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 <u>nicht</u> 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
Findst der Cablines in verschlicher Zeit (the exetication America)
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
Findst der Cablines in verschlicher Zeit (the exetication America)
Findet den Schlüssel in unendlicher Zeit (theoretischer Angriff)
Findet den Schlüssel nicht, wenn dieser mindestens 256 Bit lang ist

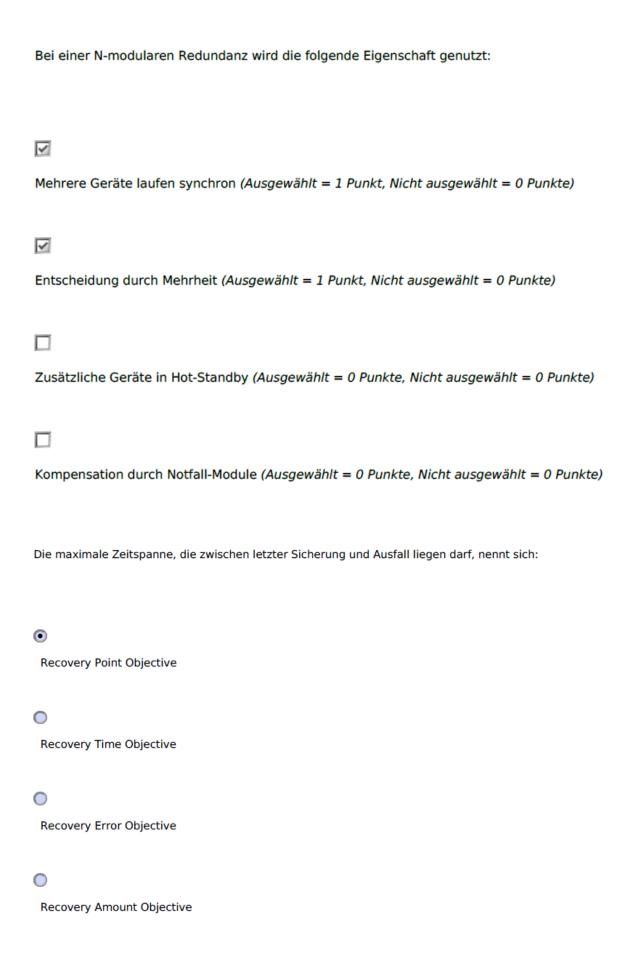
Findet den Schlüssel nicht, unabhängig von der Schlüssellänge

Eine CVE-Webseite enthält Informationen über
Schwachstellen
Bedrohungen
Maßnahmen
Schäden

Warum sollten Patches vor dem Ausrollen vom Anwender getestet werden?
O Databas kii nasa nasatiya Ayawidayasan ayf Gustawa babas
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



Folgende \	Verfahren	sind durch	Quantencomputer	bedroht
------------	-----------	------------	-----------------	---------



RSA



AES



twofish

0

ChaCha

Kriminelle, Cybersöldner, Global 150
Organisierte Kriminalität, Skript Kiddies, Hacktivisten
Kriminelle Gruppen, unzufriedene Mitarbeiter, Nationen
Global 25, Programmierer, staatlich gesponsert

Bei welcher der folgenden Antworten steigen die Motivation und Fähigkeiten der Threat Agents von links

nach rechts?

Der folgende Begriff passt nur zu Attribute-Based Access Control:
⊚
Zeitfenster (1 Punkt)
0
Access Control List (0 Punkte)
0
Clearance (0 Punkte)
0
Label (0 Punkte)

Pfeffer sorgt für eine zusätzliche Sicherheit bei der Passwort-Authentifizierung, weil:
⊚
Angreifer ein Geheimnis raten müssen (1 Punkt)
0
Vor dem Hashen ein Zufallswert ergänzt wird (0 Punkte)
0
Eine sichere Hash-Funktion garantiert wird (0 Punkte)
0
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)

In die Basis-Bewertung einer Schwachstelle fließt bei CVSS folgende Information NICHT mit ei	n:
Bedrohungslage	
Bedronungslage	
Angriffsvektor	
	21 / 81
	21701
Erforderliche Rechte	
Erforderliche Rechte	
Erforderliche Rechte	
Erforderliche Rechte Auswirkung auf die Vertraulichkeit	

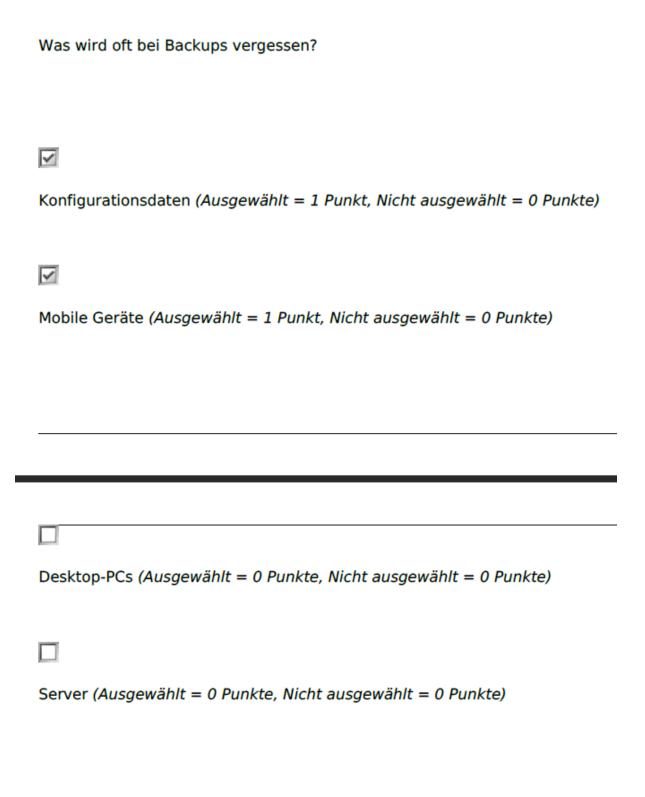
Folgende Verfahren sind sicher in Bezug auf Quantencomputer:
AES
RSA
ElGamal
Diffie Hellman

Dies zählt NICHT als physische Bedrohung:

0		
Absturz		
Feuer		
0		
Schmutz		

Stoß

Ransomware verschlüsselt die Benutzerdaten mit
dem öffentlichen Schlüssel des Angreifers
dem privates Schlüssel des Appreifers
dem privaten Schlüssel des Angreifers
mit dem geheimen symmetrischen Schlüssel des Angreifers
mit einer kryptographischen Hashfunktion



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	genort	NICHI	zu	den	Autgab	en e	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 Punkt
Software-Lizenzen (Ausgewählt = 0 Punkte, Nicht ausgewählt = 0 Punkt

Was wird beim Raten von Passwörtern von Angreifern häufig nicht getestet
•
Rainbow Tables
Tastaturzeichenfolgen
Fußballvereine
Telefonnummern