# Kundeninformation "IT und Sicherheit"

## 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
- 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

In den frühen Kindertagen des (Personal-)Computers verstand man unter Computersicherheit die Sicherstellung der korrekten Funktionalität von Hardware (Ausfall von zum Beispiel Bandlaufwerken oder anderen mechanischen Bauteilen) und Software (richtige Installation und Wartung von Programmen). Mit der Zeit änderten sich die Anforderungen an die Computer (Internet, Speichermedien); die Aufgaben zur Computersicherheit mußten anders gestaltet werden. Somit bleibt der Begriff der Computersicherheit wandelbar.

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit, Privatpersonen in den meisten Belangen des täglichen Lebens auf IT-Systeme angewiesen. Da neben der Abhängigkeit auch die Risiken für IT-Systeme in Unternehmungen in der Regel größer sind als für Computer und Netzwerke in privaten Haushalten, ist Informationssicherheit überwiegend Aufgabe von Unternehmen.

Entsprechende Verpflichtungen lassen sich im gesamten deutschsprachigen Raum aus den verschiedenen Gesetzen zum Gesellschaftsrecht, Haftungsrecht, Datenschutz, Bankenrecht usw. herleiten. Dort stellt Informationssicherheit einen Baustein des Risikomanagements dar. International spielen Vorschriften wie Basel II und der Sarbanes-Oxley Act eine wichtige Rolle.

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch eine anspruchsvolle Abwehr beantwortet werden kann. Der Kauf und die Installation einer Software ist kein Ersatz für eine umsichtige Analyse der Risiken, möglicher Verluste, der Abwehr und von Sicherheitsbestimmungen. Ist einmal die Sicherheit eines Systems verletzt worden, muss es als kompromittiert betrachtet werden, was Maßnahmen zur Verhinderung weiterer Schäden und ggf. zur Datenrettung erfordert. Die Maßnahmen müssen im Rahmen der Erstellung eines Sicherheitskonzeptes an den Wert der zu schützenden Unternehmenswerte angepaßt werden. Zu viele Maßnahmen bedeuten zu hohe finanzielle, organisatorische oder personelle Aufwände. Akzeptanzprobleme treten auf, wenn die Mitarbeiter nicht genügend in den Prozess der IT-Sicherheit eingebunden werden. Implementiert man zu wenig Maßnahmen, bleiben für Angreifer lohnende Sicherheitslücken offen.

# Wichtige Passagen aus dem Grundschutzkatalog des BSI

Bundesamt für Sicherheit in der Informationstechnik

*Warum muß der Zugang zu Arbeitsplatzrechnern zeitlich eingeschränkt werden ?*

*Warum müssen PCs nach ca. 20 Minuten automatisch geschützt werden ?*

**Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung**

Verantwortlich für Initiierung: Geschäftsführung, Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Geschäftsführung, Leiter IT, IT-Sicherheitsmanagement, Benutzer

Wird ein IT-System oder eine IT - Anwendung von mehreren Benutzern verwendet (Verfahren im Netzwerk) und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet.

Ist es einem Dritten möglich, an einem IT-System oder in einer IT – Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT – Anwendung abzumelden.

Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT - Systemen und IT - Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen (siehe auch M 4.2 Bildschirmsperre). Bei längerer Abwesenheit sollte die Bildschirmsperre **automatisch aktiviert** werden.

Einige IT - Systeme und IT - Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom System abgemeldet wird.

## G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen **dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind**.

Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu **Sicherheitslücken**, falls über die notwendigen Rechte hinaus weitere vergeben werden.

## M 2.7 Vergabe von Zugangsberechtigungen

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

Dies ist für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung (siehe M 2.5 Aufgabenverteilung und Funktionstrennung), im einzelnen festzulegen.

Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT – Anwendung (Anwender). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Der Zugang soll - sofern technisch möglich - erst nach einer Identifikation (z. B. durch Name, User-ID oder Chipkarte) und Authentisierung (z. B. durch ein Passwort) des Nutzungsberechtigten möglich sein und protokolliert
werden.

