

Aufgabe 1:

Schutzziele

Auf den Folien 23 und 24 werden eine Reihe von Schutzzielen definiert. Ein sicheres informationstechnologisches System muß zumindest in Bezug auf die Erfüllung dieser Schutzziele ein eindeutig positives Urteil erlauben.

In der Übung zur letzten Veranstaltung haben sie das Protokoll SMTP entsprechend RFC 821 kennengelernt. Betrachten sie das Protokoll nun vor dem Hintergrund der Schutzziele:

1. Welche Subjekte, Objekte und Kommunikationskanäle gibt es in einem E-Mail-System mit einem SMTP-Server und zwei lokalen Nutzern?
2. Prüfen sie das Protokoll auf die Erfüllung jedes einzelnen Schutzzieles. Begründen Sie, ob das Ziel erfüllt wird oder nicht. Gibt es Schutzziele, die im Kontext des E-Mail-Protokolls irrelevant sind?
3. Prüfen sie, ob SMTP revisionsfähig ist.
4. Für alle Kriterien, die SMTP nicht erfüllt: Geben sie einen kurzen Vorschlag zur Verbesserung des Protokolls an.

Aufgabe 2:

Safety, Security und Angreifer

1. Geben sie den Unterschied zwischen den Begriffen *Safety* und *Security* mit eigenen (deutschen) Worten wieder.
2. Macht die Unterscheidung aus ihrer Sicht Sinn?
3. Ein Rechenzentrum befindet sich an der Aussenwand eines Bürogebäudes und verfügt über schöne große Fenster. Ein Angreifer wirft eine Flasche mit einer brandbeschleunigenden Flüssigkeit durch das geschlossene Fenster, das Rechenzentrum steht kurzzeitig in Flammen, ein Brandschutzsystem greift ein und löscht das Feuer, der Schaden beläuft sich auf 50 € für eine neue Fensterscheibe und 100 € für eine Generalreinigung. Hat ein *Safety*- oder ein *Security*-System des Rechenzentrums reagiert? Hat das Sicherheitssystem des Rechenzentrums funktioniert? könnte man das *Security*-System möglicherweise verbessern? Wie? Begründen sie ihre Antworten kurz.
4. Im Rahmen der Beantwortung der Fragen auf Folie 17 wurden die Motivationen von Angriffen aufgezählt und einige Typen von Angreifern benannt. Ordnen sie Motivationen und Angreifer einander zu. Was sind eigentlich Hacker? Was sind Skript-Kiddies?

Aufgabe 3:

Schwachstellen, Verwundbarkeiten und Risiken

1. Sie alle benutzen täglich informationstechnologische Systeme. Diese haben Schwachstellen und Verwundbarkeiten. Welche davon sind Ihnen bekannt? Zählen Sie einige (möglichst weit verbreitete) auf.
2. Geben Sie zu mindestens zwei Ihrer Schwachstellen eine Möglichkeit des Angriffs entsprechend der Ergebnisse der Beantwortung der ersten Frage von Folie 17 an.
3. Wie schätzen Sie das von den möglichen Angriffen ausgehende Risiko ein? Begründen Sie Ihre Entscheidung.
4. Wie gefährdet sind Sie selbst durch diese Art von Angriffen? Um eine selbstkritische Einschätzung wird gebeten.

Aufgabe 4:

Betrachtung von Sicherheitssystemen

Ein Wurm ist ein selbstständiges, selbstreproduzierendes Programm, das sich in einem System ausbreitet. Der Angriff eines Wurms verläuft meist in zwei Stufen. Zunächst nutzt er Schwachstellen in den angegriffenen Systemen aus, um schließlich ein Stück Programmcode ausführen zu lassen, welches die Übertragung des kompletten Wurmprogrammes ermöglicht. Ist ein Rechner erfolgreich attackiert worden, wird er als Ausgangsbasis für andere angeschlossene Systeme benutzt (vgl. Fuhrberg, *Internet Sicherheit*, S. 60). Würmer führen möglicherweise zusätzliche Schadfunktionen aus. Viele Würmer verbreiten sich teilweise per E-Mail.

1. Inwiefern verletzen E-Mail-Würmer die Schutzziele der IT-Sicherheit?
2. Welche Sicherheitsmechanismen können gegen E-Mail-Würmer eingesetzt werden?
3. Beantworten sie für einen Sicherheitsmechanismus die Fragen auf den Folien 35 und 36. Zu welchem Ergebnis kommen sie?