Kariera w dziedzinie cyberbezpieczeństwa

Przy globalnym niedoborze kompetentnych specjalistów ds. cyberbezpieczeństwa nigdy nie było lepszego czasu na karierę - zwłaszcza, że niedobór wydaje się rosnąć wraz z upływem czasu. W wyniku niewystarczającej liczby specjalistów ds. cyberbezpieczeństwa do zaspokojenie popytu na osoby z odpowiednimi umiejętnościami, pakiety wynagrodzeń zdobyte przez specjalistów ds. cyberbezpieczeństwa należą do najlepszych wśród pracowników technologicznych. W tym rozdziale dowiesz się o niektórych rolach zawodowych w dziedzinie cyberbezpieczeństwa, potencjalnych ścieżkach kariery i certyfikatach.

Role zawodowe w cyberbezpieczeństwie

Specjaliści ds. cyberbezpieczeństwa mają szeroki zakres obowiązków, które różnią się znacznie w zależności od ich dokładnych ról, ale większość, jeśli nie wszyscy, ostatecznie pracuje, aby pomóc albo chronić dane i systemy przed naruszeniem, albo, w przypadku niektórych stanowisk rządowych, naruszać systemy i ujawniać dane adwersarzy. Nie ma jednej ścieżki kariery zwanej „cyberbezpieczeństwem". Zawód ma wiele niuansów i różne ścieżki, którymi mogą się kierować kariery ludzi

Inżynier bezpieczeństwa

Istnieje wiele rodzajów inżynierów ds. bezpieczeństwa, ale zdecydowana większość to wykwalifikowani technicy, którzy budują, konserwują i debugują systemy bezpieczeństwa informacji w ramach projektów organizacyjnych (korporacyjnych, rządowych lub non-profit). Inżynierowie ds. Bezpieczeństwa pracujący w specjalistycznych oddziałach dostawców mogą również pomóc zapewnić, że oprogramowanie wdrażane u klientów odbywa się w bezpieczny sposób.

Menadżer ochrony

Menedżerowie ds. Bezpieczeństwa to zazwyczaj kierownictwo średniego szczebla w większych przedsiębiorstwach, które jest odpowiedzialne za określony obszar bezpieczeństwa informacji. Na przykład jeden menedżer ds. Bezpieczeństwa może być odpowiedzialny za całe szkolenie firmy w zakresie bezpieczeństwa, a inny może być odpowiedzialny za nadzorowanie wszystkich zapór sieciowych połączonych z Internetem. Osoby na stanowiskach kierowników ds. Bezpieczeństwa zazwyczaj wykonują mniej praktycznych, technicznie szczegółowych czynności związanych z bezpieczeństwem niż osoby, które im podlegają.

Dyrektor ds. Bezpieczeństwa

Dyrektorzy bezpieczeństwa to ludzie, którzy nadzorują bezpieczeństwo informacji w organizacji. W mniejszych firmach dyrektor jest zazwyczaj de facto szefem ochrony informacji (CISO). Większe firmy mogą mieć kilku dyrektorów odpowiedzialnych za różne podzbiory programu bezpieczeństwa informacji firmy; tacy ludzie z kolei zwykle zgłaszają się do CISO.

Główny Specjalista ds. Bezpieczeństwa informacji (CISO)

CISO jest osobą odpowiedzialną za bezpieczeństwo informacji w całej organizacji. Można myśleć o roli CISO jako szefa sztabu wojskowego wojska obronnego organizacji. CISO to stanowisko kierownicze wyższego szczebla. Pełnienie funkcji CISO zwykle wymaga dużej wiedzy i doświadczenia w zarządzaniu, a także zrozumienia kwestii bezpieczeństwa informacji.

Analityk bezpieczeństwa

Analitycy bezpieczeństwa pracują nad zapobieganiem naruszeniom bezpieczeństwa informacji. Dokonują przeglądu nie tylko istniejących systemów, ale także analizują pojawiające się zagrożenia, nowe luki i tak dalej, aby zapewnić, że organizacja pozostaje bezpieczna.

