Opracowanie eksperckie dotyczące zawodów przyszłości związanych z branżą motoryzacyjną w następującym obszarze tematycznym:

Cyberbezpieczeństwo

Rozwój nowych technologii w motoryzacji jest oparty głównie na automatyzacji, cyfryzacji i stosowaniu zaawansowanych systemów informatycznych. Oprogramowanie stało się najważniejszą częścią pojazdów bez którego samochód nie jest zdolny do użytku. Mimo wielkiemu postępowi, który się dokonuje w motoryzacji dzięki digitalizacji pojawiły się również zagrożenia związane z cyberbezpieczenstwem. Może to być szczególnie niebezpieczne w razie przejęcia kontroli nad oprogramowaniem samochodu, ale nie tylko. Ingerencja przestępców cybernetycznych w systemy zarządzania produkcja lub logistykę mogą spowodować paraliż i wielomilionowe straty. Często dochodzi do żądań okupu ze strony cyber agresorów. To wszystko powoduje konieczność wzmacniania roli cyberbezpieczenstwa w motoryzacji i tworzenie nowych zawodów z tym związanych które potrafią ustrzec firmy przed atakiem i usprawnić oraz zabezpieczyć działające systemy. Badania wskazują ze 89% firm z obszaru motoryzacji doświadczyło już ataku cybernetycznego i będzie rozwija obszar cyberbezpieczenstwa.

Jakie nowe stanowiska trzeba tworzyć lub rozwijać, żeby móc nie tylko szybko reagować, ale także aby zabezpieczyć się przed potencjalnymi cyber katastrofami i chronić dane poufne organizacji:

*** Inżynier cyberbezpieczeństwa:**

Specjaliści ci będą nadal bardzo poszukiwani, ponieważ są odpowiedzialni za monitorowanie sieci, analizowanie luk w zabezpieczeniach i wdrażanie środków w celu ochrony przed zagrożeniami cybernetycznymi.
Inżynier cyberbezpieczeństwa buduje systemy bezpieczeństwa informacji i architektury IT oraz chroni je przed nieautoryzowanym dostępem i cyberatakami. Inżynierowie ds.

cyberbezpieczeństwa opracowują i egzekwują plany bezpieczeństwa, standardy, protokoły i najlepsze praktyki, a także opracowują plany awaryjne, aby szybko rozpocząć pracę w przypadku katastrofy.

*** Analityk cyberbezpieczeństwa:**

Rola analityka bezpieczeństwa jest dość szeroka i może obejmować wiele obowiązków, takich jak monitorowanie najlepszych praktyk bezpieczeństwa, protokołów i procedur za pomocą odpowiednich narzędzi oraz zapewnianie, że praktyki są odpowiednio wdrażane i przestrzegane. Analityk analizuje raporty z tych narzędzi, aby proaktywnie identyfikować nietypowe lub nietypowe zachowania w sieci. Powinien również kontrolować dostęp do plików i poświadczenia, aktualizacje sieci i konserwację zapory.

Dobrze wyszkolony analityk bezpieczeństwa będzie miał wiedzę na temat przechowywania i zarządzania danymi oraz różnych rodzajów zagrożeń cyberbezpieczeństwa, w tym ataków typu ransomware, inżynierii społecznej i kradzieży danych. Może przeprowadzać testy penetracyjne i skanowanie luk w zabezpieczeniach oraz zalecać odpowiednie zmiany w celu poprawy bezpieczeństwa.

W dużych firmach analitycy bezpieczeństwa mogą pracować w centrum operacji bezpieczeństwa, aby monitorować, wykrywać, powstrzymywać i usuwać zagrożenia. W średnich i mniejszych organizacjach analitycy bezpieczeństwa mogą odgrywać szeroką rolę, zajmując się wszystkim, od analizy bezpieczeństwa i wykrywania włamań po konserwację zapory ogniowej, aktualizacje programów antywirusowych i aktualizacje poprawek. Ponieważ mają doświadczenie w zakresie zagrożeń bezpieczeństwa i najlepszych praktyk, mogą również szkolić pracowników w zakresie cyberbezpieczeństwa.

