Grundlagen der IT Sicherheit

Aufgabenblatt 1

Julian Bertol

1. **Erläutern Sie die drei Schutzziele. Wieso ist deren Einhaltung wichtig?**

   Vertraulichkeit, Integrität, Verfügbarkeit
   Vertraulichkeit:
   ist das verschlüsseln der gesendeten oder geispeicherten Daten
   Integrität:
   Ist die Manipulationsdetektion durch beispielsweise die Mac Adresse oder eine Digitale Signatur.

   Verfügbarkeit:
   Ist der Schutz vor Sabotage durch Firewalls, Monitoring,Backups, usw…

2. **Welche Gefahren bedrohen die Schutzziele? Nennen Sie drei Beispiele und beschreiben Sie wie welches Schutzziel dadurch gefährdet wird.**

   Malware: Malware wie Viren oder Trojaner kann die Vertraulichkeit gefährden, indem sie sensible Daten ausspäht.

   Datenmanipulation: Angriffe auf Datenbanken oder Netzwerke können die Integrität gefährden, wenn Daten unbefugt geändert werden.

   DoS-Angriffe (Denial of Service): Diese können die Verfügbarkeit eines Systems einschränken, indem sie es überlasten und somit unzugänglich machen.

3. **Nutzen Sie zur Bearbeitung dieser Aufgabe nach Möglichkeit die Rollen Alice, Bob und Eve.**
   Alice hat an Bob eine Email mit den Informationen gesendet. Es gibt mehrere Möglichkeiten die dazu geführt haben, das Eve alles mitlesen konnte.
   Möglichkeit 1:
   Eve hat das Passwort von Bob herausgefunden und hat alles Mails mitgelesen. Hierbei wurde die Vertraulichkeit verletzt. Aus dem STRIDE Modell ist der Fall Information Disclosure (Confidentiality) eingetroffen, da ein unautorisierter Zugang erfolgte. Der Angreifer könnte durch mehrere Möglichkeiten an das Passwort gekommen sein. Beispielsweise durch eine einfach Brute-Force-Attacke. Hierbei werden beliebige Passwörter ausprobiert bis das korrekte gefunden wurde. Dies kann durch vorgefertigte Liste geschehen oder durch das ausprobieren von zufälligen Zeichenkombinationen. Wenn aber ein „sicheres Passwort“ verwendet wurde ist diese Möglichkeit ziemlich unwahrscheinlich. Es besteht außerdem die Möglichkeit, das dass Passwort durch eine Phishing-Mail herausgefunden wurde. In dem Bob zum Beispiel auf einen Link geklickt hat der zu einem

Login-Fenster führt und Bob sich dort mit seinen Daten angemeldet hat. Dadurch bekam Eve die Anmeldedaten von Bob. Dies alles hätte man verhindern können in dem man ein Sicheres Passwort verwendet und man einen Spamschutz für seine Emails einrichtet und auf die Inhalt und Absender der Email achtet. Außerdem sollte man immer auf die URL der Internetseite achten auf der man sich gerade befindet und seine Anmeldedaten eingibt (wichtig HTTPS).

