Datensicherheit

Lösungsansätze und Prozessvorschläge zum Security-Management für IT-Anlagen

Michael Thoss
Leiter Zentrale Dienste Organisation und IT
DRK Kliniken Berlin

Grundlagen

- Mehrstufiges Sicherheitskonzept in einer integrierten Umgebung:
- Internetzugangssicherheit
- Email-Kommunikationssicherheit
- Mail(Groupware)-Kommunikationssicherheit
- Netzwerksicherheit in den LANs
- Arbeitsplatzsicherheit (internes Hacking)
- Datensicherheit (Datenschutz personenbezogener Daten z.B. Patienten)
- Netzwerksicherheit im WAN (VPN)
- Organisationssicherheit (Schwachstelle Mensch)
- Verfügbarkeitssicherheit
- Datensicherung
- Raumsicherheit (Serverräume)

Potentielle Konzeptlücken

- Fehlende Mittel
- Vorgaben / Sonderwünsche (fehlende Leitlinien)
- Technische / Bauliche Sicherheit
- Fehlende Überwachungssicherheit (fehlende Technik z.B. Zugangskontrolle, Videoüberwachung, mangelhafte Überwachung vorhandener Störungsmeldungen (z.B. Temperatur Serverräume))
- Fehlendes Risiko- und Sicherheitsbewusstsein der Mitarbeiter
- Faktor „Mensch“ allgemein

Internetzugang

- Internetzugang von jedem Unternehmens-PC innerhalb eines physikalischen Netzes
- Zugangskontrolle via persönlichen Account und Passwort (u.a. Disziplinarische Optionen)
- Browserbeschränkung auf ein Produkt
- Ein zentraler Zugang für das Unternehmen
- Firewall-Technologie (ggf. plus Proxy zur Kostenreduzierung)
- Contentfiltering
- ScanWall
- Protokollierung der Webaktivitäten (Nicht oder geregelt Nutzerbezogen)
- Virenscanner auf dem Front-End

Internetpräsenz

- Externes Hosting der Präsenz (Provider)
- Mail-Transfer via internen Server
- Serverplattform außerhalb des Unternehmens-WAN / LAN-Bereiches (außerhalb DMZ)
- FAZIT: Angriffe erschwert
- Bei Domain-Mißbrauch oder -Angriff einfacher UpLoad möglich
- Keine „Schleusen“ in der Security
- Prinzipiell natürlich Ermittlung der „Hausadresse IP“ (Firewall) möglich
- Prinzipiell natürlich „Mail-Risiko“

RAS

- Remote Access Services für Software-Systempartner und Hardwareservicepartner z.B. MedTech
- Zugangsrouter für Remote Access
- IP und Rufnummer-Authentifizierung
- Account und Passwort-Kontrolle
- Firewall-Plattform für Protokoll und Portkontrolle
- ... ftp, telnet und ähnliche Dienste trotz Security-Einschränkungen für Service notwendig
- Ggf. MAC-ID-Einschränkung für Arbeitsplätze mit Sonderfunktionen

E-Mail Kommunikation (extern)

- Ein zentraler Ein- und Ausgang für das Unternehmen
- Virenscanning aller eingehenden Nachrichten (Allgemeine Notwendigkeit)
- Virenscanning aller ausgehenden Nachrichten (Haftungsrisiko begrenzen)
- Täglicher automatischer (ggf. mehrmaliger) Patternupdate
- Virenscanning aller internen Nachrichten an und zwischen Standorten
- Benutzereinschränkungen. Jedem Groupwarenutzer steht das interne Mailsystem zur Verfügung, jedoch nur auf Antragsbasis die externe Kommunikation

I-Mail Kommunikation (intern)

- Virenscanning aller Nachrichten an und zwischen Unternehmensstandorten
- Limitierung der Benutzerpostfächer auf 5 – 250 MB (nach Userklassen)
- Keyuser entsprechend mit größerem Space
- „Knigge“ für die Mail-Kommunikation
- Keine Benutzerbeschränkung in der Groupware
- Zwei Postfachkonzepte:
  - 1. Gruppenpostfach für z.B. Stationen zum Zweck der ungerichteten Kommunikation
  - 2. Persönliche Postfächer zum Zweck der gerichteten Kommunikation

Netzwerksicherheit (LAN)

