# Ihr Ergebnis der Lernkontrolle: InfSi1_V01_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V01_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 12:05:46 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 32 |
| **Maximal mögliche Punktezahl:** | 83 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 14:34:31 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 14:55:19 |
| **Benötigte Zeit:** | 00:20:48 |
| **Resultat beste Durchführung:** | 75/83 (90%) |

**Frage 1: Was versteht man unter "Magnitude of a Risk"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Produkt aus Likelihood und Consequences |
| ✗ | ✓ | die Grösse einer Katastrophe |
| ✓ | ✗ | eine durchschnittlich erwartete Schadenshöhe |
| ✗ | ✗ | Die Wahrscheinlichkeit, dass etwas passiert |

**Frage 2: Welche beiden Aktivitäten umfasst eine Risikoanalyse?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Risikoidentifikation |
| ✓ | ✓ | Risikobewertung |
| ✗ | ✗ | Risikobewältigung |
| ✗ | ✗ | Riskovermeidung |

**Frage 3: Was wird mit einer Man-in-the-Middle-Attacke gestört?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Vertraulichkeit |
| ✓ | ✓ | Echtheit |
| ✗ | ✗ | Verfügbarkeit |

**Frage 4: Wofür steht das "C" bei den "CIA" Sicherheitszielen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Vertraulichkeit |
| O | O | Echtheit |
| O | O | Verfügbarkeit |
| O | O | Datenschutz |

**Frage 5: In der Vorlesung wurde darauf hingewiesen, dass man bei der Beurteilung von Informationen**

**besonders auf zwei Eigenschaften der Autoren achten soll. Geben Sie an, welche das sind.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | akademischer Titel |
| ✓ | ✓ | Unabhängigkeit |
| ✓ | ✓ | Fachkenntnis |
| ✗ | ✗ | Bekanntheit |
| ✗ | ✗ | Alter |

**Frage 6: Der passendste englische Begriff für "Vertraulichkeit der Information" lautet ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Secrecy |
| O | O | Privacy |
| ◉ | ◉ | Confidentiality |
| O | O | Availability |
| O | O | Integrity |

**Frage 7: Bei den Information Security Standards der ISO 27000 Serie versteht man unter einer Bedrohung (Threat) ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Einen möglichen Grund f□ür einen ungewollten Vorfall, der das System oder die Organisation schädigen kann |
| O | O | Fehler in einem Abwehrdispositiv |
| O | O | Verletzlichkeiten (Vulnerabilites) in einem System |
| O | O | Den Diebstahl von Informationen |

**Frage 8: Was beschreibt die Managementaufgabe am besten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Plan - Do - Check - Act |
| O | O | Führen |
| O | O | kommandieren - kontrollieren-korrigieren |

**Frage 9: Welcher der beiden Begriffe betrifft eher Situationen, welche effektiv zu einem Schaden f•ühren?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Gefährdung |
| O | O | Bedrohung |

**Frage 10: Welche der drei in den Übungen studierten Dokumente zu Informationssicherheitsbegriffen ist das Kürzeste?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | ISO 27000 Vocabulary |
| O | O | NIST Glossary of Key Information Security Terms |
| O | O | RFC4949 Internet Security Glossary |

**Frage 11: Ein Zufallsexperiment liefert die Ereignisfolge 1, 4, 7, 2, 6. Wie verändert sich hier die Standardabweichung, wenn anstatt "7" das Ergebnis "12" erschienen wäre?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | die Standardabweichung verändert sich nicht |
| ◉ | ◉ | die Standardabweichung wird grösser |

| | | |
|---|---|---|
| O | O | die Standardabweichung wird kleiner |

**Frage 12: Welche Aussagen zur "Fehlerkultur" treffen zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Mit einer guten Fehlerkultur reduziert man vor allem die Eintretenswahrscheinlichkeit von Ereignissen. |
| ✓ | ✓ | Mit einer guten Fehlerkultur reduziert man vor allem die den Schaden von Ereignissen. |

**Frage 13: Welche beiden Formulierungen beschreiben den Begriff "Risiko" am besten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Kombination aus der Wahrscheinlichkeit eines Ereignisses (Vorfalls) und dessen Auswirkungen. |
| ✗ | ✓ | Gefahr, dass Angriff stattfindet. |
| ✗ | ✗ | Wahrscheinlichkeit, dass eine Verletzlichkeit ausgenutzt wird. |
| ✓ | ✓ | Möglichkeit, dass eine Bedrohung eine Schwachstelle ausnutzen und dadurch der Institution Schaden zufügen |

**Frage 14: Ein Zufallsexperiment liefert die Ereignisfolge 1, 4, 7, 2, 6. Wie gross ist hier der Mittelwert?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 1 |
| O | O | 2 |
| O | O | 3 |
| ◉ | ◉ | 4 |
| O | O | 5 |

**Frage 15: Der passendste englische Begriff für "Geheimhaltung" lautet ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Secrecy |
| O | O | Privacy |
| O | O | Confidentiality |
| O | O | Availability |
| O | O | Integrity |

**Frage 16: Der passendste englische Begriff für "Privatsphärenschutz" lautet ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Secrecy |
| ◉ | ◉ | Privacy |
| O | O | Confidentiality |
| O | O | Availability |
| O | O | Integrity |

**Frage 17: Was trifft auf den Begriff "Verletzlichkeit" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | ist eine Unzulänglichkeit in einer Abwehrmassnahme |
| ✓ | ✓ | wird englisch als "vulnerability" bezeichnet |
| ✗ | ✗ | ist das Resultate eines Hackerangriffs |
| ✗ | ✗ | ist das Resultat einer Bedrohung |
| ✗ | ✓ | ist das Resutat einer Gefährdung |

**Frage 18: Anhand von welchem Parameter sollte man entscheiden, zu welchen Ereignissen der Risikoliste zuerst Massnahmen ergriffen werden sollen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | vorhandenes Budget |
| O | O | Eintretenswahrscheinlichkeit |
| O | O | Schadensausmass |
| ◉ | ◉ | Risiko |

**Frage 19: Der Begriff "Gefährdung" wurde durch folgende Organisation eingef•ührt:**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | ISO |
| ◉ | ◉ | BSI |
| O | O | OWASP |
| O | O | IEEE |

**Frage 20: Welche Organisation/Berufsgruppe ist für eine besonders gute "Fehlerkultur" bekannt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Airlines |
| O | O | Spitäler |
| O | O | Informatiker |

**Frage 21: In den USA gibt es spezielle "Safety & Health (Risk Management) Regulations". Sie haben in den Übungen dazu ein Video studiert. Wer ist gemäss diesen "Regulations" für die Umsetzung des Risk Managements verantwortlich?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Jeder Mitarbeiter selbst |
| ✓ | ✓ | Der Arbeitgeber |
| ✓ | ✓ | Sie selbst, wenn Sie Selbständig erwerbstätig sind |
| ✗ | ✗ | Die Personalabteilung |

**Frage 22: Die Gesamtheit der organisatorischen und technischen Massnahmen, die Verlust und Verfälschung oder unberechtigte Aneignung von Daten verhindern, beschreibt man mit folgenden Begriffen.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Datensicherheit |
| ✓ | ✓ | Informationssicherheit |
| ✗ | ✗ | Datenschutz |

**Frage 23: Welche "Formel" passt am besten zur Berechnung des Risiko Erwartungswertes?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Erwartungswert = Schadenausmass - Eintrittswahrscheinlichkeit |
| ◉ | ◉ | Erwartungswert = Eintrittswahrscheinlichkeit x Schadenausmass |
| O | O | Erwartungswert = Eintrittswahrscheinlichkeit / Schadenausmass |
| O | O | Erwartungswert = Eintrittswahrscheinlichkeit + Schadenausmass |

**Frage 24: Welche beiden Dokumente passen am besten, wenn man die Beschreibung von "technischen" Begriffen zur Informationssicherheit sucht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|

| | | |
|---|---|---|
| ✗ | ✗ | ISO 27000 |
| ✓ | ✓ | NIST Glossary of Key Information Security Terms |
| ✓ | ✓ | RFC 4949 |

**Frage 25: Welches Dokument passt am besten, wenn man die Beschreibung von "generischen" Begriffen zur Informationssicherheit sucht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | ISO 27000 |
| O | O | NIST Glossary of Key Information Security Terms |
| O | O | RFC 4949 |

**Frage 26: Bei der Risikomatrix sollen beim Schadensausmass ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | ... möglichst viele Bereiche von Schadenswerten unterschieden werden. |
| ✗ | ✗ | ... Schadenswerte in Franken angegeben werden. |
| ✓ | ✓ | ... maximal 5 Bereiche mit Schadenswerten unterschieden werden. |
| ✓ | ✓ | ... Schadenswerte unterschiedlicher Art (z.B. finanzielle Schäden, Image, Recht) geschreiben werden können. |

**Frage 27: Für welchen Bereich in der Risikomatrix macht der Abschluss einer Versicherung am meisten Sinn?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | kleine Eintretenswahrscheinlichkeit, kleiner Schaden |
| ◉ | ◉ | kleine Eintretenswahrscheinlichkeit, hoher Schaden |
| O | O | hohe Eintretenswahrscheinlichkeit, kleiner Schaden |
| O | O | hohe Eintretenswahrscheinlichkeit, hoher Schaden |

**Frage 28: Welche der drei in den Übungen studierten aktuellen Dokumente zu Informationssicherheitsbegriffen das Teuerste?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | ISO 27000 Vocabulary |
| O | O | NIST Glossary of Key Information Security Terms |
| O | O | RFC4949 Internet Security Glossary |

**Frage 29: Authentication gehört zu folgendem CIA-Begriff.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | C |
| ◉ | ◉ | I |
| O | O | A |

**Frage 30: Wofür steht das "A" bei den "CIA" Sicherheitszielen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Accessability |
| ◉ | ◉ | Availability |
| O | O | Authorization |
| O | O | Authentication |

**Frage 31: Dass jemand den Empfang von Nachrichten nicht abstreiten kann, bezeichnet man mit dem Fachbegriff…**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | non repudiation |
| O | O | Verbindlichkeit |
| O | O | Empfänger Authentizität |
| O | O | Integrity |

**Frage 32: Welche Aussage trifft auf das Zufallsexperiment "Gewicht von zufällig ausgewählten Personen messen".**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Die Gewichtswerte werden gleichverteilt um den Mittelwert liegen. |
| ◉ | ◉ | Die Gewichtswerte werden normalverteilt um den Mittelwert liegen. |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V02_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V02_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 13:25:09 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 32 |
| **Maximal mögliche Punktezahl:** | 89 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 15:02:51 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 15:23:25 |
| **Benötigte Zeit:** | 00:20:34 |
| **Resultat beste Durchführung:** | 63/89 (71%) |

**Frage 1: Was versteht man bei ISMS unter "Control"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Schutzmassnahme |
| O | O | Überprüfung |
| O | O | Ueberwachung |
| O | O | Check |

**Frage 2: ITIL konzentriert sich auf ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | IT-Service Management |
| O | O | Information Security Management |
| O | ◉ | Business Requirements |
| O | O | Evaluation Assurance Levels |

**Frage 3: Die Bestimmung des finanziellen Schadens von Sicherheitszwischenfällen …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | kann in der IT-Abteilung vorgenommen werden |
| ◉ | ◉ | erfordert die Mitwirkung von Business Units |
| O | O | erfolgt typischerweise in der Finanzabteilung |

**Frage 4: An welche Stelle sollte man sich wenden, wenn man in der Schweiz von einer Internet Sicherheitsverletzung mit krimineller Absicht betroffen ist.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | KOBIK |
| O | O | MELANI |
| O | O | SWITCH |
| O | O | BSI |

**Frage 5: Was steht bei COBIT im Vordergrund?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | IT-Governance |
| O | O | Information Security Management |
| O | O | Konkrete Anleitungen zur Sicherheit bestimmter Objekte |

**Frage 6: Dinge, welche man unbedingt erf•üllen muss, um standardkonform zu sein beschreibt man mit ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | must |
| ✓ | ✓ | shall |
| ✗ | ✗ | should |
| ✓ | ✓ | required* |
| ✗ | ✗ | recommended |

