Nowe technologie niosą ze sobą nowe zagrożenia

Świat przeszedł radykalną przemianę w ostatnich dziesięcioleciach, w wyniku dodania korzyści z cyfrowej mocy obliczeniowej do niemal każdego aspektu ludzkiego życia. W ciągu zaledwie jednego pokolenia zachodnie społeczeństwo ewoluowało od jednozadaniowych kamer filmowych, kserokopiarek, telewizji przemysłowej i odbiorników muzycznych opartych na falach radiowych do podłączonych urządzeń posiadających funkcje wszystkich tych urządzeń i wielu innych - wszystko w jednym. pojedyncze urządzenie. Jednocześnie pojawiły się nowe, zaawansowane modele technologii komputerowych, stwarzające olbrzymi potencjał do jeszcze większego wykorzystania technologii w codziennym życiu. Oferty, które jeszcze kilka lat temu byłyby uważane za nierealne science fiction, stały się dziś tak całkowicie normalne i wszechobecne, że dzieci nie zawsze wierzą dorosłym, kiedy ci ostatni wyjaśniają, jak to zrobić w ostatnich latach wiele się zmieniło. Jednak wraz z pojawieniem się nowych technologii i cyfrowej transformacji ludzkiego doświadczenia wiąże się również duże zagrożenie bezpieczeństwa informacji. W tym rozdziale poznasz technologie, które szybko zmieniają świat i ich wpływ na cyberbezpieczeństwo. Ta lista pojawiających się technologii nie są bynajmniej wszechstronne. Technologie stale ewoluują i dlatego stale tworzą nowe wyzwania bezpieczeństwa informacji

Poleganie na Internecie przedmiotów

Jeszcze nie tak dawno jedynymi urządzeniami podłączonymi do internetu były klasyczne komputery - komputery stacjonarne, laptopy i serwery. Dziś jest jednak inny świat.

Od smartfonów i kamer monitorujących po ekspresy do kawy i sprzęt do ćwiczeń - urządzenia elektroniczne wszelkiego rodzaju mają teraz wbudowane komputery, a wiele z tych komputerów jest stale i bez przerwy połączonych z Internetem. Internet rzeczy (IoT), jako powszechnie znany ekosystem połączonych urządzeń, rozwijał się wykładniczo w ciągu ostatnich kilku lat. I, jak na ironię, konsumenci widzą wiele takich połączonych urządzeń , sprzedawane im w sklepach i Internecie, zdecydowana większość urządzeń IoT to w rzeczywistości elementy systemów komercyjnych i przemysłowych. W rzeczywistości niektórzy eksperci uważają nawet, że aż 99 procent podłączonych nietradycyjnych urządzeń komputerowych żyje w środowiskach komercyjnych i przemysłowych. Niezawodność zakładów użyteczności publicznej, fabryk i innych zakładów produkcyjnych, szpitali i większości innych elementów kręgosłupa dzisiejszej egzystencji gospodarczej i społecznej w dużej mierze zależy od stabilnej i bezpiecznej technologii. Oczywiście wszystkie urządzenia komputerowe - czy to klasyczne komputery, czy inteligentne urządzenia innego typu - mogą cierpieć na luki i są potencjalnie hakowalne i nadające się do wykorzystania w nikczemnych celach. Na przykład kamery połączone z Internetem, które są zaprojektowane tak, aby umożliwić ludziom oglądanie domów lub firm z daleka, mogą potencjalnie pozwolić nieautoryzowanym hakerom na oglądanie tych samych kanałów wideo. Ponadto takie urządzenia można zarekwirować w celu ataków na inne urządzenia. W rzeczywistości w październiku 2016 r. Atak Mirai Botnet wykorzystał jednocześnie wiele zainfekowanych urządzeń IoT i spowodował wyłączenie popularnej usługi Dyn DNS. DNS to system, który konwertuje ludzkie nazwy komputerów na zrozumiałe dla maszyn adresy numeryczne protokołu internetowego (adresy IP). W wyniku ataku na Dyn wiele znanych witryn i usług, w tym Twitter, Netflix, GitHub i Reddit, doznało de facto awarii, ponieważ ludzie nie mogli dotrzeć do witryn, ponieważ nazwy w adresach URL witryn nie mogły być przetłumaczone na ich właściwe adresy internetowe. Podobnie IoT stwarza ogromny potencjał do poważnego sabotażu. Rozważ możliwe skutki włamania do systemu przemysłowego związanego z produkcją niektórych urządzeń medycznych. Czy ludzie mogliby umrzeć, gdyby błędy lub backdoory zostały wstawione do kodu działającego na komputerze wbudowanym w urządzenie, a następnie wykorzystane, gdy urządzenie było używane? Hacki podważające systemy kontrolowane przez podłączone urządzenia są możliwe - nawet wtedy, gdy takie systemy nie są podłączone do