Die Ausgabe bzw. der Einzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentisierungsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung, siehe M 2.11 Regelung des Passwortgebrauchs) müssen ebenfalls getroffen werden.

Zugangsberechtigungen sollten bei länger währender Abwesenheit einer berechtigten Person vorübergehend gesperrt werden, um Mißbrauch zu verhindern, z. B. bei Krankheit oder Urlaub. Es ist notwendig, die vorgenannten Festlegungen auf ihre korrekte Einhaltung zu kontrollieren.

*Warum müssen (Kunden-) Daten vor Manipulation geschützt werden ?*

**G 3.24 Unbeabsichtigte Datenmanipulation**

Je umfangreichere Zugriffsberechtigungen auf eine Datenbank für die Anwender bestehen, um so größer ist auch das Risiko einer unbeabsichtigten Datenmanipulation. Dies kann prinzipiell von keiner Anwendung verhindert werden.

Die grundsätzlichen Ursachen für unbeabsichtigte Datenmanipulationen können z. B. sein:
- mangelhafte oder fehlende Fachkenntnisse,
- mangelhafte oder fehlende Kenntnisse der Anwendung,
- zu umfangreiche Zugriffsberechtigungen und
- Fahrlässigkeit (z. B. das Verlassen des Arbeitsplatzes ohne korrekte Beendigung der Anwendung).

*Warum muß die Dateiablage / Datenorganisation strukturiert organisiert sein ?*

**G 3.31 Unstrukturierte Datenhaltung**

Durch **Mißachtung von Vorgaben** durch Mitarbeiter kann es zu einer unübersichtlichen Speicherung der Daten auf den benutzten Datenträgern kommen.

Dadurch kann es zu verschiedenen Probleme kommen wie:
- Speicherplatzverschwendung durch mehrfache Speicherung von Dateien,
- vorschnelle Löschung oder nicht erfolgte Löschung von Daten, da keiner mehr weiß, was in welchen Dateien gespeichert ist,
- unbefugte Zugriffe, wenn sich Dateien in Verzeichnisse oder auf Datenträgern befinden, die Dritten zugänglich gemacht werden, oder
- nicht konsistente Versionsstände in verschiedenen Verzeichnen und IT - Systemen.

*Warum müssen Paßwörter sicher sein und öfter gewechselt werden ?*

**G 3.43 Ungeeigneter Umgang mit Passwörtern**

Selbst die Nutzung von durchdachten Authentifikationsverfahren hilft wenig, wenn die Benutzer nicht sorgfältig mit den benötigten Zugangsmitteln umgehen. Unabhängig davon, ob Passwörter, PINs oder Authentikationstoken zum Einsatz kommen, werden diese immer wieder weitergegeben oder unsicher aufbewahrt.

Benutzer geben oft aus Bequemlichkeit Passwörter an andere Benutzer weiter. Häufig werden Passwörter innerhalb von Arbeitsgruppen geteilt, um jedem Mitarbeiter den Zugriff auf gemeinsam zu bearbeitende Dateien zu erleichtern. Der Zwang zur Passwortbenutzung wird oft als lästig empfunden und dadurch **unterlaufen**, dass Passwörter nie gewechselt werden oder alle Mitarbeiter dasselbe Passwort benutzen.

*Warum so ein „Zinnober“ um die Datensicherung und -archivierung ?*

**G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen**

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Vorgaben zu beachten, deren Nichteinhaltung zivil- oder strafrechtliche Konsequenzen haben kann. Hervorzuheben sind hier u. a. die Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben, Vorgaben an die Höchstaufbewahrungsdauer, die sich aus Datenschutzregelungen ableiten, Zugriffsrechte, die für Externe - wie z. B. Steuerbehörden - gewährt werden müssen, sowie die Rechtslage zur digitalen Signatur.

Einige Quellen für rechtliche Rahmenbedingungen sind in der Maßnahme M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung aufgeführt.

*Warum sind "meine" Zugriffsrechte beschränkt ?*

**G 2.7 Unerlaubte Ausübung von Rechten**

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um eine sichere und ordnungsgemäße IT - Nutzung zu gewährleisten.

Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, können sich eine Vielzahl von Gefährdungen ergeben, die die Vertraulichkeit und Integrität des IT – Verbundes gefährden.

**M 4.17 Sperren und Löschen nicht benötigter Accounts und Zugänge**

Verantwortlich für Initiierung: Geschäftsführung, Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Administrator

Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt und später gelöscht werden. Wenn beim Löschen von Accounts Dateien übrigbleiben, die keinem existierenden Benutzereintrag mehr zugeordnet sind, besteht die Gefahr, dass diese Dateien später eingerichteten Benutzern unberechtigt zugeordnet werden.

Ebenso sollten Zugänge, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später entfernt werden.

*Warum ggf. ein "Gastzugang" ?*

Wenn ein neu einzurichtender Benutzer seinen Account nur für einen begrenzten Zeitraum benötigt, sollte dieser nur befristet eingerichtet werden. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen bei Bedarf zu verlängern.

Ist absehbar, dass ein Benutzer eines lokalen Netzes längere Zeit abwesend ist (Urlaub, Krankheit, Abordnung, ...), so sollte sein Account für diese Zeit im Netz gesperrt werden, so dass das Arbeiten unter seiner Benutzerkennung für diese Zeit nicht mehr möglich ist. Jeder Benutzer sollte dem Netzadministrator Zeiten längerer Abwesenheit mitteilen.

*Warum keine Memory – Sticks oder unbeschränkter Digitalkameragebrauch ?*

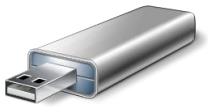
**G 2.8 Unkontrollierter Einsatz von Betriebsmitteln**

Betriebsmittel - gleich welcher Art - dürfen nur entsprechend dem Verwendungszweck eingesetzt werden.

Die für die Beschaffung und den Einsatz der Betriebsmittel verantwortlichen Personen müssen sowohl **den unkontrollierten Einsatz verhindern als auch den korrekten Einsatz überwachen**. Wird jedoch der Einsatz von Betriebsmitteln nicht ausreichend kontrolliert, können als Folge vielfältige Gefährdungen auftreten.

## Beispiel

Der Einsatz privater Datenträger durch Mitarbeiter kann zu einem Befall des dienstlichen Netzwerks durch Malware (z.B. Computer-Schadprogramme) führen.



## M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Geschäftsführung, Leiter IT, IT-Sicherheitsmanagement, Verantwortlich für Umsetzung: Geschäftsführung, Leiter IT

Es ist durchaus üblich, dass Mitarbeiter eigene Hard- und Software wie beispielsweise private Mobiltelefone, PDAs oder Kameras auch dienstlich oder zumindest in den Diensträumen verwenden. Da die Nutzung von zusätzlicher Hardware über Standardschnittstellen wie USB und weitgehende Plug-and-Play-Funktionalität immer einfacher wird, muss deren Einsatz geregelt werden. Die IT-Sicherheit kann dabei beispielsweise durch externe USB - Speichermedien (z. B. Festplatten, Memory - Sticks) oder private PDAs beeinträchtigt werden.

Es muss daher geregelt sein, wie Hard- und Software abgenommen, freigegeben, installiert bzw. benutzt werden darf. Maßnahmen, die zu diesem Zweck umgesetzt werden sollten, sind z. B.:
M 2.216 Genehmigungsverfahren für IT-Komponenten,
M 2.62 Software-Abnahme- und Freigabe-Verfahren bzw. Baustein
B 1.10 Standardsoftware und M 4.4

Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern:

**Das Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muß verboten und außerdem durch technische Möglichkeiten soweit wie möglich verhindert werden.**

Bei den meisten Betriebssystemen kann dies durch Einschränkung der Benutzerumgebung erreicht werden.

Damit soll verhindert werden, dass Programme mit unerwünschten Auswirkungen eingebracht werden. Zusätzlich soll verhindert werden, dass das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird.