*** Etyczny haker:**

Etyczni hakerzy, czyli pracownicy atakujący systemy i zasoby cyfrowe własnej firmy celem testowania bezpieczeństwa systemów, próbując wykorzystać luki w zabezpieczeniach w

kontrolowany sposób. Dzięki temu pomagają przedsiębiorstwom zidentyfikować słabe punkty, zanim złośliwi hakerzy będą mogli je wykorzystać. Ponieważ często pracują nad wysoce poufnymi i wrażliwymi na czas projektami, etyczni hakerzy powinni być godni zaufania i zdolni tolerować wysoki poziom stresu i niepewności. Powinni również być kreatywni i wysoce zorganizowani, aby skutecznie rejestrować i śledzić swoje projekty. Co najważniejsze, muszą stale aktualizować swoją wiedzę, umiejętności i techniki, aby zapobiegać działaniom cyberprzestępców oraz pomagać w obsłudze incydentów i analizie kryminalistycznej w celu poprawy stanu bezpieczeństwa organizacji.

*** Architekt Bezpieczeństwa Sieci / Struktury Bezpieczeństwa Cyfrowego:**

Architekci bezpieczeństwa projektują i wdrażają bezpieczne systemy i sieci. Opracowują strategie ochrony danych i zapewniają, że środki bezpieczeństwa są zintegrowane z każdym aspektem infrastruktury organizacji. Architekt bezpieczeństwa sieci odgrywa kluczową rolę w zwiększaniu siły bezpieczeństwa architektury korporacyjnej, przy jednoczesnym utrzymaniu produktywności, wydajności, dostępności i wydajności sieci. Architekci bezpieczeństwa sieciowego pomagają przekładać potrzeby biznesowe na funkcjonalne systemy, definiować odpowiednie zasady i procedury dla tych systemów, pomagają szkolić użytkowników i administratorów. Zwracają również uwagę na ograniczenia budżetowe i operacyjne. Właśnie dlatego umiejętności menedżerskie są ważnymi umiejętnościami, które należy posiadać w tej roli.

Aby zapewnić ciągłe bezpieczeństwo w całym cyklu życia sieci, architekci bezpieczeństwa sieci podejmują środki obronne, takie jak konfiguracja zapory i oprogramowania antywirusowego, oraz środki ofensywne, takie jak testy penetracyjne. Nadzorują również zmiany w sieci, aby zminimalizować ryzyko dla organizacji. Oczekuje się od nich zaawansowanej wiedzy na temat różnych narzędzi i technik bezpieczeństwa związanych z zaporami ogniowymi, testami penetracyjnymi i reagowaniem na incydenty. Muszą także być świadomi wymagań sieciowych systemów komputerowych, w tym routingu, przełączania i

domen zaufania, a także najlepszych praktyk w zakresie bezpieczeństwa, technologii i ram zgodnych ze standardami branżowymi.

Przeprowadzają analizy sieci i systemów, aby zidentyfikować i wybrać najlepsze mechanizmy kontrolne dla wymaganego poziomu bezpieczeństwa. Muszą być świadomi różnych mechanizmów kontroli dostępu, w tym kontroli dostępu opartej na rolach, obowiązkowej kontroli dostępu i uznaniowej kontroli dostępu.

*** Inspektor ochrony danych – koordynator danych cyfrowych i analogowych:**

Zawód znany już szeroko obecnie nabierze nowego znaczenia i będzie wymagał umiejętności informatycznych. Wraz ze wzrostem znaczenia przepisów o ochronie danych, takich jak RODO i CCPA, inspektorzy ochrony danych odgrywają kluczową rolę w zapewnianiu, że organizacje przestrzegają przepisów i zarządzają danymi w sposób szanujący prywatność użytkowników. Będzie to coraz bardziej skomplikowane, gdyż zdigitalizowane systemy przedsiębiorstw w tym HR są atrakcyjne dla potencjalnych złodziei danych osobowych.

*** Specjalista ds. Reagowanie na incydenty:**

Ta funkcja jest odpowiedzialna za zarządzanie skutkami cyberataku i łagodzenie ich. Specjalista bada incydenty związane z bezpieczeństwem, analizują ich wpływ i pracują nad zminimalizowaniem szkód. Ten zawód jest reaktywny, ale wobec wzrastającej liczby cyberataków przez najbliższe lata będzie nieodzowny.

*** Inżynier automatyzacji zabezpieczeń:**

Ponieważ zagrożenia cyberbezpieczeństwa stają się coraz bardziej złożone i częste, automatyzacja będzie odgrywać kluczową rolę w zarządzaniu tymi zagrożeniami i reagowaniu na nie. Inżynierowie automatyzacji zabezpieczeń projektują i wdrażają zautomatyzowane rozwiązania do wykrywania, analizowania i reagowania na incydenty związane z bezpieczeństwem.

