NOWOCZESNE ROZWIĄZANIA W BIZNESIE

Chmura jako fundament nowoczesnego biznesu

Chmura obliczeniowa, będąca jednym z filarów cyfrowej transformacji, zrewolucjonizowała sposób, w jaki firmy przechowują dane i nimi zarządzają, tworzą swoje aplikacje oraz rozwijają biznes.

WOJCIECH FURMANKIEWICZ
dyrektor Red Hat ds. technologii i rozwiązań w regionie Europy Środkowo-Wschodniej

Z raportu KPMG „Monitor Transformacji Cyfrowej Biznesu 2024" wynika, że 71 proc. firm w Polsce wdrożyło już rozwiązania chmurowe. Dwa na pięć przedsiębiorstw korzysta z modelu chmurowego SaaS (Software-as-a-Service), wykupując subskrypcyjny dostęp do usług i narzędzi IT oferowanych przez zewnętrznych dostawców. Na drugim miejscu wśród preferencji plasuje się chmura prywatna – 39 proc. podmiotów w kraju decyduje się na inwestycję we własną moc obliczeniową utrzymywaną lokalnie (on-premise), na serwerach firmy.

Sporo korzyści, ale wyzwań też nie brak

Rosnąca popularność technologii chmurowej wynika z jej elastyczności, skalowalności oraz dynamicznej kontroli kosztów, jaką zapewnia. Dzięki chmurze firmy zyskują dostęp do zasobów IT, które mogą rozszerzać zgodnie z aktualnymi potrzebami biznesowymi. Pozwala im to ograniczyć koszty związane z utrzymywaniem infrastruktury IT oraz wdrażać innowacje bez konieczności inwestowania z góry w drogi sprzęt lub oprogramowanie. Model subskrypcyjny (SaaS) umożliwia płacenie jedynie za rzeczywiste wykorzystanie zasobów, co czyni go atrakcyjnym dla firm o ograniczonych budżetach, szczególnie w sektorze MŚP.

Mimo licznych korzyści z użycia chmury 98 proc. podmiotów w Polsce badanych w raporcie KPMG podchodzi do tej technologii z pewnym niepokojem. Zdecydowana większość z nich (79 proc.) obawia się o bezpieczeństwo danych. W dobie rosnących cyberzagrożeń to zrozumiałe, choć należy zauważyć, że dostawcy rozwiązań chmurowych – świadomi ryzyka naruszeń cybernetycznych – oferują coraz bardziej zaawansowane mechanizmy ochrony. Ponad trzy na pięć firm dostrzega problem rosnących kosztów usług, nad którymi nie będą mieć pełnej kontroli, a 56 proc. martwi się o wystąpienie zjawiska tzw. vendor lock-in. Chodzi o sytuację, w której przedsiębiorstwo uzależnia się od usług oferowanych przez jednego dostawcę chmury do tego stopnia, że ich zmiana jest utrudniona lub nawet niemożliwa ze względu na koszty i czas potrzebny do przeprowadzenia migracji do innego rozwiązania.

Chmura hybrydowa – złoty środek w cyfrowym świecie

Jedną z odpowiedzi na te i inne zagrożenia, które mogą pojawić się w związku z korzystaniem z technologii chmurowych, jest model chmury hybrydowej. Łączy on zalety infrastruktury lokalnej, chmury prywatnej oraz publicznej, umożliwiając firmom przenoszenie zasobów między różnymi środowiskami w zależności od potrzeb. Przekłada się to na większą kontrolę nad optymalizacją kosztów. Firmy korzystają z własnych zasobów IT, a gdy ich wymagania przewyższają możliwości infrastruktury prywatnej, mogą zaczerpnąć ze zbiorów chmury publicznej. Takie rozwiązanie doskonale sprawdza się w przypadku przedsiębiorstw działających w branżach charakteryzujących się sezonowością (np. w sektorze e-commerce czy publicznym).