publicznego Internetu. Czy widziałeś hakerów żądających okupu w zamian za niewypuszczenie materiału wideo z kamer monitorujących ludzi? Czy możesz zobaczyć hakerów żądających okupu w zamian za to, że nie powodują wyłączenia lodówek ludzi i zrujnowania ich żywności - lub nawet znaleźć przestępców, którzy wyłączają lodówki, gdy ludzie wychodzą do pracy i włączają je, zanim ofiary wrócą do domu, powodując zepsucie żywności w próba zatrucia wybranych osób? Ponieważ inteligentne samochody (które obejmują zasadniczo każdy pojazd wyprodukowany w ciągu ostatniej dekady lub więcej) stają się coraz bardziej powszechne, czy przestępcy mogą potencjalnie hakować je i powodować wypadki? Albo szantażować ludzi, aby płacili okup w zamian za to, że nie rozbili swoich samochodów? Zanim odpowiesz na to pytanie, weź pod uwagę, że badacze bezpieczeństwa niejednokrotnie wykazali, jak hakerzy mogą przejąć kontrolę nad niektórymi pojazdami i spowodować, że hamulce przestaną działać.

A co z sytuacjami, gdy samochody samojezdne i samojezdne ciężarówki są normą? Stawka będzie rosła wraz z postępem technologicznym. IoT otwiera świat możliwości. Zwiększa to również dramatycznie powierzchnię ataku, którą przestępcy mogą wykorzystać, i zwiększa stawkę, jeśli cyberbezpieczeństwo nie jest odpowiednio utrzymywane.