**Frage 7: Womit wird bestätigt, dass eine Firma einen Standards richtig umgesetzt hat?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Akkreditierung |
| ⊙ | ⊙ | Zertifizierung |
| O | O | Standardisierung |

**Frage 8: Womit wird bestätigt, dass die fachliche und organisatorische Kompetenz einer Konformitätsbewertungsstelle anerkannt wird.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | Akkreditierung |
| O | O | Zertifizierung |
| O | O | Standardisierung |

**Frage 9: Welches sind "Schichten" der BSI IT-Grundschutzvorgehensweise?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | IT-Verbund |
| ✓ | ✓ | Infrastruktur |
| ✗ | ✗ | Personal |
| ✓ | ✓ | IT-Systeme |
| ✓ | ✓ | Übergreifende Aspekte |

**Frage 10: Common Criteria (CC) konzentriert sich auf ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | IT-Service Management |
| O | O | Information Security Management |
| O | O | Business Requirements |
| ⊙ | ⊙ | Evaluation Assurance Levels |

**Frage 11: Diese Standards sind in der Regel kostenlos erhältlich:**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | ISO Standards |
| ✓ | ✓ | RFCs |

| | | |
|---|---|---|
| ✓ | ✓ | Standards des BSI Deutschland |
| ✗ | ✗ | IEEE Standards |
| ✗ | ✗ | ANSI Standards |

**Frage 12: ISO 27001 konzentriert sich auf ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | ◉ | IT-Service Management |
| ◉ | O | Information Security Management |
| O | O | Business Requirements |
| O | O | Evaluation Assurance Levels |

**Frage 13: Die Abk•ürzung ISMS steht im Vorlesungsmodul Informationssicherheit f•ür ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Information Security Management System |
| O | O | Information Security Monitoring System |
| O | O | Information Security Monitoring Software |

**Frage 14: Standardisierungsprozesse laufen in der Regel bei folgendem Gremium am schnellsten ab (Zeit von der Idee bis zum publizierten Standard):**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | IETF |
| O | O | ISO |
| O | O | IEEE |
| O | O | ANSI |

**Frage 15: Dinge, welche man ohne spezielle Begr•ündung weglassen kann und trotzdem standardkonform ist, beschreibt man mit ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | shall |
| ✗ | ✗ | should |
| ✓ | ✓ | may |
| ✗ | ✓ | recommended |
| ✓ | ✓ | optional |

**Frage 16: Sie suchen bei der Schweizerischen Akkreditierungsstelle SAS nach einer akkreditierten ISO 27001 Zertifizierungsstelle. Welchen Akkreditierungstyp sollten Sie im Suchformular anwählen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | SCESm - Zertifizierungssstelle für Managementsysteme |
| O | O | SECSp - Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen |
| O | O | SECSe - Zertifizierungsstelle für Personen |
| O | ◉ | SIS - Inspektionsstelle |

**Frage 17: Zu welcher Gefährdungskategorie gemäss BSI IT-Grundschutzvorgehensweise sind Hackerangriffe zu zählen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | höhere Gewalt |
| O | O | organisatorische Mängel |

| | | |
|---|---|---|
| O | O | Menschliche Fehlhandlungen |
| O | O | Technisches Versagen |
| ⊙ | ⊙ | Vorsätzliche Handlungen |

**Frage 18: Welches ist keine sinnvolle Motivation für eine ISO 27001 Zertifizierung?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Gesetzliche Vorgaben und Richtlinien erfüllen |
| O | O | Anforderungen von Kunden erfüllen |
| O | O | Nutzung als Marketingargument |
| O | O | Streben nach besserer Sicherheit |
| ⊙ | ⊙ | Gewährleistung der Kompatibilität |

**Frage 19: Welche Aussage trifft auf den "Evaluation Assurance Level (EAL)" bzw. den "erreichten Sicherheitslevel" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✗ | Das ist ein Konzept, welches in den Common Criteria des DoD verwendet wird. |
| ✓ | ✗ | Das Konzept wird unter unterschiedlichen Bezeichnungen in verschiedenen Standards genutzt. |
| ✓ | ✓ | Die höchsten EAL Stufen (z.B. Formally verified design and tested) sind nur sehr schwer zu erreichn. |
| ✗ | ✓ | Das ist ein Konzept, welches von Cobit eingeführt wurde. |

**Frage 20: Welche Aussage trifft auf "Bausteine" der BSI IT-Grundschutzvorgehensweise zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Bausteine enthalten Informationen zur Gefährdungslage |
| ✓ | ✓ | Bausteine enthalten Massnahmenempfehlungen |
| ✓ | ✓ | Bausteine sind nach "Schichten" gruppiert |
| ✗ | ✗ | Bausteine sind für die meisten aktuellen Systeme verfügbar. |

**Frage 21: RFCs werden durch folgende Organisation veröffentlicht:**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | IETF |
| O | O | IANA |
| O | O | ANSI |
| O | O | IEEE |

**Frage 22: Ein "Angriffsvektor" ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✗ | beschreibt eine mögiche Art, wie auf Werte zugegriffen werden kann. |
| ✗ | ✗ | zeigt an, ob der Angriff auf Vertraulichkeit, Echtheit oder Verfügbarkeit abzielt. |
| ✓ | ✓ | bezeichnet einen möglichen Angriffsweg, den ein unbefugter Eindringling nehmen kann, um ein fremdes Com |
| ✓ | ✓ | ist ein Begriff, welcher beim Open Web Application Security Project (OWASP) verwendet wird. |

**Frage 23: Nach welchem "Sicherheitsstandard" kann man sich zertifizieren lassen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | ISO 27000 Overview and Vocabulary |
| ⊙ | ⊙ | ISO 27001 ISMS Requriements |

| | | |
|---|---|---|
| O | O | ISO 27002 Code of Practice IS Controls |
| O | O | ISO 27005 IS Risk Management |

**Frage 24: Welches der folgenden Themen hat sich "OWASP" vor allem auf die Fahne geschrieben"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Netzwerksicherheit |
| ◉ | ◉ | Sicherheit von Web Anwendungen |
| O | O | Firewalls |
| O | O | Standardisierung |

**Frage 25: Wann sollten bei einem Software Entwicklungsprojekt Security-Aspekte beachtet werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Schon zu Beginn des Projekts |
| ✗ | ✗ | Erst bei der Go-Live-Phase |
| ✗ | ✗ | Ausschliesslich während der Design-Phase |
| ✓ | ✓ | Während dem gesamten Endwicklungsprozess |

**Frage 26: Wieso soll man  RFC direkt bei der IETF suchen und nicht nur via Google Suche?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | weil dort auch  angegeben wird, ob der RFC noch gültig ist. |
| O | O | weil die Suche dort schneller ist. |
| O | O | weil man so auch die Autoren des RFC angezeigt erhält. |

**Frage 27: Welchen beiden  Massnahmenkategorien gemäss BSI IT-Grundschutzvorgehensweise gibt es klar am meisten Einträge?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | M1 Infrastruktur |
| ✓ | ✗ | M2 Organisation |
| ✗ | ✗ | M3 Personal |
| ✓ | ✓ | M4 Hardware/Software |
| ✗ | ✗ | M5 Kommunikation (Netze) |

**Frage 28: botswatch.de**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | zeigt an, wo in der Welt Bots aktiv sind. |
| ◉ | ◉ | versucht automatisch generierte Tweets zu erkennen |
| O | O | ist eine Aktion der EU |
| O | O | ist eine Aktion des BSI |

**Frage 29: In welcher Phase des Software Life Cycles ist die Behandlung von Security Problemen am aufwändigsten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Define |
| O | O | Design |
| O | O | Develop |
| O | O | Deploy |

| | | |
|---|---|---|
| ◉ | ◉ | Maintain |

**Frage 30: Was beschreibt gemäss Information Security Standards der ISO 27000 Serie den Begriff Wert (Asset) am besten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Alles was für eine Organisation von Wert ist |
| O | O | Confidentiality (Vertraulichkeit) |
| O | O | Integrity (Echtheit) |
| O | O | Reputation |
| O | O | Availability (Verfügbarkeit) |

**Frage 31: Die OWASP-Top-10 Liste ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | ist eine Liste von Schwachstellen. |
| ✗ | ✗ | ist seit 2010 geordnet nach der Auftretenshäufigkeit. |
| ✓ | ✓ | ist seit 2010 geordnet nach dem Risiko. |
| ✗ | ✗ | ist eine Liste von Abwehrmassnahmen. |

**Frage 32: Welches dieser Dokumente dürfte Sie am ehesten betreffen, wenn Sie an der Entwicklung von Kreditkarten Zahlungssystemen beteiligt sind?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | ISO 27001 |
| ◉ | ◉ | PCI DSS |
| O | O | HIPPA |
| O | O | ISO 27000 |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V03_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V03_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 13:29:20 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 20 |
| **Maximal mögliche Punktezahl:** | 66 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 15:44:39 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:06:03 |
| **Benötigte Zeit:** | 00:21:24 |
| **Resultat beste Durchführung:** | 48/66 (73%) |

**Frage 1: Dies ist der Begriff bzw. die Abkürzung für eine gezielte Bedrohung?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | APT |
| ✓ | ✓ | Spear Phishing |
| ✗ | ✗ | Sexploitation |
| ✗ | ✗ | Zero Day Attack |

**Frage 2: Was ist unter "Critical Infrastructures" zu verstehen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Das Internet of Things |
| ⊙ | ⊙ | Für die Gesellschaft überlebenswichtige Infrastrukturen |
| O | O | Infrastrukturen welche unzuverlässig funktionieren. |
| O | O | Das Internet Backbone Netz. |

**Frage 3: Um welche beiden  Informationssicherheitsaspekte geht es beim "Viren Tatbestand" in erster Linie?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Confidentialiy |
| ✓ | ✓ | Integrity |
| ✓ | ✓ | Availability |
| ✗ | ✗ | Authentication |

**Frage 4: Welche der folgenden Aussagen treffen auf den Begriff  "Clickjacking"  zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Clickjacking heisst ein spezielles Programm, mit welchem das Einstecken von Steckern in Buchsen Mausklicks a |
| ✓ | ✓ | Mausklicks auf Webseiten werden zum unwissentlichen Starten von Programmen missbraucht. |
| ✓ | ✓ | Clickjacking nutzte Schwachstellen von Browsern aus. |
| ✗ | ✗ | Beim Clickjacking wird anhand des Clickgeräusches herausgefunden, welche Maushardware im Einsatz ist. |

**Frage 5: Um welche Informationssicherheitsfrage geht es beim "Hacking Tatbestand" in erster Linie?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Confidentialiy |
| O | O | Integrity |
| O | O | Availability |
| O | O | Authentication |

**Frage 6: Welche der folgenden Beschreibungen passt am besten zum Begriff "Drive-by-Download"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | herunerladen von Malware bei der Vorbeifahrt an WLAN-Accesspoints |
| ◉ | ◉ | herunterladen von Malware beim blossen Aufruf einer Webseite |
| O | O | herunterladen von Malware beim zufälligen Anklicken bestimmter Icons |
| O | O | herunterladen von Malware während einem Musikdownload |

**Frage 7: Bei welchen Angriffsarten versuchen die Angreifer möglichst geheim zu halten, dass eine Attacke stattgefunden hat?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Attacken von staatlichen Organisationen |
| ✗ | ✗ | Attacken von Protestorganisationen (Haktivismus) |
| ✗ | ✗ | Attacken von Script Kiddies |
| ✓ | ✓ | Attacken von kriminellen Organisationen |

**Frage 8: Welche Aussagen treffen für den DNS-Spoofing-Angriff  mit Hilfe von Cain&Abel zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Damit wird im Default DNS-Server angegriffen.etwas verändert. |
| ◉ | ◉ | Damit werden falsche DNS-Reply Meldungen kreiert. |
| O | O | Damit wird auf dem DNS-Server etwas verändert. |
| O | O | Damit wird auf dem aufgerufenen Webserver  etwas verändert. |

