



Aufgaben, Tätigkeiten und Ergebnisse im Rahmen von Sicherheitsprojekten



Aufgaben, Tätigkeiten und Ergebnisse im Rahmen von Sicherheitsprojekten

Ziel von IT-Sicherheit ist es, mit Hilfe eines umfassenden IT-Sicherheitsmanagements die Datensicherheit und den Schutz geschäftlich genutzter Daten zu gewährleisten und dabei die Erstellung von Risikoanalysen und Sicherheitskonzepten zu unterstützen.

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wieder aufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.*

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

Der Sicherheits-Philosophie, basierend auf dem „Need-to-do-Prinzip“, steht oftmals kein ganzheitliches, wirksames Konzept gegenüber, welches ausreichenden Schutz für die IT dieser Unternehmen sichert. Die IT-Sicherheit ist jedoch als ein sehr bedeutender Partner zu verstehen, ohne den kein Unternehmen erfolgreich sein kann.

Die networker, projektberatung GmbH kann aufgrund langjähriger, praktischer Erfahrung bei der Implementierung und Pflege von IT-Sicherheitskonzepten in Ihrem Unternehmen Unterstützung leisten.

Hierzu zählen die für dieses sensible Thema unabdingbare Implementierung einer unternehmenseinheitlichen Sicherheitsrichtlinie, die sowohl die Anforderungen der Kunden, der Fachseiten und des Betriebs berücksichtigt. Des Weiteren fehlt in vielen Fällen ein Notfallplan sowie die Beschreibung und Festsetzung von Maßnahmen in Ausnahmefällen (Disaster-Recovery).

Nicht selten vergeht wertvolle Zeit, weil niemand in der Firma weiß, wer in Notfällen zu kontaktieren ist, und Hacker würden in vielen Netzwerken problemlos Zugang erhalten. Ebenso häufig ist unklar, welche Geschäftsprozesse dringend Sicherheitsmaßnahmen bedürfen, weil sie zu unterbrechen eine Katastrophe für Ihr Unternehmen bedeuten würde.

networker, projektberatung GmbH kann erfahrende Projektleiter für solche Projekte stellen oder innerhalb der Projektkoordination mitwirken.

Ausgangspunkt für alle weiteren Maßnahmen ist eine detaillierte Ist-Analyse der IT- und Gebäudeinfrastruktur, sowie sämtliche von IT-Sicherheit betroffenen Geschäftsprozesse. Diese stellt eine Grundlage für die Erstellung einer unternehmensweiten IT-Sicherheitsrichtlinie, sowie deren vollständige Implementierung dar. Des Weiteren sollte im Rahmen von Sicherheitsprojekten ein Notfallplan, sowie ein Backup- und Recoveryplan implementiert, bzw. existierende Pläne überprüft werden.

* Vgl. hierzu auch das IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik (IT-GSHB, siehe <http://www.bsi.de/gshb/deutsch/b/34.htm> bzw. <http://www.bsi.bund.de/gshb/deutsch/menue.htm>) als Maßnahmenempfehlung für den Schutzbedarf und als Mindeststandard für Informationstechnik und Kommunikation.

Die vollständige Implementierung von Sicherheit im Unternehmen endet mit einem unternehmensweiten Sicherheitsaudit und anschließender Auswertung des Audits, sowie die Übergabe sämtlicher Dokumente, wie z.B. das IT-Sicherheitshandbuch, an den Kunden.

Stufen eines potenziellen Sicherheitskonzeptes als Projekt

1. Implementierung einer Security-Projektorganisation

Definition, Organisation, Umsetzung und Inbetriebnahme eines zeitlich und ökonomisch exakt definierten Projektes „Sicherheit im IT-Bereich“

Tätigkeiten:

- Aufbau der Projektorganisation (bei Bedarf nach PRINCE2)
- Zusammenstellung des Projektleitteams, inkl. Überprüfung fachlicher Qualifikationen (Skill Assessment)
- Stellen des Projektleiters
- Projektunterstützung
- Organisatorische Unterstützung
 - Bindeglied zwischen Ansprechpartnern verschiedener Abteilungen
 - Koordination der Arbeiten, Zuteilung der Mitarbeiter

Das Ergebnis dieser Maßnahme ist eine für die Einführung von IT Sicherheit optimierte Projektorganisation. Sie gewährleistet die Einführung der Sicherheitsstandards zu einem exakt definierten Zeitpunkt.