Korzystanie z kryptowalut i Blockchain

Kryptowaluta to zasób cyfrowy (czasami uważany za cyfrowy waluty) zaprojektowany do pracy jako środek wymiany, który wykorzystuje różne aspekty kryptografii do kontrolowania tworzenia jednostek, weryfikacji dokładności transakcji i zabezpieczania transakcji finansowych. Nowoczesne kryptowaluty pozwalają stronom, które nie ufają sobie nawzajem, na interakcję i prowadzenie interesów bez konieczności korzystania z zaufanej strony trzeciej. Kryptowaluty wykorzystują technologię blockchain - czyli ich transakcje są rekodowane w rozproszonej księdze, której integralność jest chroniona przy użyciu wielu technik, które powinny zapewnić, że tylko dokładne transakcje będą respektowane przez inne osoby przeglądające kopię księgi. Ponieważ kryptowaluty są śledzone za pomocą list transakcji w księgach, technicznie nie ma portfeli kryptowalut. Waluta jest wirtualna i nie jest nigdzie przechowywana, nawet elektronicznie. Właściciele kryptowalut to raczej strony, które kontrolują różne adresy w księdze, które mają powiązaną z nimi kryptowalutę po wykonaniu wszystkich dotychczasowych transakcji w księdze. Na przykład, jeśli adres 1 ma 10 jednostek kryptowaluty, a adres 2 ma 5 jednostek kryptowaluty, a transakcja jest rejestrowana, pokazując, że adres 1 wysłał 1 jednostkę kryptowaluty na adres 2, wynik jest taki, że adres 1 ma 9 jednostek kryptowaluty a adres 2 ma 6 jednostek kryptowaluty. Aby mieć pewność, że tylko prawowici właściciele kryptowaluty mogą wysyłać pieniądze ze swoich adresów, krioptowaluty zazwyczaj wykorzystują wyrafinowaną implementację PKI, w której każdy adres ma własną parę kluczy publiczny-prywatny, a właściciel jest jedynym posiadaczem klucza prywatnego. Wysłanie kryptowaluty z adresu wymaga podpisania transakcji wychodzącej skojarzonym z nią kluczem prywatnym. Ponieważ każdy, kto zna klucz prywatny powiązany z określonym adresem w księdze, może ukraść dowolną ilość kryptowaluty zarejestrowanej w księdze jako należącą do tego adresu, oraz ponieważ kryptowaluty są zarówno płynne, jak i trudne do wyśledzenia z powrotem do ich prawdziwych ludzi lub organizacji właściciele, przestępcy często próbują ukraść kryptowaluty poprzez hakowanie. Jeśli oszust uzyska klucz prywatny do adresu kryptowaluty z czyjegoś komputera, może szybko i łatwo przenieść kryptowalutę swojej ofiary na inny adres kontrolowany przez przestępcę. W rzeczywistości, jeśli przestępca w jakikolwiek sposób zdobędzie klucz, może ukraść kryptowalutę bez hakowania czegokolwiek. Wystarczy, że wystawi transakcję wysyłając pieniądze na inny adres i podpisze transakcję kluczem prywatnym. Ponieważ kryptowaluty nie są zarządzane centralnie, nawet w przypadku wykrycia takiej kradzieży prawowity właściciel ma niewielkie szanse na odzyskanie swoich pieniędzy. Odwrócenie transakcji wymagałoby w większości przypadków nieosiągalnego konsensusu większości operatorów w ekosystemie

kryptowaluty i jest bardzo mało prawdopodobne, chyba że skradziono wystarczającą ilość kryptowaluty, aby podważyć integralność całej waluty. Nawet w takich przypadkach może być konieczne rozwidlenie nowej kryptowaluty, aby osiągnąć takie odwrócenie, a wielu operatorów nadal prawdopodobnie odrzuci cofnięcie transakcji jako jeszcze większe zagrożenie dla integralności kryptowaluty niż poważna kradzież. Oprócz zapewnienia hakerom łatwego sposobu na kradzież pieniędzy, kryptowaluty ułatwiły również inne formy cyberprzestępczości. Na przykład większość okupów żądanych przez oprogramowanie ransomware musi zostać zapłacona w kryptowalucie. W rzeczywistości kryptowaluta jest siłą napędową oprogramowania ransomware. W przeciwieństwie do płatności dokonywanych przelewem bankowym lub kartą kredytową, sprytnie dokonywane płatności kryptowalutowe są niezwykle trudne do prześledzenia z powrotem do prawdziwych ludzi i są faktycznie nieodwracalne po rozliczeniu transakcji. Podobnie przestępcy mają możliwość wydobywania kryptowaluty - to znaczy wykonywania różnych złożonych obliczeń potrzebnych zarówno do rozliczania transakcji kryptowalutowych, jak i tworzenia nowych jednostek kryptowaluty - poprzez kradzież mocy obliczeniowej od innych. Na przykład szkodliwe oprogramowanie wydobywające kryptowaluty potajemnie przejmuje cykle procesora zainfekowanego komputerów w celu wykonania takich obliczeń, a gdy generowane są nowe jednostki kryptowaluty, przekazuje kontrolę nad nimi przestępcom obsługującym szkodliwe oprogramowanie. Kopanie kryptowalut zapewnia przestępcom prosty sposób zarabiania na hakowaniu. W ten sposób zhakowane komputery mogą być wykorzystywane do „drukowania pieniędzy" bez udziału ofiar, co jest zwykle potrzebne w przypadku wielu innych form monetyzacji, takich jak oprogramowanie ransomware.

