovery und Konsistenzsicherung von elektronischen Archivsystemen. In : VOI NEWS, Ausgabe 1/96.

Kampffmeyer, Dr. Ulrich (2003) : Revisionssichere Archivierung im Licht neuer rechtlicher Anforderungen.

Kampffmeyer, Dr. Ulrich ; Rogalla, Jörg (1997) : Grundsätze der elektronischen Archivierung „Code of Practice“ zum Einsatz von Dokumenten- Management- und elektronischen Archivsystemen, In : VOI-Schriftenreihe Kompendium Band 3.

Keitel, Christian (2002) : Die Archivierung elektronischer Unterlagen in der baden-württembergischen Archivverwaltung. Eine Konzeption (12.6.2002),

Köpke, Gernot; Scherer, Mathias (2002) : Leitfaden „Aufbewahrung von Dokumenten“ für Hersteller, Lieferanten und Anwender von Elektronischen Bauelementen und Baugruppen auf dem deutschen Markt. Frankfurt.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder [Hrsg.] : Datenschutzgerechtes E-Government. Handlungsempfehlungen.

Rathje, Ulf (2002) : Technisches Konzept für die Datenarchivierung im Bundesarchiv. In : Der Achivar, Jg. 55 (2002), S.117-120.

Richter, Rolf D. (2003) : Storage-Infrastrukturen nach Maß. http ://www.speicherguide.de/magazin/background.asp?theID=189

Schäfer, Udo ; Nicole Bickhoff [Hrsg.] (1999) : Archivierung elektronischer Unterlagen (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg : Serie A, Landesarchivdirektion, H. 13), Stuttgart, S. 165–181.

Verein schweizerischer Archivarinnen und Archivare (VSA) [Hrsg.] : Arbeitsgruppe „Archivierung elektronischer Akten“ : Aktionsprogramm 1999/2000 : Basisdokument.

Victorian Electronic Records Strategy (VERS) : http ://www.prov.vic.gov.au/vers/standards/pros9907vers2/default.htm

Wettengel, Michael : Technische Infrastruktur für die Archivierung von digitalen Datenbeständen - Anforderungen und Verfahrensweisen. In : INSAR Beilage II (1997) (Vorträge und Ergebnisse des DLM-Forums über elektronische Aufzeichnungen), S. 190 - 198.

Aktuelle Information und Charakteristika elektronischer Speichermedien finden sich unter folgenden Webadressen :

http ://de.wikipedia.org/wiki/Speichermedien

http ://www.speicherguide.de/