Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

06
Verschlüsselung Signatur

Grundlagen

Symmetrische & Asymmetrische Verschlüsselung

Verschlüsselungs-protokolle und ihre Anwendung

Signaturen

07
IDS, IPS, Firewalls

Intrusion Detection System

Intrusion Prevention System

Honeypot

Firewall

Sandbox

08
Proaktive Sicherheit

Defensive Programmierung

Gehärtete Betriebssysteme

Patches

Vulnerability Assessment

Aktive Sicherheit von Netzwerk-komponenten

09
Urheberrecht

Der Urheber

Das Werk

Urheber-persönlichkeitsrecht

Verwertungsrechte

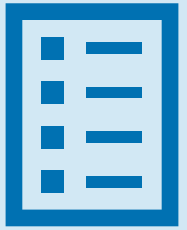
Nutzungsrechte

Ausnahmen

Dauer

Recht am eigenem Bild

10
Lernstands-messung



Agenda

- Defensive Programmierung
- Gehärtete Betriebssysteme
- Patches
- Vulnerability Assessment
- Aktive Sicherheit von Netzwerkkomponenten

01 Defensive Programmierung

01 Defensive Programmierung

Was bedeutet defensive Programmierung ?

- Im weitesten Sinn könnte man vereinfacht sagen, dass defensiv programmierte Anwendungen im allgemeinen deutlich misstrauischer sind.

  Sie überprüfen vor dem eigentlichen Zweck möglichst viele Voraussetzungen ab, bevor sie mit ihrer eigentlichen „Arbeit“ beginnen.

  In der Regel beenden defensiv programmierte Applikationen laufende Prozesse, wenn einzelne oder mehrere Voraussetzungen nicht erfüllt werden.

01 Defensive Programmierung

Was bedeutet defensive Programmierung ?

- Ein System muss sich nicht einem einzigen Konzept verschreiben.

  Grundsätzlich lässt es sich so aufteilen, dass Einwirkungen von außen (Benutzereingaben, Datenimport, Programmierschnittstellen) defensiv zu handhaben sind, während das bei inneren Abläufen nicht erforderlich ist.

01 Defensive Programmierung

Was bedeutet defensive Programmierung ?

- Beispiele
  - Eine potenziell unerwartete Benutzereingabe, mit der nicht wie geplant umgegangen werden kann und die deshalb bei defensivem Programmieren abgefangen werden muss.
  - Eingabe geforderter Angaben in eine vorgefertigte Datenmaske
  - PLZ muss 5 Stellen lang sein, sonnst Eingabefehler, ähnlich auch bei TT.MM.JJJJ
  - Eine Datei soll kopiert werden. Ein defensives Programm prüft vorher Quell- und Zielverzeichnis, Lese- und schreibrechte, etc.

02 Gehärtete Betriebssysteme

02 Gehärtetes Betriebssystem

Was ist ein gehärtetes Betriebssystem ?

- Der Begriff “Systemhärtung” ist die Übersetzung des Englischen “System Hardening”. Im IT-Sprachgebrauch wird vereinfacht auch nur von der “Härtung” bzw. dem “Härten” gesprochen.
- Da auf IT-Systemen unter anderem auch höchst sensible Informationen eines Unternehmens sowie personenbezogene Daten verarbeitet und gespeichert werden, müssen die verwendeten Systeme besonderen Schutzmaßnahmen unterzogen werden. Eine sehr wirkungsvolle Maßnahme zur Absicherung stellt die Systemhärtung dar.

02 Gehärtetes Betriebssystem

Was ist ein gehärtetes Betriebssystem ?

- Die Systemhärtung sichert das Betriebssystem ab, unabhängig davon, ob es sich um ein physikalisches, virtuelles oder Cloud-basiertes System handelt.

- Gängige IT-Systeme mit Betriebssystemen wie beispielsweise Windows, werden von den Herstellern auf größtmögliche Kompatibilität vorkonfiguriert. Die Folge davon, die IT-Systeme werden dadurch angreifbar. Zudem sind oft Features und Komponenten verfügbar, welche ungenutzt bleiben und ebenfalls dadurch ein zusätzliches Sicherheitsrisiko darstellen.