Architekt bezpieczeństwa

Architekci bezpieczeństwa projektują i nadzorują wdrażanie organizacyjnych środków ochrony informacji. Często muszą rozumieć, projektować i testować złożone infrastruktury bezpieczeństwa i regularnie służyć jako członek zespołu ds. Bezpieczeństwa, który jest również zaangażowany w projekty poza działem bezpieczeństwa - na przykład pomagając w projektowaniu zabezpieczeń potrzebnych do niestandardowej aplikacji, którą organizacja projektuje i buduje lub pomaga w prowadzeniu ludzi pracujących w sieci, podczas gdy ci drudzy projektują różne elementy korporacyjnej infrastruktury sieciowej IT.

Administrator bezpieczeństwa

Administratorzy zabezpieczeń to praktyczni ludzie, którzy w imieniu organizacji instalują, konfigurują, obsługują, zarządzają i rozwiązują problemy z zabezpieczeniami informacji. To ci ludzie to osoby, do których często odnoszą się nietechniczni specjaliści, gdy mówią „Mam problem i muszę zadzwonić do ochroniarza lub specjalisty ds. Ochrony".

Audytor bezpieczeństwa

Audytorzy bezpieczeństwa przeprowadzają audyty bezpieczeństwa - to znaczy sprawdzają, czy zasady bezpieczeństwa, procedury, technologie itp. Działają zgodnie z zamierzeniami oraz czy skutecznie i odpowiednio chronią firmowe dane, systemy i sieci.

Kryptograf

Kryptografowie są ekspertami w dziedzinie szyfrowania używanego do ochrony poufnych danych i pracują z nim. Niektórzy kryptolodzy pracują nad opracowaniem systemów szyfrowania w celu ochrony poufnych danych, podczas gdy inni, znani jako kryptoanalitycy, robią odwrotnie: analizują zaszyfrowane informacje i systemy szyfrowania w celu złamania szyfrowania i odszyfrowania informacji. W porównaniu do innych zawodów związanych z bezpieczeństwem informacji kryptolodzy nieproporcjonalnie pracują dla agencji rządowych, wojska i środowisk akademickich. W Stanach Zjednoczonych wiele rządowych stanowisk w kryptografii wymaga obywatelstwa USA i aktywnego poświadczenia bezpieczeństwa.

Analityk oceny podatności

Analitycy oceny podatności badają systemy komputerowe, bazy danych, sieci i inne części infrastruktury informacyjnej w poszukiwaniu potencjalnych luk. Osoby pracujące na takich stanowiskach muszą mieć na to wyraźne pozwolenie. W przeciwieństwie do testerów penetracji, opisanych w następnej sekcji, osoby oceniające podatność zazwyczaj nie działają jako osoby z zewnątrz próbujące włamać się do systemów, ale jako osoby z wewnątrz, które mają dostęp do systemów i mają możliwość ich szczegółowego zbadania od samego początku.

Hacker z zasadami

Etyczni hakerzy próbują atakować, penetrować i w inny sposób naruszać bezpieczeństwo systemów i sieci w imieniu - i za wyraźną zgodą - właścicieli technologii w celu wykrycia luk w zabezpieczeniach, które właściciele mogą następnie naprawić. Etyczni hakerzy są czasami nazywani testerami penetracji lub testerami penetracyjnymi. Podczas gdy wiele korporacji zatrudnia własnych etycznych hakerów,

znaczna liczba osób, które pracują na takich stanowiskach, pracuje dla firm konsultingowych oferujących swoje usługi stronom trzecim.

Badacz bezpieczeństwa

Badacze bezpieczeństwa to wybiegający w przyszłość ludzie, którzy chcą odkryć luki w istniejących systemach i potencjalne konsekwencje nowych technologii i innych produktów dla bezpieczeństwa. Czasami opracowują nowe modele i podejścia do bezpieczeństwa w oparciu o swoje badania. Jeśli chodzi o etykę, to w większości jurysdykcji badacz bezpieczeństwa, który włamuje się do organizacji bez wyraźnej zgody tej organizacji, nie jest badaczem bezpieczeństwa ani etycznym hakerem, ale po prostu kimś, kto łamie prawo.

Ofensywny haker

Ofensywni hakerzy próbują włamać się do systemów przeciwników, aby uszkodzić je lub ukraść informacje. W Stanach Zjednoczonych nielegalne jest podejmowanie przez firmę ofensywy i atakowanie kogokolwiek - w tym atakowanie hakerów, którzy aktywnie próbują spenetrować organizację. W związku z tym wszystkie obraźliwe legalne prace hakerskie w Stanach Zjednoczonych są stanowiskami rządowymi, na przykład w agencjach wywiadowczych. Jeśli lubisz atakować i nie satysfakcjonuje Cię tylko etyczne hakowanie, możesz chcieć rozpocząć karierę w rządzie lub wojsku. Wiele ofensywnych pozycji hakerskich wymaga odpraw bezpieczeństwa.