Przestępcy skorzystali również na dramatycznym wzroście wartości kryptowaluty. Na przykład ci, którzy kilka lat temu zaakceptowali Bitcoin jako zapłatę za ransomware i którzy nie wypłacili do końca swojej kryptowaluty, cieszyli się niesamowitymi zwrotami - czasami zwiększając swoje zasoby o wartości w dolarach setki, a nawet tysiące. Niektórzy tacy przestępcy prawdopodobnie wypłacili część swoich kryptowalut podczas szału rynkowego w 2017 roku i mogą mieć małe fortuny, które teraz inwestują w tworzenie nowych technologii cyberprzestępczych. Technologia blockchain, która służy jako podstawowy silnik napędzający kryptowaluty, ma również potencjalne zastosowania w środkach zaradczych w zakresie cyberbezpieczeństwa. Rozproszona baza danych może okazać się lepszym sposobem przechowywania informacji o serwerach zapasowych i możliwościach redundantnych niż istniejące struktury, ponieważ rozproszony charakter radykalnie zwiększa liczbę punktów awarii koniecznych do wyłączenia całego systemu. Również, rozproszone zabezpieczenia przed atakami DDoS (rozproszona odmowa usługi) mogą okazać się bardziej skuteczne i opłacalne niż obecny model wykorzystania pojedynczej ogromnej infrastruktury do zwalczania takich ataków. Blockchain oferuje również sposób na tworzenie przejrzystych zapisów transakcji lub działań - transakcji, które są widoczne dla każdego, ale nie mogą być modyfikowane przez nikogo, i tylko upoważnione strony mogą tworzyć odpowiednie nowe transakcje.

Optymalizacja sztucznej inteligencji

Sztuczna inteligencja, technicznie rzecz biorąc, odnosi się do zdolności systemu elektronicznego do postrzegania otoczenia i podejmowania działań maksymalizujących prawdopodobieństwo osiągnięcia celów, nawet bez wcześniejszej wiedzy o specyfice środowiska i sytuacji, w której się znajduje. Jeśli ta definicja brzmi skomplikowanie, to tak. Definicja sztucznej inteligencji z praktycznego punktu widzenia wydaje się być celem ruchomym. Koncepcje i systemy, które dekadę lub dwie lata temu uważano za formy sztucznej inteligencji - na przykład technologie rozpoznawania twarzy - są dziś często traktowane jako klasyczne systemy komputerowe. Obecnie większość ludzi używa terminu sztuczna inteligencja w odniesieniu do systemów komputerowych, które się uczą - to znaczy naśladują sposób, w jaki ludzie uczą się na podstawie przeszłych doświadczeń, aby podejmować określone działania, gdy napotykają

nowe doświadczenie. Zamiast być wstępnie zaprogramowanym do działania w oparciu o zbiór określonych reguł, systemy sztucznie inteligentne analizują zbiory danych, aby tworzyć własne zestawy uogólnionych reguł i odpowiednio podejmować decyzje. Następnie systemy optymalizują swoje własne reguły, gdy napotykają więcej danych i widzą skutki zastosowania ich reguł do tych danych. Sztuczna inteligencja prawdopodobnie zmieni ludzkie doświadczenie przynajmniej w takim samym stopniu, jak rewolucja przemysłowa. Rewolucja przemysłowa oczywiście zastąpiła ludzkie mięśnie maszynami - te ostatnie okazały się szybsze, dokładniejsze, mniej podatne na zmęczenie lub choroby i mniej kosztowne niż poprzednie. Sztuczna inteligencja zastępuje ludzkie mózgi z komputerowym myśleniem - i ostatecznie się to również okaże być znacznie szybszym, dokładniejszym i mniej podatnym na choroby lub senność niż jakikolwiek biologiczny umysł. Era sztucznej inteligencji ma kilka głównych wpływów na cyberbezpieczeństwo:

* Zwiększona potrzeba cyberbezpieczeństwa

* Wykorzystanie sztucznej inteligencji jako narzędzia bezpieczeństwa

* Wykorzystanie sztucznej inteligencji jako narzędzia hakerskiego

Zwiększona potrzeba cyberbezpieczeństwa

Ponieważ sztucznie inteligentne systemy stają się coraz bardziej powszechne, dramatycznie rośnie potrzeba silnego cyberbezpieczeństwa. Systemy komputerowe mogą podejmować coraz ważniejsze decyzje bez udziału ludzi, co oznacza, że negatywne konsekwencje niewłaściwego zabezpieczenia systemów komputerowych mogą dramatycznie wzrosnąć. Wyobraź sobie, że szpital wdrożył sztucznie system do analizy obrazów medycznych i zgłaszania diagnoz. Jeśli taki system lub jego dane zostaną zhakowane, mogą pojawić się nieprawidłowe raporty i spowodować cierpienie, a nawet śmierć ludzi. Niestety taki problem nie jest już teoretyczny, ale takie badania to oczywiście tylko wierzchołek góry lodowej. Przemysłowymi systemami sztucznej inteligencji można manipulować, aby zmieniać produkty w sposób zwiększający zagrożenie, a sztucznie inteligentna technologia transportowa zaprojektowana w celu optymalizacji tras i poprawy bezpieczeństwa może być zasilana danymi, które zwiększają zagrożenie lub tworzą trasy i poprawiają bezpieczeństwo, mogą być zasilane danymi, które zwiększają zagrożenie lub tworzą niepotrzebne opóźnienia. Ponadto, ponieważ złoczyńcy mogą podważyć integralność sztucznie inteligentnych systemów bez hakowania systemów, ale raczej przez proste wprowadzanie trudnych do znalezienia małych zmian w dużych zbiorach danych oraz ponieważ decyzje podejmowane przez sztucznie inteligentne systemy nie są oparte na predefiniowanych regułach znanych ludzie, którzy tworzą system, chronią wszystkie elementy takich systemów, stają się krytyczne.

Gdy problemy zostaną wprowadzone, ludzie i maszyny prawdopodobnie nie będą w stanie ich znaleźć lub nawet wiedzieć, że coś jest nie tak. Najważniejsze jest to, że aby projekty sztucznej inteligencji zakończyły się sukcesem, muszą obejmować zaawansowane cyberbezpieczeństwo.

Użyj jako narzędzia cyberbezpieczeństwa

Jednym z największych wyzwań stojących obecnie przed specjalistami ds. Cyberbezpieczeństwa jest to, że praktycznie niemożliwe jest poświęcenie wystarczającej ilości czasu na analizę wszystkich alertów generowanych przez technologie cyberbezpieczeństwa i podjęcie odpowiednich działań. Jednym z pierwszych głównych zastosowań sztucznej inteligencji w dziedzinie cyberbezpieczeństwa jest agent, który pomaga ustalać priorytety alertów. Agent ten najpierw dowiaduje się, w jaki sposób systemy są zwykle używane i jakie typy działań są anomalne, a także które stare alerty faktycznie wskazywały na poważne problemy, a nie łagodne działania lub drobne problemy. Przyszłe iteracje takich sztucznie

inteligentnych systemów prawdopodobnie będą obejmować samą sztuczną inteligencję, która faktycznie będzie działać na podstawie alertów, zamiast kierować je do ludzi.