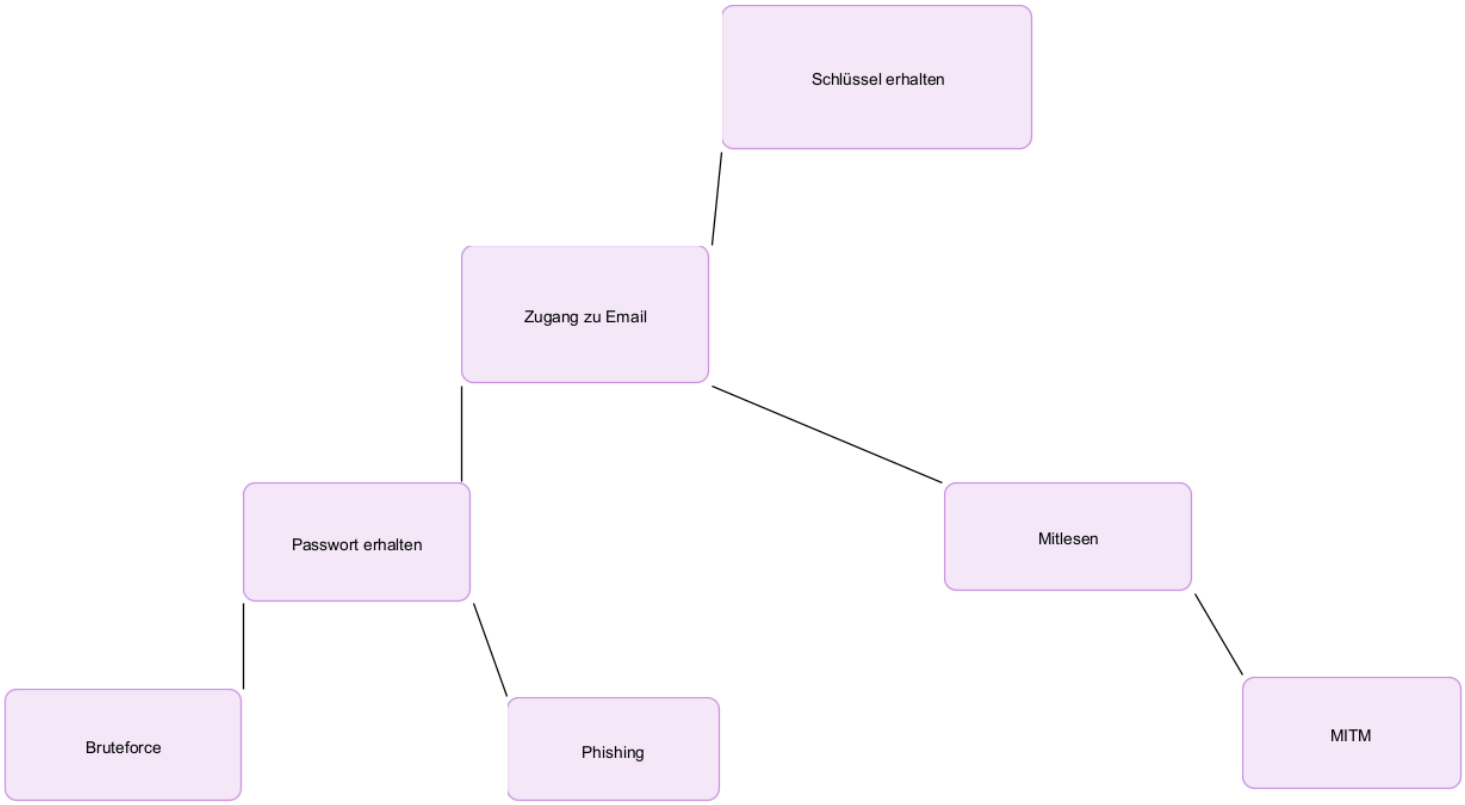
Möglichkeit 2:
Man in the Middle Attacke. Eve könnte sich als Bob ausgeben und so durch eine Man in the Middle Attacke die Emails von Bob mitlesen. Die Teilaufgaben b und c sind gleich wie in der 1. Möglichkeit. Man hätte dieses Szenario durch eine Ende zu Ende verschlüsselung verhindern können. Hierbei werden Daten während der übertragung verschlüsselt und nur die Kommunikationspartner können diese Nachricht entschlüsseln.

4. **Informieren Sie sich im Internet zum Thema Responsible (Vulnerability) Disclosure / Coordinated Disclosure, zu Deutsch vertrauensvolle Offenlegung von Sicherheitsschwachstellen. Sie können hierzu unter anderem Informationen der Wikipedia, des OWASP (Open Web Application Security Project) oder von FIRST (Forum of Incident Response and Security Teams) nutzen**

   a) Das Veröffentlichen von Schwachstellen und deren Behebung ist eine kritische Phase, weil während der Zeit zwischen der Veröffentlichung der Schwachstelle und dem Patch-Aktualisierung (Fix) Angreifer die Schwachstelle ausnutzen können. Diese Phase wird oft als "Zero-Day"-Schwachstelle bezeichnet.

   b) Full Disclosure bedeutet die vollständige und sofortige Veröffentlichung aller Informationen über eine Schwachstelle, was Druck auf den Softwareanbieter ausübt, schnell zu handeln. Um solche Situationen zu vermeiden, sollten Softwareentwickler Coordinated Disclosure verfolgen, wo die Schwachstelle zuerst dem Entwickler gemeldet und ausreichend Zeit zur Behebung gegeben wird, bevor die Informationen veröffentlicht werden.

Bonus:


Schlüssel erhalten
Zugang zu Email
Passwort erhalten
Mitlesen
Bruteforce
Phishing
MITM