DLMIMWCK01\_Lektion01\_Frage01

Welche Beschreibung umfasst alle Taten der Computerkriminalität?

* alle Taten, welche sich gegen Computer richten oder Computer als Werkzeug nutzen (1 Pts)
* nur die Taten, welche sich gegen Computer richten (0 Pts)
* nur die Taten, welche Computer als Werkzeug nutzen (0 Pts)
* alle Taten, welche sich gegen Computer richten und das Internet als Werkzeug nutzen (0 Pts)

DLMIMWCK01\_Lektion01\_Frage02

Welches Ziel verfolgt Ransomware?

* Ransomware stört Datenverarbeitungsprozesse und versucht, ein Lösegeld zu erpressen. (1 Pts)
* Ransomware hat das Ziel, sich unbemerkt zu verbreiten. (0 Pts)
* Ransomware zeigt dem Opfer aufdringliche Werbung. (0 Pts)
* Ransomware hat das Ziel, den Computer des Opfers für weitere Angriffe zu nutzen. (0 Pts)

DLMIMWCK01\_Lektion01\_Frage03

Welche der folgenden Schwachstellen befindet sich auf der Organisationsebene?

* fehlendes Vier-Augen-Prinzip (1 Pts)
* fehlende Softwareupdates (0 Pts)
* Netzwerk ohne Firewall (0 Pts)
* Stammdatensystem ohne Authentifizierung (0 Pts)

DLMIMWCK01\_Lektion01\_Frage04

Welche Art Schwachstelle nutzen Social Engineering-Angriffe per Definition aus?

* menschliche Schwachstelle (1 Pts)
* technische Schwachstelle (0 Pts)
* infrastrukturelle Schwachstelle (0 Pts)
* Schwachstelle auf Managementebene (0 Pts)

DLMIMWCK01\_Lektion01\_Frage05

Welche der folgenden Angriffe zielt dem Namen nach auf das Passwort des Opfers ab?

* Phishing (1 Pts)
* Dumpster Diving (0 Pts)
* Baiting (0 Pts)
* Whaling (0 Pts)

DLMIMWCK01\_Lektion02\_Frage01

Welche der folgenden Paragrafen kann auf Identitätsmissbrauch angewendet werden?

* § 202a StGB (1 Pts)
* § 142 PatG (0 Pts)
* § 153 StGB (0 Pts)
* § 146 StGB (0 Pts)

DLMIMWCK01\_Lektion02\_Frage02

Welches der folgenden Gesetze ist Hauptbestandteil des Immaterialgüterrechts?

* Gebrauchsmustergesetz (1 Pts)
* Gesetz gegen unlauteren Wettbewerb (0 Pts)
* Telekommunikationsgesetz (0 Pts)
* Datenschutz-Grundverordnung (0 Pts)

DLMIMWCK01\_Lektion02\_Frage03

Als Reaktion auf die Nicht-Anwendbarkeit welches Deliktes wurde § 269 StGB eingeführt?

* Urkundenfälschung (1 Pts)
* Betrug (0 Pts)
* Geldfälschung (0 Pts)
* Beleidigung (0 Pts)

DLMIMWCK01\_Lektion02\_Frage04

Welche der folgenden Handlungen ist nicht die Voraussetzung für § 263a StGB (Computerbetrug)?

* unbefugte Ausführung eines Programms (1 Pts)
* unbefugte Verwendung von Daten (0 Pts)
* unrichtige Gestaltung eines Programms (0 Pts)
* Verwendung unrichtiger oder unvollständiger Daten (0 Pts)

DLMIMWCK01\_Lektion02\_Frage05

Welcher der folgenden Paragrafen ist nicht auf den Diebstahl und Missbrauch von Zugangsdaten zu einem Onlinekonto mithilfe eines Virus anwendbar?

* § 185 StGB (1 Pts)
* § 269 StGB (0 Pts)
* § 202a StGB (0 Pts)
* § 263a StGB (0 Pts)

DLMIMWCK01\_Lektion03\_Frage01

Welche der folgenden technischen Entwicklungen begünstigt Datendiebstahl nicht?

* Multi-Faktor-Authentifizierung (1 Pts)
* Mobile Geräte (0 Pts)
* Internet-of-Things (0 Pts)
* Soziale Netzwerke (0 Pts)

DLMIMWCK01\_Lektion03\_Frage02

Welche der folgenden Eigenschaften eines Back-ups verstärkt die Folgen eines Ransomware-Angriffs?

* online (1 Pts)
* vollständig (0 Pts)
* aktuell (0 Pts)
* offline (0 Pts)

DLMIMWCK01\_Lektion03\_Frage03

Welche Aussage trifft nicht auf einen DDoS-Angriff zu?