Użyj jako narzędzia hakerskiego

Sztuczna inteligencja to nie tylko narzędzie obronne; może być również potężną bronią w rękach napastników. Z oczywistych powodów nie przedstawiam w tej książce szczegółów, jak używać sztucznej inteligencji do przeprowadzania zaawansowanych ataków, ale omawiam kilka ogólnych przykładów. Systemy sztucznej inteligencji można na przykład wykorzystać do skanowania i analizowania innych systemów w celu znalezienia błędów programistycznych i błędów konfiguracji. Systemy sztucznej inteligencji mogą być również wykorzystywane do analizowania schematów organizacyjnych, mediów społecznościowych, witryn firmowych, informacji prasowych itp. W celu projektowania - a być może nawet wdrażania - maksymalnie skutecznych ataków socjotechnicznych. Sztuczną inteligencję można również wykorzystać do osłabienia systemów uwierzytelniania. Na przykład system, który otrzymuje nagranie osoby mówiącej wiele różnych rzeczy, może być w stanie oszukać system uwierzytelniania głosowego, naśladując odpowiedniego człowieka - nawet jeśli system uwierzytelniania prosi sztuczną inteligencję o wypowiedzenie słów, dla których sztuczna inteligencja ma brak nagrania ludzkiego głosu. Najważniejsze jest to, że jeśli chodzi o wykorzystanie sztucznej inteligencji jako narzędzia do cyberbezpieczeństwa, jest to prawdopodobnie bitwa szpieg-szpieg między cyberatakami a cyberobrońcami, w których każdy próbuje zbudować coraz lepsze sztuczną inteligencję, aby pokonać siebie nawzajem.

Doświadczanie wirtualnej rzeczywistości

Rzeczywistość wirtualna odnosi się do doświadczenia, które ma miejsce w rzeczywistości generowanej komputerowo, a nie w świecie rzeczywistym. Obecna technologia wirtualnej rzeczywistości zazwyczaj wymaga od użytkowników noszenia pewnego rodzaju zestawu słuchawkowego, który wyświetla użytkownikowi obrazy i blokuje wizję rzeczywistego świata. (W niektórych przypadkach zamiast noszenia zestawu słuchawkowego użytkownik wchodzi do specjalnego pomieszczenia wyposażonego w projektor lub kilka projektorów, co daje podobny efekt). Obrazy te w połączeniu z dźwiękami, aw niektórych przypadkach z ruchami fizycznymi i innymi ludźmi wrażenia zmysłowe, powodują, że użytkownik doświadcza wirtualnego środowiska tak, jakby był w nim fizycznie obecny. Osoba korzystająca ze sprzętu do wirtualnej rzeczywistości może zwykle poruszać się, patrzeć i wchodzić w interakcje z wirtualnym światem. Rzeczywistość wirtualna zazwyczaj obejmuje co najmniej elementy wizualne i dźwiękowe, ale może również dostarczać wibracji i innych wrażeń zmysłowych. Nawet bez dodatkowych informacji sensorycznych człowiek może doświadczać wrażeń, ponieważ ludzki mózg często interpretuje to, co widzi i słyszy w wirtualnym środowisku, tak jakby było to rzeczywiste. Na przykład ktoś jadący na kolejce górskiej w środowisku wirtualnym może poczuć, że jego żołądek spada, gdy kolejka górska gwałtownie spada, mimo że w rzeczywistości się nie porusza. Wciągające środowiska wirtualne mogą być podobne lub zupełnie inne od tego, czego dana osoba doświadczyłaby w prawdziwym świecie. Popularne zastosowania rzeczywistości wirtualnej obejmują już turystykę (na przykład chodzenie po muzeum sztuki bez przebywania w nim), rozrywkę (gry z widokiem z perspektywy pierwszej osoby) i cele edukacyjne (wirtualne sekcje). Systemy rzeczywistości wirtualnej są oczywiście oparte na komputerach iw rezultacie mają wiele takich samych problemów z bezpieczeństwem, jak inne systemy komputerowe. Ale rzeczywistość wirtualna wprowadza również wiele nowych zabezpieczeń i prywatności. Ale rzeczywistość wirtualna wprowadza również wiele nowych problemów związanych z bezpieczeństwem i prywatnością:

* Czy ktoś może włamać się do ekosystemów VR i przeprowadzić wizualne ataki, które wywołują ataki lub bóle głowy? (Mrugające światła stroboskopowe w różnych kreskówkach i innych wyświetlaczach powodują drgawki).