Es kann sinnvoll sein (z. B. um Makro-Viren vorzubeugen), dieses Nutzungsverbot auch auf das Einspielen privater Daten auszudehnen. Bei Software ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden (inklusive Erstellungsdatum und Dateigröße). Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

**M 3.26 Einweisung des Personals in den sicheren Umgang mit IT**

Verantwortlich für Initiierung: Leiter Personal, Geschäftsführung, Leiter IT, IT – Sicherheitsmanagement. Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Viele IT-Sicherheitsprobleme entstehen durch fehlerhafte Nutzung bzw. Konfiguration der IT. Um solchen Problemen vorzubeugen, sollten alle Mitarbeiter in den sicheren Umgang mit der IT eingewiesen werden. Hierzu sollten alle Mitarbeiter entsprechend geschult werden (siehe auch M 3.4 Schulung vor Programmnutzung, M 3.5 Schulung zu IT-Sicherheitsmaßnahmen und M 2.198 Sensibilisierung der Mitarbeiter für IT-Sicherheit).

Den IT-Benutzern sollten spezifische Richtlinien an die Hand gegeben werden, was sie im Umgang mit der IT beachten müssen. In einer solchen Richtlinie sollte verbindlich vorgeschrieben werden, welche Randbedingungen beim Einsatz der betrachteten IT-Systeme einzuhalten und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Dabei sind die Benutzer klar und unmißverständlich darauf hinzuweisen, was sie auf keinen Fall machen dürfen.

Diese Richtlinien sollten verbindlich, verständlich und verfügbar sein. Um die Verbindlichkeit zu dokumentieren, sollten sie von der Behörden- bzw. Unternehmensleitung oder zumindest vom IT-Verantwortlichen unterzeichnet sein. Sie sollten kurz und verständlich gehalten sein, so dass sie beispielsweise als Merkzettel aufgehängt werden können. Zusätzlich sollten sie im Intranet abrufbar sein.

Beispiel

"Alle IT-Systeme werden in einer Standardkonfiguration ausgeliefert, die auf *Ihre* spezifischen Arbeitsbedingungen angepaßt wurde und *Ihnen* maximale Sicherheit bietet.

Bei Problemfällen können wir *Ihnen* durch eine Neuinstallation der Standardkonfiguration eine schnelle Problemlösung garantieren.

Bitte verändern *Sie* daher die Einstellungen möglichst nicht. Wenn *Sie* zusätzliche Hard- oder Software benötigen, wenden *Sie* sich bitte an den Benutzerservice."

Eine **Benutzerrichtlinie** für die allgemeine IT-Nutzung sollte mindestens die folgenden Punkte umfassen:

(1) Hinweis, dass keine IT-Systeme oder IT-Komponenten ohne ausdrückliche Erlaubnis benutzt werden dürfen;

(2) Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind.

(3) Umgang mit Passwörtern
(siehe M 2.11 Regelung des Passwortgebrauchs)

(4) Nutzungsverbot nicht freigegebener Software
(siehe M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software)

(5) Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen

(6) Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern

(7) Schutz vor Computer-Viren

(8) Durchführung von Datensicherungen

(9) Nutzung von Internet-Diensten

Neben solchen Richtlinien müssen klare Aussagen darüber vorliegen, welche Benutzer auf welche Informationen zugreifen dürfen, an wen diese weitergegeben werden dürfen und welche Maßnahmen bei einem Verstoß gegen diese Richtlinien unternommen werden.

Bei Verlassen des Arbeitsplatzes sollte sich jeder Benutzer davon überzeugen, dass jedes Arbeitsmittel (Dokumente, Datenträger, etc.) sicher verwahrt ist (siehe auch M 2.37 "Der aufgeräumte Arbeitsplatz").

Alle IT-Systeme sollten durch Passwörter gegen unbefugten Zugriff geschützt sein. Bei unbeaufsichtigten IT - Systeme sollten alle offenen Sitzungen beendet worden sein oder zumindest ein Bildschirmschoner aktiviert sein.

Die Grundkonfiguration aller IT-Systeme sollte möglichst eingeschränkt sein. In der Standardkonfiguration von Arbeitsplatzrechnern sollten nur die Dienste vorhanden sein, die von allen Benutzern einer Gruppe benötigt werden (siehe auch M 4.109 Software-Re-Installation bei Arbeitsplatzrechnern).