* Für DDoS-Angriffe werden Zugangsdaten zum Zielsystem benötigt. (1 Pts)
* DDoS-Angriffe erzeugen eine Überlast auf dem Zielsystem. (0 Pts)
* DDoS-Angriffe werden von einer Vielzahl von Computern gestartet. (0 Pts)
* DDoS-Angriffe nutzen häufig Botnetze. (0 Pts)

DLMIMWCK01\_Lektion03\_Frage04

Welcher der folgenden Begriffe ist ein Synonym für Industriespionage?

* Betriebsspionage (1 Pts)
* Wirtschaftsspionage (0 Pts)
* Competitive Intelligence (0 Pts)
* aggressive Marktforschung (0 Pts)

DLMIMWCK01\_Lektion03\_Frage05

Gegen welche Art Schadsoftware hilft ein Decryptor?

* Ransomware (1 Pts)
* Adware (0 Pts)
* AES-256 (0 Pts)
* SMB (0 Pts)

DLMIMWCK01\_Lektion04\_Frage01

Welcher der folgenden Begriffe ist kein Seiteneffekt, welcher für einen Seitenkanalangriff genutzt werden kann?

* Prozessliste (1 Pts)
* Zeitmessung (0 Pts)
* elektromagnetische Wellen (0 Pts)
* Stromverbrauch (0 Pts)

DLMIMWCK01\_Lektion04\_Frage02

Was ist ein grundlegender Abwehrmechanismus von Betriebssystemen gegen Angriffe?

* Rechtetrennung (1 Pts)
* Out-of-Order-Execution (0 Pts)
* Multithreading (0 Pts)
* SMB (0 Pts)

DLMIMWCK01\_Lektion04\_Frage03

Welche Eigenschaft eines Dienstes schränkt einen DoS-Angriff ein?

* Verfügbarkeit (1 Pts)
* Vertraulichkeit (0 Pts)
* Integrität (0 Pts)
* Authentizität (0 Pts)

DLMIMWCK01\_Lektion04\_Frage04

Welches Protokoll wird üblicherweise auf dem TCP-Port 443 genutzt?

* HTTPS (1 Pts)
* DNS (0 Pts)
* VoIP (0 Pts)
* POP3 (0 Pts)

DLMIMWCK01\_Lektion04\_Frage05

Was ist keine organisatorische Regelung?

* Log-Eintrag (1 Pts)
* Rollenverteilung (0 Pts)
* Aufbauorganisation (0 Pts)
* Prozessbeschreibungen (0 Pts)

DLMIMWCK01\_Lektion05\_Frage01

Wie entsteht ein Polymorphismus?

* Umordnung von Funktionen (1 Pts)
* Befall eines neuen Systems (0 Pts)
* Callback an den Command & Control-Server (0 Pts)
* Abfangen von Passwörtern (0 Pts)

DLMIMWCK01\_Lektion05\_Frage02

Was ist kein Verfahren zur Detektion von Schadsoftware?

* Dateisystemstruktur-basierte Detektion (1 Pts)
* Signatur-basierte Detektion (0 Pts)
* Verhaltens-basierte Detektion (0 Pts)
* Heuristik-basierte Detektion (0 Pts)

DLMIMWCK01\_Lektion05\_Frage03

Welche Daten können während einer Post-mortem-Analyse genutzt werden?

* Dateisystemstruktur (1 Pts)
* Arbeitsspeicher (0 Pts)
* Prozessliste (0 Pts)
* Liste der aktiven Netzwerkverbindungen (0 Pts)

DLMIMWCK01\_Lektion05\_Frage04

Welche Technik wird angewandt, wenn die Dateisystemstruktur eines Datenträgers zerstört ist?

* File carving (1 Pts)
* Tcpdump (0 Pts)
* NTFS-Reload (0 Pts)
* Fragmented binary (0 Pts)

DLMIMWCK01\_Lektion05\_Frage05

Welches Verfahren oder welche Anwendung hilft bei einem wipe out?

* Wiederherstellung des Back-ups (1 Pts)
* Einsatz eines Decryptors (0 Pts)
* File carving (0 Pts)
* Wiederherstellen des Papierkorbs (0 Pts)

DLMIMWCK01\_Lektion06\_Frage01

Was bedeutet die Abkürzung ISMS?

* Informationssicherheitsmanagementsystem (1 Pts)
* Informationsschutzmanagementsystem (0 Pts)
* IT Security Monitoring System (0 Pts)
* Information and Safety Management Service (0 Pts)

DLMIMWCK01\_Lektion06\_Frage02

Welchen Nutzen erzeugt ein TPM nicht?

* Schutz vor Diebstahl (1 Pts)
* Speicherung von kryptografischen Schlüsseln (0 Pts)
* Beginn einer Vertrauenskette (0 Pts)
* Verwaltung von kryptografischen Schlüsseln (0 Pts)

DLMIMWCK01\_Lektion06\_Frage03

Welchen Prozess sichert eine MFA ab?

