Ausgabedatum: 2/1/2019
Geändertes Datum: 1/29/2020
Version: 1.3

CertNexus CyberSAFE 2019 Prüfung CBS-310

Informationen zur Prüfung

Eignung der Kandidaten:

Für die *CyberSAFE* 2019-Zertifizierung sind keine Gebühren, unterstützende Unterlagen oder andere Massnahmen zur Überprüfung der Berechtigung erforderlich. Kaufen Sie einfach einen Zugangsschlüssel für den *CyberSAFE* 2019-Kurs im CertNexus Store hier. Dieser Kurs beinhaltet den Zugang zum Berechtigungsnachweisprozess direkt über die CHOICE-Plattform.

Prüfungsvoraussetzungen

Es gibt zwar keine formellen Voraussetzungen, um den CyberSAFE-Zertifizierungsprozess zu absolvieren, aber es wird empfohlen, dass Sie Erfahrung mit der grundlegenden Nutzung herkömmlicher Endbenutzertechnologie haben, wie z. B. Desktop-, Laptop- und Tablet-Computern, mobilen Geräten und grundlegenden Internetfunktionen, wie z. B. Web-Browsing und E-Mail kennen.

Sobald Sie die oben genannten Voraussetzungen erfüllen, empfiehlt CertNexus, dass Sie sich auf die CyberSAFE-Zertifizierung vorbereiten, indem Sie das CertNexus-Training zur *CyberSAFE 2019: Prüfung CBS-310* besuchen.

Prüfungsspezifikationen

Anzahl der Fragen: 10

Bestehendes Ergebnis: 8 von 10 (80 %)

Dauer: Es gibt kein offizielles Zeitlimit für das Ablegen des CyberSAFE-Zertifikats. Sie sollten jedoch erwarten, dass Sie die Prüfung in etwa 15-30 Minuten absolvieren können.

Prüfungsoptionen: Online über das CHOICE LMS - die Prüfung ist open-book

Aufgabenformate: Multiple Choice/Multiple Response/Wahr-Falsch

Beschreibung der Prüfung

Zielgruppe:

Dieser Berechtigungsnachweis ist für alle Endbenutzer von Computern, mobilen Geräten, Netzwerken und dem Internet gedacht, um sicherzustellen, dass sie die Technologie sicher nutzen können, um Sicherheitsrisiken zu minimieren.

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

Prüfungsziel Erklärung:

Die Prüfung bescheinigt, dass Sie über das Wissen, die Fertigkeiten und die Fähigkeiten verfügen, um die üblichen Risiken bei der Verwendung herkömmlicher Endbenutzergeräte zu erkennen und sich und Ihr Unternehmen vor Sicherheitsrisiken zu schützen.

Um sicherzustellen, dass die Kandidaten über die oben genannten Kenntnisse, Fertigkeiten und Fähigkeiten verfügen, werden Sie bei der *CyberSAFE* 2019-Zertifizierungsprüfung in den folgenden Bereichen mit der folgenden Gewichtung geprüft:

Domain	% der Untersuchung
1.0 Compliance	12%
2.0 Social Engineering	20%
3.0 Geräte- und Datensicherung	37%
4.0 Online-Sicherheit	31%
Gesamt	**100%**

Die folgenden Informationen sollen Ihnen helfen, sich auf Ihre CertNexus-Zertifikatsprüfung vorzubereiten. Diese Informationen stellen keine vollständige Liste aller Konzepte und Fähigkeiten dar, die bei der Prüfung abgefragt werden können. Die Lernziele innerhalb dieser Themengebiete bilden die essentiellen Kenntnisse ab, welche zur sicheren Nutzung von Computergeräten benötigt werden. Die Informationen ausserhalb der Bereiche und Lernziele sollen Beispiele für die Arten von Konzepten, Werkzeugen, Fertigkeiten und Fähigkeiten liefern, die sich auf die entsprechenden Bereiche und Lernziele beziehen. Diese Beispiele stimmen nicht unbedingt eins zu eins mit den Inhalten überein, die in Ihrem Trainingsprogramm oder in Ihrer Prüfung behandelt werden. CertNexus empfiehlt dringend, dass Sie sich vor der Prüfung selbständig mit den Konzepten vertraut machen, die hier genannt werden und mit denen Sie nicht vertraut sind.

Themen:

Domain 1.0 Compliance

Objective 1.1 Anforderungen an die Sicherheit im Betrieb

- Quellen für Compliance-Anforderungen im Betrieb
  - Passwort-Richtlinien
  - Richtlinien zur Internetnutzung
  - Datenschutz
  - Persönlich identifizierbare Informationen (PII)
  - AUP
    - Vor Ort vs. Remote
    - Equipment
    - Gemeinsam genutzte Ressourcen (Passwörter, Mailboxen, etc.)

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

        - Ausnahmen und Verzichtserklärungen
        - Eskalationspfade/Vorfallmeldungen
    - Richtlinien des Unternehmens
        - Zugang für Mitarbeiter/Gäste
        - Badge-Anforderungen
        - Wichtige Richtlinien
    - Konsequenzen bei Nichtbeachtung

Objective 1.2 Identifizieren Sie die rechtlichen Anforderungen

- Quellen für gesetzliche Compliance-Anforderungen
    - Verordnung/Gesetz
        - HIPAA
        - SOX
        - PCI DSS
        - Lokale Verordnungen
    - Rechtsfolgen bei Nichtbeachtung

Objective 1.3 Identifizieren Sie Ressourcen für Sicherheit und Compliance

- Organisatorische und rechtliche Compliance-Ressourcen
    - Organisatorische Handbücher/Webseiten
    - AUP-Dokumentation
        - Aktualisierungen
        - Standort/Zugang
    - Organisatorische Abteilungen
        - Legal
        - HR
        - Gesundheits-Informations-Management
        - IT
    - Industrieverbände/Berufsgruppen
    - Webseiten der Regierung

Domain 2.0 Social Engineering

Objective 2.1 Erkennen von Social Engineering-Angriffen

- Angriffs-Vektoren
    - Benutzername/Kennwort
    - Organisatorische/personelle Informationen
    - Physikalischer Zugang
    - Persönliche Informationen des End-Anwenders
- Angriffsziele
    - Datenvernichtung
    - Datendiebstahl
    - Finanzieller Gewinn
    - Politischer Gewinn

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

        - Reputation
        - Rache
    - Hochwertige Ziele
        - C-Stufen
        - Personal der Buchhaltung
        - HR-Personal
        - IT-Personal
    - Angriffsarten
        - Phishing
            - Whaling
            - Spear FIshing
        - Vishing
        - Pharming
        - Baiting
        - Pretexting
        - Nachahmung
        - Quid pro quo
        - Tailgating/Piggybacking
        - Shoulder Surfing

Objective 2.2 Verteidigen Sie sich gegen Social-Engineering-Angriffe

- Ressourcen zur Verteidigung
    - Organisatorische Hardware/Geräte
    - Organisatorische Daten
    - Netzwerkzugriff
    - Zugang zu den Räumlichkeiten
    - Benutzeranmeldeinformationen
- Abschwächungstechniken
    - Situationsbewusstsein
    - Ausweissysteme/Sicherheitskontrollen
    - Türschlösser
    - Verifizierung von Anfragen
    - Ordnungsgemässe Entsorgung/Löschung von sensiblen Informationen
    - Bildung/Kommunikation

Domain 3.0 Schutz von Geräten und Daten

Objective 3.1 Aufrechterhaltung der physischen Sicherheit der Geräte

- Geräte mit potenziell sensiblen Daten
    - Laptops/Computer
    - Handys
    - Tablets
    - Wechselspeicher (USB-Sticks)

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

- Organisatorische Anforderungen an die Gerätesicherheit
    - Begrenzung der Geräte, die Zugriff auf sensible Daten haben
    - Akzeptable Geräte zur Datenspeicherung
    - Entsorgungs-/Löschungsanforderungen
- Digitale Präsenz
    - Geräteprotokolle
    - Temporäre Dateien
    - Browser-Verlauf
    - Zwischengespeicherte/gespeicherte Anmeldeinformationen
- Physikalische Sicherheitstechniken für Geräte
    - Ordnungsgemässe Lagerung/Entsorgung/Recycling
    - Verlust-/Diebstahlmeldung
    - Sperren unbeaufsichtigter Maschinen/Geräte

Objective 3.2 Passwörter sicher verwenden

- Passwörter/PINs
    - Häufiges Wechseln
    - Komplexität
    - Verbot der Wiederverwendung/Weitergabe
    - Auswendiglernen vs. Aufnehmen/Dokumentieren
- Biometrie
- Multi-Faktor-Authentifizierung vs. Zwei-Schritt-Authentifizierung
- Passwort-Manager
- Passwort/PIN-Sicherheitstechniken
    - Verdeckte Eingabe (stellen Sie sicher, dass niemand Sie bei der Eingabe beobachten kann)
    - Unmittelbar nach Verletzung/Vorfall ändern
    - Sichere Speicherung von Passwörtern
    - Entscheidende Bedeutung des Schutzes von E-Mail-Passwörtern
    - Multifaktor-Authentifizierung verwenden, wenn möglich
    - Komplexität im Vergleich zur Empfindlichkeit der Daten
    - Eindeutige Passwörter für alle Standorte und Systeme
    - Vermeiden der Verwendung von leicht zu erratenden Passwörtern

Objective 3.3 Einhalten der Best Practices zum Schutz von Daten und sensiblen Daten

- Datensicherungen/Speicherorte
- Überlegungen zu mobilen Geräten
    - Informationslecks durch Always-on-App-Funktionalität
    - Versehentliches oder absichtliches Aufzeichnen von sensiblen Daten
        - Kamera
        - Mikrofon
- Techniken zur Datensicherheit

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

        - Verbot des Kopierens/Druckens
        - Ordnungsgemässe Entsorgung von gedruckten Daten
        - Verbote für Wechseldatenträger
        - Verbot von mobilen Geräten in Meetings

Objective 3.4 Potenzielle Quellen von Malware identifizieren und Infektionen verhindern

- Auswirkungen von Malware
    - System-Korruption
    - Spionage/Protokollierung
    - Ablenkung/Belästigung
    - Verschlechterung der Geräteleistung
    - Daten-Hijacking/Ransoming
    - Datenvernichtung
    - Erpressung (Blackmail)
    - Werbung
- Malware-Typen
    - Tastenlogger
    - Ransomware
    - Adware/Spyware
    - Trojanisches Pferd
    - Virus
    - Wurm
    - Browser-Hijacker
- Malware-Quellen
    - Trickangebote
    - Abtrünniger Antivirus
    - Betrug mit kostenloser Software
    - Software-Piggybacking
    - Verwirrende oder verdeckte Optionen (benutzerdefinierte Installationen)
    - Unbekannte/nicht vertrauenswürdige Download-Seiten
    - E-Mail-Anhänge
    - Links
    - Skripte in Datendateien/Software
    - Infizierte Hardware
        - Thumb-Laufwerke
        - Externe Festplatten
- Techniken zur Malware-Prävention
    - Sorgfältiges Lesen von E-Mails/Dialogfeldern/Angeboten/Pop-ups/etc.
    - IT-Freigabe für Software-Installation
    - Überprüfung der Links vor der Auswahl

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

        - Nutzen/Risiko-Analyse bei der Installation von Software
        - Bewusstsein für allgemeines Systemverhalten
        - Verwendung von bekannten Herstellern und Geräten
            - Geprüfte Verlage

Objective 3.5 Drahtlose Geräte sicher verwenden

- Häufige Risiken in drahtlosen Netzwerken
    - Lauschangriff
    - Unsichere Netzwerke
        - Privat
        - Öffentlich
        - Öffnen Sie
    - Rogue Access Points
    - Böse Zwillinge (Evil Twins)
    - "Erinnern" an drahtlose Netzwerke
- Sichere Techniken für die Verwendung drahtloser Geräte
    - Verbot der Nutzung öffentlicher Netzwerke
    - Verschlüsselung
        - WEP/WPA/WPA2
        - Sichern von Wi-Fi-Passwörtern
    - Drahtloses Netzwerk "Vergessen"
    - Vermeidung des bösen Zwillings (Evil Twins)
        - Falsch geschriebene Netzwerknamen
        - Fehlende Passwortanforderungen
        - Mehrere Netzwerke mit ähnlichen Namen

Domain 4.0 Online-Sicherheit

Objective 4.1 Sicher im Internet surfen

- Bekannte Browser
    - Chrome
    - Internet Explorer
    - Edge
    - Firefox
    - Safari
- URL-Konstruktion
    - HTTP vs. HTTPS
        - Nicht-Verschlüsselung vs. Verschlüsselung
    - Top-Level-Domains
    - Domainnamen
    - Verdächtige/gefälschte URLs
        - Enge Schreibweisen/Fehlschreibweisen
- Techniken zum sicheren Surfen im Internet

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

- Aktuelle und aktualisierte Webbrowser-Nutzung
- Webadressen entschlüsseln
- Unbekanntes Add-In, Plug-In, Symbolleistenvermeidung
- Werbung und Pop-ups nicht anklicken/antippen
- Protokoll-Verifizierung
- URL-Überprüfung bei Verwendung von Links
- Tippen vs. Klicken
- Lesezeichen für allgemeine Websites
- Vorsicht bei der Verwendung von mobilen Geräten (URLs nicht immer sichtbar)

Objective 4.2 Sichere Verwendung von E-Mails

- Häufige Risiken bei der E-Mail-Nutzung
  - Häufige Social-Engineering-Angriffe
    - Sicherheitswarnungen
    - Abfragen von Benutzeranmeldeinformationen
    - Angebote zur Malware-Entfernung/IT-Support
    - Kostenlose Angebote
    - Geld-/Erbschaftsbetrug
    - Anfragen für Informationen
  - Bösartige Anhänge
    - Hochriskante Dateitypen
    - Einhaltung von Richtlinien/Regeln
- Techniken zur sicheren E-Mail-Nutzung
  - Identifizierung von Betrügern
    - Absendername vs. E-Mail-Adresse
    - Betreffzeilen-Themen
    - Tonfall/Stimme/Grammatik des Absenders
    - Signatur
    - Ungewöhnliche/atypische Anfragen von scheinbar gültigen Quellen
      - "Bank" fragt in E-Mail nach Passwort
      - "IT" fragt per E-Mail nach persönlichen Daten
  - Überprüfung des Absenders
    - Rückruf/persönliches Treffen vor dem Antworten/Klicken
  - E-Mail an die Einhaltung von Richtlinien
  - Überlegungen zur Anbringung

Objective 4.3 Soziale Netzwerke sicher nutzen

- Sicherheitsüberlegungen zu sozialen Netzwerken
  - Versehentliche Weitergabe vertraulicher Informationen
  - Abfällige Kommentare

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.

        - Eigenes Konto vs. Unternehmensprofil
    - Fehlende Kontrolle über Daten und Freigabe
        - Vertraulichkeit
        - Einmal geposted, für immer online
    - Verwirrende Sicherheitseinstellungen
    - Möglichkeiten für Social Engineering
    - Gefälschte Konten
- Sichere Techniken für soziale Netzwerke
    - Anpassung an die Nutzung von sozialen Netzwerken und Richtlinien des Unternehmens
    - Gründliche Recherche und Konfiguration von Sicherheits- und Datenschutzeinstellungen
    - Vorsicht bei der Weitergabe von potenziell sensiblen oder rufschädigenden Informationen
    - Sicherheit der Admin-Anmeldedaten
    - Bewusstsein für Social Engineering

Objective 4.4 Sichere Nutzung von Cloud-Diensten

- Risiken bei Cloud-Diensten
    - Spoofing von Cloud-Diensten
    - Änderungen beim Hersteller
        - Akquisitionen/Fusionen
        - Out of Business
    - Verwechslung von Unternehmenss- und Privatkonten (digitaler Speicherort)
- Überlegungen zu IoT-Geräten
- Techniken zur sicheren Nutzung von Cloud-Diensten
    - Genehmigungen durch das Unternehmen für alle Cloud-basierten Speicher
    - Lokale Backups
    - Zusätzliche Aufmerksamkeit bei Zugangsdaten

Anforderungen an die kontinuierliche Weiterbildung

Der *CyberSAFE 2019* Nachweis ist ab dem Zeitpunkt der Erteilung des Zertifikats 1 Jahr lang gültig. Sie müssen den Rezertifizierungsnachweis für CyberSAFE oder die aktuellste Version der CyberSAFE-Zertifizierung vor Ablauf des 1-Jahres-Zeitraums ablegen, um eine kontinuierlich gültige Zertifizierung zu erhalten.

Copyright © 2019 by Certnexus. Alle Rechte vorbehalten.
Die CertNexus CyberSAFE 2019 (CBS-310) Prüfungsziele können ohne vorherige Ankündigung geändert werden.