**Frage 9: Welche Aussagen treffen  auf die entsprechenden Rechtsartikel Betreffend Einbruch in Computersysteme (Hostfriedensbruch) und Einbruch in ein Haus (Hausfriedensbruch) zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Beim Einbruch ins Haus verstösst man auch gegen den Rechtsartikel, wenn die Türen nicht verschlossen ware |
| ✓ | ✓ | Beim Einbruch in ein Computersystem verstösst man nur gegen den Rechtsartikel,  wenn das System besonde |
| ✗ | ✗ | Beim Einbruch in ein Computersystem verstösst man nur dann gegen den Rechtsartikel,  wenn man sich damit |
| ✓ | ✓ | Beim Einbruch in ein Haus, wird man nur auf Antrag bestraft. |

**Frage 10: Welche Aussagen treffen für den ARP-Spoofing-Angriff mit Hilfe von Cain&Abel zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | Es werden die Forwarding-Tabellen in den Switches verändert. |
| ✓ | ✓ | Es werden die ARP-Caches in Stationen verändert. |
| ✓ | ✓ | Der Angriff funktioniert nur innerhalb einer Broadcast-Domain. |
| ✗ | ✗ | Der Angriff funktioniert nur bei Windows-Rechnern. |

**Frage 11: Welche Aussagen treffen auf  "Ransomware" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|

| | | |
|---|---|---|
| ✗ | ✗ | Das ist eine weltweit  nicht mehr weit verbreitete Angriffsart. |
| ✓ | ✓ | Damit werden Lösegeldforderungen gestellt. |
| ✓ | ✗ | Ransomware kann "as a service" gebucht werden. |
| ✗ | ✓ | Ransomware ist in der Schweiz kaum anzutreffen. |

**Frage 12: Was versteht man unter "Spear Phishing"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Phishing mit Hilfe des Programms "Spear". |
| ◉ | ◉ | Einen gezielten Phishing Angriff auf ausgewählte Personen. |
| O | O | Einen Phishing Angriff, der  automatisiert abläuft. |
| O | O | Einen "Software Phishing with Even Ransomware" Angriff. |

**Frage 13: Welche Aussagen treffen auf den "World Economic Forum Hack" aus dem Jahre 2001 zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Es wurde eine Person verhaftet. |
| ✗ | ✓ | Beim Angriff wurde die "Integrity" von Daten verletzt. |
| ✓ | ✗ | Beim Angriff wurde die "Confidentiality" von Daten verletzt. |
| ✗ | ✓ | Der Angreifer konnte in Bezug auf "Strafgesetzbuch Art. 143 bis:  Unbefugtes Eindringen in ein Datenverarbeitu |
| ✗ | ✓ | Der Angreifer konnte in Bezug auf "Strafgesetzbuch Art 144 bis: Datenbeschädigung  " verurteilt werden. |

**Frage 14: Was ist unter der "Attack Surface" zu verstehen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Alle Punkte (Möglichkeiten), über welche ein Angriff ausgeführt werden könnte. |
| O | O | Das geografische Gebiet, in welchem eine Firma arbeitet. |
| O | O | Die Summe aller Angriffswerkzeuge (tools), über welche ein Angreifer verfügt. |

**Frage 15: Welche der folgenden Aussagen zu Botnets treffen zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Man weiss sehr gut, wie viele Rechner mit Bots befallen sind. |
| ✓ | ✓ | Um ein Botnetz nutzen zu können, benötigt man keine besondere technische Kenntnisse. |
| ✗ | ✗ | Es ist einfach festzustellen, ob ein Rechner Teil eines Botnets ist. |
| ✓ | ✓ | Die Betreiber der Botnets nutzen diese in der Regel nicht selbst für Angriffe, sondern bieten Interessierten das |

**Frage 16: Zu welcher Strafe wurde 2002 ein EDV-Experte vom Züricher Obergericht für den Vertrieb einer CD-ROM mit Quellcodes für Computerviren verurteilt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | zu 300 Franken Busse |
| ✓ | ✓ | zu 5'000 Franken Busse |
| ✓ | ✓ | zu zwei Monaten Gefängnis |
| ✗ | ✗ | Er wurde zu keiner Strafe verurteilt. |

**Frage 17: Was versteht man unter einer Zero-Day Attacke?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Attacke, welche sich mit sehr geringem Aufwand durchführen lässt |
| ◉ | ◉ | Attacke, welche ausgeführt wird, bevor Patches für die Verletzlichkeit verfügbar sind |

| | | |
|---|---|---|
| O | O | Attacke, nach deren Durchführung das angegriffene System überhaupt nicht mehr nutzbar ist |

**Frage 18: Bei einer Advanced Persistent Threats (APT) …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | … versucht ein einzelnder Angreifer mit sehr viel beharrlichkeit von irgend einem Ziel, Informationen zu beschaf |
| ✓ | ✗ | … arbeitet der Angreifer meist mit Teams von Spezialisten. |
| ✓ | ✓ | … handelt es sich um sehr zielgerichtete Attacken. |
| ✗ | ✗ | … werden vor allem die modernsten Technologien eingesetzt. |

**Frage 19: Welche Beschreibungen treffen auf den Begriff "Hacktivismus" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | krankhaft aktive Hacker |
| ✓ | ✓ | Angriffe auf Webseiten für politische Zwecke |
| ✓ | ✓ | Verwendung von Computern und Computernetzen als Protestmittel |

**Frage 20: Welche Aussagen treffen auf "Phishing Attacken" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Phishing Attacke sind mittlerweile nicht mehr weit verbreitet. |
| ✓ | ✓ | Phishing Attacken werden häufig mit Hilfe von Mails durchgeführt. |
| ✗ | ✗ | Phishing Attacken sind leicht zu erkennen. |
| ✓ | ✓ | Phishing Attacken sind effizienter wenn möglichst viel Informationen über das Ziel ausgenutzt werden können. |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V04_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V04_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 13:40:21 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 38 |
| **Maximal mögliche Punktezahl:** | 102 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:13:37 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:24:50 |
| **Benötigte Zeit:** | 00:11:13 |
| **Resultat beste Durchführung:** | 42/102 (41%) |

**Frage 1: Unter welchem Begriff fasst man den Anteil der Webseiten zusammen, welche mit einem normalen Browser erreicht werde können, aber von Suchmaschinen nicht indexiert worden sind.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Surface Web |
| ◉ | ◉ | Deep Web |
| O | O | Dark Web |

**Frage 2: Welche Aussagen treffen auf die JUST Culture zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Mitarbeitende sollen interne Regeln übertreten, wenn die Situation dies verlangt. |
| ✓ | ✓ | Sicherheitszwischenfälle sollen in jedem Fall gemeldet werden. |
| ✗ | ✗ | Bei Sicherheitszwischenfällen sollen die Verantworlichen in jedem Fall bestraft werden. |
| ✓ | ✓ | Die JUST Culture unterscheidet drei grundsätzlich verschiedene Arten von Fehlverhalten. |

**Frage 3: Welche Aussagen teffen auf die "Klassifizierung von Dokumenten" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Das gehört zur gundsätzlichen Sicherheitsmassnahme "Organisieren". |
| ✗ | ✗ | Die meisten Unternehmen in der Schweiz führen die "Klassifizierung von Dokumenten" systematisch durch. |
| ✓ | ✓ | Das ist eine Voraussetzung dafür, dass man Sicherheismassnahmen effizient umsetzen kann. |
| ✓ | ✓ | Damit legt man den Schutzbedarf von Dokumenten fest. |

**Frage 4: Welche der URLs haben "same origin" wie http://www.company.com/dir/page.html**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | http://www.company.com/dir2/other.html |
| ✗ | ✗ | https://www.company.com/secure.html |
| ✓ | ✓ | http://www.company.com/dir/inner/another.html |
| ✗ | ✗ | http://www.company.com:81/dir/etc.html |

**Frage 5: In welchen Situationen spricht man von "two factor authentication" ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Wenn zwei der drei Gundkonzepte der Authentisierung erfüllt werden. |
| ✗ | ✗ | Wenn eine Identifizierung und eine Authentifizierung durchgeführt wurde. |
| ✓ | ✓ | Wenn man seine Authentizität mittels Geheimcode und mit dem Besitz eines Sicherheitstokens unter Beweis ge |
| ✗ | ✗ | Wenn man für die Zutrittskontrolle mittels Fingerprintsensor zwei verschiedene Finger nehmen muss. |

**Frage 6: Bei welcher Schweizer Bundesstelle sollen Sicherheitszwischenfälle gemeldet werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | MELANI |
| O | O | KOBIK |
| O | O | SWITCH |
| O | O | SKP PSC |

**Frage 7: Diese Aktionen/Begriffe gehören beim Identity und Access Management zum Teil "Provisioning".**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Alarmierung |
| O | O | Accounting |
| ◉ | ◉ | Vorbereitung von Zugriffsrechten |
| O | O | Überprüfung der Authentizität der Nutzer |

**Frage 8: Welche Aussage trifft auf das "Vier-Augen-Prinzip" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Ein Entscheid muss von mindestens zwei Person getragen werden |
| O | O | Eine Person soll mehr als einmal die Lösung einer Aufgabe prüfen. |
| O | O | Nur der Chef kann sein "ok" geben bevor die Aufgabe wirklich abgeschlossen werden kann. |
| O | O | Ich muss jeden Schritt dokumentieren und von meinem Vorgesetzten absegnen lassen |

**Frage 9: Welche Abk•ürzung steht f•ür die Datenbank/Beschreibung, mit welcher bei der National Vulnerability Database (NVD) die Identifikation von Verletzlichkeiten sichergestellt wird?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | CVSS |
| ◉ | ◉ | CVE |
| O | O | CPE |
| O | O | CSRC |

**Frage 10: Welche der folgenden Aussagen zu CERT treffen zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | CERT ist die Abkürzung für Computer Emergency Response Team. |
| ✓ | ✓ | CERT wurde in den USA gegründet. |
| ✗ | ✗ | CERT gibt es nur in den USA. |
| ✗ | ✗ | CERT gibt es nur bei staatlichen Stellen. |

**Frage 11: Welche Aussagen treffen in Bezug auf die Sicherheit von Public Key Verfahren im Vergleich zu symetrischen Verschlüsselungsverfahren zu, in Bezug auf das "Knacken des System" mittels Durchprobieren aller Schlüssel?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|

| | | |
|---|---|---|
| O | O | Public Key Verfahren mit dem RSA-Algorithmus bieten die gleiche Sicherheit wie symmetrische Verschlüsselun |
| ⊙ | ⊙ | Public Key Verfahren mit Elliptische Kurven (EC) bieten eine höhere Sicherheit als symmetrische Verfahren, we |
| O | O | Die Sicherheit des symmetrischen Verschlüsselungsverfahren ist ab 2048 Bit Schlüssellänge immer besser als |

**Frage 12: Welche Aussage trifft auf die DMZ zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✗ | Die DMZ schützt interne Systeme gegen Angriffe von aussen. |
| ✗ | ✗ | Die DMZ warnt vor illegalen Requests die von einem internen Rechner kommen. |
| ✓ | ✓ | Die DMZ wird mit Hilfe von passenden Router und Firewallregeln definiert. |
| ✗ | ✗ | Die DMZ hat nur Bedeutung in Zusammenhang mit HTTP-Verkehr. |

**Frage 13: Diejenigen Informationen des Internet, welche man mit Suchmaschinen finden kann, bilden das …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | Surface Web |
| O | O | Deep Web |
| O | O | Darknet |

**Frage 14: Diejenigen Informationen des Internet, welche man nur mit speziellen Browsern finden kann, bilden ein …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Surface Web |
| O | O | Deep Web |
| ⊙ | ⊙ | Darknet |

**Frage 15: Was bedeudet opt-in?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | Es wird erst dann etwas zugelassen, wenn der Betroffene dies erlaubt hat. |
| O | O | Das was man zulässt ist optional. |
| O | O | Es wird etwas zugelassen, ausser der Betroffene verbietet es. |

**Frage 16: Welcher Begriff trifft am besten auf die National Vulnerability Database (NVD) zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | ⊙ | Metadatenbank |
| O | O | Internationaler Standard |
| O | O | Top10 Verletzlichkeitsliste |
| O | O | Einfach bedienbare Website |

