Datensicherheit, Zusammenfassung Vorlesung 3

Henry Haustein, Dennis Rössel

Welche Angriffsmethoden werden beispielsweise angewendet?

Ausnutzung von Schwachstellen in Software, Malware, Spam, Drive-by-Exploits, Botnetze, Denial-of-Service, Social Engineering

Was zeichnet Computerviren aus?

selbstreproduzierend, keine selbstständige Software - benötigt Wirt

Was sind Beispiele für Verschleierungsmethoden für Viren?

Virus wird verschlüsselt in infizierter Datei gespeichert, Polymorphe Viren, Metamorphe Viren, Stealth-Viren

Was sind grundlegende Antivirentechniken, welche Vor- und Nachteile haben sie?

Antiviren-Techniken:

- statische Techniken: Scanner mit Signaturerkennung, Heuristik, Integritätsprüfungen → teilweise nur bekannte Viren erkennbar, Identifizierung als Virus
- dynamische Techniken: Monitoring von Aktivitäten, Emulation → auch unbekannte Viren erkennbar, keine Identifizierung

Was sind Beispiele für empfohlene Maßnahmen gegen die Gefährdung durch Malware?

Empfohlene Maßnahmen:

- Regeln (Policies)
- Problembewusstsein
- Verringerung möglicher Schwachstellen
- Verringerung möglicher Bedrohungen

Was verstehen Sie unter dem Prinzip *least privilege*?

nur die Rechte vergeben, die unbedingt benötigt werden, arbeiten mit verschiedenen Nutzeraccounts

Was beschreibt ein Angreifermodell, was sind wesentliche Inhalte?

Angreifermodell: Angabe der maximal berücksichtigten Stärke eines Angreifers, das heißt Stärke des Angreifers, gegen die ein bestimmter Schutzmechanismus gerade noch sicher ist

Inhalte:

- Rolle des Angreifers
- Verbreitung des Angreifers
- Verhalten des Angreifers
- Rechenkapazität des Angreifers
- verfügbare Mittel des Angreifers

Was besagt das Prinzip der Angemessenheit?

ausgewogenes Verhältnis zwischen Sicherheitsanforderungen und Aufwand für Realisierung der Maßnahmen, Reduzierung der Risiken