Tadeusz Szulc, Ekspert IT, Członek Rady Programowej Wydawnictwa „Nowa Energia"

Ile kosztuje bezpieczeństwo informatyczne?

Horyzontem, który ogranicza moje rozważania jest 2050 r. Perspektywa stosunkowo bliska, jak na próbę wizjonerstwa i futurologii, a jednocześnie odległa, jeśli wziąć pod uwagę przyspieszenie technologiczne i tempo zmian cywilizacyjnych.

fot: Pixabay.com

Lata po 2050 r. to światy syntetyczne, pełne immersji (proces zanurzania albo pochłaniania przez rzeczywistość elektroniczną), innymi słowy: będzie to świat o rozszerzonej rzeczywistości, całkowicie wirtualny i cyberprzestrzenny, ale nie ten ze światów gier, a świat wirtualny „na serio", globalna szybkoprzestrzeń. Oparty na trudnych obecnie do wyobrażenia wynalazkach i rewolucyjnych zdobyczach nauki i techniki.

Ta transformacja przyniesie istotne przemiany społeczne, gospodarcze i polityczne, wpływając praktycznie na wszystkie sfery aktywności człowieka, przeobrażając zasadniczo modele życia.

Ludzkość zderzy się z rozbudowanym rynkiem medialnym przekraczającym możliwości percepcji odbiorców. Dyfuzyjny rozwój mediów komunikowania wpłynie na transformację prze-

strzenną i czasową uwarunkowań życia społecznego, wykreuje nowe formy działania i współdziałania, które nie będą już połączone z jednością miejsca i czasu.

Część osób z pozoru lepiej się będzie czuła w świecie wirtualnym niż realnym. Wywoła to cały szereg nowych chorób. Uzależnienia te znajdują się od szeregu lat na międzynarodowej liście klasyfikacji chorób OCD-10 (Międzynarodowa Statystyczna Klasyfikacja Chorób i Problemów Zdrowotnych).

Prognozuje się, że po 2050 r. roboty staną się integralną częścią codziennego życia wszystkich ludzi. Automatyzacja i robotyzacja będzie wszechobecna, a dzisiejsi informatycy ewoluują do … roli nauczycieli maszyn i opiekunów sztucznych inteligencji. Pojawią się też nowe zawody, bezpośrednio wynikające z rozwoju technologicznego.

Tworzenie oprogramowania zostanie całkowicie zautomatyzowane. To zoptymalizuje tempo jego powstawania i zapewni wysoką jakość.

Cyber fabryki przejdą kolejną faza digitalizacji i wykorzystując automatyczne procesy samoplanowania, samoadaptacji i samokonfiguracji będą produkować krótkie serie wyrobów i spersonalizowane egzemplarze urządzeń.

To oznacza, że trzeba być gotowym do objęcia umysłem i skoordynowania działanie gigantycznej ilości czujników (liczbę urządzeń podpiętych do sieci określa się w miliardach sztuk).

Sytuację dodatkowo skomplikuje lawinowy wzrost ilości cyfrowych narzędzi produkcji i dystrybucji.

Dwie dekady wcześniej (około 2030 r.) rozpadowi uległ ład świata, który opierał się na filarze państwa narodowego. Nastał świat opanowany globalizacją, świat kumulowania się nierównowagi finansowej, handlowej, płatniczej, demograficznej, surowcowej i ekologicznej; świat kolejnego, ogólnoświatowego kryzysu gospodarczego, a perspektywa cyberwojny doprowadziła do kolejnego wyścigu zbrojeń.

Był to czas, gdzie iluzoryczność wykształcenia odgrywała coraz większą rolę, a świat był pełen chaosu i niepewności. Kryzys, jaki zapanował, był wynikiem oddziaływania czynników o różnym charakterze i występujących w różnym horyzoncie czasowym, którym nie towarzyszyły konieczne zmiany regulacyjne i nadzorcze.

> Szyfrowanie kwantowe wykorzystuje zjawisko nielokalności, określone przez Alberta Einsteina jako „upiorne działanie na odległość". Nielokalność uwikłana jest w znane eksperymentalnie zjawiska, takie jak splątanie czy kwantowa teleportacja - które przez szereg dekad były tylko ciekawostkami

Niestety, przestępcy takie technologie jak robotyka, biologia syntetyczna, sztuczna inteligencja, nanotechnologia i komputery kwantowe stale skutecznie kompromitowali. Wykorzystując każdą słabość tych technologii: kradli dane, atakowali urządzenia i obiekty OT i manipulowali rzeczywistością, którą mieli wokół siebie.

Słowo „ransomware" (oprogramowanie szantażujące) wciąż pojawiało się w nagłówkach wiadomości i było jednym z największych zagrożeń w cyberprzestrzeni.

Również każda nowa technologia niosła za sobą nowe luki bądź błędy. Największym zagrożeniem dla firm były ataki zero day. Luka zero-day (lub exploit zero-day) to właściwość nowych produktów z luką bezpieczeństwa.

Sytuacja stała się jeszcze bardziej dramatyczna pod koniec drugiej dekady XXI wieku. Zidentyfikowano w sieciach korporacyjnych w kilku regionach (głównie w Ameryce Łacińskiej) szkodliwą koparkę kryptowaluty o nazwie PowerGhost. PowerGhost był rozprzestrzeniany poprzez infekcję zarówno stacji roboczych, jak i serwerów i stosował wiele różnych technik bezplikowych. Skomplikowało to bardzo mocno procesy wykrywania i neutralizowania zagrożenia. To był bardzo groźny sygnał, oznaczał bowiem, że atakowanie cyberprzestępców rozszerzyło się i już nie tylko użytkownicy indywidualni są atakowani, ale również duże przedsiębiorstwa. Niestety, nawet czołowe agencje wywiadowcze sporo przegapiły i nie zapobiegły tym poważnym atakom. Agresorzy pozostali nieznani, nie wiadomo było, czy to są państwa, organizacje, czy jednostki.

Była to również konsekwencja istnienia globalnej sieci. Upowszechnienie dostępu do internetu miało być triumfem demokracji, a tak naprawdę, zaczęło… zagrażać wolności i demokracji.

Społeczeństwo nie rozumiało, dlaczego, skoro byliśmy w stanie sfotografować galaktyki oddalone o miliardy lat świetlnych, manipulować genami sterującymi procesami życiowymi i dotrzeć do wnętrza atomu, nie możemy uporać się z cyberprzestępcami.

Sprawy zaszły za daleko. Nasza cywilizacja, jeśli miała przetrwać, musiała na nowo określić warunki w jakich działa cyberprzestrzeń.

Potrzebna były spektakularne zmiany!

I wreszcie nadeszły.

Dostosowano metodologię do problemu, który wydawał być się nierozwiązywalny. Pomogło przestawienie się na myślenie poza schematami. Zrezygnowano z dopasowywania rozwiązań na siłę do określonej metodologii. Trochę przypadkowo sięgnięto do zasady ekonomii myślenia zwanej „brzytwą Ockhama". Rozwiązania następnie wzbogacono o elementy Artificial Life i struktury emergentne.

Ale, po kolei.

William Ockham to żyjący na przełomie XIII i XIV w. angielski filozof i teolog franciszkański. Zradykalizował on sformułowane przez Platona i Arystotelesa zasady ekonomii myślenia. W XVII w.

brzytwa Ockhama została oddzielona od swego średniowiecznego kontekstu i jako zasada ekonomii myślenia stała się podstawą nowożytnej metodologii nauki. Zgodnie z tym ujęciem, nie należy wprowadzać nowych pojęć i założeń, jeśli nie ma się ku temu mocnych podstaw, a najprostsze rozwiązania teoretyczne, przyjmujące najmniejszą liczbę założeń, uważane są za najlepsze.

Z kolei, Artificial Life to dziedzina silnie interdyscyplinarna i obejmująca takie obszary jak sztuczna inteligencja, robotyka, matematyka, fizyka, biologia, lingwistyka, filozofia i informatyka.

Emergencja to ogólna cecha tzw. układów złożonych powodująca, że są one nieredukowalne - z praw opisujących ich elementy składowe nie wynikają logicznie właściwości i zachowania systemu jako całości. Mówiąc w skrócie i w mocnym uproszczeniu: całość to coś więcej niż suma części.

W oparciu o te rozwiązania opracowano całkowicie zautomatyzowany, zintegrowany, trójwarstwowy, wzajemnie uzupełniający się system bezpieczeństwa. System ten łączy ze sobą różne elementy – wielowarstwową obronę, systemy ofensywne oraz rozwiązania, pozwalające na minimalizację skutków ataku.

W chwili uruchomienia składał się on z 27 naziemnych stacji odbiorczo-nadawczych zlokalizowanych w różnych miejscach świata i 64 satelitów, umieszczonych na orbitach okołoziemskich, a jego pracę wspomagało 12 superkomputerów.