Inżynier bezpieczeństwa oprogramowania

Inżynierowie ds. Bezpieczeństwa oprogramowania integrują zabezpieczenia z oprogramowaniem podczas jego projektowania i opracowywania. Testują również oprogramowanie, aby upewnić się, że nie ma w nim luk. W niektórych przypadkach mogą to być kodery samego oprogramowania.

Audytor bezpieczeństwa kodu źródłowego oprogramowania

Audytorzy bezpieczeństwa kodu źródłowego oprogramowania przeglądają kod źródłowy programów w poszukiwaniu błędów programistycznych, luk w zabezpieczeniach, naruszeń zasad i standardów korporacyjnych, problemów regulacyjnych, naruszeń praw autorskich (i, w niektórych przypadkach, naruszeń patentów) i innych kwestii, które muszą być, lub powinien zostać rozwiązany.

Menedżer bezpieczeństwa oprogramowania

Menadżerowie ds. Rozwoju Bezpieczeństwa nadzorują bezpieczeństwo oprogramowania przez cały cykl jego życia - od zebrania wstępnych wymagań biznesowych, aż po ich utylizację.

Konsultant ds. Bezpieczeństwa

Istnieje wiele różnych typów konsultantów ds. Bezpieczeństwa. Niektórzy, doradzają dyrektorom korporacji w zakresie strategii bezpieczeństwa, pełnią rolę ekspertów lub pomagają firmom ochroniarskim rozwijać się i odnosić sukcesy. Inni są praktycznymi testerami penetracji. Inni mogą projektować lub obsługiwać elementy infrastruktury bezpieczeństwa, koncentrując się na określonych technologiach. Jeśli chodzi o doradztwo w zakresie bezpieczeństwa, możesz znaleźć stanowiska w prawie każdym obszarze bezpieczeństwa informacji.

Specjalista ds. Bezpieczeństwa

Tytułowy specjalista ds. Bezpieczeństwa jest używany w odniesieniu do osób pełniących różne rodzaje ról. Wszystkie różne role wymagają jednak co najmniej kilkuletniego doświadczenia zawodowego w dziedzinie bezpieczeństwa informacji.

Członek zespołu reagowania na incydenty

Zespół reagowania na incydenty składa się de facto z pierwszych ratowników, którzy zajmują się incydentami bezpieczeństwa. Członkowie zespołu starają się powstrzymać i wyeliminować ataki, jednocześnie minimalizując wynikające z nich obrażenia. Często też przeprowadzają analizę tego, co się stało - czasami stwierdzając, że nic nie wymaga żadnych działań naprawczych. Możesz myśleć o reagujących na incydenty jako o odpowiedniku strażaków z cyberbezpieczeństwa - radzą sobie z niebezpiecznymi atakami, ale czasami są wzywani, aby sprawdzić, czy nie ma pożaru.

Analityk kryminalistyczny

Analitycy kryminalistyczni są faktycznie cyfrowymi detektywami, którzy po jakimś zdarzeniu komputerowym badają dane, komputery i urządzenia komputerowe oraz sieci w celu gromadzenia, analizowania i właściwego przechowywania dowodów oraz wywnioskowania, co dokładnie się wydarzyło, jak to się stało i kto zrobił to. Możesz myśleć o analitykach sądowych jako z grubsza odpowiedniku inspektorów organów ścigania i firm ubezpieczeniowych, którzy analizują nieruchomości po pożarze, aby ustalić, co się stało i kto może być za to odpowiedzialny.

Ekspert ds. Regulacji Cyberbezpieczeństwa

Eksperci w zakresie przepisów dotyczących cyberbezpieczeństwa posiadają wiedzę na temat różnych przepisów związanych z cyberbezpieczeństwem i pomagają zapewnić, że organizacje przestrzegają tych przepisów. Często, choć nie zawsze, są to prawnicy, którzy mają wcześniejsze doświadczenie w pracy z różnymi sprawami dotyczącymi zgodności.