2. Implementierung einer unternehmensweiten Sicherheitsrichtlinie

Tätigkeiten:

- Dokumentation der aktuellen IT- und Gebäudeinfrastruktur
 - Ist-Aufnahme IT-Infrastruktur (Netzstruktur, Strom) wie z.B. Patchfelder, Stromschienen, etc.
 - Ist-Aufnahme Hardware (Server, Storage, USV, etc), insbesondere auch Spezialkarten, Modems, etc. und aufteilen der Server in Sicherheitsklassen
 - Ist-Aufnahme Firmenstandards wie Namenskonvention (Hostnamen, DNS, User-GroupIDs, etc.)

- Ist-Aufnahme Applikationen und deren Schnittstellen und Abhängigkeiten
 - Ist-Aufnahme der Patchstände aller Server, ggf. Releases / Versionen
 - Scannen aller Server mit Securityscannern
 - Ist-Aufnahme Betriebsprozesse
 - Ist-Aufnahme SLA
- Dynamische Recherche, Analyse und Evaluierung sicherheitsrelevanter Informationen und deren Dokumentation
 - Schwachstellenanalyse in der Produktionskette automatisierter Installationsverfahren
 - Auswahl und Evaluierung von Werkzeugen zur Überprüfung der Sicherheit
 - Verträglichkeitstests der gewählten Lösungen
 - Umsetzung von Passworrichtlinien
 - Flächendeckende Einführung von Transportverschlüsselung wie SSH, SFTP etc.
 - Vertrauenswürdigkeit und Transparenz durch eindeutige Identifizierung
 - Erstellung von Prototypen und Piloten für kritische Systeme
 - Entwicklung von sicherheitsrelevanten Applikationen und Integration in die vorhandene Überwachungsstruktur und somit
 - Verbesserung der Überwachungsprozedur
 - Entwicklung und Pflege von Applikationen zur Beurteilung der Qualität im Bereich Sicherheit
 - Begehung der Gebäudeinfrastruktur
 - Ist-Aufnahme Gebäudezugänge (Personen-, Auto-, Lieferantenzugänge)
 - Besondere Prüfung der RZ, bzw. Sicherheitszugänge für interne und besonders externe Mitarbeiter
 - Erstellung eines IT-Sicherheitshandbuches auf Basis gesammelter und ausgewerteter Informationen
 - Definition von Zugriffen auf System-Ressourcen durch die Anwender
 - Definition der Verwendung von System-Ressourcen durch die Anwender
 - Festlegung einer Zugangsdefinition zu den System-Ressourcen, insbesondere über den Zugriff von Außen
 - Definition der root Policies (Welcher Admin ist Superuser)
 - Grundsätzliche Redefinition von User- und Grouprechten
 - Definition von Verfahren ausscheidender User (Root & Anwender)
 - Definition über den Umgang mit sensiblen Daten
 - Definition über den Umgang und die Wahl von Passwörtern
 - Definition der Aufgaben des Managements zur Umsetzung der neuen Sicherheitsrichtlinie
 - Definition einer Regel, nach der die Sicherheitsregel in regelmäßigen Sicherheitsaudits überprüft und bekannt gemacht wird
 - Namentliche Benennung eines Sicherheitsverantwortlichen (ggf. Schulung, Einführung in die Prozesse)

- Definition eines Verfahrens, das den Zugang zu EDV-Bereichen, insbesondere sensible RZ-Bereiche aufzeichnet

- Implementierung von neuen Sicherheitsrichtlinien, basierend auf dem neuen Sicherheitshandbuch

- Umsetzung der neuen IT-Sicherheitsregeln in Referenz-Projekten, im weiteren Verlauf Übernahme in den Betrieb

Das Ergebnis ist eine Gesamtdokumentation des IST-Zustandes aus sicherheitstechnischen Aspekten und ein Sollkonzept in Form eines neuen IT-Sicherheitshandbuches. Hinzu kommt eine Projektdefinition für eine nach neuen Sicherheitsregeln definierte Betriebsumgebung.