**Frage 17: Welche Aussagen treffen auf die National Vulnerability Database (NVD) zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Hilft zur Vereinheitlichung von verschiedenen, firmenspezifischen Vulnerability Scoring Systemen. |
| ✗ | - | Liefert ein direktes Mass zum Business Impact. |
| ✓ | - | Erleichtert die Identifikation von identischen Verletzlichkeiten, welche verschiedene Organisationen entdeckt ha |
| ✓ | - | Führt leicht zu falschen Statistiken, wenn man bei der Suche nicht sorfältig arbeitet. |

**Frage 18: Welche Schweizer Bundeststelle kümmert sich um die koordinierte Bekämpfung der Internet-Kriminalität?**

| Richtige | Deine | Fragetext |
|---|---|---|

| Antwort | Antwort | |
|---|---|---|
| O | O | MELANI |
| ◉ | O | KOBIK |
| O | O | SWITCH |
| O | O | SKP PSC |

**Frage 19: Welche Abk•ürzung steht bei der National Vulnerability Database (NVD) fü•r die Metric zur Bewertung des Schweregrades von Verletzlichkeiten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | CVSS |
| O | O | CVE |
| O | O | CPE |
| O | O | CSRC |

**Frage 20: Welche Abkü•rzung steht bei der National Vulnerability Database (NVD) fü•r die Identifikation von Plattformen (Produkten/Geräten/Anwendungen)?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | CVSS |
| O | O | CVE |
| ◉ | O | CPE |
| O | O | CSRC |

**Frage 21: Mit welchem Begriff wird die Zugangskontrolle "Aktionen nur innerhalb eines bestimmten Bereichs zulassen" am besten beschrieben?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Sandbox |
| O | O | Opt-In |
| O | O | Black Listing |
| O | O | Principle of least priviledge |

**Frage 22: Welche beiden Begriffe passen am besten zum Verfahren, bei welchem man nur Zugang auf ausgewählte Webseiten zulässt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | White Listing |
| ✗ | - | Black Listing |
| ✗ | - | Opt-Out |
| ✓ | - | Alles verbieten, was nicht explizite erlaubt ist |

**Frage 23: Was sind typische Funktionen von HTTP-Proxies?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Unnötige Datenübertragung vermeiden |
| ✓ | - | Internetverkehr einer Firma kanalisieren |
| ✓ | - | Möglichkeit zur Malware Detektion bieten |
| ✗ | - | HTTP-Request Bodypart verändern |

**Frage 24: Welche Aussagen teffen auf den NVD CVSS Serverity Wert zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|

| | | |
|---|---|---|
| ✓ | - | Der Base Score Anteil "Exploitability Metrics" wird entsprechend der Verletzlichkeit automatisch berechnet. |
| ✓ | - | Die Score-Werte liegen zwischen 0 und 10. |
| ✗ | - | Die Temporal Score Metrics Werte werden in den meisten Fällen entsprechende der Vulnerability automatisch be |

**Frage 25: Was bedeudet opt-out?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Es wird erst dann etwas zugelassen, wenn der Betroffene dies erlaubt hat. |
| ◉ | O | Es wird etwas zugelassen, ausser der Betroffene verbietet es. |
| O | O | Das was man zulässt ist optional. |

**Frage 26: Was versteht man unter dem "Principle of least privilege"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Nur zulassen was unbedingt nötig ist. |
| O | O | Zusätzliche Berechtigungen erteilen, um in bestimmten Fällen schneller an Informationen zu gelangen. |
| O | O | Sie können sich selber Berechtigungen ab einer bestimmten Stufe erteilen. |
| O | O | Das es keine Rollenverteilung in diesem Unternehmen gibt. |

**Frage 27: Welches ist ein korrekt formatierter CVE Identifier?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | CVE-2014-1886 |
| O | O | CVE-aa11-1299 |
| O | O | CPE-2016-1121 |
| O | O | CPE-ha98-1337 |

**Frage 28: Welches sind "grundsätzliche Massnahmen zur Verbesserung der Sicherheit" (gemäss InfSi1-Vorlesung)?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Organisieren |
| ✓ | - | Massnahmen kombinieren |
| ✓ | - | Zutritt kontrollieren |
| ✗ | - | Verschlüsseln |

**Frage 29: Welche Aussagen treffen auf "Honeypots" zur Detektion von Angreifern zu.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Ein Honeypot bietet Dienste an, welche normalerweise niemand nutzt. |
| ✓ | - | Ein Problem beim Einsatz von Honeypots ist die hohe Anzahl von Fehlalarmen. |
| ✗ | - | Der Honeypot überwacht den gesamten Verkehr auf dem Netz, an welches er angeschlossen ist. |
| ✓ | - | Honeypots gibt es für verschiedene Betriebssysteme. |

**Frage 30: Welche beiden Begriffe passen am besten zum Verfahren, bei welchem der Zugang auf ausgewählte Webseiten gesperrt wird?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | White Listing |
| ✓ | - | Black Listing |
| ✗ | - | Opt-Out |
| ✓ | - | Alles erlauben, was nicht explizite verboten ist |

**Frage 31: Es gibt Konfigurationen, bei welchen der Angreifer mehrere Firewalls überbrücken muss, um zu einem bestimmten Angriffsziel zu gelangen. Welche Aussagen treffen in diesem Zusammenhang zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Dies ist eine Beispiel für das Sicherheitsgrundkonzept "Massnahmen kombinieren". |
| ✓ | - | Es sollten Firewalls von verschiedenen Herstellern eingesetzt werden, weil so eine bestimmte Lücke nicht gleich |
| ✗ | - | Es sollten möglichst Firewalls vom selben Hersteller eingesetzt werden, weil man so günstiger einkaufen kann. |

**Frage 32: Wofür steht der Begriff "just" in Zusammenhang mit der Just Culture?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | gerecht |
| O | O | schnell |
| O | O | Joint US Exposure Organization |

**Frage 33: Was ist das Hauptziel der Just Culture?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Verbesserung der Sicherheit |
| O | O | Findung eines gerechten Strafmasses |
| O | O | Sammlung von Informationen über Fehlverhalten |

**Frage 34: Wie kommen Organisationen, welche Security Reports veröffentlchen, zu relativ verlässlichen Aussagen über die aktuell typischen Angriffsarten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Sie unterhalten ein Netz von "Sicherheitssensoren" (z.B. Firewalls) und analysieren die detektierten Angriffe. |
| O | O | Sie befragen die Chief Security Officers von Firmen. |
| O | O | Sie führen Hackingwettbewerbe durch. |

**Frage 35: Falls man die Verbindung zu einem Web-Server über einen gewöhnlichen Web-Proxy aufbaut, kann der Web-Server prinzipiell nicht erkennen, in welchem Land der Client steht, welcher den Webseitenaufruf getätigt hat.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | richtig |
| ◉ | O | FALSCH |

**Frage 36: Wofür steht die Abkürzung DMZ im Rahmen der InfSi1-Vorlesung?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Demilitarized Zone |
| O | O | Demarked Zone |
| O | O | Domain Zone |
| O | O | Angriffsfreie Zone |

**Frage 37: Welche Formulierungen passen zu "Attack Vector"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Angriffspunkte und Verfahren, über welche ein Angreifer Daten abgreifen oder einspeisen kann. |
| O | O | Schnittstellen beim Zielsystem, über welche ein Angreifer kommuniziert. |
| O | O | Pfeil auf die Verletzlichkeit eines Systems. |

**Frage 38: Menschen tendieren dazu, dass Strafmass bei Sicherheitszwischenfällen…**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | abhängig von der Schwere des Zwischenfalls festzulegen. |
| O | O | unbhängig von der Schwere des Zwischenfalls  nur von der Schwere des Vergehens festzulegen. |
| O | O | abhängig von der Art des Vergehens festzulegen. |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V05_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V05_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 14:22:20 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 25 |
| **Maximal mögliche Punktezahl:** | 58 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:25:05 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:25:06 |
| **Benötigte Zeit:** | 00:00:01 |
| **Resultat beste Durchführung:** | 0/58 (0%) |

**Frage 1: Wie viele mögliche Schlüssel gibt es beim Caesar-Code?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | 26 |
| O | O | 26^2 |
| O | O | 26! |

**Frage 2: Welche Aussagen treffen zu "Steganographie" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Steganographie wird auch mit "Covert Channel" umschrieben. |
| ✗ | - | Eine mit Steganographie verarbeitete Nachricht, kann nur bei Kenntnis des richtigen Schlüssels gelesen werden. |
| ✓ | - | Bei der Steganographie benötigt man ein Hostfile. |
| ✓ | - | Die Methode der Steganographie kommt bei modernen Farb-Laser-Druckern zum Einsatz. |

**Frage 3: Welche Teile eines Kryptosystems müssen geheim gehalten werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Verschlüsselungsalgorithmus |
| O | O | Entschlüsselungsalgorithmus |
| ◉ | O | Schlüssel |
| O | O | Systemarchitektur |

**Frage 4: Bei einem System wird eine Geheimzahl (z.B. der PIN-Code) aus einer völlig zufällig gewählten Kombination mit vier Zeichen erstellt. Für die vier Zeichen steht der Zeichensatz 0, ..., 9 zu Verfügung, d.h. es sind Geheimcodes zwischen "0000" und "9999" möglich. Welche Entropieangabe liegt am nächsten bei der Entropie der daraus abgeleiteten Binärschlüssels?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 10 Bit |
| ◉ | O | 13 Bit |
| O | O | 20 Bit |
| O | O | 40 Bit |

**Frage 5: 8 zufällig gewählte Hex-Zeichen haben einen Informationsgehalt von...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 4 Bit |
| O | O | 16 Bit |
| ◉ | O | 32 Bit |
| O | O | 64 Bit |
| O | O | 128 Bit |

**Frage 6: Der Informationsgehalt eines Symbols, welches mit der Wahrscheinlichkeit 1/68 vorkommt, beträgt ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 5.1 Bit |
| O | O | 6 Bit |
| ◉ | O | 6.09 Bit |
| O | O | 7.2 Bit |
| O | O | 8 Bit |

**Frage 7: Die Entropie (bzw. der mittlere Informationsgehalt) einer zufällig gewählten Zeichenfolge ist dann am höchsten, ....**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | wenn einige Zeichen sehr selten vorkommen. |
| ◉ | O | wenn alle Zeichen gleich häufig vorkommen. |
| O | O | wenn einige Zeichen sehr häufig vorkommen. |

**Frage 8: Unter Berücksichtigung des Zusammenhangs aufeinanderfolgender Zeichen beträgt die Entropie englischer Texte etwa ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 8 Bit |
| O | O | 5 Bit |
| O | O | 3 Bit |
| ◉ | O | 2 Bit |

**Frage 9: Wer gilt als Begründer der Informationstheorie und hat die Einheit zum Informationsgehalt definiert?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Auguste Kerckhoffs |
| ◉ | O | Claude Shannon |
| O | O | Alain Touring |
| O | O | Gilbert Vernam |

**Frage 10: Angreifer können das Chiffrat eines Textes am besten entschlüsseln, wenn ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | der Klartext viel Redundanz enthält. |
| O | O | die Entropie des Klartexts 4.7 Bit beträgt. |
| O | O | alle Zeichen des Chiffrats gleich häufig auftreten. |

**Frage 11: Bei welchem Verfahren zeigt die Autokorrelation der verschlüsselten Zeichenfolge des Märchentextes "Ali Baba und die 40 Räuber" Periodizitäten?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Caesar |
| ◉ | O | Vigenère |

**Frage 12: Bei welchem Verfahren ist die typische Buchstabenhäufigkeit einer Sprache im Chiffrat weniger klar ersichtlich?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Caesar |
| ◉ | O | Vigenère |

**Frage 13: Beim One-Time-Pad Verschlüsselungsverfahren ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | ist der Schlüssel gleich lang wie der Klartext. |
| ✗ | - | müssen alle Klartextzeichen gleich häufig auftreten. |
| ✓ | - | darf der Schlüssel nicht mehrfach verwendet werden. |
| ✗ | - | wird der Schlüssel nach jeweils 1000 Zeichen gewechselt. |