Początkowo był bliźniaczo podobny do projektu Echelon (sieć wywiadu elektronicznego zarządzana przez amerykańską służbę wywiadu NSA). W kolejnych dekadach XXI w. był rozwijany niezależnie od sieci Echelon.

Pozwala on przeglądać 100% całego ruchu internetowego świata, monitorować rozmowy telefoniczne przez linie naziemne i komórkowe, czytać faksy, monitorować połączenia satelitarne, a także śledzić historie kliknięć w komputerowych przeglądarkach.

Stale monitorowane są podstawowe procesy związane z bezpiecznym wprowadzaniem danych, integralnością pamięci operacyjnej, rozróżnianiem danych i kodu, przepływem informacji i ograniczeniami w ramach kontroli dostępu. Elementy nie spełniające określonych norm (anomalie) zostają albo wyłączone albo wyeliminowane.

Osiągnięto w ten sposób niesamowitą moc samooczyszczania, regeneracji i rewitalizacji systemów zbliżoną do procesów neurogenezy (proces tworzenia nowych neuronów w mózgu). Procesowi regeneracji i przywróceniu właściwości użytkowych podlega każdy niespełniający integralności element zbioru. Zabezpieczają to kryptograficzne algorytmy ochrony integralności danych, które rozwinęły się i rozwijają się w sposób niezwykle dynamiczny. Bezpieczna informatyka zyskała neuronalne korelaty integralności, potrafi sama się odtwarzać. Również technologia rejestrów rozproszonych (blockchain) przeszła kolejne etapy rozwoju, co uniemożliwia niezauważoną ingerencję w dane. Technologia ta, przez szereg dekad XXI w., odgrywała wiodącą rolę na rynku rozwiązań IT.

Olbrzymi wpływ na poprawę bezpieczeństwa miała również budowa bardzo szerokiej sieci sensorów zapewniających wczesne ostrzeganie o wydarzeniach w sieci, zautomatyzowaną analizę kryminalistyczną i neutralizację zagrożeń.

Zadbano również o rozwój kwantowych systemów szyfrowania danych. Osiągnięto bardzo wysoką szybkość dystrybucji klucza, a nowe systemy były w stanie transmitować zaszyfrowane dane z szybkością kilkudziesięciu megabitów na sekundę.

Działania te umożliwiły stworzenie światowej sieci komunikacyjnej opartej na szyfrowaniu kwantowym 4D odpornej na turbulencje powietrzne i promieniowanie elektromagnetyczne.

Szyfrowanie kwantowe wykorzystuje zjawisko nielokalności, określone przez Alberta Einsteina jako „upiorne działanie na odległość". Nielokalność uwikłana jest w znane eksperymentalnie zjawiska, takie jak splątanie czy kwantowa teleportacja - które przez szereg dekad były tylko ciekawostkami.

Rozwiązania te miały i mają jednak swoje ograniczenia. Konsumują bowiem bardzo dużo zasobów.

Ograniczenia początkowo wynikały z wydajności komputerów. Wprawdzie konstruktorzy i programiści stale ją zwiększali wykorzystując przy budowie systemów obliczeniowych rozwiązania hybrydowe, łączące wielordzeniowe procesory ogólnego przeznaczenia i dedykowane, masywnie zrównoleglone akceleratory obliczeniowe, ale to wszystko za mało. Problem został złagodzony gdy pojawiły się komputery kwantowe (logika wielowartościowa), które następnie zostały zastąpione maszynami budowanymi w oparciu o DNA. Te z kolei zostały wyparte przez komputery neuronowe. Kolejny skok wydajnościowy osiągnięto stosując rekonfigurowalne układy programowalne.

Zadbano również, z myślą o wzmocnieniu bezpieczeństwa, o rozwinięcie programów szkoleniowych dla wszystkich grup społecznych. W szkołach wprowadzono nauczanie oparte na konektywizmie (uczenie zdolności do tworzenia sieci i przechodzenia przez nie).

Spowodowało to wzrost kultury i myślenia o bezpieczeństwie.

To był przełom na skalę globalną. Poziom bezpieczeństwa informatycznego wzrósł wielokrotnie.

Potrafiliśmy, więc ... daliśmy radę.

Trwało to ponad 30 lat i kosztowało.... nieco ponad 25 bilionów USD (dla porównania: budżet USA na 2018 r.to 4,1 bilionów USD).

□