3. Implementierung eines Notfallplans

Tätigkeiten:

- Überprüfen eines evt. vorhandenen Notfallplans, ansonsten Erstellung eines neuen, unternehmensweiten Notfallplans für den Betrieb aus sicherheitstechnischen Aspekten
 - Analyse und anschließende Bewertung eines evt. vorhandenen Notfallplans, bzw. Notfallhandbuches
 - Bei Bedarf Neuentwicklung des Notfallplans / Notfallhandbuches
 - Folgende Aspekte sollten auf jeden Fall enthalten sein:
 - Alarmierung im Notfall
 - Alarmierung und Meldewege
 - Adresslisten betroffener Mitarbeiter
 - Festlegung konkreter Aufgaben für einzelne Personen / Funktionen
 - Definition der Rollen im Rahmen eines Notfallplanes
 - Krisenmanager / Manager on Duty
 - Krisenstab
 - IT-Security-Team
 - Sonst. Ansprechpartner
 - Zustandsdefinition
 - Normalzustand
 - Warnzustand
 - Alarmzustand
 - Zustandswechsel

- Gründe für Zustandswechsel
 - Auslösen eines Zustandswechsels
- Definition von Sofortmassnahmen des Operating / Manager on Duty (MoD) im Falle eines Sicherheitsvorfalles
- Erstellen von Namenslisten mit Telefon-, Mobil-, und ggf. Pagernummern von zuständigen Managern, Administratoren, die benachrichtigt werden sollen
- Definition von Prozessen, wenn Sicherheitsverantwortliche nicht erreichbar sind Definition, wann ein Sicherheitsvorfall den Behörden gemeldet werden muss
- Definition der Beweissicherung von Daten im Falle eines ungewollten Zugriffs auf die Systeme
- Wiederanlaufpläne nach einem Störfall
- Überprüfung der Backup- und Recoverystrategie, so dass im Falle eines Systemausfalls durch Manipulation die betroffenen Systeme wiederhergestellt werden können
- Definition von Verfahren zur Weiterentwicklung der Sicherheitsrichtlinien und Notfallpläne
 - Anpassung der Sicherheitsrichtlinien bei Änderungen in der Unternehmensorganisation
 - Anpassung bei Einführung neuer Hard- und Software
 - Anpassung bei Bekanntgabe neuer Sicherheitslücken in vorhandener Hard- und Software

Das Ergebnis ist ein überarbeiteter bzw. neu entwickelter Notfallplan für den Umgang der Situation von ungewollten Sicherheitsvorfällen.

4. Durchführung eines abschließenden Sicherheitsaudits

Tätigkeiten:

- Durchführung eines Sicherheitsaudits durch networker – unter anderem mit:
 - Netzwerkscan offener Ports
 - Analyse des Portscans
 - Überprüfen der Patchstände
 - Überprüfung der Passwortsicherheit wie z.B. Mindestpasswortlänge, Aging, etc.
 - Boot-Services wie z.B. Überprüfung der Init-Skripte
 - Kernel: Überprüfung sicherheitsrelevanter Kernelparameter mit:
 - Stack Protection
 - TCP Sequenz Number
 - Netzwerkparameter

- Überprüfen der Zugriffsrechte auf Dateien und Verzeichnisse wie z.B. Auflistung der Dateien mit `suid-Flag`
 - Einstellungen bzgl. Systemzugriffen, Authentifizierung und Berechtigungen prüfen
 - Unbenutzte Accounts sperren / löschen
 - Anonymes Root-login auf Systemconsole beschränken
 - Zugriff auf `at` und `cron` beschränken
 - Weitere Prüfungen und Einstellungen
- Abgleich Ist-Analyse zu Projektstart mit Sicherheitsaudit zu Projektende
- Einschätzung und weitere Empfehlungen
- Übergabe sämtlicher Dokumente an den Betrieb

Das Ergebnis ist implementierte Sicherheit im Unternehmen, inkl. Überprüfung auf deren Umsetzung in Form des Audits.