**Frage 14: Dass die Sicherheit eines Verschlüsselungssystems einzig und allein von der Sicherheit des geheimen Schlüssels abhangen soll, wurde gefordert von ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Auguste Kerckhoffs |
| O | O | Claude Shannon |
| O | O | Alain Touring |
| O | O | Gilbert Vernam |

**Frage 15: An der Entschlüsselung von Enigma-Meldungen im 2. Weltkrieg war folgende Person massgeblich beteiligt:**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Auguste Kerckhoffs |
| O | O | Claude Shannon |
| ◉ | O | Alan Touring |
| O | O | Gilbert Vernam |

**Frage 16: Security by Obscurity heisst, ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | dass die Sicherheit auf der Geheimhaltung von Systemeigenschaften, Verfahren und Systemdesign basiert. |
| O | O | dass die Sicherheit darauf beruht, dass sehr komplexe Verfahren eingesetzt werden. |
| O | O | dass möglichst undurchsichtige, nicht erratebare Passwörter verwendet werden. |

**Frage 17: Das Caesar Verschlüsselungsverfahren ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | ist ein Transpositionsverfahren. |
| ✓ | - | ist ein Substitutionsverfahren. |
| ✓ | - | verwendet monoalphabethische Verschlüsselung. |
| ✗ | - | verwendet polyalphabethische Verschlüsselung. |

**Frage 18: Das Vigenère Verschlüsselungsverfahren ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | ist ein Transpositionsverfahren. |
| ✓ | - | is ein Substitutionsverfahren. |
| ✗ | - | verwendet monoalphabethische Verschlüsselung. |
| ✓ | - | verwendet polyalphabethische Verschlüsselung. |

**Frage 19: Welche Inhalte werden bei Aktivierung von Google SafeSearch blockiert?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Seiten mit anstössigen Bilder und Videos |
| O | O | Seiten mit Sicherheitsrisiken |
| O | O | Seiten, welche die Browsereinstellungen verändern |
| O | O | Seiten mit zu viel Werbebannern |

**Frage 20: Bei welchen Inhalten liefert Google Safe Browsing eine Warnung?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Seiten mit anstössigen Bilder und Videos |
| ◉ | O | Seiten mit Sicherheitsrisiken |
| O | O | Seiten, welche die Browsereinstellungen verändern |
| O | O | Seiten mit zu viel Werbebannern |

**Frage 21: Welchen Wert liefert die Autokorrelation einer Folge von 10'000 zufällig aus 26 Grossbuchstaben ausgewählten Zeichen bei der Verschiebung um ein Zeichen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | etwa 7.6% Übereinstimmungen |
| ◉ | O | etwa 4% Übereinstimmungen |
| O | O | etwa 3% Übereinstimmungen |
| O | O | etwa 1% Übereinstimmungen |

**Frage 22: Welchen Wert liefert die Autokorrelation einer Folge von 10'000 zufällig aus 26 Grossbuchstaben ausgewählten Zeichen bei der Verschiebung um mehr als ein Zeichen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | etwa 7.6% Übereinstimmungen |
| ◉ | O | etwa 4% Übereinstimmungen |
| O | O | etwa 3% Übereinstimmungen |
| O | O | etwa 1% Übereinstimmungen |

**Frage 23: Der Informationsgehalt eines einzelnen Zeichens ist dann am höchsten, …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | wenn das Zeichen sehr selten vorkommt. |
| O | O | wenn das Zeichen gleich häufig vorkommt, wie alle anderen Zeichen. |
| O | O | wenn das Zeichen sehr häufig vorkommt. |

**Frage 24: Gegeben ist ein deutscher Text mit 10'000 Zeichen, der nur mit Grossbuchstaben geschrieben wurde. Wie gross ist die Autokorrelation bei der Verschiebung um genau ein Zeichen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | etwa 7.6% Übereinstimmungen |

| | | |
|---|---|---|
| O | O | etwa 4% Übereinstimmungen |
| ◉ | O | etwa 3% Übereinstimmungen |
| O | O | etwa 1% Übereinstimmungen |

**Frage 25: Wie viele mögliche Schlüssel gibt es beim Vigenère-Code mit n Zeichen bzw. Buchstaben Schlüssellänge?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 26 |
| O | O | 26^2 |
| O | O | 26! |
| ◉ | O | 26^n |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V06_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V06_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 14:26:21 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 23 |
| **Maximal mögliche Punktezahl:** | 68 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:25:31 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:25:57 |
| **Benötigte Zeit:** | 00:00:26 |
| **Resultat beste Durchführung:** | 0/68 (0%) |

**Frage 1: Welche der folgenden Verfahren sind Symmetric Key Verfahren?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | RSA |
| ✗ | - | DH |
| ✓ | - | AES |
| ✓ | - | DES |

**Frage 2: Was ergibt die Verknüpfung y = a EXOR b EXOR a ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 1 |
| O | O | a |
| ◉ | O | b |
| O | O | 0 oder 1 abhängig von a |

**Frage 3: Wenn man die Länge eines Schlüssels um ein Bit erhöht ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | verdoppelt sich die Sicherheit des Systems. |
| ✗ | - | verdoppelt sich der Informationsgehalt des Schlüssels. |
| ✓ | - | nimmt der Informationsgehalt des Schlüssels um ein Bit zu. |
| ✗ | - | wird die Sicherheit des Systems vier mal grösser. |

**Frage 4: AES steht für ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Advanced Encryption Standard |
| O | O | American Encryption Standard |
| O | O | Adopted Encryption Security |
| O | O | Algorithmic Enctyption Security |

**Frage 5: Welche (effektive) Schlüssellänge wird bei "normaler" DES-Verschlüsselung verwendet?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | 56 Bit |
| O | O | 64 Bit |
| O | O | 112 Bit |
| O | O | 128 Bit |
| O | O | 192 Bit |

**Frage 6: Welche (effektive) Schlüssellänge muss bei einer Brute Force Attacke Triple-DES-Verschlüsselung "verarbeitet" bzw. durchprobiert werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 56 Bit |
| O | O | 64 Bit |
| ◉ | O | 112 Bit |
| O | O | 128 Bit |
| O | O | 192 Bit |

**Frage 7: Welche der folgenden Begriffe beschreiben AES?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | Stream Cipher |
| ✓ | - | Block Cipher |
| ✓ | - | Advanced Encryption Standard |
| ✗ | - | American Encryption Standard |

**Frage 8: Bei welchem Block Cipher Betriebsmodus können Periodizitäten im Klartext erhalten bleiben?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Electronic Codebook (ECB) Mode |
| O | O | Cipher Block Chaining (CBC) |
| O | O | Cipher Feedback Mode (CFB) |
| O | O | Counter Mode (CTR) |

**Frage 9: Welche EXOR-Inputs führen auf den Output "1"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | 0 (+) 0 |
| ✓ | - | 1 (+) 0 |
| ✓ | - | 0 (+) 1 |
| ✗ | - | 1 (+) 1 |

**Frage 10: Welche Aussagen treffen auf einen Pseudo Random Number Generator (PRNG) zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | PRNG wird in Stream Cipher Verfahren eingesetzt |
| ✓ | - | PRNG liefert Sequenzen, welche sich irgendwann wiederholen |
| ✗ | - | Mit AES kann man keinen PRNG realisieren. |

**Frage 11: Welche Parameter müssen der Sender und der Empfänger beim Einsatz von Block Codes miteinander absprechen? (Der Algorithmus sei festgelegt.)**

| Richtige | Deine | Fragetext |
|---|---|---|

| Antwort | Antwort | |
|---|---|---|
| ✓ | - | Blocklänge |
| ✓ | - | Paddingverfahren |
| ✓ | - | Schlüssellänge |
| ✗ | - | Anzahl der zu übertragenden Bits |

**Frage 12: Welche Parameter müssen der Sender und der Empfänger beim Einsatz von Stream Ciphers miteinander absprechen? (Der Algorithmus sei festgelegt.)**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | Blocklänge |
| ✗ | - | Paddingverfahren |
| ✓ | - | Schlüssellänge |
| ✓ | - | Anzahl der zu übertragenden Bits |

**Frage 13: Beim Einsatz von Block Codes im Electronic Codebook (ECB) Modus …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | könnte der Sender die Verschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✓ | - | könnte der Empfänger die Entschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✓ | - | führen gleiche Klartextblöcke immer auf die gleichen Ciphertextblöcke. |
| ✗ | - | müssen sich Sender und Empfänger auf denselben Initialisierungsvektor einigen. |

**Frage 14: Beim Einsatz von Block Codes im Cipherblock Chaining (CBC) Modus …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | könnte der Sender die Verschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✓ | - | könnte der Empfänger die Entschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✗ | - | führen gleiche Klartextblöcke immer auf die gleichen Ciphertextblöcke. |
| ✓ | - | müssen sich Sender und Empfänger auf denselben Initialisierungsvektor einigen. |

**Frage 15: Bei der Verschlüsselung eines langen deutschen Textes (z.B. Ali Baba und die vierzig Räuber) mit AES wird die Häufigkeit der Ciphertext-Bytes untersucht. Welche Aussage trifft zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Die Häufigkeit der Buchstaben ist auch im Chiffrat zu erkennen. |
| ◉ | O | Alle Ciphertext-Bytes treten etwa gleich häufig auf. |

**Frage 16: Bei AES beträgt die Schlüssellänge mindestens …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 56 Bit |
| O | O | 64 Bit |
| O | O | 112 Bit |
| ◉ | O | 128 Bit |
| O | O | 196 Bit |

**Frage 17: Die maximale Entropie einer Zeichenkette bestehend aus zufällig gewählten, mit Wahrscheinlichkeit 1/26 auftretenden Buchstaben beträgt …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | ld(26) |
| ✓ | - | 4.7 Bit |

| | | |
|---|---|---|
| ✓ | - | log(26)/log(2) |
| ✗ | - | ld(1/26) |
| ✗ | - | 5 Bit |

**Frage 18: Bei DES (CBC) wird im Cryptool X.923-Padding verwendet. Der letzte Datenblock des Klartextes enthalte nur die drei Bytes AA BB CC. Welche Aussagen treffen auf das in diesem Fall durchgeführte Padding zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | Der letzte entschlüsselte Datenblock lautet AA BB CC 00 00 00 00 00. |
| ✓ | - | Der effektiv zu verschlüsselnde Datenblock lautet AA BB CC 00 00 00 00 03. |
| ✓ | - | Beim Entschlüsseln wird das Padding wieder entfernt. |
| ✗ | - | Der effektiv zu verschlüsselnde Datenblock lautet AA BB CC 00 00 00 00 00. |

**Frage 19: Welche Kryptoverfahren wurde beim Wired Equivalent Protocol (WEP) für WLAN-Verschlüsselung verwendet?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | AES |
| ◉ | O | RC4 |
| O | O | DES |
| O | O | SEAL |

**Frage 20: Falls beim Cipher Block Chaining (CBC) Verfahren bei der Übertragung ein Bitfehler auftritt …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | … treten in allen folgenden entschlüsselten Datenblöcken Bitfehler auf. |
| O | O | … treten nur im zugehörigen entschlüsselten Datenblock Bitfehler auf. |
| ◉ | O | … treten im zugehörigen entschlüsselten Datenblock und im nächsten Datenblock Bitfehler auf. |

**Frage 21: Falls beim Electronic Codebook (ECB) Verfahren bei der Übertragung ein Bitfehler auftritt …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | … treten in allen folgenden entschlüsselten Datenblöcken Bitfehler auf. |
| ◉ | O | … treten nur im zugehörigen entschlüsselten Datenblock Bitfehler auf. |
| O | O | … treten im zugehörigen entschlüsselten Datenblock und im nächsten Datenblock Bitfehler auf. |

**Frage 22: Wieviele Bytes lang wird das Chiffrat, wenn man einen 5 Byte Klartext Block mit DES verschlüsselt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 5 Bytes |
| ◉ | O | 8 Bytes |
| O | O | 16 Bytes |

**Frage 23: Wieviele Bytes lang wird das Chiffrat, wenn man einen 5 Byte Klartext Block mit AES verschlüsselt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 5 Bytes |
| O | O | 8 Bytes |
| ◉ | O | 16 Bytes |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V07_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V07_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 14:43:21 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 32 |
| **Maximal mögliche Punktezahl:** | 75 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:26:11 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:26:32 |
| **Benötigte Zeit:** | 00:00:21 |
| **Resultat beste Durchführung:** | 0/75 (0%) |