* Authentifizierung (1 Pts)
* Autorisierung (0 Pts)
* Vergabe von Zugangsberechtigungen (0 Pts)
* Zutrittskontrolle (0 Pts)

DLMIMWCK01\_Lektion06\_Frage04

Was ist das Hauptziel von Sensibilisierungsmaßnahmen?

* Schaffen von Awareness (1 Pts)
* Etablierung von SSO (0 Pts)
* Intrusion Detection (0 Pts)
* Einführung von Security Incident Handling (0 Pts)

DLMIMWCK01\_Lektion06\_Frage05

Welcher Prozess hängt nicht direkt mit der Vorfallreaktionsplanung zusammen?

* Change Management (1 Pts)
* Notfallmanagement (0 Pts)
* IT-Forensik (0 Pts)
* Planung der Behandlung von Sicherheitsvorfällen (0 Pts)

DLMIMWCK01\_Lektion07\_Frage01

Welche der folgenden Maßnahmen wird als reaktive Maßnahme kategorisiert?

* Deaktivieren aller Administratorkonten nach einem Schadsoftwarebefall (1 Pts)
* Aktualisierung der Anti-Viren-Muster (0 Pts)
* Beauftragung eines Beraters, um ein ISMS aufzubauen (0 Pts)
* Aktivierung der Protokollierung auf einem Domain Controller (0 Pts)

DLMIMWCK01\_Lektion07\_Frage02

Welche Schadenskategorien gibt es in Bezug auf Computerkriminalität?

* physisch, digital, ökonomisch, reputationsbezogen (1 Pts)
* physisch, ökonomisch, transistorisch, psychologisch (0 Pts)
* reputationsbezogen, motorisch, psychologisch, monetär (0 Pts)
* ökonomisch, sozial, digital, axiomatisch (0 Pts)

DLMIMWCK01\_Lektion07\_Frage03

Welche Art Threat Intelligence wird auch mit TTP bezeichnet?

* tactical (1 Pts)
* strategic (0 Pts)
* technical (0 Pts)
* taxonomic (0 Pts)

DLMIMWCK01\_Lektion07\_Frage04

Ist es als privatrechtliche Organisation in Deutschland verpflichtend, der Allianz für Cybersicherheit beizutreten?

* Nein, es ist nicht verpflichtend. (1 Pts)
* Ja, es ist verpflichtend. (0 Pts)
* Ja, wenn man als Betreiber kritischer Infrastruktur zählt. (0 Pts)
* Ja, wenn man unter das Geheimschutzgesetz fällt. (0 Pts)

DLMIMWCK01\_Lektion07\_Frage05

Welche Punkte gehören zu den organisatorischen Handlungsempfehlungen der Allianz für Cybersicherheit?

* Einrichtung eines Krisenstabs, interne und externe Kommunikation sowie externe Unterstützung (1 Pts)
* interne und externe Kommunikation, Monitoring des Netzwerks sowie externe Unterstützung (0 Pts)
* interne Kommunikation, Monitoring des Netzwerks sowie Einberufung des internen Krisenstabs (0 Pts)
* externe Kommunikation, Einberufung des Krisenstabs und externe Unterstützung (0 Pts)

DLMIMWCK01\_Lektion08\_Frage01

Welche der folgenden Organisationen ist eine Quelle für Berichte zur aktuellen Sicherheitslage bezogen auf Computerkriminalität?

* Information Security Forum (1 Pts)
* Institute of Electrical and Electronics Engineers (0 Pts)
* Bundesamt für Informationssicherheit (0 Pts)
* Cybersicherheit e.V. (0 Pts)

DLMIMWCK01\_Lektion08\_Frage02

Gegen welche der folgenden Angriffe in der eigenen Organisation hilft Patchmanagement nicht?

* DDoS (1 Pts)
* Botnetze (0 Pts)
* Schadprogramme (0 Pts)
* Ransomware (0 Pts)

DLMIMWCK01\_Lektion08\_Frage03

Ab welchem Zeitpunkt wird beim Security by Design an den Sicherheitsaspekt gedacht?

* Entwurf von Systemen (1 Pts)
* User Acceptance Test (0 Pts)
* Rollout (0 Pts)
* Entwicklungsphase (0 Pts)

DLMIMWCK01\_Lektion08\_Frage04

Von wem wird die Europol Awareness Campaign initiiert?

* EC3 (1 Pts)
* CIA (0 Pts)
* BSI (0 Pts)
* ECC (0 Pts)

DLMIMWCK01\_Lektion08\_Frage05

Welche Themen hat die Europol Awareness bereits bearbeitet?

* Mobile Awareness und Cyberscam (1 Pts)
* Mobile Awareness und Kryptoagility (0 Pts)
* Cyberscam und Mobile Agility (0 Pts)
* Cyberscam und Security by Design (0 Pts)