Ekspert ds. Regulacji Prywatności

Eksperci w zakresie przepisów dotyczących prywatności mają wiedzę na temat różnych przepisów związanych z prywatnością i pomagają zapewnić przestrzeganie tych przepisów przez organizacje. Często, choć nie zawsze, są to prawnicy, którzy mają wcześniejsze doświadczenie w pracy z różnymi sprawami dotyczącymi zgodności.

Odkrywanie ścieżek kariery

Osoby zajmujące się bezpieczeństwem informacji mogą podążać różnymi ścieżkami kariery. Niektóre wymagają zostania technicznymi guru skoncentrowanymi na określonych podsekcjach bezpieczeństwa, podczas gdy inne wymagają szerokiej wiedzy z tej dyscypliny i interakcji z wieloma różnymi obszarami biznesu. Jeszcze inni koncentrują się na zarządzaniu. Planując karierę, ludzie powinni brać pod uwagę swoje długoterminowe cele. Na przykład, jeśli chcesz zostać CISO, możesz chcieć pracować na różnych praktycznych stanowiskach, zdobyć tytuł MBA i ubiegać się o awanse i certyfikaty w obszarach zarządzania bezpieczeństwem informacji, a jeśli chcesz zostać starszy architekt, prawdopodobnie lepiej będzie ci skupić się na awansach na różne stanowiska związane z analizą i projektowaniem bezpieczeństwa, przeprowadzaniem testów penetracyjnych i zdobywaniem stopni technicznych. W poniższych sekcjach podano przykłady niektórych potencjalnych ścieżek kariery.

Ścieżka kariery: starszy architekt ds. Bezpieczeństwa W Stanach Zjednoczonych architekci ds. Bezpieczeństwa zazwyczaj zarabiają znacznie ponad 100 000 USD - a na niektórych rynkach znacznie więcej - co czyni tego typu stanowisko dość atrakcyjnym. Chociaż ścieżka kariery każdej osoby jest wyjątkowa, typowym sposobem zostania starszym architektem bezpieczeństwa może być podążanie ścieżką kariery podobną do poniższej:

1. Wykonaj jedną z następujących czynności: Zdobądź tytuł licencjata w dziedzinie informatyki. Zdobądź dyplom w dowolnej dziedzinie i zdaj certyfikat na poziomie podstawowym egzamin z cyberbezpieczeństwa (na przykład Bezpieczeństwo +). Zdobądź pracę techniczną bez dyplomu i wykaż się biegłością w zakresie odpowiednich technologii używanych w ramach pracy.

2. Pracuj jako administrator sieci lub administrator systemów i zdobądź doświadczenie w zakresie bezpieczeństwa.

3. Uzyskaj nieco bardziej szczegółowe referencje (na przykład CEH).

4. Pracuj jako administrator bezpieczeństwa - najlepiej administrując szeregiem różnych systemów bezpieczeństwa przez okres kilku lat.

5. Zdobądź jeden lub więcej ogólnych certyfikatów bezpieczeństwa (na przykład CISSP).

6. Zostań architektem bezpieczeństwa i zdobądź doświadczenie w tej roli.

7. Zdobądź certyfikat zaawansowanej architektury zabezpieczeń (np. CISSP-ISSAP).

8. Zostań architektem bezpieczeństwa wyższego szczebla.

Nie spodziewaj się, że z dnia na dzień zostaniesz architektem wyższego szczebla; często osiągnięcie takiego stanowiska wymaga 10 lub więcej lat odpowiedniego doświadczenia.

Ścieżka kariery: CISO

W Stanach Zjednoczonych szefowie bezpieczeństwa informacji zazwyczaj zarabiają 150 000 USD lub więcej (dużo więcej w niektórych branżach), ale praca może być dość stresująca - CISO są odpowiedzialni za bezpieczeństwo informacji korporacyjnych - co często wiąże się z radzeniem sobie w sytuacjach awaryjnych. Chociaż ścieżka kariery każdej osoby jest wyjątkowa, typowym sposobem zostania CISO może być podążanie ścieżką kariery podobną do poniższej:

1. Zdobądź tytuł licencjata w dziedzinie informatyki lub technologii informacyjnej.

2. Wykonaj jedną z następujących czynności:

*Pracuj jako analityk systemowy, inżynier systemowy, programista lub na innym pokrewnym, praktycznym stanowisku technicznym.

