Profil ID: EBLCJH5DQO

Wohnort des Spezialisten: Deutschland, 60437

Cyber Security Consultant: Cyber Defense, Cyber Forensic, Penetration Test, Certified Ethical Hacker (CEH)

Mitarbeiterkurzprofil

Herr H. A. geboren 1988

Position

Freiberuflicher Cyber / IT Security Consultant

Cyber Security: Cyber Defense, Cyber Forensic, Penetrationstest, Netzwerk-Sicherheit, Certified Ethical Hacker (CEH), CISA (Certified Information Systems Auditor), DIN ISO/IEC 27001, Security Awareness, Mobile Security, Social Media Security

Tools und Methoden: SIEM und Anomalieerkennung, IT-Audit, MaRISK, BAIT, PSD2, IT/Technical Due Diligence, IT Revision

Branchen: Automobilindustrie, Chemieindustrie, Handel, Banken

Sprachen

Deutsch (Muttersprache), Englisch (fließend)

Verfügbarkeit

Kurzfristig nach Absprache in Vollzeit

Projekterfahrung

2 Monate

Automobilindustrie

Penetration Tester für Connected Car Apps

Automobilindustrie, Hannover

Tätigkeitsbeschreibung

Im Rahmen einer neuen Produktstrategie für Connected Car wurde eine App zur digitalen Fahrtenbucherfassung entwickelt. Im Rahmen eines Penetrationstests wurde ermittelt, inwiefern die App und das zugehörige Backend angegriffen werden können, unter anderem durch:

Angriffe auf das Certificate Pinning

Angriffe auf die Kunden-/Mandantentrennung

Manipulation von Fahrzeug- und GPS-Daten

Auslesen von Zugangsdaten von den Geräten

Eingesetzte Qualifikationen

Cyber Security, IT Sicherheit (allg.), Netzwerk-Sicherheit, DIN ISO/IEC 27001, Penetrationstest

3 Monate

Handel

Penetration Tester, Forensic Analyst, Security Berater

Einzelhandelskette, NRW

Tätigkeitsbeschreibung

Um mögliche Angriffswege in das interne Netzwerk der Einzelhandelsgruppe zu identifizieren, wurde ein Red Team Penetrationstest durchgeführt. Nach dem Aufdecken möglicher Angriffswege werden nun forensische Analysen der betroffenen Server durchgeführt. Weiterhin erfolgt eine schrittweise Erstellung eines Maßnahmenplans im Rahmen von Workshops.

Eingesetzte Qualifikationen

Cyber Security, IT Sicherheit (allg.), Netzwerk-Sicherheit, DIN ISO/IEC 27001, Penetrationstest, Risikomanagement

7 Monate

Banken

IT Security Auditor und Berater

Landesbank, Frankfurt am Main

Tätigkeitsbeschreibung

Um ein einheitliches Sicherheitsniveau in der Landesbank zu erhalten, werden durch die Abteilung Information Security Management regelmäßige Security Audits und Beratungen durchgeführt, um die Sicherheit von Anwendungen und Infrastrukturkomponenten zu erhalten und zu optimieren. Aufgaben im Projekt:
Durchführung von Security Audits und Penetration Tests
Erstellung von Sicherheitskonzepten, z.B. für iOS und MDM
Erstellung von Sicherheitsbewertungen
Erstellung von Stellungnahmen der Information Security

Eingesetzte Qualifikationen

Cyber Security, IT Sicherheit (allg.), Netzwerk-Sicherheit, DIN ISO/IEC 27001, Risikomanagement

3 Monate

Banken

IKS Analyst / Anforderungsmanager

IT-Dienstleister für Banken, München

Tätigkeitsbeschreibung

Im Rahmen eines großen EZB-Finding-Remediationprogramms habe ich für den Kunden das interne Kontrollsystem für IT-Sicherheitsmanagement sowie IT-Risikomanagement neu aufgebaut. Die elementaren Projektschritte waren:

Aufnahme der Prozesslandschaft des Unternehmens

Aufnahme der Anforderungen von CISO und CRO an die Geschäftsprozesse

Entwicklung von Kontrollen für IT-Sicherheit sowie IT-Risikomanagement zur Einarbeitung ins Prozessframework

Übergabe der Kontrollen an die Prozessdesigner

Eingesetzte Qualifikationen

Cyber Security, DIN ISO/IEC 27001, Risikomanagement

4 Monate

Banken

Identity & Access SME

DAX Top 30 Bank, Frankfurt am Main

Tätigkeitsbeschreibung

Um die steigenden regulatorischen Anforderungen an Identity & Access gerecht zu werden, mussten mögliche Lösungen für den Identity Lifecycle für Kunden-Benutzer in bankinternen Anwendungen identifiziert werden. Ergebnis des Projektes war eine Case Study mit 3 möglichen Lösungen sowie einer Entscheidungsvorlage für das seniore Management.

Eingesetzte Qualifikationen

Cyber Security, IT Sicherheit (allg.)

2 Monate

Automobilindustrie

Lead Penetration Tester

Automobilindustrie, Ingolstadt

Tätigkeitsbeschreibung

Für die sichere Bereitstellung einer hochkritischen Anwendung hat der Kunde eine smartcardbasierte Authentifizierung durch den Hersteller der Anwendung implementieren lassen. Um sicherzustellen, dass kein unberechtigter Zugriff auf die Anwendung erfolgen kann, wurde ein Penetrationstest auf die diese Authentifizierungslösung durchgeführt. Dabei konnten verschiedene Schwachstellen im Zertifikatsmanagement, der Signaturprüfung sowie kryptographischer Sicherungsverfahren identifiziert werden, die sich in Summe dazu ausnutzen ließen, unberechtigten Zugriff auf die Anwendung zu erhalten. Im Anschluss wurden mögliche Verbesserungen an der Anwendung sowie dem Authentifizierungsverfahren mit dem Hersteller besprochen und nachgetestet.