Ważną zaletą chmury hybrydowej jest również możliwość swobodnego rozwijania innowacji przy jednoczesnym sprawowaniu kontroli nad danymi firmy. W ramach tego modelu chmurowego firmy zyskują dostęp do zaawansowanych narzędzi analitycznych oraz narzędzi bazujących na sztucznej inteligencji i uczeniu maszynowym, co pozwala im lepiej analizować dane i podejmować trafniejsze decyzje biznesowe. Jednocześnie, dzięki możliwości przechowywania wrażliwych danych w lokalnej infrastrukturze, przedsiębiorstwa mogą zapewnić wysoki poziom bezpieczeństwa informacji, spełniając przy tym wymagania dotyczące suwerenności danych, a także przepisy prawne związane z ochroną danych, w tym RODO. To szczególnie ważne dla podmiotów działających w wysoce regulowanych branżach, jak np. finansowa.

Firma na miarę XXI wieku

Migracja do chmury obliczeniowej, a szczególnie wybór modelu hybrydowego, to krok w stronę nowoczesności, innowacyjności i efektywności operacyjnej. Firmy zyskują nie tylko dostęp do zasobów IT najwyższej klasy, ale także możliwość dostosowania ich do swoich indywidualnych potrzeb, minimalizując jednocześnie ryzyko tego, że wpadną w sidła kosztownej pułapki vendor lock-in. Chmura hybrydowa to rozwiązanie, które pozwala połączyć najlepsze cechy różnych środowisk chmurowych, gwarantując elastyczność, bezpieczeństwo i skalowalność – a wszystko to przy zachowaniu kontroli nad wydatkami.

W dobie cyfryzacji odpowiedzialne i przemyślane wdrożenie chmury może stać się fundamentem długoterminowego sukcesu każdej firmy. Dlatego nie dziwi, że technologia ta jest przez respondentów badania EY „Cyfrowa Transformacja 2024" wymieniana w pierwszej trójce najważniejszych obszarów inwestycyjnych. Co trzecia firma w Polsce zamierza w ciągu najbliższego roku zwiększyć swój budżet na projekty związane z rozwiązaniami chmurowymi.

Źródła:
Raport KPMG „Monitor Transformacji Cyfrowej Biznesu 2024"
Raport EY „Cyfrowa Transformacja 2024"

Wszyscy w organizacji odpowiadają za cyfrowe bezpieczeństwo

Cyberbezpieczeństwo w organizacjach jest obecnie kluczowym elementem, który bezpośrednio wpływa na ochronę danych, zachowanie ciągłości operacyjnej oraz budowanie zaufania wśród klientów i partnerów biznesowych.

ROBERT ŁUGOWSKI
Cybersecurity Architect w Safesqr

Pracownicy mają kluczowy wpływ na cyfrowe bezpieczeństwo organizacji, stanowiąc zarówno linię obrony, jak i potencjalne źródło zagrożeń.
Dlatego tak istotne jest zbudowanie kultury organizacyjnej, w której cyberbezpieczeństwo – traktowane jako wspólna odpowiedzialność – będzie zmniejszało ryzyko naruszeń. Kiedy pracownicy rozumieją, że ich działania mają wpływ na całą organizację, są bardziej skłonni do przestrzegania zasad i procedur bezpieczeństwa. Ważną rolę odgrywają tutaj liderzy i menedżerowie, mając kluczowy wpływ na budowanie kultury cyberbezpieczeństwa.

Zobowiązania prawne
Organizacje muszą przestrzegać wielu regulacji prawnych związanych z ochroną danych, szczególnie że często przetwarzają wrażliwe informacje o pracownikach i firmie. Oto kluczowe regulacje, które mogą wymagać od tych działów szczególnych działań w zakresie ochrony danych firmowych:
• RODO (GDPR), czyli Ogólne Rozporządzenie o Ochronie Danych Osobowych;
• Ustawa o ochronie danych osobowych w Polsce;
• Prawo pracy i ochrona prywatności pracowników.
• Ustawa o krajowym systemie cyberbezpieczeństwa (KSC)
Te regulacje kładą duży nacisk na współpracę poszczególnych działów w zakresie ochrony danych osobowych, cyberbezpieczeństwa oraz odpowiedniego zarządzania dostępem. Wdrożenie tych zasad i przestrzeganie przepisów prawnych pomaga zminimalizować ryzyko naruszeń i zwiększa bezpieczeństwo organizacji.