*Pracuj jako inżynier sieci.

3. Przenieś się w kierunku bezpieczeństwa i pracuj jako inżynier bezpieczeństwa, analityk bezpieczeństwa lub konsultant ds. Bezpieczeństwa - przyjmując różne role w organizacji lub jako konsultant w organizacjach, w ten sposób narażając się na różne obszary bezpieczeństwa informacji.

4. Uzyskaj ogólne certyfikaty w zakresie bezpieczeństwa informacji (na przykład CISSP).

5. Przejdź w kierunku zarządzania bezpieczeństwem, stając się menadżerem zespołu ds. Bezpieczeństwa. Idealnie byłoby, gdyby z biegiem czasu zarządzać wieloma zespołami ds. Bezpieczeństwa informacji, z których każdy zajmuje się innymi obszarami bezpieczeństwa informacji niż pozostałe.

6. Wykonaj jedną z następujących czynności:

* Zdobądź tytuł magistra w dziedzinie cyberbezpieczeństwa (najlepiej ze szczególnym uwzględnieniem zarządzania bezpieczeństwem informacji).

* Zdobądź tytuł magistra informatyki (najlepiej z naciskiem na cyberbezpieczeństwo).

* Zdobądź tytuł magistra w zarządzaniu systemami informatycznymi (najlepiej z naciskiem na bezpieczeństwo informacji).

* Zdobądź MBA.

7. Wykonaj jedną z następujących czynności:

* Zostań CISO oddziału (de facto lub de iure).

* Zostań CISO stosunkowo małej firmy lub organizacji non-profit.

8. Uzyskaj zaawansowane poświadczenie bezpieczeństwa informacji dotyczące zarządzania bezpieczeństwem informacji (na przykład CISSP-ISSMP).

9. Zostań CISO większej firmy.

Droga do zostania CISO może z łatwością zająć dekadę, a nawet dziesięciolecia, w zależności od wielkości organizacji, w której CISO pracuje.

Zaczynamy od bezpieczeństwa informacji

Wiele osób zajmujących się bezpieczeństwem informacji rozpoczęło swoją karierę w innych obszarach technologii informacyjnej. W niektórych przypadkach ludzie po raz pierwszy zostali narażeni na niesamowity świat cyberbezpieczeństwa, pełniąc funkcje techniczne. W innych sytuacjach ludzie podejmowali prace techniczne niezwiązane bezpośrednio z bezpieczeństwem informacji, ale robili to z zamiarem rozwijania różnych umiejętności i wykorzystywania tych stanowisk jako odskoczni do świata bezpieczeństwa. Miejsca pracy w dziedzinie analizy ryzyka, inżynierii i rozwoju systemów oraz sieci są często dobrym punktem wyjścia. Na przykład administrator poczty e-mail prawdopodobnie dowie się wiele o bezpieczeństwie poczty e-mail, a być może także o architekturze bezpiecznych projektów sieci i ogólnie o zabezpieczaniu serwerów. Osoby opracowujące systemy internetowe prawdopodobnie dowiedzą się o bezpieczeństwie sieci, a także o projektowaniu bezpiecznego oprogramowania. Administratorzy systemów i sieci dowiedzą się o bezpieczeństwie elementów, za które są odpowiedzialni. Niektóre z zadań technicznych, które mogą pomóc w przygotowaniu się do ról związanych z cyberbezpieczeństwem, obejmują

*Programista

*Inżynier oprogramowania

*Web Developer

* Inżynier wsparcia systemów informacyjnych (specjalista ds. Wsparcia technicznego)

*Administrator systemów

* Administrator poczty e-mail

*Administrator sieci

*Administrator bazy danych

* Administrator serwisu

Niektóre stanowiska nietechniczne mogą również pomóc w przygotowaniu ludzi do kariery w nietechnicznych rolach bezpieczeństwa informacji. Oto kilka przykładów:

