Notizen Seminar 01909: Maßnahmen zur Absicherung von privaten und kleinen Unternehmensnetzwerken

Kerstin Lapp 5105200

November 12, 2018

Schutzziele und Bedrohungen

Angriffsziele (nach 1866 KE1 S.11):

- Kommunikationswege
- Computer
- Daten

Schutzziele (nach 186 KE1 S.12-16):

- Vertraulichkeit: Daten sind nur befugten Personen zugänglich.
  Bedrohung: unbefugter Informationsgewinn.
- Integrität: Daten sind korrekt und unverändert.
  Bedrohung: Unbefugte Modifikation
- Authentizität: Daten stammen von vorgeblichen Erzeuger.
  Bedrohung: unbefugte Erzeugung
- Verfügbarkeit: Daten können von befugten Personen gelesen/bearbeitet werden.
  Bedrohung: unbefugte Unterbrechung

Clientsicherheit

Nach [3]:

- Benutzergruppen mit verschiedenen rechten : lesen, schreiben, ausführen
- Minimalsystem auf Arbeitsplatz PCs
- Verschlüsselung (Festplatte und Kommunikation)
- Gerätekontrolle, Ausführungskontrolle
- Logging
- Personal Firewall
-

VLAN

VLANs = Virtuelle Netze
[10, S.167-169]
[1]

VLANs dienen der logischen Segmentierung von Netzen. Es sind logische Teilnetze, die an Switches gebildet werden. Es können Gruppen gebildet werden, ohne dass in die physische Vernetzung eingegriffen wird. Gründe für den VLAN Einsatz nach [10, S.167]:

- Eindämmung von Broadcast durch mehrere Broadcast Domänen
- Abbildung der betrieblichen Organisationsstruktur (Abteilungen)

- Einteilung des Netzes nach Anwendung

Arten von VLANs:

1. Statische VLANs = Portbasierte VLANs: Switch-Ports werden fest einem VLAN zugeordnet. Port kann nur einem VLAN zugeordnet werden.
2. Dynamisches VLAN = Paketbasiertes VLAN, auch tagged VLAN: Ein Port kann mehreren VLANs angehören. Pakete werden gekennzeichnet welchem VLAN sie angehören. Achtung hohe Manipulationsgefahr.

VPN Virtuelles privates Netzwerk

[11, S. 372-378]

- Verbindung zweier Teilnetze oder
- Verbindung eines Einzelrechners mit einem LAN/Intranet

[8]

- Ein Netzwerk, das ein anderes,öffentliches Netzwerk benutzt, um privte Daten zu transportieren.
- EIn VPN trennt den Transport privater Datenpakete oder privater Datenframes von anderen, es bietet nur die Sicherheit, dass die Pakete nicht zu falschen Empfänger geleitet werden. Weitere Sicherheitsmaßnahmen sind optional
- Gründe für VPN:
  - Veränderung der Geschäftsprozesse (B2B, B2C)
  - Dezentralisierung, Globalisirung
  - Veränderung der Wettbewerbssituation
  - Mobilität und Flexibilität
  - Kostenoprimierung
  - Sicherheit
- VPN-Typen:
  - Remote Access VPN : Verbindet Einzelrechner mit dem Intranet
  - Branch office VPN = site to site VPN: Verbindet verschiedene Intranets miteinander.
  - Extranet VPN: öffnet das private Netz auch für externe Personen =¿ Datenpakete müssen gesondert behandelt werden
- Anforderungen an die VPN Sicherheit: (Kapitel 2)
  - Datenvertraulichkeit → Verschlüsselungsverfahren
  - Schlüsselmanagement: Schlüselerzeugung, Integritätsprüfung, Authentifizierung, Schlüsselverteilung.
  - Paketauthentifizierung: Jedes Paket muss Authentifiziert werden, dass es tatsächlich vom Absender stammt.
  - Datenintigrität: Wurde Paket während des Transports verändert?