Zasady cyfrowego bezpieczeństwa
Podstawowe zabezpieczenie to stosowanie silnych haseł. Częstym błędem, który wiele osób uważa za bezpieczny, jest spisywanie sobie haseł do notatnika schowanego w szafie – absolutnie to odradzam. Szczególnie zalecane jest stosowanie menedżera haseł typu Keepass, który oprócz przechowywania bazy dostępów do systemów wygeneruje również unikalne, niemal niemożliwe do złamania hasła. Konieczne w organizacjach powinno być również uwierzytelnianie wieloskładnikowe, które jest dodatkową warstwą bezpieczeństwa, pozwalającą uchronić się przed przestępcami. Powinniśmy je stosować wszędzie, gdzie tylko otrzymujemy taką możliwość – nie tylko w kluczowych systemach firmowych zawierających poufne dane. Uwierzytelnianie wieloskładnikowe wymaga od użytkownika potwierdzenia tożsamości za pomocą co najmniej dwóch elementów, takich jak hasło i kod SMS lub aplikacja autoryzacyjna.
W coraz większej liczbie systemów pojawia się uwierzytelnianie biometryczne, które opiera się na unikalnych cechach biologicznych osoby. Może ono wykorzystywać odciski palców, rozpoznawanie twarzy, skanowanie tęczówki czy rozpoznawanie głosu. Biometria ma wiele zalet – przede wszystkim jest bardzo wygodna dla użytkownika, a jednocześnie trudna do przełamania dla cyberprzestępców. Warto dodać, że w praktyce biometria nie jest stosowana samodzielnie, ale wraz z innymi metodami uwierzytelniania – hasłami i kodami PIN.
Istotne praktyki, które również warto wdrożyć w organizacji, to blokowanie urządzeń przez pracowników zawsze, gdy nie są używane, oraz aktualizowanie oprogramowania.

Edukacja w zakresie nowych metod cyberataków
Coraz częściej cyberprzestępcy przeprowadzają cyberataki z wykorzystaniem inżynierii społecznej. Stanowią one poważne zagrożenie dla pracowników, ponieważ opierają się na manipulacji psychologicznej i wykorzystaniu słabości ludzkiego zachowania. Jakie konkretnie zagrożenia mogą wynikać z takich ataków?
Cyberprzestępcy mogą wyłudzić dane osobowe, takie jak PESEL, numer dowodu osobistego, numer telefonu czy dane logowania do systemów firmowych. Mogą również próbować uzyskać dane adresowe, finansowe lub informacje dotyczące rodziny. Bardzo niebezpiecznym skutkiem przejęcia takich informacji jest wykorzystane ich do kradzieży tożsamości i np. zaciągnięcia pożyczki na dane pracownika. Takie wykradzione informacje mogą być następnie sprzedane innym przestępcom.
Pracownik, który jest ofiarą phishingu, może nieświadomie przekazać dane logowania do firmowych systemów, takich jak poczta e-mail, CRM czy aplikacje stosowane w firmie. Skutkiem w tym wypadku może być wyciek danych firmowych, przejęcie korespondencji czy uzyskanie przez przestępców dostępu do poufnych dokumentów.
W atakach phishingowych często używane są linki, które prowadzą do zainstalowania złośliwego oprogramowania na komputer pracownika. Może ono umożliwić hakerom zdalny dostęp do komputera, śledzenie naciśnięć klawiszy (keylogging), a nawet przejęcie kamery czy mikrofonu. Skutkiem może być wyciek danych oraz osłabienie ochrony. Wykorzystanie przez konkurencję wykradzionych informacji może skutkować stratami finansowymi lub problemami prawnymi.