- Reine Switch-Technologie statt HUBs
- Nur genutzte Anschlußdosen sind auch beschaltet (im Ethernet-CAT5(ff)-Netz)
- Nur genutzte Switch-Ports sind auch aktiviert
- Alle Switche über Accounts und Passwörter im Administrationsbereich geschützt (nicht Herstellerstandards)
- Funknetze nur im Sonderfall und über MACid-Authorisierung, Verschlüsselung
- Physikalische Sicherheit: Verteilerschränke mit speziellem Schließsystem für bestimmte Personalgruppen (IT/TK)
- Verteilerräume mit speziellem Schließsystem

Arbeitsplatzsicherheit

- Lokale Virenscanner
- Zugriff auf Wechselmedien (Diskette, CD, USB) nur mit Ausnahmeregelung
- Zugriff auf BIOS generell nicht (Passwortschutz)
- Zugriff auf Desktop u.ä. eingeschränkt (Profile, Policys)
- Separate Account und Passwortregelungen für:
  - Allgemeiner Netzwerkzugang (Groupware)
  - Zugang auf KIS-Server (Personendaten)
  - Ggf. Zugang auf Subsysteme (Personendaten)
  - Internetzugang (Regelwerk, Contentfilter, url-Closing)

Datensicherheit / Datenschutz

- Umsetzung und Audits durch externen Datenschutzbeauftragten
- Datenschutzhandbuch für das Unternehmen
- Leitlinie der organisatorischen Sicherheit, Einheitliche Richtlinie auf standardisierter Basis für alle Benutzer

Netzwerksicherheit (WAN)

- Sicherheit durch verschlüsseltes VPN (IPSec)
- Strukturverantwortung und Verfügbarkeit in Verantwortung des Carriers bis zum Endpunkt / Übergabepunkt (Router inklusive)
- Steuerung der Router via Switche des Betreibers z.B. auf Basis OSPF-Protokolle zur Vereinfachten Administration bei Änderungen / Anpassungen
- Any-to-Any oder Point-to-Point Prüfungen hinsichtlich der Bedarfssituation

Organisationssicherheit

- Security-Konzepte (IT)
- Datenschutz-Konzepte (DSB)
- „Vier-Augen-Prinzip“ für alle Accounts (Benutzeranmeldungen, Internetzugänge, usw.)
- Kontrolllisten für Personalzu- und abgänge
- Personalanmeldungen via Personalverwaltung bzw. Dienstvorgesetzte
- Anmeldungen für Wechselmedien (Diskette, CD, USB), email und internet nur über Anträge / Formulare und definierte Organisation / Prozesse

Verfügbarkeit

- Serversysteme in Cluster- oder hochredundanter Technologie in Abhängigkeit zur Risikoeinstufung z.B. durch Eintrittshäufigkeit und wirtschaftlichen Schaden
- KIS-Server auf Basis UNIX-Server mit eigenen Storage-Systemen zum DB-optimierten Betrieb (z.B. SunFire-Server und T3 / T4-Storages)
- BackOffice-Server auf Basis Intel-Technologie mit SAN-Storage-Systemen (z.B. HP/Compaq Proliant und MSA1000 – EMA8000)
- Redundante Netzteile und Komponenten in allen Systemen, USV-Absicherung als Standard
- Vertragliche Serviceabsicherung nach Prioritäten der Systeme von 7*24 bis 5*10 abgestuft

Datensicherung

- Logische Datensicherungskonzepte (Stunden- / Tages- / Wochensicherungen)
- Physikalische Datensicherungskonzepte mit Librarys und/oder Robotern auf Basis DLT-Technologie
- Physikalische Datensicherungskonzepte zum Brandschutz und Schadenabwehr über klassische Safe-Techniken (aber auch Verteilte Installationen)
- Physikalisch/Logistische Konzepte wie z.B. regelmäßiger Medientausch u.ä.
- Organisationsmaßnahmen (tägliche Kontrolle der Sicherungen, Protokoll-Auswertung)
- Online-DB-Spiegel ins externe Data-Center für Primärsysteme als Rückversicherung

Raumsicherheit Serverräume

- Brandmelder / Rauchmelder
- Klimakontrolle (Temperaturkontrolle)
- Feuchtigkeitsüberwachung
- Beschränkte Zugangsberechtigung über Schließkonzept
- „Personal-free“ Remotebetrieb der Server
- Serverräume nicht in EG oder UG
- Serverräume außerhalb von „Verkehrszonen“
- Eigene Stromunterverteilungen
- Trennung in Server- und Betriebstechnikraum (z.B. Klimabasis und USV-Anlagen in getrennten Räumen und echter Serverbetrieb „begehungsfrei“)