**Frage 1: 33 mod (7) ist gleich**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | 5 |
| O | O | 2 |
| O | O | 3 |
| O | O | 1 |

**Frage 2: Welche Aussagen treffen auf Hybride Verschlüsselungssysteme zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | sind sicherer als symmetrische Verschlüsselungssysteme |
| ✓ | - | werden bei TLS/SSL eingesetzt |
| ✓ | - | arbeiten mit Public Key und Symmetric Key Verfahren |
| ✓ | - | werden bei der SMIME E-Mail-Verschlüsselung eingesetzt |

**Frage 3: Alice schickt Bob eine mittels Public-Key-Verfahren verschlüsselte Nachricht. Welchen Schlüssel muss Bob für die Entschlüsselung verwenden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | seinen Public Key |
| ◉ | O | seinen Private Key |
| O | O | den Public Key von Alice |
| O | O | den Private Key von Alice |

**Frage 4: 33 mod (13) ist gleich**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | 7 |
| O | O | 6 |
| O | O | 20 |
| O | O | 5 |

**Frage 5: Welche Eigenschaften zeichnen symmetrische Verschlüsselungsverfahren gegenüber asymmetrischen Verfahren aus?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | kürzere Schlüssel |
| ✓ | - | einfachere Ver- und Entschlüsselung |
| ✗ | - | kleinere Anzahl geheime Schlüssel bei mehr als 2 Teilnehmern |
| ✗ | - | sind generell sicherer |

**Frage 6: Welchen Teil des Schlüssels muss der Empfänger einer mit einem Public Key Verfahren verschlüsselten Nachricht für die Entschlüsselung verwenden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | den Public Key des Empfängers |
| ◉ | O | den Private Key des Empfängers |
| O | O | den Public und den Private Key des Empfängers |
| O | O | den Public Key des Senders |
| O | O | den Private Key des Senders |

**Frage 7: Welchen Teil des Schlüssels muss der Sender einer Nachricht zur Verschlüsselung mit einem Public Key Verfahren verwenden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | den Public Key des Empfängers |
| O | O | den Private Key des Empfängers |
| O | O | den Private Key des Senders |
| O | O | den Public Key des Senders |

**Frage 8: Welches ist die beste Art zur Gewinnung "echter Zufallszahlen"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Aufruf einer Pseudo-Random Generator Funktion |
| O | O | Verwendung des Resultate von zufälligen Mausbewegungen |
| ◉ | O | Nutzung elektrischer Rauschsignale |
| O | O | Verschlüsselung eines Zeitstempels mit Verwendung eines geheimen Schlüssels |

**Frage 9: Wie viele Primzahlen gibt es?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | endlich viele |
| ◉ | O | unendlich viele |

**Frage 10: Bei welcher Schlüssellänge erzielt RSA eine vergleichbare Sicherheit wie AES-128(bzw. AES mit 128 Bit Schlüssel)?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 128 Bit |
| O | O | 256 Bit |
| ◉ | O | 3072 Bit |
| O | O | 15360 Bit |

**Frage 11: Bei welcher Schlüssellänge erzielt Elliptic Curve Verschlüsselung (EC) eine vergleichbare Sicherheit wie AES-128 (bzw. AES mit 128 Bit Schlüssel)?**

| Richtige | Deine | Fragetext |
|---|---|---|

| Antwort | Antwort | |
|---|---|---|
| O | O | 128 Bit |
| ◉ | O | 256 Bit |
| O | O | 3072 Bit |
| O | O | 15360 Bit |

**Frage 12: Die (multiplikativ) inverse Zahl von 5 mod(7) ist gleich …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 1 |
| O | O | 2 |
| ◉ | O | 3 |
| O | O | 4 |
| O | O | 5 |

**Frage 13: Wie mittlerweile bekannt wurde, heissen die Erfinder des ersten Public Key Verschlüsselungsverfahrens …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Diffie, Hellman |
| O | O | Rivest, Shamir, Adleman |
| ◉ | O | Ellis, Cocks, Williamson |

**Frage 14: Ein Schlüssel habe 512 Bit. Wie vielen möglichen Schlüsseln bzw. Binärkombinationen entspricht das etwa (Angabe als Dezimalzahl) ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 10^512 |
| ◉ | O | 10^154 |
| O | O | 10^50 |
| O | O | 10^1536 |

**Frage 15: Falls die Schlüssellänge von 56 auf 64 Bit erhöht wird, so gibt es …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 8 mal mehr mögliche Schlüssel |
| O | O | 64 mal mehr mögliche Schlüssel |
| ◉ | O | 256 mal mehr mögliche Schlüssel |
| O | O | 512 mal mehr mögliche Schlüssel |

**Frage 16: In einem hybriden Cryptosystem mit n Teilnehmenden benötigt man …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | n geheime asymmetrische Schlüssel |
| O | O | n(n-1)/2 gemeime asymmetrische Schlüssel |
| O | O | n^2 geheime asymmetrische Schlüssel |
| O | O | n(n-1) geheime asymmetrische Schlüssel |

**Frage 17: Um einer Person eine verschlüsselte Meldung schicken zu können, braucht der Sender der Meldung …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | den Public Key des Empfängers |

| | | |
|---|---|---|
| O | O | den Private Key des Empfängers |
| O | O | den Public und den Private Key des Empfängers |
| O | O | den Public Key des Senders der Meldung |

**Frage 18: Welche sind Abkürzungen von Public Key Verfahren?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | AES |
| ✗ | - | RC4 |
| ✗ | - | DES |
| ✓ | - | RSA |
| ✓ | - | ECC |

**Frage 19: Das Produkt der ersten 10 Primzahlen ist …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | gerade |
| O | O | ungerade |

**Frage 20: Welcher Prozentsatz der 128 Zahlen zwischen 128 und 256 sind Primzahlen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | <10% |
| ◉ | O | 10% … <25% |
| O | O | 25% … 50% |
| O | O | >50% |

**Frage 21: Warum ist bei RSA die Verschlüsselung meist schneller als die Entschlüsselung?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Weil die Verschlüsselungsoperation (Verschlüsselungsformel) einfacher aufgebaut ist. |
| ◉ | O | Weil der Exponent bei der Verschlüsselung typischerweise besonders günstig gewählt wird. |
| O | O | Weil die Chiffrate typischerweise länger sind als die Meldungen. |
| O | O | Weil Logarithmieren einfacher ist als Exponentieren. |

**Frage 22: Wie viele verschiedene Kombinationen von drei Zeichen sind möglich, wenn man von einem Alphabeth mit 5 Zeichen auswählen muss? ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 5 |
| O | O | 25 |
| ◉ | O | 125 |
| O | O | 500 |

**Frage 23: Wieviele Dezimalstellen benötigt man etwa, um alle möglichen Dezimalzahlen von Binärzahlen mit 512 Bit darzustellen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 512 |
| O | O | 256 |
| ◉ | O | 154 |
| O | O | 5120 |

**Frage 24: Beim Schlüsselaustausch mit dem Diffie Hellman Verfahren berechnet A den Key K_AB mit der Formel K_AB = DH_B^X mod(p) . Was stellt dabei der Wert "X" dar?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Das ist eine Geheime Zahl, welche A gewählt hat. |
| O | O | Das ist eine Geheime Zahl, welche B gewählt hat. |
| O | O | Das ist der öffentliche Schlüssel von B. |
| O | O | Das ist ein Teil der zu verschlüsselnden Meldung. |

**Frage 25: Beim Schlüsselaustausch mit dem Diffie Hellman Verfahren berechnet A den Key K_AB mit der Formel K_AB = DH_B^X mod(p) . Welche dieser Werte sind öffentlich?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | DH_B |
| ✗ | - | K_AB |
| ✗ | - | X |
| ✓ | - | p |

**Frage 26: Welche Aussage trifft auf den Rechenaufwand zur Faktorisierung einer Zahl zu, welche das Produkt aus zwei etwa ähnlich grossen Primzahlen ist?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Der Aufwand für die Faktorisierung der Zahl ist immer grösser als der Aufwand für die Multiplikation der beiden |
| ◉ | O | Der Aufwand für die Faktorisierung der Zahl steigt bei wachsender Anzahl Stellen der Primzahlen stärker an, a |
| O | O | Der Aufwand für die Faktorisierung der Zahl steigt linear mit der Anzahl Stellen der Zahl. |

**Frage 27: Mit dem Cryptool verschlüsseln Sie ein File mit 256 Bytes Länge mit RSA mit einem 512 Bit Schlüssel. Wie gross wird das verschlüsselte File?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 256 Bytes |
| ◉ | O | 320 Bytes |
| O | O | 512 Bytes |
| O | O | 1024 Bytes |

**Frage 28: Falls bei einem RSA Public Key eine Schlüssellänge von 512 Bit angegeben wird, so heisst das, dass …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | der öffentliche Modulus n 512 Bit lang ist. |
| ✗ | - | der öffentliche Modulus n und der Exponent e zusammen 512 Bit lang sind. |
| ✗ | - | der öffentliche Exponent e 512 Bit lang ist. |
| ✓ | - | dass RSA Blöcke von 512 Bit aufs Mal verschlüsseln kann. |

**Frage 29: In welchen Situationen müssen Sie bei der Ver- und Entschlüssellung mit RSA im Cryptool einen PIN eingeben?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | bei der Entschlüsselung |
| O | O | Bei der Verschlüssellung |
| O | O | bei der Entschlüsselung und bei der Verschlüsselung |

**Frage 30: Welcher dieser Primzahltests ist ein deterministischer Primzahltest?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|

| | | |
|---|---|---|
| O | O | Miller-Rabin |
| O | O | Solavay-Strassen |
| O | O | Ferman |
| ◉ | O | Agrawal-Kayal-Saxena (AKS) |

**Frage 31: Wie viel länger dauert die Verschlüsselung, wenn man die Länge des zu verschlüsselnden Files verdoppelt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Die Verschlüsselungszeit ändert sich nicht. |
| ◉ | O | Die Verschlüsselungszeit wird auch etwa doppelt so gross.. |
| O | O | Die Verschlüsselungszeit wird wesentlich mehr als doppelt so gross. |
| O | O | Das kann man nicht sagen, das hängt von der Schlüssellänge ab. |

**Frage 32: Ein File werde mit einem 512 Bit Schlüssel verschlüsselt. Wie verändert sich die Verschlüsselungszeit, wenn man das selbe File mit einem 1024 Bit Schlüssel verschlüsselt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Die Verschlüsselungszeit ändert sich nicht. |
| ◉ | O | Die Verschlüsselungszeit wird rund 50% grösser… |
| O | O | Die Verschlüsselungszeit wird etwa doppelt so gross. |
| O | O | Die Verschlüsselungszeit wird wesentlich mehr als doppelt so gross. |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V08_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V08_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 14:46:18 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 17 |
| **Maximal mögliche Punktezahl:** | 46 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:26:51 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:26:53 |
| **Benötigte Zeit:** | 00:00:02 |
| **Resultat beste Durchführung:** | 0/46 (0%) |

**Frage 1: Geben Sie an, welches Abkürzungen von Hashverfahren sind.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | MD5 |
| ✓ | - | SHA |
| ✗ | - | RSA |
| ✗ | - | DH |
| ✓ | - | RIPEMD |

**Frage 2: Ist es möglich, dass unterschiedliche Nachrichten gleiche Hashes ergeben?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Ja |
| O | O | Nein |

**Frage 3: Mit welchem Begriff beschreibt man die Hash-Eigenschaft, dass es nicht effizient möglich sein darf, zwei Meldungen m_x und m_y mit demselben Hash-Wert h=H(m_x)=H(m_y) zu finden.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Preimage-Resistenz |
| ◉ | O | Kollisionsfreiheit |
| O | O | Nicht-Umkehrbarkeit |

**Frage 4: Mit welchem Begriff beschreibt man die Hash-Eigenschaft, dass zu einer vorgegebenen Meldung m_i keine andere Meldung m_j mit gleichem Hash-Wert gefunden werden darf.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Preimage-Resistenz |
| O | O | Kollisionsfreiheit |
| O | O | Nicht-Umkehrbarkeit |