  - Benutzerauthentifizierung: Wichtig beim Remote Access VPN. Nutzer muss Identität zuverlässig nachweisen.
  - Benutzerauthorisierung: Vor allem bei Extranet, Aufgabe der Betriebssysteme.
  - Schutz vor Sabotage
  - Schutz vor unerlaubtem Eindringen
- Sicherheitstechnologien: (Kapitel 4):
  - Datenanalyse(Allgemein zur Datensicherheit, nicht nur VPN betreffend): Welche Daten müssen wie lange und vor wem gesichert werden. Wie sichd verletzungen dieser Sicherheut zu bewerten, zu welchem Preis dürfen die Sicherheitsziele erreicht werden.
  - Die Sicherheitsanforderungen an ein VPN leiten sich aus der Security Policy (Sicherheitsrichtlinie) eines Unternehmens ab.
  - Vom Standpunkt der Sicherheit wäre eine Ende zu Ende Verschlüsselung der Daten auf Applikationsebene die beste Methode. ABER technisch und organisatorisch nicht handhabbar(stand 2007).
  - Verbreitete Lösung: Sicherheit auf Netzwerkebene: OSI Schicht 3
  - Für ein Internet VPN ist Verschlüsselung auf Ebenedes IP-Protokolls das Sicherste und Sinnvollste. Weil bei Verschlüsselung in den Schichten 1 und 2 lägen die Daten an den Vermittlungssystemen im Klartext vor, da sie in der Schicht 3 verarbeitet werden.

Firewall/DMZ

Kurs 1866 KE4 S199:

Screened Subnet/DMZ: Eigenes Teilnetz zwischen Intranet und Internet, welches an beiden Eden durch Paketfilter geschützt wird.
Architektur: Internet-Router-ALG-Rechner-Router-Intranet.
Router auf Seite des Internet lässt nur Pakete zum Rechner innerhalb der DMZ durch. Router zum Intranet lässt nur Pakete vom Rechner aus der DMZ durch. Die andere Richtung analog. Angreifer muss also mehrere Systeme angreifen ehe er das Intranet erreichen kann. ALG filtert zusätzlich Kommunikation auf der Anwendungsebene. Bei erhöhtem Arbeitsaufkommen sind verschiedene ALG für verschiedene Anwendungen möglich (ftp, telnet, http). Öffentliche Webserver sollten sich auch in der DMZ befinden.
DMZ kann auch mit einem Router mit 3 Anschlüssen verwirklicht werden:

1. Internet
2. DMZ
3. Intranet

mit entsprechend konfiguriertem Paketfilter.

Sicherheitsleitlinie/Polocies

Siehe 1866 KE4 Kapitel 4.4 ab S.209 und BSI Grundschutzkatalog

Es müssen Richtlinien existieren WER fürdie Sicherheit verantwortlich ist ([8]).

Datenschutz und Jugendschutz

References

[1] Hans-Christian Brockmann. Effizientes und verantwortungsvolles datenmanagement im zeitalter der dsgvo. *Datenschutz und Datensicherheit - DuD*, 42(10):634–639, Oct 2018.

[2] Bundesamt für Sicherheit in der Informationstechnik. M 5.62 geeignete logische segmentierung.

[3] Bundesamt für Sicherheit in der Informationstechnik. Virtuelles privates netz (isi-vpn). 2009.

[4] Bundesamt für Sicherheit in der Informationstechnik. Absicherung eines pc-clients (isi-client),bsi-studie zur internet-sicherheit (isi-s). 2011.

[5] Bundesamt für Sicherheit in der Informationstechnik. Absicherung eines servers (isi-server),bsi-studie zur internet-sicherheit (isi-s). 2013.

[6] Johannes Hubertz. Lehmanns Media Berlin, 2013.

[7] Wolfgang Lassmann, editor. *IT-Sicherheit*, pages 349–408. Gabler, Wiesbaden, 2006.

[8] Manfred Lipp. Addison-Wesley, 2007.

[9] Adam Merschbacher. In *Sicherheitsfibel*. Springer, 2018.

[10] Armand Portmann and Oliver Hirschi. *Cybersecurity in Schweizer Unternehmen*, pages 456–473. Springer Fachmedien Wiesbaden, Wiesbaden, 2018.

[11] Harald Zisler. *Computer-Netzwerke: Grundlagen, Funktionsweise, Anwendung*. Rheinwerk Verlag GmbH, 2018.