Eingesetzte Qualifikationen

Certified Ethical Hacker (CEH), Cyber Security, Penetrationstest

2 Monate

Medienbranche

IT Due Diligence SME

Medienbranche, München

Tätigkeitsbeschreibung

Im Rahmen einer M&A Transaktion für den Betreiber von Reiseportalen wurde eine IT Due Diligence durchgeführt.

Inhalte des Projektes waren:

Wertanalyse des Codes durch COCOMO II

Bewertung der IT-Sicherheitsmaßnahmen

Bewertung des Software Stacks

Bewertung der Skalierbarkeit der Lösung

Bewertung der Codequalität

Eingesetzte Qualifikationen

Cyber Security, IT Sicherheit (allg.), Risikomanagement

7 Monate

Chemieindustrie

Lead Cyber Forensic Analyst

DAX Top 30 Chemiekonzern, Köln

Tätigkeitsbeschreibung

Durchführung einer forensischen Analyse zur Aufarbeitung eines Advanced Persistent Threat Cyberangriffes auf ein DAX Top 30 Unternehmen. Projektbestandteile waren unter anderem:

Malwareanalyse

Loganalysen

Root-Cause-Analysen

What-If-Analysen

Angriffspfadermittlung

Weiterhin wurden nach der Aufarbeitung des Vorfalls ein Penetrationstest sowie eine Schwachstellenanalyse zur Verhinderung weiterer Angriffe durchgeführt.

Eingesetzte Qualifikationen

Certified Ethical Hacker (CEH), Cyber Security, Penetrationstest

3 Jahre

Handel

Lead Penetration Tester

Einzelhandelskette, remote

Tätigkeitsbeschreibung

Für eine große Einzelhandelskette wurden die Online Shops bei Inbetriebnahme sowie bei neuen Releases getestet. Die Penetrationstests umfassten unter anderem:

Information Gathering / Informationsbeschaffung

Schwachstellenanalyse (OWASP Top 10)
Prüfung der Checkout-Logik
Prüfung der Sicherheit der Paymentanbindungen

Eingesetzte Qualifikationen
Certified Ethical Hacker (CEH), Cyber Security, Penetrationstest

3 Jahre

Banken

Technical IT Security Auditor

IT-Dienstleister für Banken, München

Tätigkeitsbeschreibung

Der Kunde unterliegt hohen regulatorischen Anforderungen an den IT-Betrieb sowie das Risikomanagement. Als Unterstützung der internen Revision habe ich über mehrere Jahre Prüfungen im Bereich IT-Sicherheit und IT-Risikomanagement durchgeführt, unter anderem in den Bereichen:

Mainframe z/OS

Netzwerkinfrastruktur

Systemsicherheit Windows und UNIX

Middleware, u.a. IBM WebSphere

Sicherheitsdesign

projektbegleitende IT-Prüfungen

Weiterhin habe ich das Unternehmen bei der Vorbereitung sowie während einer aufsichtsrechtlichen Prüfung der Europäischen Zentralbank unterstützt.

Eingesetzte Qualifikationen

CISA (Certified Information Systems Auditor), Cyber Security, IT Sicherheit (allg.), Netzwerk-Sicherheit, Penetrationstest, DIN EN ISO 27001

1 Jahr, 11 Monate

Finanzbranche

IT Security Auditor

Diverse Kunden der Finanzbranche, verschiedene Orte

Tätigkeitsbeschreibung

Für diverse Kunden aus dem Finanzsektor (Banken, Versicherungen, Leasinggesellschaften) wurden IT Security Audits in verschiedenen

Bereichen durchgeführt:

Überprüfung des Netzwerkdesigns

Durchführung von Architekturreviews

Sicherheit von Betriebssystemen (Windows, UNIX)

Eingesetzte Qualifikationen

Netzwerk-Sicherheit, Cyber Security, CISA (Certified Information Systems Auditor), IT Sicherheit (allg.), DIN ISO/IEC 27001

1 Jahr, 11 Monate

diverse Branchen

Penetration Tester

Diverse Kunden, verschiedene Orte

Tätigkeitsbeschreibung

Für diverse Kunden verschiedener Branchen (u.a. Banken, Unterhaltungsindustrie, Automobilzulieferer) wurden verschiedene Penetrationstests

durchgeführt. Diese umfassten unter anderem:

Information Gathering / Informationsbeschaffung

Schwachstellenanalyse (OWASP Top 10 und andere)

Analyse möglicher Angriffswege für APT

Privilege Escalation

Eingesetzte Qualifikationen

Certified Ethical Hacker (CEH), Cyber Security, Penetrationstest

4 Jahre, 5 Monate

diverse Branchen

Sicherer IT-Betrieb / Systemadministration

Diverse Kunden verschiedener Branchen, München

Tätigkeitsbeschreibung

Für diverse Kunden verschiedener Branchen wurden IT-Systeme betrieben, unter anderem:

Microsoft Windows

Microsoft Exchange

Linux Webserver / sicheres CMS-Hosting

Linux Mailserver

Optimierung der Sicherheit bestehender Systeme

Eingesetzte Qualifikationen

Netzwerk-Sicherheit, IT Sicherheit (allg.), Systemadministration (allg.)

Quellen-URL (abgerufen am 06.05.2024 - 12:19):

<https://www.sps-profis.de/profil/eb1cjh5dgo/cyber-security-consultant-cyber-defense-cyber-forensic-penetration-test-certified-ethical-hacker-ceh>