Weitere Programme oder Funktionalitäten sollten nur dann aufgespielt bzw. freigeschaltet werden, wenn die Benutzer in deren Handhabung eingewiesen und für eventuelle Sicherheitsprobleme sensibilisiert wurden.

Jede Benutzerordnung sollte in Zusammenarbeit mit Vertretern aller beteiligten Gruppen erstellt werden, insbesondere sollten Betriebs- bzw. Personalrat und Datenschutz- sowie IT-Sicherheitsbeauftragte rechtzeitig beteiligt werden.

Bei jeder Änderung einer Benutzerordnung ist darauf zu achten, daß diese wieder im Vorfeld beteiligt werden. Die geänderte Benutzerordnung muss allen Benutzern bekanntgegeben werden.

Die Aufgabenbeschreibung sollte alle für die IT-Sicherheit relevanten Aufgaben und Verpflichtungen enthalten. Dazu gehört u. a. die Verpflichtung auf die hausinternen IT-Sicherheitsleitlinien (siehe auch M 2.198 Sensibilisierung der Mitarbeiter für IT-Sicherheit).

Werden IT-Systeme oder Dienste in einer Weise genutzt, die den Interessen der Behörde bzw. des Unternehmens widersprechen, sollte jeder, der davon Kenntnis erhält, dies seinen Vorgesetzten mitteilen.

**M 6 Maßnahmenkatalog Notfallvorsorge**

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen
M 6.2 Notfall-Definition, Notfall-Verantwortlicher
M 6.3 Erstellung eines Notfall-Handbuches
M 6.4 Dokumentation der Kapazitätsanforderungen der IT - Anwendungen
M 6.5 Definition des eingeschränkten IT-Betriebs
M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten
M 6.7 Regelung der Verantwortung im Notfall
M 6.8 Alarmierungsplan
M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse
M 6.10 Notfall-Plan für DFÜ-Ausfall
M 6.11 Erstellung eines Wiederanlaufplans
M 6.12 Durchführung von Notfallübungen
M 6.13 Erstellung eines Datensicherungsplans
M 6.14 Ersatzbeschaffungsplan
M 6.15 Lieferantenvereinbarungen
M 6.16 Abschließen von Versicherungen
M 6.17 Alarmierungsplan und Brandschutzübungen
M 6.18 Redundante Leitungsführung
M 6.19 Datensicherung am PC
M 6.20 Geeignete Aufbewahrung der Backup-Datenträger
M 6.21 Sicherungskopie der eingesetzten Software
M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
M 6.23 Verhaltensregeln bei Auftreten eines Computer-Virus
M 6.24 Erstellen eines Notfall-Bootmediums
M 6.25 Regelmäßige Datensicherung der Server-Festplatte
M 6.26 Regelmäßige Datensicherung der TK - Anlagen - Konfigurationsdaten
M 6.27 Sicheres Update des BIOS
M 6.28 Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen
M 6.29 TK-Basisanschluss für Notrufe
M 6.30 Katastrophenschaltung
M 6.31 Verhaltensregeln nach Verlust der Systemintegrität
M 6.32 Regelmäßige Datensicherung
M 6.33 Entwicklung eines Datensicherungskonzepts
M 6.34 Erhebung der Einflussfaktoren der Datensicherung
M 6.35 Festlegung der Verfahrensweise für die Datensicherung
M 6.36 Festlegung des Minimaldatensicherungskonzeptes
M 6.37 Dokumentation der Datensicherung
M 6.38 Sicherungskopie der übermittelten Daten

