© OptiOrg Roten www.102.ch

Sicherheits konzept

Struktur

Vorbeugende Massnhamen

Organisatorische Massnahmen
- Dienstanweisungen
- Notfallplan
- Alarmierungsplan
- Ausweiswesen
- Schliess-Oranisation
- Umgang mit Betriebs-geheimnissen
- vertragliche Vereinbarungen
- Arbeitsanweisungen
- Rest-Risiko
- Datensicherheit
- Versicherungen

techinsche Massnahmen
- Einbruch-Meldeanlagen
- Brand-Meldeanlagen
- Aussensicherung
- Panzer-Geldschränke
- Datensicherung
- Zutrittskontrollesysteme
- Brandschutztüren
- Brandschutzmauern
- Rettungswege
- Meldezentralen
- USV
- Notstrom-Konzept

personelle Massnahemen
- Hinweise auswerten
- Begehungen
- Kontrolle
- Uebungen
- Unterweisungen
- Schulung
- Ausbildung
- Training

Abwehrende Mamssnahmen

technische Massnahmen
- Löschgeräte
- automatische Löscheinrichtungen
- Schiebetore, Drehtüren, Schleusen
- Beleuchtung, Sirenen, Kameras
- Rettungsgeräte
- Rettungsfahrzeuge

personelle Massnahmen
- Betriebschutz (Feuerwehr Sanität)
- Objektschutz
- Rettungsdienst
- Personenschutz
- technische Dienste

Rückwirkende Massnahemen
- Ereignis-Analyse/Korrekturen
- Analyse der Elnsatz-Dipositive und mögliche Korrekturen
- Ermittlungen
- Erfahrungsaustausch mit Spezialisten, Verantwortlichen
- Statistische Auswertungen/Vergleiche

Informationsschutz

Datenschutz Datensicherheit

Besonders schützenserte Personendaten
- religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten
- Gesundheit, Intimsphäre oder Rassenzugehörigkeit
- Massnahmen der sozialen Hilfe
- administrative oder strafrechtliche Verfolgungen oder Sanktionen

Risiken im Umgang mit Daten

Aktive Bedrohung
- vorsätzliche unberechtigte, verbotene Nutzung von Hard- und Software
- vorsätzliche Veränderungen von Daten (Manipulation)
- vorsätzliche Einbinden gefälschter Daten
- Diebstahl von Daten durch Kopierprozesse
- vorsätzliches Verändern von System- und Kommunikationsstati zum Zweck der Sabotage oder des Hackings

Passive Bedrohung
- unberechtigtes Verfolgen/Auswerten von Daten in der Datenkommunikation
- Ausspähen von Daten
- Abhören von Datenkommunikationsprozessen

Daten
- Datenintegrität heißt, daß die Daten vollständig, widerspruchsfrei , konsistent, redundant und korrekt sind.

Disaster Recovery Plan

Ziel
Die Verfügbarkeit der wichtigsten Applikationen und Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehrungen zur Schadensbegrenzung im Katastrophenfall zu treffen

- Definition von Verfügbarkeitsklassen
- Erfassung aller Anwendungen und Klassifikation nach Verfügbarkeitsanforderungen
- Festlegung der Schadnesereignisse, gegen die Vorkehrungen zu treffen sind; Risikoakzeptanz bei nicht abzudeckenden Ereignissen
- Notfallorganisation und Notlaufplan
- Erstellung eines Backup-Konzepts
- Erstellung von Wiederanlaufplänen
- Regelmässige Tests und Training
- Weiterentwicklung und Anpassung des Disaster Recovery Plans

Vorgehen Sicherheitsstrategie

1. Gefahrenkataster
   - Auflistung aller Ressourcen: Computer, Drucker, Netzwerkkomponenten, Routen, Fireall, Kabel (Steigleitungen), Gebäude, Räume wo Sicherungskopien lagern, Putzequippe, Hauswart, Mitarbeiter, Feuerwehr
2. Katalogisierung
   - wer muss wann physisch Zugang haben und wer muss wann logisch auf welche Informationen zugreifen?
3. Risikoanalyse
   - Alle Gefahren können nicht abgewendet werden - welche Gefahren können ignoriert werden? Welcher Schaden ist 'tragbar'? Was ist wie schnell und mit welchem Aufwand wiederhestellbar
4. Sicherheitssystem einführen/anpassen
   - Zum Schutz der wahrscheindlichsten Gefahren müssen Investitonen getätigt werden die nie zurückfliessen. Allenfalls wurde aber der Verlauf von viel Geld vermieden....
5. ständige Kontrolle und Audit

By M.Roten www.102.ch

© OptiOrg Roten Organisation & Projektleitung Morgenhölzlistr. 27a CH-8912 Obfelden www.102.ch info@102.ch