Jak zapobiegać?
Podstawą są szkolenia, prowadzone rzeczywiście regularnie, nie tylko w ramach onboardingu nowych pracowników, ale także cyklicznie, oraz zawsze w przypadku wprowadzania nowych środków bezpieczeństwa lub pojawienia się zagrożeń nowego typu. Bo warto pamiętać, że z rozwoju nowych technologii, np. ostatnio sztucznej inteligencji, korzystają zarówno firmy, jak i przestępcy, którzy stale pracują nad nowymi metodami oszustw. Warto wykorzystywać nowe technologie w edukowaniu na temat cyberbezpieczeństwa, np. w formie platform e-learningowych, symulacji VR czy grywalizacji, czyli włączania do szkolenia elementów gier. Oprócz szkoleń niezwykle ważne są testy wiedzy pracowników oraz organizowanie symulacji ataków phishingowych, które pomagają w aktualnej ocenie świadomości pracowników i wskazują słabsze obszary. Dzięki temu można na bieżąco korygować wszelkie braki i niewłaściwe zachowania pracowników.
Działania związane z edukacją w obszarze cyberbezpieczeństwa warto oczywiście mierzyć, choćby za pomocą regularnie realizowanych ankiet, które pozwolą na bieżącą ocenę skuteczności. Można także stosować własne kluczowe wskaźniki efektywności (KPI), np. odsetek zgłoszonych podejrzanych wiadomości e-mail czy liczba pomyślnie zdanych testów z wiedzy dotyczącej cyberbezpieczeństwa.
Podsumowując – cyberbezpieczeństwo staje się nieodzownym elementem zarządzania współczesnymi organizacjami, a skuteczne wdrożenie narzędzi i procedur, które mu służą, wymaga zaangażowania wszystkich pracowników.

Automatyzacja w polskim przemyśle – konieczność, nie wybór

Polskie firmy produkcyjne stoją przed koniecznością redefinicji swoich strategii działania. Wysoka jakość produktów i konkurencyjne ceny, choć ważne, przestają wystarczać.

MICHAŁ ŻELICHOWSKI
dyrektor ds. rozwoju biznesu i zarządzania produktami PSI Polska

Kluczowym wyzwaniem staje się szybka adaptacja do oczekiwań klientów, którzy wymagają nie tylko niezawodności, ale także rekordowo krótkich terminów realizacji. Odpowiedzią na te potrzeby może być transformacja w duchu Przemysłu 4.0 – automatyzacja procesów logistycznych i pełna synchronizacja produkcji z zaopatrzeniem, które nie tylko zwiększą efektywność, ale także otworzą drogę do trwałej przewagi konkurencyjnej.

W dobie Przemysłu 4.0 rynek stawia przed firmami produkcyjnymi nowe wymagania. Precyzja, szybkość realizacji zamówień i elastyczność w organizacji pracy stają się kluczowe. Polskie przedsiębiorstwa muszą dostosować się do tej rzeczywistości, inwestując w technologie, które pomogą im sprostać bieżącym wyzwaniom i utrzymać konkurencyjność.

Automatyzacja procesów, integracja danych w czasie rzeczywistym czy wykorzystanie takich rozwiązań, jak sztuczna inteligencja (AI) i internet rzeczy (IoT), to już nie tylko modne hasła, ale wcodzienność, która zmienia sposób działania firm. Inwestycje w nowoczesne systemy zarządzania produkcją (APS i MES) pozwalają na lepsze planowanie, monitorowanie i optymalizację procesów – od dostaw, przez produkcję, aż po obsługę klienta.

Rosnące znaczenie systemów MES w polskim przemyśle

W Polsce systemy realizacji produkcji (MES) oraz systemy wspierające zaawansowane harmonogramowanie (APS) zyskują na popularności jako narzędzie do optymalizacji procesów i zwiększania efektywności. W 2018 r. rozwiązania te stosowało 12 proc. średnich i 27 proc. dużych przedsiębiorstw. Pięć lat później odsetki te wzrosły odpowiednio do 18,7 proc. i 36,7 proc., co świadczy o rosnącym zainteresowaniu automatyzacją.