*Rewident księgowy

* Detektyw z organów ścigania

* Prawnik specjalizujący się w obszarach prawa związanych z cyberbezpieczeństwem

* Prawnik zajmujący się przestrzeganiem przepisów

* Prawnik zajmujący się dziedzinami prawa związanymi z prywatnością

* Analityk ds. Zarządzania ryzykiem

Odkrywanie popularnych certyfikatów

Uznane certyfikaty cyberbezpieczeństwa oraz, w mniejszym stopniu, certyfikaty potwierdzające pomyślne ukończenie kursów cyberbezpieczeństwa, mogą udowodnić pracodawcy, że Twoja wiedza na temat cyberbezpieczeństwa spełnia określone standardy i pomoże Ci przejść na pożądanej ścieżce kariery. Obecnie na rynku dostępnych jest wiele różnych certyfikatów bezpieczeństwa informacji. Niektóre koncentrują się na określonych technologiach lub obszarach bezpieczeństwa informacji, podczas gdy inne są szersze. Chociaż omówienie wszystkich dostępnych obecnie certyfikatów wykracza poza zakres tej książki, poniżej przedstawiono pięć najpopularniejszych - i lepiej rozpoznawalnych - certyfikatów niezależnych od dostawców, które mogą być idealne dla osób na stosunkowo wczesnym etapie kariery w dziedzinie cyberbezpieczeństwa.

CISSP

Certyfikat Certified Information Systems Security Professional (CISSP), wprowadzony po raz pierwszy w 1994 r., obejmuje szeroki zakres dziedzin związanych z bezpieczeństwem, w niektórych obszarach bardziej zagłębiając się w szczegóły. Zapewnia pracodawcom komfort, wiedząc, że pracownicy rozumieją ważne aspekty więcej niż jednego lub dwóch obszarów bezpieczeństwa informacji; Ponieważ elementy bezpieczeństwa informacji są często silnie ze sobą powiązane, szeroka wiedza jest cenna i staje się absolutnie niezbędna w miarę wspinania się po drabinie zarządzania bezpieczeństwem informacji. CISSP jest przeznaczony dla osób z kilkuletnim doświadczeniem w dziedzinie bezpieczeństwa informacji - w rzeczywistości, podczas gdy do egzaminu CISSP można przystąpić bez doświadczenia, to tak naprawdę uwierzytelnienie nie otrzyma się, dopóki nie podejmie się pracy w terenie na wymagane Liczba lat. W rezultacie osoby posiadające referencje CISSP, które zawsze mają za sobą kilkuletnie doświadczenie, często otrzymują wyższe pensje niż zarówno ich niecertyfikowani rówieśnicy, jak i koledzy posiadający inne certyfikaty. Poświadczenie CISSP, wydane przez wysoko cenioną organizację (ISC) 2, jest zarówno niezależne od dostawców, jak i bardziej wiecznie zielone niż wiele innych certyfikatów. Materiały szkoleniowe i kursy przygotowujące do egzaminu CISSP są powszechnie dostępne, a testy są przeprowadzane w większej liczbie lokalizacji i w większej liczbie terminów niż większość innych, jeśli nie wszystkie inne certyfikaty z zakresu cyberbezpieczeństwa. Dostępnych jest wiele dodatków do CISSP dla tych, którzy chcą wykazać się biegłością w zakresie architektury bezpieczeństwa informacji (CISSP-ISSAP), zarządzania (CISSPISSMP) i inżynierii (CISSP-ISSEP)

(ISC) 2 wymaga, aby posiadacze referencji CISSP wyrazili zgodę na przestrzeganie określonego Kodeksu Etycznego i aby prowadzili istotne działania w zakresie kształcenia ustawicznego w celu zachowania swoich poświadczeń, które muszą być odnawiane co trzy lata.

CISSP nie ma na celu testowania praktycznych umiejętności technicznych - i tego nie robi. Osoby, które chcą wykazać się biegłością w określonych technologiach lub obszarach technologii - na przykład testach penetracyjnych, administrowaniu bezpieczeństwem, audytach itp. - mogą chcieć rozważyć

uzyskanie bardziej skoncentrowanej technicznie, ogólnej certyfikacji lub niektórych konkretnych certyfikatów dotyczących produktów i umiejętności. (Aby uzyskać pełne informacje, autor tej książki posiada certyfikat CISSP, a także dwa dodatkowe poświadczenia - CISSP-ISSAP i CISSP-ISSMP - oraz jest autorem (ISC) 2 oficjalnego podręcznika do egzaminu CISSP-ISSMP).

CISM

Uznany certyfikat Certified Information Security Manager (CISM) wydany przez Stowarzyszenie Audytu i Kontroli Systemów Informacyjnych (ISACA) zyskał na popularności od czasu jego powstania nieco poniżej dwóch dekad temu. Pochodzące z organizacji zajmującej się audytem i kontrolami, poświadczenie CISM jest, ogólnie rzecz biorąc, nieco bardziej skoncentrowane niż CISSP na zasadach, procedurach i technologiach dla systemów zarządzania i kontroli bezpieczeństwa informacji , jak to zwykle ma miejsce w dużych przedsiębiorstwach lub organizacjach. Podobnie jak w przypadku CISSP, aby uzyskać CISM, kandydat musi mieć kilkuletnie doświadczenie zawodowe w zakresie bezpieczeństwa informacji. Pomimo różnic między CISSP i CISM - przy czym pierwsza zagłębia się w tematy techniczne, a druga robi podobnie w kwestiach związanych z zarządzaniem - obie oferty również w znacznym stopniu się pokrywają. Obie są szanowane.

CEH

Certyfikat Certified Ethical Hacker (CEH), oferowany przez International Council of E-Commerce Consultants (EC-Council), jest przeznaczony dla osób z co najmniej dwuletnim doświadczeniem zawodowym, które chcą udowodnić swoją wiarygodność jako etycznych hakerów (innymi słowy , testery penetracji). CEH to praktyczny egzamin, który sprawdza umiejętności kandydatów w zakresie hakowania: od przeprowadzania rozpoznania i penetrowania sieci po eskalację uprawnień i kradzież danych. Ten egzamin sprawdza różne umiejętności praktyczne, w tym pojazdy atakujące, takie jak różne rodzaje złośliwego oprogramowania; techniki ataku, takie jak wstrzyknięcie SQL; metody analizy kryptograficznej stosowane w celu osłabienia szyfrowania; metody inżynierii społecznej w celu osłabienia obrony technicznej poprzez błąd ludzki; i jak hakerzy mogą unikać wykrywania przez zatarcie śladów. EC-Council wymaga, aby posiadacze poświadczeń CEH zdobyli znaczną liczbę punktów z tytułu kształcenia ustawicznego, aby zachować poświadczenie CEH - coś bardzo ważnego w przypadku egzaminu sprawdzającego wiedzę praktyczną - zwłaszcza jeśli weźmie się pod uwagę, jak szybko zmieniają się technologie w dzisiejszym świecie.

Seurity +

Security + to niezależny od dostawcy ogólny certyfikat cyberbezpieczeństwa, który może być cenny zwłaszcza dla osób na wczesnym etapie kariery. Jest oferowany i administrowany przez szanowaną organizację non-profit zajmującą się edukacją techniczną, CompTIA. Chociaż technicznie rzecz biorąc, nie ma minimalnej liczby lat doświadczenia zawodowego wymaganej do uzyskania tytułu CompTIA Security +, z praktycznego punktu widzenia większości ludzi prawdopodobnie łatwiej będzie zdać egzamin po pracy w terenie i zdobyciu praktycznej wiedzy. doświadczenie przez rok lub dwa. Egzamin Security + zazwyczaj zawiera bardziej szczegółowe informacje techniczne niż CISSP lub CISM, bezpośrednio odnosząc się do wiedzy potrzebnej do pełnienia ról, takich jak te związane z audytem IT na poziomie podstawowym, testami penetracyjnymi, administracją systemami, administracją siecią i administracją bezpieczeństwa; stąd CompTIA Security + to dobry początek kariery certyfikacji dla wielu osób. Każdy, kto zdobędzie tytuł Security + od 2011 r., Musi zdobyć punkty za kontynuację edukacji, aby zachować poświadczenie.

GSEC

Global Information Assurance Certification Security Essentials Certification (GSEC) to podstawowy certyfikat bezpieczeństwa obejmujący materiały na kursach prowadzonych przez SANS Institute, szanowaną firmę szkoleniową z zakresu bezpieczeństwa informacji. Podobnie jak Security +, GSEC zawiera o wiele więcej praktycznych materiałów praktycznych niż certyfikaty CISM lub CISSP, dzięki czemu certyfikat ten jest cenniejszy niż wyżej wymienione alternatywy w niektórych scenariuszach i mniej pożądany w innych. Pomimo tego, że egzamin GSEC jest sprzedawany jako podstawowy, ogólnie rzecz biorąc, jest uważany za trudniejszy i bardziej wszechstronny niż test wymagany do uzyskania oznaczenia Security +. Wszyscy posiadacze referencji GSEC muszą wykazywać ciągłe doświadczenie zawodowe lub rozwój edukacyjny w dziedzinie bezpieczeństwa informacji, aby zachować swoje referencje.

Sprawdzalność

Wydawcy wszystkich głównych poświadczeń bezpieczeństwa informacji zapewniają pracodawcom możliwość sprawdzenia, czy dana osoba posiada jakiekolwiek poświadczenia. Ze względów bezpieczeństwa taka weryfikacja może wymagać znajomości numeru identyfikacyjnego certyfikatu użytkownika, którego posiadacze danych uwierzytelniających zwykle nie publikują.

Jeśli zdobędziesz certyfikat, pamiętaj o aktualizowaniu informacji w bazie danych wydawcy. Nie chcesz stracić certyfikatu, ponieważ nie otrzymałeś przypomnienia o przedłożeniu punktów za kontynuację edukacji lub uiszczeniu opłaty za utrzymanie.

Etyka

Wiele certyfikatów bezpieczeństwa wymaga, aby posiadacze poświadczeń przestrzegali kodeksu etycznego, który nie tylko nakazuje posiadaczom przestrzeganie wszystkich odpowiednich praw i przepisów rządowych, ale także nakazuje ludziom działać właściwie, nawet w sposób wykraczający poza literę prawa. Pamiętaj, aby zrozumieć takie wymagania. Utrata referencji z powodu nieetycznego zachowania może oczywiście poważnie podważyć zaufanie, jakim inni ludzie darzą osobę, i może mieć różnego rodzaju negatywne konsekwencje dla Twojej kariery w dziedzinie bezpieczeństwa informacji.

Pokonywanie rejestru karnego

Chociaż rejestr karny nie uniemożliwia komuś uzyskania wielu stanowisk związanych z cyberbezpieczeństwem, to rejestr karny może stanowić barierę nie do pokonania, jeśli chodzi o uzyskanie określonych stanowisk. Na przykład wszystko, co uniemożliwia komuś uzyskanie poświadczenia bezpieczeństwa, mogłoby zdyskwalifikować tę osobę z wykonywania pewnych funkcji rządowych i wykonawców rządowych. W niektórych przypadkach charakter, czas i wiek popełnienia przestępstw z przeszłości mogą mieć duże znaczenie dla decyzji pracodawcy. Pewne bezpieczeństwo informacji organizacje mogą być w porządku z zatrudnieniem zreformowanego, byłego, na przykład nastoletniego hakera, ale może mieć niechęć do zatrudniania osoby, która jako osoba dorosła została skazana za brutalne przestępstwo. Podobnie osoba, która odbyła karę w więzieniu za przestępstwo komputerowe, które popełnił dwie dekady temu, ale której przeszłość została od tego czasu czysta, może być postrzegana przez potencjalnego pracodawcę zupełnie inaczej niż osoba niedawno zwolniona z więzienia po odbyciu kary. wyrok za podobne przestępstwo.

Spojrzenie na inne zawody z naciskiem na cyberbezpieczeństwo

Oprócz bezpośredniej pracy w dziedzinie cyberbezpieczeństwa istnieje wiele możliwości pracy w dziedzinach, które łączą się bezpośrednio ze specjalistami ds. cyberbezpieczeństwa i które czerpią korzyści z globalnego wzrostu zainteresowania cyberbezpieczeństwem. Prawnicy mogą na przykład zdecydować się na specjalizację w przepisach związanych z cyberbezpieczeństwem lub przestrzeganiu

przez firmy przepisów dotyczących prywatności, a pracownicy organów ścigania mogą zdobyć wiedzę z zakresu kryminalistyki wykorzystywanej do prowadzenia dochodzeń w sprawie cyberprzestępczości. Najważniejsze jest to, że cyberbezpieczeństwo stworzyło, tworzy i nadal będzie stwarzać w dającej się przewidzieć przyszłości wiele lukratywnych możliwości zawodowych dla ludzi z wielu dziedzin. Nie musisz być geniuszem technicznym, aby czerpać korzyści z rozkwitu tej dyscypliny. Jeśli uważasz, że cyberbezpieczeństwo jest fascynujące, możesz zechcieć zbadać możliwości, które może ci zaoferować