

Modulprüfung IT-Sicherheit

Sie haben zum Lösen der Aufgaben 90 Minuten Zeit. Es können 48 Punkte erreicht werden. Sie dürfen alle Papierunterlagen verwenden. Bitte antworten Sie sichpunktartig, kurz und prägnant!

Aufgabe 1. (6) Schutz vor Trojanischen Pferden.

- (2) Warum ist für einen Automaten (automatisches Erkennprogramm für Trojanische Pferde) nicht entscheidbar, ob eine ausführbare Datei ein Trojanisches Pferd ist?
- (2) Ändert sich etwas, wenn dem Automaten der Quelltext des zu analysierenden Programms gegeben wird?
- (2) Angenommen, Computersysteme führten nur noch digital signierte Dateien aus. Ließe sich dadurch verhindern, dass man einem trojanischen Pferd zum Opfer fällt?

Begründen Sie jeweils Ihre Antworten!

Aufgabe 2. (6) Schutz vor Außenstehenden.

Es soll verhindert werden, dass durch Web-Zugriffe auf das Internet die Netz- und Organisationsstruktur eines Unternehmens bekannt wird. Insbesondere sollten die IP-Adressen vor Außenstehenden verborgen werden und die PCs von außen unerreichbar sein. Wählen Sie geeignete Sicherheitsmechanismen aus und erläutern Sie Ihr Sicherheitskonzept.

Aufgabe 3. (6) Virenschutz.

Warum gibt es (praktisch) keinen hundertprozentigen Schutz vor Viren? Nennen und erläutern Sie wenigstens 3 Gründe!

Aufgabe 4. (5) Tunneling.

- (1) Was ist Tunneling?
- (2) Nennen und erläutern Sie eine Nutzenanwendung für Tunneling!
- (2) Gibt es einen perfekten Schutz vor Tunneling? Begründen Sie Ihre Antwort!

Aufgabe 5. (3) Wenn Verschlüsselung und Signieren von Nachrichteninhalten erforderlich sind, müssen Sie entscheiden, ob Sie erst verschlüsseln und dann signieren oder umgekehrt. Man könnte auch auf den Gedanken kommen, die Reihenfolge zufällig zu wählen. Entscheiden Sie sich für eine der drei Varianten und begründen Sie Ihre Wahl!

Aufgabe 6. (7) Zugangs und Zugriffskontrolle.

- (6) Nennen und erläutern Sie drei Beispiele für Zugangskontrollmechanismen in PCs.
- (1) Warum ist Zugangskontrolle für die Realisierung von Zugriffskontrollmechanismen eine notwendige Voraussetzung?

Aufgabe 7. (8) Authentikation und Verschlüsselung.

Von einem Sensor soll zu einer Zentrale regelmäßig (z.B. $1 \times$ pro Sekunde) genau 1 Bit so übermittelt werden, dass ein Angreifer nicht in der Lage ist, dieses Bit zu verfälschen. Der Wert des Bits ist dem Angreifer bekannt, er darf ihn aber nicht unerkant verändertern. (Es könnte sich beispielsweise um das Signal eines Türsensors handeln, der von einem Einbrecher natürlich nicht manipuliert werden können soll.)

- (4) Entwerfen Sie ein geeignetes Authentikationssystem.
- (2) Beschreiben Sie, welche Probleme zu lösen sind.
- (2) Erweitern Sie Ihr System so, dass auch der Wert des Bits vor dem Angreifer vertraulich bleibt.

Aufgabe 8. (7) Maskerade-Angriffe.

- (3) Erläutern Sie am Beispiel zweier IT-Systeme, die miteinander kommunizieren, wie ein Maskerade-Angriff (auch: man-in-the-middle attack) aufgebaut ist.
- (4) Was ist das Angreifermodell und wie kann der Angriff verhindert werden? Entwerfen Sie ein entsprechendes System, das Maskerade-Angriffe verhindert.

Viel Erfolg!