**M 6 Maßnahmenkatalog Notfallvorsorge**

M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung
M 6.40 Regelmäßige Batterieprüfung/-wechsel
M 6.41 Übungen zur Datenrekonstruktion
M 6.42 Erstellung von Rettungsdisketten für Windows NT
M 6.43 Einsatz redundanter Windows NT/2000 Server
M 6.44 Datensicherung unter Windows NT
M 6.45 Datensicherung unter Windows 95
M 6.46 Erstellung von Rettungsdisketten für Windows 95
M 6.47 Aufbewahrung der Backup-Datenträger für Telearbeit
M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität
M 6.49 Datensicherung einer Datenbank
M 6.50 Archivierung von Datenbeständen
M 6.51 Wiederherstellung einer Datenbank
M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
M 6.53 Redundante Auslegung der Netzkomponenten
M 6.54 Verhaltensregeln nach Verlust der Netzintegrität
M 6.55 Reduzierung der Wiederanlaufzeit für Novell Netware Server
M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren
M 6.57 Erstellen eines Notfallplans für den Ausfall des Managementsystems
M 6.58 Managementsystem zur Behandlung von Sicherheitsvorfällen
M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
M 6.60 Verhaltensregeln und Meldewege bei Sicherheitsvorfällen
M 6.61 Eskalationsstrategie für Sicherheitsvorfälle
M 6.62 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
M 6.63 Untersuchung und Bewertung eines Sicherheitsvorfalls
M 6.64 Behebung von Sicherheitsvorfällen
M 6.65 Benachrichtigung betroffener Stellen
M 6.66 Nachbereitung von Sicherheitsvorfällen
M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
M 6.68 Effizienzprüfung Managementsystem Behandlung von Sicherheitsvorfällen
M 6.69 Notfallvorsorge und Ausfallsicherheit bei Faxservern
M 6.70 Erstellen eines Notfallplans für den Ausfall des RASSystems
M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems
M 6.72 Ausfallvorsorge bei Mobiltelefonen
M 6.73 Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
M 6.74 Notfallarchiv
M 6.75 Redundante Kommunikationsverbindungen
M 6.76 Erstellen Notfallplan für den Ausfall von Windows 2000/XP/2003-Systemen
M 6.77 Erstellung von Rettungsdisketten für Windows 2000

**M 6 Maßnahmenkatalog Notfallvorsorge**

M 6.78 Datensicherung unter Windows 2000/XP
M 6.79 Datensicherung beim Einsatz von Internet-PCs
M 6.80 Erstellen Notfallplan für Ausfall eines Novell eDirectory Verzeichnisdienstes
M 6.81 Erstellen von Datensicherungen für Novell eDirectory
M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen
M 6.83 Notfallvorsorge beim Outsourcing
M 6.84 Regelmäßige Datensicherung der System- und Archivdaten
M 6.85 Erstellung eines Notfallplans für den Ausfall des IIS
M 6.86 Schutz vor schädlichem Code auf dem IIS
M 6.87 Datensicherung auf dem IIS
M 6.88 Erstellen eines Notfallplans für den Webserver
M 6.89 Notfallvorsorge für einen Apache-Webserver
M 6.90 Datensicherung und Archivierung von E-Mails
M 6.91 Datensicherung und Recovery bei Routern und Switches
M 6.92 Notfallvorsorge bei Routern und Switches
M 6.93 Notfallvorsorge für z/OS-Systeme
M 6.94 Notfallvorsorge bei Sicherheitsgateways
M 6.95 Ausfallvorsorge und Datensicherung bei PDAs
M 6.96 Notfallvorsorge für einen Server
M 6.97 Notfallvorsorge für SAP Systeme
M 6.98 Notfallvorsorge für Speichersysteme
M 6.99 Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server
M 6.100 Erstellung eines Notfallplans für den Ausfall von VoIP
M 6.101 Datensicherung bei VoIP
M 6.102 Verhaltensregeln bei WLAN-Sicherheitsvorfällen
M 6.103 Redundanzen für die Primärverkabelung
M 6.104 Redundanzen für die Gebäudeverkabelung
M 6.105 Notfallfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten
M 6.106 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes
M 6.107 Erstellung von Datensicherungen für Verzeichnisdienste
M 6.108 Datensicherung für Domänen-Controller
M 6.109 Notfallplan für den Ausfall eines VPNs

Quellen :

- Bundesamt für die Sicherheit in der Informationstechnik (BSI)

- id-newmedia " ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen"