CISO Sprechstunde

04.12.2024

Aktuelles aus der FAU

SIEM

- Entwurf der DV ist erstellt
- Absprache mit GPR erfolgt Anfang Feb 2025

Informationssicherheitsrichtlinie

- Abstimmung mit Juristen aus Kanzlerbüro erfolgt aktuell
- Absprache mit GPR 1. Q. 2025?

Phishing Simulation durch das SOC der FAU

- Testbetrieb mit Freiwilligen

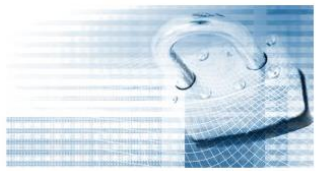
Aktuelles aus der FAU

Informationssicherheitsbeauftragter LS/Department/Fakultät

DFN-CERT UNTERNEHMEN LEISTUNGEN INFORMATIONEN KA

HOME > INFORMATIONEN > TERMINE > WEITERBILDUNG ZUR/ZUM INFORMATIONSSICHERHEITSBEAUFTRAGTEN ALS WEBINAR

Weiterbildung zur/zum Informationssicherheitsbeauftragten als Webinar



05.11.2024, 09:00 – 05.12.2024, 11:15 | Webinar

https://www.dfn-cert.de/informationen/termine/weiterbildung-zurzum-informationssicherheitsbeauftragten-als-webinar/

Block 1 (dreitägig)

- Einführung und Motivation
  - Aufgaben eines ISB
  - BSI-Grundschutzmethode
  - ISO 27001
  - Risikoanalysen
  - Praktische Informationssicherheit
  - Designprinzipien
  - Sichere Netzwerkarchitekturen
  - Client- und Browsersicherheit

Block 2 (zweitägig)

- Kryptographie und Authentisierung
  - Rechtliche Aspekte: IT-Sicherheitsgesetz / EU-Datenschutzgrundverordnung
  - Sicherheitskonzepte
  - Security-Awareness
  - Interne und externe Audits
  - Notfallmanagement

Der nächste Kurs Weiterbildung zur/zum Informationssicherheitsbeauftragten findet als Präsenzveranstaltung in Hamburg 2025 vom **01.04.- 03.04.2025 Block I und 06. & 07.05.2025 Block II, optionale Prüfung 08.05.2025** statt.

Aktuelles aus der FAU

Datenbanken im Internet

Warum sind an der FAU Datenbanken ohne Frontend im Internet erreichbar?

Incident ID	3639718
Title	Exposed Critical Service Detected on 5432 Port (Port Default Usage: PostgreSQL Ports)
Incident Product	Attack Surface Management
Incident Main Type	Configuration Weakness
Incident Sub Type	Network Security
Assets	FAU
Risk Level	HIGH

Incident ID	3626882
Title	Critical Open "3306 MySQL" Port Detected
Incident Product	Attack Surface Management
Incident Main Type	Configuration Weakness
Incident Sub Type	Network Security
Assets	FAU
Risk Level	HIGH

Incident ID	3605766
Title	Critical Open "27017 MongoDB" Port Detected
Incident Product	Attack Surface Management
Incident Main Type	Configuration Weakness
Incident Sub Type	Network Security
Assets	FAU
Risk Level	HIGH

Aktuelles aus dem Rest der Welt

Massive technische Probleme an der Uni Potsdam

- Uni Potsdam [1] hat seit Mittwoch 27.11.24 technische Probleme: Internet und Telefonie präventiv gekappt
- Homepage und die Telefonverbindung des Hasso Plattner Instituts (HPI) sind ebenfalls betroffen
- Lehre laufe weiter, sei aber durch nicht nutzbare IT-Systeme etwas eingeschränkt
- Ob es sich um eine Cyberattacke handelt, sei noch unklar
- Aus Universitätskreisen hieß es zunächst, es habe einen „Bug“ in einer Firmware gegeben
- Auf X und LinkedIn beginnen Mitarbeiter jedoch, sich zu beschweren: dass Updates zur aktuellen Lage zu spät kommen, und dass eine „effektive Arbeit“ zunehmend schwierig würde
- Eine Professorin bezeichnet das Vorgehen als „sehr improvisiert“ und erkundigt sich nach einem Notfallplan
- Eine Pressemitteilung zum Thema „Volkskrankheiten“ verschickte die Pressesprecherin am Freitag von einer privaten Mailadresse

[1] https://www.tagesspiegel.de/potsdam/landeshauptstadt/technische-probleme-an-der-universitat-potsdam-internet-und-telefonie-praventiv-gekappt-12783503.html

Aktuelles aus der Welt

Top 10 der Software-Schwachstellen 2024

1. Cross-site Scripting [CWE-79]
2. Out-of-bounds Write [CWE-787]
3. SQL Injection [CWE-89]
4. Cross-Site Request Forgery (CSRF) [CWE-352]
5. Path Traversal [CWE-22]
6. Out-of-bounds Read [CWE-125]
7. OS Command Injection [CWE-78]
8. Use After Free [CWE-416]
9. Missing Authorization [CWE-862]
10. Unrestricted Upload of File with Dangerous Type [CWE-434]

zu 2.) Heap-Schwachstelle zu einem beliebigen Speicherlese- und -schreib-Primitiv ausgenutzt.

zu 4.) einfache CSRF-Attacken die DSL-Router von A wie AVM Fritz!Box bis Z wie ZyXEL über das Internet von außen angreifen

zu 5.) most common special elements is the "../" sequence

zu 6.) https://www.youtube.com/watch?v=1S0aBV-Waeo&t=273s

Die vollständige Liste der Top 25 Schwachstellen können Sie direkt auf der Webseite von MITRE einsehen.

Laut BSI wurden bislang 78 Schwachstellen pro Tag in 2024 entdeckt

Sicherheitslücken im Linux-Kernel haben in den letzten Jahren erheblich zugenommen

Anforderungen durch externe Projektpartner

Drittmittelprojekt – Fragenkataloge und Anforderungen

Ein Beispiel

Technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit

Physische Sicherheitsmaßnahmen und Zutrittskontrollen

Maßnahmen, um zu verhindern, dass Unbefugte Zugriff auf die Datenverarbeitungsanlagen (Datenbank- und Applikationsserver sowie zugehörige Hardware) erhalten. Dazu werden die folgenden Maßnahmen ergriffen:

a) Einrichtung von Sicherheitsbereichen
b) Sicherung und Einschränkung der Zugangswege
c) Sicherung der dezentralen Datenverarbeitungsanlagen und Personalcomputer
d) Festlegung von Zugriffsberechtigungen für Mitarbeiter und Dritte, einschließlich der entsprechenden Dokumentation
e) Regelung zu den Zugangsrechten
f) Beschränkung der Zugangsrechte
g) Protokollierung, Überwachung und Nachverfolgung aller Zugriffe auf das Rechenzentrum
h) Sicherung des Rechenzentrums durch Zugangskontrollen und andere geeignete Sicherheitsmaßnahmen
i) Wartung und Inspektion in IT-Bereichen und Rechenzentren nur durch autorisiertes Personal

Drittmittelprojekt - Anforderungen

Ein Beispiel

Zugriffskontrolle (IT-Systeme und/oder IT-Anwendungen)

Der Auftragnehmer implementiert ein Rollen- und Berechtigungskonzept.

Der Auftragnehmer implementiert ein Autorisierungs- und Authentifizierungs-Framework, das unter anderem die folgenden Elemente umfasst:

a) Rollenbasierte Zugriffskontrollen
b) Verfahren zum Erstellen, Ändern und Löschen von Accounts
c) Schutz des Zugriffs auf IT-Systeme und IT-Anwendungen durch Authentifizierungsmechanismen
d) Nutzung geeigneter Authentifizierungsmethoden, basierend auf den Eigenschaften und technischen Möglichkeiten des IT-Systems oder der IT-Anwendung
e) Erfordernis einer angemessenen Authentifizierung für den Zugang zu IT-Systemen und IT-Anwendungen
f) Protokollierung, Überwachung, Nachverfolgung sämtlicher Zugriffe auf Projekt-Daten
g) Autorisierungs- und Protokollierungsmaßnahmen für ein- und ausgehende Netzwerkverbindungen zu IT-Systemen und IT-Anwendungen (insbesondere Firewalls zum Zulassen oder Verweigern eingehender Netzwerkverbindungen)
h) Vergabe privilegierter Zugriffsrechte auf IT-Systeme, IT-Anwendungen und Netzwerkdienste nur an Personen, die diese zur Erfüllung ihrer Aufgaben benötigen (Least-Privilege-Prinzip)

Drittmittelprojekt - Anforderungen

Ein Beispiel

i) Dokumentation und laufende Aktualisierung der privilegierten Zugriffsrechte auf IT-Systeme und IT-Anwendungen

j) Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte auf IT-Systeme und –Anwendungen

k) Passwort-Policy mit Anforderungen an die Komplexität von Passwörtern, Mindestlänge und Ablauf nach angemessener Zeit, sowie keiner Wiederverwendung von kürzlich verwendeten Passwörtern

l) Technische Durchsetzung der Passwort-Policy durch IT-Systeme und IT-Anwendungen

m) Entzug der Zugriffsrechte von Mitarbeitern und externem Personal auf IT-Systeme und IT-Anwendungen bei Beendigung des Arbeitsverhältnisses oder des Vertrages

n) Verwendung von sicheren, dem Stand der Technik entsprechenden Authentifizierungszertifikaten

Drittmittelprojekt - Anforderungen

Ein Beispiel

IT-Systeme und IT-Anwendungen sperren sich automatisch oder beenden die Sitzung nach Überschreiten einer zuvor definierten, angemessenen Leerlaufzeit

Der Auftragnehmer beschränkt den privilegierten Zugang zu Cloud-Ressourcen auf einzelne oder bestimmte Bereiche von IP-Adressen

Der privilegierte Zugang zu Cloud-Ressourcen erfolgt über einen Bastion-Host

Der Auftragnehmer unterhält Anmeldeverfahren an IT-Systemen mit Schutzmaßnahmen gegen verdächtige Anmeldeaktivitäten (z. B. gegen Brute-Force- und Password-Guessing-Angriffe)

Drittmittelprojekt - Anforderungen

Ein Beispiel

Verfügbarkeitskontrolle
Der Auftragnehmer implementiert geeigneter und dem Stand der Technik entsprechender Anti-Malware-Lösungen zum Schutz der Systeme und Anwendungen vor Schadsoftware
Der Auftragnehmer definiert, dokumentiert und implementiert ein Datensicherungskonzept für IT-Systeme, das die folgenden technischen und organisatorischen Elemente umfasst: a) Schutz der Backup-Speichermedien vor unberechtigtem Zugriff und vor Umweltbedrohungen (z. B. Hitze, Feuchtigkeit, Feuer) b) vordefinierte Backup-Intervalle c) regelmäßiges Testen der Wiederherstellung von Daten aus Backups entsprechend der Sensibilität des IT-Systems oder der IT-Anwendung
Der Auftragnehmer speichert Backups an einem anderen physischen Ort als dem Ort, an dem das laufende System gehostet wird
IT-Systeme und IT-Anwendungen in Nicht-Produktionsumgebungen sind logisch oder physikalisch von IT-Systemen und IT-Anwendungen in Produktionsumgebungen getrennt
Rechenzentren sind gegen Naturkatastrophen, physische Angriffe und Unfälle geschützt
Unterstützende Einrichtungen in IT-Bereichen und Rechenzentren, wie z. B. Kabel, Strom, Telekommunikationseinrichtungen, Wasserversorgung oder Klimaanlagen, sind vor Störungen und unbefugter Manipulation geschützt

Drittmittelprojekt - Anforderungen

Ein Beispiel

Der Auftragnehmer unterhält und implementiert ein unternehmensweites ISO 27001 Information Security Framework, das regelmäßig überprüft und aktualisiert wird
Der Auftragnehmer protokolliert sicherheitsrelevante Ereignisse, wie z.B. Aktivitäten der Benutzerverwaltung (z.B. Anlegen, Löschen), fehlgeschlagene Anmeldungen, Änderungen an der Sicherheitskonfiguration des Systems auf IT-Systemen und IT-Applikationen
Der Auftragnehmer analysiert kontinuierlich die jeweiligen Protokolldaten der IT-Systeme und IT-Applikationen auf Anomalien, Unregelmäßigkeiten, Hinweise auf Kompromittierung und andere verdächtige Aktivitäten
Der Auftragnehmer scannt und testet IT-Systeme und IT-Anwendungen regelmäßig auf Sicherheitslücken
Der Auftragnehmer implementiert und unterhält einen Change-Management-Prozess für IT-Systeme und IT-Applikationen
Der Auftragnehmer unterhält einen Prozess zur Aktualisierung und Implementierung von Security Fixes und Updates der Hersteller auf den jeweiligen IT-Systemen und IT-Applikationen
Der Auftragnehmer löscht Daten unwiederbringlich oder vernichtet die Datenträger physisch, bevor ein IT-System entsorgt oder wiederverwendet wird

Drittmittelprojekt - Anforderungen

Ein Beispiel

Übertragungssteuerung
Der Auftragnehmer dokumentiert und aktualisiert regelmäßig die Netzwerktopologien und deren Sicherheitsanforderungen
Der Auftragnehmer überwacht kontinuierlich und systematisch IT-Systeme, IT-Anwendungen und relevante Netzwerkzonen, um bösartige und abnormale Netzwerkaktivitäten zu erkennen, durch: a) Firewalls (z.B. Stateful Firewalls, Application Firewalls) b) Proxy-Server c) Intrusion Detection Systems (IDS) und/oder Intrusion Prevention Systems (IPS) d) UR-Filterung und e) Security Information and Event Management (SIEM) Systeme
Der Auftragnehmer verwaltet IT-Systeme und IT-Anwendungen unter Verwendung von verschlüsselten Verbindungen, die dem Stand der Technik entsprechen
Der Auftragnehmer schützt die Integrität von Inhalten bei der Übertragung durch modernste Netzwerkprotokolle, wie z.B. TLS
Der Auftragnehmer verschlüsselt oder ermöglicht die Verschlüsselung von Kundendaten, die über öffentliche Netze übertragen werden
Der Auftragnehmer verschlüsselt oder ermöglicht die Verschlüsselung von Daten, wenn diese auf Datenbanken des Auftragnehmers gespeichert werden

Drittmittelprojekt - Anforderungen

Ein Beispiel

Sicherheitstechnische Vorfälle

Der Auftragnehmer unterhält und implementiert einen Prozess zur Behandlung von sicherheitstechnischen Vorfällen, der unter anderem Folgendes umfasst:

a) Aufzeichnungen über Sicherheitsverstöße

b) Prozesse zur Benachrichtigung des Auftragnehmers/-gebers

c) ein Konzept für die Reaktion auf einen Vorfall, das Folgendes zum Zeitpunkt des Vorfalls regelt:
(i) Rollen, Verantwortlichkeiten sowie Kommunikations- und Kontaktstrategien im Falle einer Kompromittierung,
(ii) spezifische Verfahren für die Reaktion auf den Vorfall und
(iii) die Absicherung und Behandlung aller kritischen Systemkomponenten.

Drittmittelprojekt - Anforderungen

Ein Beispiel

Asset Management, Systembeschaffung, Entwicklung und Wartung
Der Auftragnehmer identifiziert und dokumentiert die Anforderungen an die Informationssicherheit vor der Entwicklung und Beschaffung neuer IT-Systeme und IT-Anwendungen sowie vor Verbesserungen an bestehenden IT-Systemen und IT-Anwendungen
Der Auftragnehmer implementiert einen formalen Prozess zur Kontrolle und Durchführung von Änderungen an entwickelten Anwendungen
Der Auftragnehmer konzipiert und integriert Sicherheitstests in den System Development Life Cycle von IT-Systemen und IT-Anwendungen
Der Auftragnehmer implementiert einen angemessenen Security-Patching-Prozess, der Folgendes umfasst:
a) Überprüfung der Komponenten auf mögliche Schwachstellen (CVEs)
b) Prioritätseinstufung der Fehlerbehebungen
c) rechtzeitige Implementierung des Fixes
d) das Herunterladen von Patches aus vertrauenswürdigen Quellen

Drittmittelprojekt - Anforderungen

Ein Beispiel

Personalsicherheit
Der Auftragnehmer setzt im Bereich der Personalsicherheit folgende Maßnahmen um:
a) Verpflichtung von Mitarbeitern mit Zugang zu Daten zur Vertraulichkeit
a) Regelmäßige Schulung von Mitarbeitern mit Zugang zu Daten hinsichtlich anwendbarer Datenschutzgesetze und –vorschriften
Der Auftragnehmer implementiert einen Offboarding-Prozess für Mitarbeiter des Auftragnehmers und externe Lieferanten

Drittmittelprojekt - Anforderungen

Ein Beispiel

Kryptographie
Der Auftragnehmer verwendet sichere, dem Stand der Technik entsprechende Zertifikate und setzt Folgendes um:
a) Digitale Zertifikate werden nur dann akzeptiert und als vertrauenswürdig eingestuft, wenn das digitale Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde,
b) Zertifikate werden verwendet und dedizierten IT-Systemen und Anwendungen zugeordnet und die Gültigkeit von digitalen Zertifikaten überprüft wird.
Der Auftragnehmer implementiert einen Prozess für die Verwaltung und Implementierung von kryptographischen Schlüsseln, einschließlich Regeln und Anforderungen für die Erzeugung, Speicherung, Sicherung, Verteilung und den Widerruf von kryptographischen Schlüsseln.

Ihre Fragen?

Ihre Wünsche?