

Womit wirbt ein Trojanisches Pferd für sich selbst?



Mit der Nützlichkeit des Wirtsprogramms



Mit schadhaft verlinkten Werbebannern



Mit der Qualität von Partnerprogrammen



Mit einfacher Verbreitung

Wie können Angreifer Passwörter nicht herausfinden?



Salt Calculation



Social Engineering



Shoulder Surfing



Interception

---

Was trifft für einen *offline Brute Force Angriff* auf einen verschlüsselten Text zu?



Findet den Schlüssel in endlicher Zeit



Findet den Schlüssel in unendlicher Zeit (theoretischer Angriff)



Findet den Schlüssel nicht, wenn dieser mindestens 256 Bit lang ist



Findet den Schlüssel nicht, unabhängig von der Schlüssellänge

---

Was trifft für einen *offline Brute Force Angriff* auf einen verschlüsselten Text zu?



Findet den Schlüssel in endlicher Zeit



Findet den Schlüssel in unendlicher Zeit (theoretischer Angriff)



Findet den Schlüssel nicht, wenn dieser mindestens 256 Bit lang ist



Findet den Schlüssel nicht, unabhängig von der Schlüssellänge

Eine CVE-Webseite enthält Informationen über...



Schwachstellen



Bedrohungen



---



---

Maßnahmen

Schäden

Warum sollten Patches vor dem Ausrollen vom Anwender getestet werden?



Patches können negative Auswirkungen auf Systeme haben



Patches können nicht vom Hersteller getestet werden



Testen gehört beim Entwickeln von Software einfach dazu

---

---

---

Ein Test nach der Installation ist nicht möglich

Was gehört NICHT zur Verschlüsselung gespeicherter Daten?



Hauptspeicherverschlüsselung



Festplattenverschlüsselung



Dateisystemverschlüsselung



---

---

Datenbankverschlüsselung

## Honeypots ...



... können unbekannte Angriffe einfach erkennen



... haben einen produktiven Wert



... kommunizieren mit anderen Systemen im internen Netz



... korrelieren sicherheitsrelevante Ereignisse



Bei einer N-modularen Redundanz wird die folgende Eigenschaft genutzt:



Mehrere Geräte laufen synchron (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Entscheidung durch Mehrheit (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Zusätzliche Geräte in Hot-Standby (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)



Kompensation durch Notfall-Module (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)

Die maximale Zeitspanne, die zwischen letzter Sicherung und Ausfall liegen darf, nennt sich:



Recovery Point Objective



Recovery Time Objective



Recovery Error Objective



Recovery Amount Objective

Folgende Verfahren sind durch Quantencomputer bedroht:



RSA



AES



twofish



ChaCha

Bei welcher der folgenden Antworten steigen die Motivation und Fähigkeiten der **Threat Agents** von links nach rechts?



Kriminelle, Cybersöldner, Global 150



Organisierte Kriminalität, Skript Kiddies, Hacktivisten



Kriminelle Gruppen, unzufriedene Mitarbeiter, Nationen



Global 25, Programmierer, staatlich gesponsert

Der folgende Begriff passt nur zu Attribute-Based Access Control:



Zeitfenster (1 Punkt)



Access Control List (0 Punkte)



Clearance (0 Punkte)



Label (0 Punkte)

Pfeffer sorgt für eine zusätzliche Sicherheit bei der Passwort-Authentifizierung, weil:



Angreifer ein Geheimnis raten müssen *(1 Punkt)*



Vor dem Hashen ein Zufallswert ergänzt wird *(0 Punkte)*



Eine sichere Hash-Funktion garantiert wird *(0 Punkte)*



Das Passwort vor der Übertragung verändert wird *(0 Punkte)*

Schritte, die immer zu Ransomware-Angriffen gehören:



Verschlüsselung (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Erpressung (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Phishing (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)



Datendiebstahl (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)

Was ist eine Bedrohung?



Diebstahl von Geräten



Defizite bei der Autorisierung



Fehlende Patches in einem System



Unzureichend Schulung der Mitarbeiter

In die Basis-Bewertung einer Schwachstelle fließt bei CVSS folgende Information NICHT mit ein:



Bedrohungslage



Angriffsvektor

---

21 / 81

---

Erforderliche Rechte

Auswirkung auf die Vertraulichkeit



Folgende Verfahren sind sicher in Bezug auf Quantencomputer:



AES



RSA



ElGamal



Diffie Hellman

Dies zählt **NICHT** als physische Bedrohung:



Absturz



Feuer



Schmutz



Stoß

Ransomware verschlüsselt die Benutzerdaten mit...



dem öffentlichen Schlüssel des Angreifers



dem privaten Schlüssel des Angreifers



mit dem geheimen symmetrischen Schlüssel des Angreifers



mit einer kryptographischen Hashfunktion

Was wird oft bei Backups vergessen?



Konfigurationsdaten (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Mobile Geräte (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)

---



Desktop-PCs (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)



Server (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)

Warum ist Patching manchmal schwierig?



Zeit zum Patchen ist oft limitiert



Jeder Anwender kann patchen



Hersteller haften für Probleme mit Patches



Es sind meist zu viele Patches verfügbar

Warum sind Hacker ein Problem für verschlüsselt gespeicherte Daten?



Hacker haben Zugriff auf Daten, wenn diese unverschlüsselt sind



Hacker knacken die gängigen Verschlüsselungstechniken



Hacker finden die Passwörter für die Verschlüsselung heraus



Hacker können die Verschlüsselungsprogramme reverse-engineeren

??

Dies gehört **NICHT** zu den Aufgaben eines SIEM:



Sicherheitsvorfälle verhindern



Informationen sammeln



Ereignisse korrelieren



Managementberichte generieren

Was wird sinnvollerweise redundant ausgestattet?



Kommunikation (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Stromversorgung (*Ausgewählt = 1 Punkt, Nicht ausgewählt = 0 Punkte*)



Feuerlöschanlagen (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)



Software-Lizenzen (*Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkte*)



Was wird beim Raten von Passwörtern von Angreifern häufig **nicht** getestet ...



Rainbow Tables



Tastaturzeichenfolgen



Fußballvereine



Telefonnummern