*** Architekt Bezpieczeństwa Chmury:**

Wraz z rosnącą popularnością chmury obliczeniowej architekci bezpieczeństwa chmury projektują i wdrażają środki bezpieczeństwa specyficzne dla środowisk chmurowych, zapewniając ochronę danych i aplikacji w zwirtualizowanych ustawieniach.

*** Ekspert Bezpieczeństwa Łańcucha Bloków (Blockchain Security Expert):**

Technologia blockchain jest wykorzystywana w różnych branżach, a specjaliści w tej dziedzinie koncentrują się na zabezpieczaniu rozproszonych baz danych i zapewnianiu integralności transakcji.

*** Konsultant / doradca ds. Bezpieczeństwa cybernetycznego:**

Organizacje będą nadal poszukiwać wiedzy konsultantów ds. Bezpieczeństwa cybernetycznego, którzy mogą ocenić ich stan bezpieczeństwa, przedstawić zalecenia i opracować dostosowane strategie bezpieczeństwa.

*** Specjalista ds. bezpieczeństwa sztucznej inteligencji i uczenia maszynowego:**

Ponieważ technologie sztucznej inteligencji i uczenia maszynowego stają się coraz bardziej powszechne, specjaliści w tej dziedzinie skoncentrują się na opracowywaniu środków bezpieczeństwa w celu ochrony modeli sztucznej inteligencji przed atakami i zapewnienia etycznego wykorzystania sztucznej inteligencji w cyberbezpieczeństwie.

*** Trener/Coach w zakresie cyberbezpieczeństwa**:

W związku z ciągłym zapotrzebowaniem na wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, edukatorzy i szkoleniowcy będą odgrywać istotną rolę w przygotowywaniu kolejnego pokolenia ekspertów.

*** Analityk złośliwego oprogramowania:**

Typy i możliwości złośliwego oprogramowania stale ewoluują, dlatego coraz więcej organizacji pada ofiarą tego zagrożenia. Wiele firm stara się nadążyć za nowymi i pojawiającymi się formami złośliwego oprogramowania, które szybko się rozprzestrzeniają i są trudne do wykrycia.

Właśnie dlatego zapotrzebowanie na analityków złośliwego oprogramowania rośnie bardzo szybko. Analityk złośliwego oprogramowania identyfikuje i bada zagrożenia związane ze złośliwym oprogramowaniem. Analizują również incydenty związane ze złośliwym oprogramowaniem, które już miały miejsce. Ich celem jest zrozumienie natury takich zagrożeń i ataków.

Ponieważ analitycy złośliwego oprogramowania muszą rozumieć zarówno kod, jak i zagrożenia, muszą łączyć umiejętności zarówno inżynierów bezpieczeństwa, jak i programistów. Kompetentny analityk złośliwego oprogramowania musi również posiadać silne umiejętności w zakresie kryminalistyki cyfrowej, wiedzieć, jak korzystać z narzędzi do debugowania, a także znać najnowocześniejsze techniki ataków i metody zapobiegania atakom.

Podsumownie

Oczywiście nowe stanowiska pracy powiązane z Cyberbezpieczenstwem w branży motoryzacyjnej będą zależeć zarówno od wielkości firmy jak i od stopnia automatyzacji i cyfryzacji. Niektóre z przytoczonych powyżej zawodów nieco się pokrywają w zakresie obowiązków, ale w małej lub średniej firmie jeden inżynier ds. cyberbezpieczeństwa może wystarczyć a w firmach dużych czy globalnych korporacjach musi powstać silny zespół dbający o cyberbezpieczenstwo składający się z wielu specjalistów.

To tylko kilka przykładów z wielu potencjalnych nowych zawodów w cyberbezpieczeństwie. Wraz z rozwojem technologii, pojawianiem się nowych zagrożeń i zmianami przepisów, dziedzina będzie się nadal dostosowywać, tworząc nowe możliwości dla profesjonalistów, aby przyczynić się do bezpieczeństwa systemów cyfrowych i danych.

Autor opracowania:
Andrzej Korpak
Wrzesień, 2023 r.

Źródła i Literatura:

Raport World Economic Forum WEF_Future_of_Jobs_2023
(Raport przedstawiony na Światowym Forum Ekonomicznym dot. przyszłości pracy_2023 r. – tłumacz tekstu Andrzej Korpak),
Rahul Awati Techtarget.com – „Osiem najbardziej poszukiwanych miejsc pracy w dziedzinie cyberbezpieczeństwa w 2023 r. i później”
Internet – Google, Chat GPT
Doświadczenia własne z pracy w GM, Isuzu, PSA, Stellantis.