**Frage 5: Sie erhalten eine signierte Nachricht, welche an mehrere Personen gerichtet ist. Sie möchten allen antworten. Welche Aussage trifft zu?**

| Richtige | Deine | Fragetext |
|---|---|---|

| Antwort | Antwort | |
|---|---|---|
| ✓ | - | Ich kann problemlos allen mit einer ebenfalls signierten Mail antworten. |
| ✗ | - | Ich kann problemlos allen mit einer verschlüsselten Mail antworten. |
| ✓ | - | Ich kann problemlos dem Absender der Mail mit einer verschlüsselten Mail antworten. |
| ✓ | - | Ich kann nur denjenigen Personen verschlüsselt antworten, deren Zertifikat ich bereits habe. |

**Frage 6: Um einer Person eine signierte Meldung schicken zu können, brauche ich ....**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | den Public Key dieser Person |
| O | O | den Private Key dieser Person |
| O | O | meinen Public Key |
| ◉ | O | meinen Private Key |

**Frage 7: Susanne hat ein Dokument digital signiert. Geben Sie an, mit welchem Schlüssel man die Signatur von Susanne überprüfen kann.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | mit dem Public Key von Susanne |
| O | O | mit dem Private Key von Susanne |

**Frage 8: Was versteht man unter einer "Rainbow Table"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Vorberechnete Tabelle, in denen Passwörter und deren Hashes abgelegt sind |
| O | O | Tabelle die alle aktuellen Hashverfahren beinhaltet |
| O | O | Eine Tabelle von Hashes, die besonders leicht zurückrechenbar sind |
| O | O | Eine Tabelle mit Passwörtern, die genau die gleiche Zeichenfolge wie deren Hashes haben |

**Frage 9: Was versteht man unter einer Kollision bei Hashes?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Dass man mehrere Meldungen gefunden hat, welche auf den selben Hash abgebildet werden. |
| O | O | Dass die Hash-Funktion Fehler aufweist. |
| O | O | Dass der Hash nicht immer mit dem selben Algorithmus berechnet wird. |
| O | O | Dass Umlaute nicht korrekt gehasht werden. |

**Frage 10: Welche Aussagen treffen auf den Meldungsaustausch mittels "Keyed Hash" Verfahren zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Sender und/oder Empfänger können davon ausgehen, dass Dritte die Meldung nicht verändern konnten. |
| ✗ | - | Mit der Angabe des Keyed Hash zu einer Meldung, kann B beweisen, dass die Meldung von A so erstellt wurde. |
| ✓ | - | Der Empfänger kann die Echtheit der Meldung nur überprüfen, wenn er den geheimen Schlüssel kennt. |

**Frage 11: Welche Aussagen treffen auf die Integritätsprüfung durch den Empfänger einer Meldung mittels "Digitaler Signatur" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Sender und/oder Empfänger können davon ausgehen, dass Dritte die Meldung nicht verändern konnten. |
| ✗ | - | Der Sender kann die Meldung verändern, ohne die Signatur zu verändern. |
| ✗ | - | Der Empfänger kann die Echtheit der Meldung nur überprüfen, wenn er einen geheimen Schlüssel kennt. |
| ✓ | - | Der Empfänger kann die Echtheit der Meldung überprüfen, wenn er den Public Key des Signierers hat. |

**Frage 12: Welche Aussagen treffen beim Password-Hashing auf das Hashverfahren zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Das Hashing Verfahren soll möglichst schnell sein. |
| ⊙ | O | Das Hashing Verfahren soll eher langsam sein. |
| O | O | Das Hashing Verfahren darf nicht bekannt sein. |

**Frage 13: Welche Hashverfahren sollten gemäss US CERT nicht mehr verwendet werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | MD5 |
| ✓ | - | SHA-1 |
| ✗ | - | MD6 |
| ✗ | - | RIPEMD-160 |

**Frage 14: Wie viele verschiedene Meldungsmöglichkeiten gibt es für einen SHA-1-Hash von 160 Bit?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 2^(2^16 -1) |
| O | O | 2^64 - 1 |
| O | O | 2^160 |
| ⊙ | O | unendlich viele |

**Frage 15: Wie viele verschiedene Hashes sind bei SHA-1 mit 160 Bit Hashlänge maximal möglich?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 2^(2^16 -1) |
| O | O | 2^64 - 1 |
| ⊙ | O | 2^160 |
| O | O | unendlich viele |

**Frage 16: Welcher Anteil von allen möglichen Meldungen von 1060 Bit Länge führt auf gleiche SHA-1 160 Bit Hashes?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | O | 2^(-900) |
| O | O | 2^(-160) |
| O | O | 2^(-1060) |
| O | O | 2^(-1220) |

**Frage 17: Bei einem System wurden im "Passwort File" salted MD5 Hashes abgespeichert. Der Salt ist s-Bit lang. Ein Angreifer kommt in den Besitz des "Passwort Files", d.h. von Username, Salt und Hash für jeden User. Welche Aussagen treffen zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Einfache (kurze) Passwörter kann der Angreifer mittels Brute Force Attacke finden. |
| ✓ | - | Gleiche Passwörter haben in der Regel unterschiedliche Hashes. |
| ✗ | - | Anhand der Hashes sollte man die Passwörter über eine Rainbow Tabelle finden können. |
| ✗ | - | Der Aufwand für eine Brute Force Attacke auf eines der Passwörter ist 2^s mal grösser als wenn kein Salt verwe |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V09_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V09_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 31. July 2017 10:00:29 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 23 |
| **Maximal mögliche Punktezahl:** | 61 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 10. August 2017 16:27:07 |
| **Endzeitpunkt Teilnahme:** | 10. August 2017 16:27:10 |
| **Benötigte Zeit:** | 00:00:03 |
| **Resultat beste Durchführung:** | 0/61 (0%) |

**Frage 1: Bei welcher Organisation wurden die Public Key Cryptography Standards (PKCS) entwickelt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | RSA |
| O | O | Symantec |
| O | O | ISO |
| O | O | IEEE |

**Frage 2: Welche Aussagen treffen auf einen "Extended Validation Zertifikate" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | werden vor allem von Finanzinstituten verwendet |
| ✗ | - | liefern höhere Sicherheit bei der Verschlüsselung |
| ✓ | - | werden in den meisten Browsern speziell angezeigt |
| ✗ | - | können nur von Comodo bezogen werden |

**Frage 3: Welche Aussagen treffen für einen PKCS#12 "Transport Container" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Kann alle Zertifikate der Certificate Chain enthalten. |
| ✗ | - | Kann keinen Private Key enthalten. |
| ✗ | - | Besteht aus druckbaren ASCII-Characters. |
| ✓ | - | Kann mehrere Zertifikate enthalten. |

**Frage 4: Welche Signatur ist der handschriftlichen Signatur rechtlich gleichgestellt (im Rahmen des Schweizer Signaturgesetztes)?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | digitale Signatur |
| O | O | elektronische Signatur |
| O | O | fortgeschrittene elektronische Signatur |
| ◉ | O | qualifizierte elektronische Signatur |

**Frage 5: Welche "Certificate Validation" Art ist bei Webserver Zertifikaten am weitesten verbreitet?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Domain Validation |
| O | O | Organisation Validation |
| O | O | Extended Validation |

**Frage 6: Der zum Zertifikat im Browser angezeigte Fingerprint ist immer derjenige Hash, welcher signiert wird.**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Richtig |
| ◉ | O | Falsch |

**Frage 7: Mit welchem Zertifikatetyp kann man Domainnamen aus unterschiedlichen Domains abdecken?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Wild Card Certificate |
| O | O | Extended Validation Certificate |
| ◉ | O | Unified Communication Certificate |
| O | O | Domain Validated Certificate |

**Frage 8: Welche Aussagen treffen auf "Root Zertifikate" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | sind self-signed |
| ✓ | - | haben in der Regel eine längere Gültigkeitsdauer |
| ✗ | - | werden vor allem bei bekannten Webservern eingesetzt |
| ✗ | - | enthalten immer RSA-Schlüssel |

**Frage 9: Welche Organisation wurde in der Schweiz dafür akkreditiert, Zertifikate-Diensteanbieter anzuerkennen?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Verisign |
| ◉ | O | KPMG |
| O | O | SwissSign |
| O | O | Swisscom |

**Frage 10: Was sind die beiden Hauptaufgaben einer Certificate Authority?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Überprüfung der Echtheit des Besitzers eines Public Keys |
| ✓ | - | Signierung und Aushändigung des Zertifikats |
| ✗ | - | Registrierung der Herausgeber von Zertifikaten |
| ✗ | - | Akkreditierung von Zertifikate-Herausgebern |

**Frage 11: Die EU-Richtlinien bzw. das Schweizer Signaturgesetz bezeichnen die Informationen, welche unten an die Email-Zeilen angefügt werden als . . .**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | elektronische Signatur |
| O | O | fortgeschrittene elektronische Signatur |
| O | O | qualifizierte elektronische Signatur |

**Frage 12: Für "Code Signing" benötigt der Ersteller des Codes von öffentlichen Anwendungen . . .**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | unterschiedliche Zertifikate für Java Applets und AktiveX Komponenten. |
| ◉ | O | bei jeder Signierung des Codes ein gültiges, von einer offiziellen Zertificate Authority aufgestelltes Zertifikat. |
| O | O | bei jeder neuen Version seines Codes ein neues Zertifikat. |
| O | O | eine private Certificate Authority, welche Self Signed Zertifikate ausgeben kann. |

**Frage 13: Falls man von einer CA ein signiertes Zertifikat für seinen Webserver beschaffen will, welches vonden meisten Browsern bekannt ist, . . .**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | so muss man mit Kosten von mehreren 100 Fr. pro Jahr rechnen. |
| O | O | so muss man dazu zu einem Notar gehen. |
| ◉ | O | so kann man dies in wenigen Minuten bewerkstelligen, wenn man die Rechte für die Domain oder Webserverac |

**Frage 14: Im Browser wird der Anfang des öffentlichen Schlüssels so angegeben: "30 48 02 41 00 fe 1b 84 35. . .". Im Cryptool jedoch fängt der öffentliche Schlüssel so an: "fe 1b 84 35. . . ". Was ist der Grund für diesen Unterschied?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Das Cryptool zeigt das Zertifikat im .crt Format an, der Browser im .pem Format. |
| ◉ | O | Das Cryptool zeigt die interpretierten Daten des Zertifikats an, der Browser zeigt hier die DER-codierten Daten a |
| O | O | Das sind zwei unterschiedliche öffentliche Schlüssel. |
| O | O | Das Cryptool verwendet einen anderes Padding. |

**Frage 15: Welche Aussagen treffen auf den zum Serverzertifikat angezeigten "Fingerprint" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Diese Daten nennt man auch Message Digest. |
| ✗ | - | Das ist der Hash über den Public Exponenten des RSA Schlüssels. |
| ✓ | - | Das ist ein Hashwert, welcher von Browsern für Server Zertifikate angezeigt wird. |
| ✗ | - | Das ist der von der CA signierte Hashwert. |

**Frage 16: Die Certificate Revocation Liste wird ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | . . . bei jedem https-Aufruf abgefragt. |
| ◉ | O | . . . vom der Zertifizierungsstelle unterhalten. |
| O | O | . . . immer jeweils mit den Browser Updates aktualisiert. |

**Frage 17: Welche Aussagen treffen auf "Certificate Classes" zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Sie liefern eine Aussage über die Güte der Überprüfung der Inhaber von Zertifikaten. |
| O | O | Sie liefern eine Aussage über die Güte der Überprüfung der Herausgeber von Zertifikaten. |
| O | O | Sie sind Standardisiert und haben bei allen Zertifikatsanbietern die genau gleiche Bedeutung. |
| O | O | Für jede Certificate Class zeigen Browser die Zertifikate unterschiedlich an. |