02 Gehärtetes Betriebssystem

Was ist ein gehärtetes Betriebssystem ?

- Standardmäßig werden bei Betriebssystemen keine beschränkenden Sicherheitskonfigurationen angewendet. Gerade diese oft ungenutzten und nicht konfigurierten Funktionalitäten nutzen Angreifer wie Hacker häufig als Angriffsvektor aus.

- Ziel der technischen Maßnahme “Härtung”: Diese Funktionalitäten sowie deren ungenutzte Schnittstellen werden deaktiviert oder sogar deinstalliert.

02 Gehärtetes Betriebssystem

Bedrohungen bei nicht gehärteten Systemen

- Identitätsdiebstahl, z.B. bei Angriffen auf die zentrale Identitäts-Management-Struktur oder am heimischen PC
- Daten-Manipulation von personenbezogenen Daten und/oder sensiblen Unternehmensdaten
- Datenabfluss, z.B. das Kopieren gesamter Datenbanken
- Manipulation von Anwendungen oder damit verbundener Systeme
- Sabotage oder Spionage bei Betriebs- und Produktionsabläufen
- Einschleusen und Verbreitung von Malware

03 Patches

03 Patches

- Patches, einfach übersetzt „Flicken“.

- Wenn in Programmen oder Betriebssystemen Fehler auftauchen, die Sicherheitslücken entstehen lassen, sind Hersteller bemüht schnell „Nachbesserungen“ anzubieten, um diese Lücken zu schließen. Sogenannte Patches oder aber auch Bugfixes.

- Der Funktionsumfang nimmt in aller Regel durch ein Patch nicht zu

03 Patches

- Diese „Nachbesserung“ erübrigt komplexe Neuinstallationen.
- Dateien werden gelöscht, oder der Quellcode dieser wird durch ein Patch verändert.
- Patch Management Software unterstützt die Verwaltung und Verteilung von Patches in IT-Systemen

04 Vulerability Assessment

04 Vulnerability Assessment

Schwachstellenanalyse

- Prozesse und / oder Verfahrensabläufe werden auf Schwachstellen untersucht.
- PDCA und Audits gehören zu den durchaus umfangreichen und komplexen Verfahrensweisen als Bestandteil entsprechender Analysen.
- Systeme werden auf Schwachstellen gescannt, Arbeitsabläufe und Berechtigungen werden geprüft, Richtlinien durchgespielt.

04 Vulnerability Assessment

Schwachstellenanalyse

- Der Schwachstellenanalyse folgt die Risikoanalyse
- Risikoanalyse
  - Risikomanagement z. B. nach ISO 27005
    ergibts sich aus ISO 27001
    siehe Foliensatz „Grundlagen Sicherheit“ (Tag 03) und/oder
    ISO 27005 Einführung (risikomanagement-wissen.de)
- Schwachstellenanalyse und Risikoanalyse sind feste Bestanteile eines ISMS
  (Information Security Management System)

05 Sicherheit durch Netzwerkkomponenten

05 Sicherheit durch Netzwerkkomponenten

- Die Sicherheit in einem Netzwerk setzt sich aus einer Vielzahl einzelner Komponenten zusammen.
    - Firewall
    - Managed Switch (VLAN)
    - IDS & IPS Netzsensoren
    - Subnetze

05 Sicherheit durch Netzwerkkomponenten

- Die Sicherheit in einem Netzwerk setzt sich aus einer Vielzahl einzelner Komponenten zusammen.
    - Einstellungen
    - Regeln
    - Konfigurationen
    - eine Kombination aus physischen und logischen Komponenten

05 Sicherheit durch Netzwerkkomponenten

- Es ist sehr vordergründig, die Netzwerkkomponenten selbst entsprechend abzusichern.

- Wie bereits gelernt, ein Firewall regelt den Datenverkehr in bzw. zwischen Netzen. Doch was nutzen die besten und sichersten Konfigurationen, wenn beispielsweise das Managementinterface einer Firewall aus dem Internet unautorisiert erreichbar ist?

- Hat jemand unautorisiertes ich die Möglichkeit, die Konfiguration zu beeinflussen, ist die Regelfunktion der Firewall gegenstandslos.

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com