* Czy inni mogą podejmować decyzje dotyczące twoich zdolności fizycznych na podstawie twoich wyników w aplikacjach VR? Czy na przykład rządy mogą odmówić wydania praw jazdy osobom, które słabo radzą sobie w grach VR? Czy firmy ubezpieczeniowe mogą potajemnie się zbierać dane o zwyczajach kierowania pojazdami w świecie VR i wykorzystywać je do selektywnego podnoszenia stawek?

* Czy hakerzy mogą cyfrowo zniszczyć wirtualne środowisko - zastępując sztukę treści nieprzyzwoite, na przykład w muzeum oferującym wirtualne wycieczki?

* Czy hakerzy mogą podszywać się pod autorytet, na przykład nauczyciela w wirtualnej klasie, tworząc awatara, który wygląda podobnie do tego używanego przez tę osobę i tym samym nakłaniać innych użytkowników do podjęcia szkodliwych działań (na przykład prosząc ludzi o odpowiedzi na ich testy, które następnie oszuści kradną i przekazują prawdziwemu nauczycielowi jako własne)?

* Podobnie, czy hakerzy mogą podszywać się pod współpracownika lub członka rodziny, aby w ten sposób uzyskać i wykorzystać poufne informacje?

* Czy hakerzy mogą modyfikować wirtualne światy w taki sposób, aby zarabiać pieniądze w świecie rzeczywistym - na przykład dodając opłaty za wjazd do różnych miejsc?

* Czy hakerzy mogą ukraść wirtualną walutę używaną w różnych wirtualnych światach?

* Czy hakerzy mogą przejąć kontrolę nad wrażeniami użytkownika, aby zobaczyć, co on lub ona przeżywa, a nawet modyfikuje?

Teoretycznie, jeśli chodzi o nowe zagrożenia stwarzane przez wirtualną rzeczywistość, mogę sporządzić listę, która zajęłaby całą książkę - a czas z pewnością pokaże, które zagrożenia pojawią się jako problemy w świecie rzeczywistym.

Przekształcanie doświadczeń dzięki rzeczywistości rozszerzonej

Rzeczywistość rozszerzona to technologia, w której generowane komputerowo obrazy, dźwięki, zapachy, ruchy i / lub inny materiał sensoryczny są nakładane na doświadczenie użytkownika w świecie rzeczywistym, przekształcając doświadczenie użytkownika w połączenie elementów rzeczywistych i sztucznych. Technologia rzeczywistości rozszerzonej może zarówno dodawać elementy do doświadczenia użytkownika - na przykład pokazywać użytkownikowi imię osoby nad głową, gdy ta osoba zbliża się do użytkownika - jak i usuwać lub maskować elementy, takie jak przekształcanie nazistowskich flag w czarne prostokąty z napisem „Pokonaj nienawiść". Google Glass to przykład wczesnej próby skoncentrowanej na konsumentach rzeczywistości rozszerzonej, która była nieco za wcześnie na rynek. Z drugiej strony Pokémon Go był przykładem gry wykorzystującej rzeczywistość rozszerzoną, która odniosła ogromny sukces. Rzeczywistość rozszerzona prawdopodobnie stanie się główną częścią współczesnego życia w ciągu następnej dekady. Wprowadzi wiele zagrożeń, które niesie ze sobą rzeczywistość wirtualna a także ryzyko związane z łączeniem się świata rzeczywistego i wirtualnego, takie jak konfigurowanie systemów w celu nieprawidłowego powiązania różnych elementów w świecie rzeczywistym z danymi wirtualnymi. Jak w przypadku wszystkich nowych technologii, czas pokaże. Jeśli jednak zdecydujesz się zainwestować w technologię AR lub VR, pamiętaj o zrozumieniu wszelkich istotnych kwestii bezpieczeństwa.