**Frage 18: Welche Aussagen treffen auf Let's Encrypt Zertifikate zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | Let's Encrypt Zertifikate haben bei den bekanntesten (Alexa Top 100) Webservern den grössten Marktanteil. |

| | | |
|---|---|---|
| ✓ | - | Let's Encrypt Zertifikate sind kostenlos. |
| ✗ | - | Let's Encrypt Zertifikate werden von Google herausgegeben. |
| ✓ | - | Let's Encrypt Zertifikate sind "Domain validated" Zertifikate. |

**Frage 19: Welche Informationen zu Zertifikaten gleicht man bei "Key Exchange Parties" ab?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Zertificate Fingerprint |
| O | O | Zertificate Public Key |
| O | O | Zertificate Signatur |

**Frage 20: Welche Aussagen treffen auf das Pretty Good Privacy (PGP) Verschlüsselungssystem zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | War eines der ersten im Privatbereich genutzten Public Key Systeme. |
| ✓ | - | Wurde von Phil Zimmermann entwickelt. |
| ✓ | - | Bot "starke Verschüsselung" an. |
| ✗ | - | Ist heute das meist genutzte Verschlüsselungsverfahren. |

**Frage 21: Welche Aussagen treffen auf das Certificate PKCS7 Format zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | - | Ein Zertifikat im PKCS7-Format enthält auch den private Key. |
| ✓ | - | Ein Zertifikat im PKCS7-Format kann auch die Zertifikate der Certificate Chain enthalten. |
| ✓ | - | Ein Zertifikat im PKCS7-Format kann einfach in den Zertificate Store importiert werden. |

**Frage 22: Wenn man ein Zertifikat im DER-Format ins PEM-Format umwandelt, …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | . . . wird es grösser (enthält mehr Bytes). |
| O | O | . . . werden alle Zertifikate der Certificate Chain angefügt. |
| O | O | . . . wird der Secret Key angefügt. |

**Frage 23: Der X.509 Standard …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | . . . ist ein ITU-T Standard |
| O | O | . . . ist ein IETF Standard |
| O | O | . . . ist ein ISO Standard |

# Ihr Ergebnis der Lernkontrolle: InfSi1_V10_2017

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V10_2017 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 02. August 2017 08:37:36 |
| **Endzeitpunkt:** | keine zeitliche Begrenzung |
| **Anzahl Fragen:** | 27 |
| **Maximal mögliche Punktezahl:** | 70 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Matthias Baumann (matthias.baumann@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 09. August 2017 18:01:53 |
| **Endzeitpunkt Teilnahme:** | 01. January 1970 01:00:00 |
| **Benötigte Zeit:** | 07:58:07 |
| **Resultat beste Durchführung:** | 28/70 (40%) |

**Frage 1: Bei TLS/SSL verwendete Webserver Zertifikate sollten ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | einen MD5-Hash enthalten. |
| ◉ | O | Von einer Trusted Certificate Authority ausgegeben sein. |
| O | O | Self-signed sein |
| O | O | Neben dem Servernamen auch die IP-Adresse des Servers enthalten. |

**Frage 2: Es gibt unter anderem die TLS Cipher Suite Beschreibung TLS_DHE_DSS_WITH_DES_CBC_SHA. Welches der aufgeführten Verfahren stellt die Echtheit des Servers sicher?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | DSS |
| O | O | DHE |
| O | O | DES |
| O | O | SHE |

**Frage 3: Was bedeutet beim OpenSSL-Befehl "openssl genrsa -des3 -out keyname.pem 512" der Parameter "des3"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Dass der Private Key mit 3DES verschlüsselt wird. |
| O | O | Dass nach dem Schlüsselaustausch mit 3DES verschlüsselt werden soll. |
| O | O | Dass ein 3DES Public Key generiert wird. |
| O | O | Dass die Sicherheit des Public Key etwa 3DES entspricht. |

**Frage 4: Wie viele Cipher Suites bietet ein Browser im TLS Client Hello so typisch an?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 1 |
| ◉ | O | 6 bis 25 |
| O | O | 2 bis 5 |
| O | O | mehr als 25 |

**Frage 5: Wie viele zusätzliche RTT sind für den Aufbau einer TLS/SSL-Verbindung ohne Session Resume nötig, bevor die eigentliche Datenübertragung stattfinden kann?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 0 |
| O | O | 1 |
| ◉ | O | 2 |
| O | O | 3 |

**Frage 6: Welche Aussagen treffen zu, wenn TLS Session Resume verwendet wurde?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Im Client Hello ist eine Session ID enthalten. |
| ✗ | - | Im Server Hello muss das Server Zertifikat gesendet werden. |
| ✓ | - | Der Client hatte schon früher einmal eine TLS-Verbindung zum Server eröffnet. |
| ✗ | - | Vor der Verschlüsselung müssen die Daten komprimiert werden. |

**Frage 7: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Data Link bzw. MAC Schicht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | WPA |
| O | O | IPsec |
| O | O | TLS/SSL |
| O | O | SMIME |

**Frage 8: Welches Verschlüsselungsverfahren arbeitet auf der Anwendungsschicht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | WPA |
| O | O | IPsec |
| O | O | TLS/SSL |
| ◉ | O | SMIME |

**Frage 9: Bei der Zeitdarstellung im Browser (Expert Mode) sieht man die für TLS/SSL-Verwendete Zeitdauer. Beim ersten Aufruf einer Webseite beobachtet man Werte von 200ms bis 700ms. Beim Reload der Seite sind es nur noch etwa 50ms. Was ist der wahrscheinlichste Grund dafür?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Beim zweiten Aufruf konnte "Session Resume" gemacht werden. |
| O | O | Beim zweiten Aufruf kam die Seite aus dem Browser Cache. |
| O | O | Beim zweiten Aufruf war keine DNS-Auflösung mehr nötig. |
| O | O | Beim zweien Aufruf wurde ein schnellerer Verschlüsselungalgorithmus verwendet. |

**Frage 10: Perfect Forward Secrecy (PFS) …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | … verwendet typisch Diffie-Hellman und/oder elliptische Kurven für den Schlüsselaustausch. |
| ✓ | - | … wird 2017 von mehr als 80% der Websites unterstützt. |
| ✓ | - | … verhindert, dass aufgezeichnete verschlüsselte Verbindungen mit komprimittierten Public Keys entschlüsselt |
| ✗ | - | … erfordert eine verschlüsselte Übertragung der Sessionkeys. |

**Frage 11: Wieso werden beim Qualis Test die Cipher Suites mit SHA nicht als WEAK klassiert?**

| Richtige | Deine | Fragetext |
|---|---|---|

| Antwort | Antwort | |
|---|---|---|
| ◉ | O | Dieser SHA betrifft das Hashing der Meldungen nicht die Signatur von Zertifikaten. |
| O | O | Mit SHA ist hier SHA256 gemeint und dieses Hashing Verfahren gilt noch als genügend sicher. |
| O | O | Qualis lässt SHA1 vorerst noch zu. Erst ab Mitte 2017 wird SHA als unsicher klassiert. |

**Frage 12: Wieso gilt beim Qualis Test die TLS_RSA_WITH_RC4_128_MD5 Cipher Suite als INSECURE?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | - | Gemäss OWASP soll RC4 nicht mehr verwendet werden. |
| ✓ | - | Gemäss OWASP soll MD5 nicht mehr für Message Hashing verwendet werden. |
| ✗ | - | RSA gilt als unsicher. |
| ✗ | - | Stream Cipher gelten generell als insecure. |

**Frage 13: Wie wird bei TLS die Integrität der übertragenen Daten sichergestellt?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Mit einem Keyed Message Authentication Code |
| O | O | Mit einer digitalen Signatur der Datenpakete |
| O | O | Mittels Client Zertificate |
| O | O | Durch symmetrische Verschlüsselung |

**Frage 14: HTTP Strict Transport Security (HSTS) …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | … verbessert den Schutz gegen Man-in-the-Middle Attacks. |
| ✗ | ✓ | … wird 2016 bereits von mehr als 50% der Websites unterstützt. |
| ✓ | ✗ | … kann eine Preloaded Server Liste im Browser nutzen. |
| ✓ | ✓ | … kann über HTTP-Header Felder aktiviert werden. |

**Frage 15: Welche Aussagen treffen auf das Padding beim TLS Record Body zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Padding ist nötig, wenn Block Ciphers verwendet werden. |
| ✗ | ✗ | Padding ist nötig, um die Anpassung an den RSA-Modulus sicherzustellen. |
| ✓ | ✓ | Padding kann gemäss Standard maximal 255 Bytes lang sein. |
| ✗ | ✗ | Padding wird unverschlüsselt übertragen. |

**Frage 16: Wieso gilt beim Qualis Test die TLS_RSA_WITH_3DES_EDE_CBC_SHA Cipher Suite als WEAK?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Gemäss OWASP soll DES nicht mehr verwendet werden. |
| O | O | Die 3DES Schlüssellänge gilt heutzutage als zu klein, um Brute Force Angriffen stand zu halten. |
| O | O | Der Cipher Block Chaining Mode gilt als unsicher. |
| O | O | RSA gilt als unsicher. |

**Frage 17: Erfolgreiche Angriffe auf Zertifikateherausgeber …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | sind bisher keine vorgekommen. |
| O | O | sind erst einmal vorgekommen. |
| ◉ | ◉ | sind schon mehrmals vorgekommen. |

**Frage 18: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Netzwerk Schicht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | WPA |
| ◉ | ◉ | IPsec |
| O | O | TLS/SSL |
| O | O | SMIME |

**Frage 19: Wer bestimmt, ob ein Session Resume gemacht werden soll?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | ◉ | Nur der Client |
| O | O | Nur der Server |
| ◉ | O | Client und Server |

**Frage 20: Welche Cipher Suites bieten Perfect Forward Secrecy?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | TLS_RSA_WITH_RC4_128_SHA |
| ✗ | ✗ | TLS_RSA_WITH_AES_256_CBC_SHA256 |
| ✓ | ✓ | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA□ |
| ✓ | ✗ | TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA |

**Frage 21: Welche Antwort geben Sie 2017, wenn jemand sagt: "Wir wollen kein TLS/SSL verwenden, weil dies unsere Anwendungen langsam macht."**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Diese Aussage gilt 2017 nicht mehr. Richtig implementierte TLS/SSL Anwendungen haben keine Geschwindigk |
| ✗ | ✗ | Ja, Geschwindigkeit auch 2017 immer noch ist ein Problem von TLS/SSL, man muss spezielle Hardware Modul |
| ✓ | ✓ | Durch die Verwendung von HTTP/2 kann man mit verschlüsselten Verbindungen sogar schneller werden als m |

**Frage 22: Welche Information muss beim TLS Session Resume nicht übertragen werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | SessionID |
| O | O | ClientHello.random (Challenge) |
| O | O | ClientCipherListOffer |
| ◉ | ◉ | Server Certificate |

**Frage 23: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Transport Schicht?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | WPA |
| O | O | Ipsec |
| ◉ | ◉ | TLS/SSL |
| O | O | SMIME |

**Frage 24: Wenn HTTP Strict Transport Security (HSTS) verwendet wird …**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | … kann man beim Browser TLS Alarmmeldungen nicht einfach wegklicken. |
| ✓ | ✓ | … spart man HTTP Redirects, wenn man nur noch HTTPS-Verbindungen zulassen will. |
| ✓ | ✓ | … ist man auch auf die Unterstützung/Mitarbeit vom Browser angewiesen. |

**Frage 25: Welche Aussagen zu TLS treffen zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | TLS verwendet meistens auch Datenkompression. |
| ✓ | ✓ | Gegenwärtig (2016) ist TLS1.3 die aktuellste TLS-Version. |
| ✓ | ✓ | TLS basiert auf Sicherheitslösungen der Firma Netscape. |
| ✗ | ✗ | TLS wurde von der ISO standardisiert. |

**Frage 26: Wie viele zusätzliche RTT sind für den Aufbau einer TLS/SSL-Verbindung mit Session Resume und TLS False Start nötig, bevor die eigentliche Datenübertragung stattfinden kann?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 0 |
| ◉ | ◉ | 1 |
| O | O | 2 |
| O | O | 3 |

**Frage 27: Welche Seite entscheidet bei TLS Verbindungen, mit welchem Verschlüsselungsverfahren gearbeitet werden soll?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Client |
| ◉ | ◉ | Server |