Polski przemysł, dzięki swojej różnorodności i rozbudowanej infrastrukturze, ma potencjał, by stać się liderem transformacji cyfrowej w regionie. Tempo wdrażania nowoczesnych rozwiązań, takich jak MES (manufacturing execution systems) czy APS (advanced planning and scheduling), wciąż jest jednak zbyt wolne. Wiele firm obawia się kosztów inwestycji lub nie zna dostępnych możliwości. Często brakuje też świadomości, że technologie mogą nie tylko usprawnić procesy, ale również znacząco obniżyć koszty w dłuższej perspektywie. Doświadczenia firm, które już wdrożyły nowoczesne narzędzia, pokazują, że korzyści są widoczne niemal natychmiast. Efekty różnią się w zależności od wielkości firmy, branży czy poziomu zaawansowania technologicznego, ale wspólnym mianownikiem pozostaje wzrost efektywności i poprawa konkurencyjności.

Klienci nie chcą czekać

Z perspektywy klientów czas oczekiwania na realizację zamówienia stał się równie ważny, co jakość produktu. W gospodarce opartej na szybkim obrocie i dynamicznej reakcji na zmieniające się potrzeby rynku przedsiębiorstwa muszą maksymalnie skracać tzw. lead time. Jak to osiągnąć? Tu kluczowe okazują się technologie umożliwiające automatyzację, integrację i precyzyjne planowanie działań.

Przykładem są systemy APS i MES, które stanowią niejako „system nerwowy" nowoczesnej fabryki. Dzięki nim decyzje podejmowane są na podstawie aktualnych danych, co minimalizuje przestoje i marnotrawstwo. A co z logistyką wewnętrzną? Automatyczne pojazdy AGV czy roboty AMR to już nie przyszłość, lecz teraźniejszość, pozwalająca na dostarczanie surowców „just in time". Efekt? Mniej magazynowania, więcej efektywności.

Nie chodzi tylko o technologię – chodzi o strategię

Kluczowym pytaniem nie jest jednak, jaką technologię wdrożyć, lecz jak zrobić to mądrze. Automatyzacja to nie zakup kolejnego urządzenia do fabryki, ale przemyślana strategia, która obejmuje całość procesów w firmie – od zaopatrzenia, przez produkcję, po dystrybucję. Firmy, które podejdą do tego fragmentarycznie, ryzykują, że zamiast usprawnień otrzymają chaos.

Warto zacząć od analizy potrzeb i zrozumienia słabych punktów w obecnym systemie. Czy największym wyzwaniem jest harmonogramowanie produkcji? A może brak synchronizacji między działem zakupów a liniami produkcyjnymi? Dopiero po identyfikacji problemów można skutecznie wdrożyć odpowiednie rozwiązania. Systemy APS i MES pozwalają nie tylko na automatyzację, ale także na stworzenie spójnego ekosystemu, w którym każda decyzja jest poparta danymi.

Inwestycja, która się zwraca

Oczywiście, automatyzacja wiąże się z kosztami – to fakt, ale warto spojrzeć na nią jak na inwestycję, a nie wydatek. Firmy, które już wdrożyły nowoczesne technologie, szybko dostrzegły korzyści. Skrócenie czasu dostaw, ograniczenie strat wynikających z przestojów, optymalizacja zasobów ludzkich i redukcja kosztów – to tylko niektóre z nich.

Co więcej, automatyzacja otwiera drzwi do innowacji. Uwolnieni od monotonnych czynności pracownicy mogą skupić się na zadaniach wymagających kreatywności i analitycznego myślenia. Dzięki temu przedsiębiorstwa stają się bardziej elastyczne i gotowe do reagowania na zmieniające się potrzeby rynku.

Przyszłość polskiego przemysłu: szybka, precyzyjna, zautomatyzowana

Automatyzacja to nie trend, który przeminie, lecz fundament nowoczesnego przemysłu. Polskie firmy, które jako pierwsze zdecydują się na pełną transformację, zyskają przewagę, którą trudno będzie zniwelować konkurencji. Klucz tkwi jednak w odpowiednim podejściu: inwestycje w technologię muszą być połączone z rozwojem kompetencji zespołu i strategią długoterminową.

Czy polskie przedsiębiorstwa są na to gotowe? Wiele z nich już postawiło pierwsze kroki, wdrażając roboty transportowe, systemy planowania i integrując działy za pomocą narzędzi ERP. Przed większością jeszcze długa droga. Nie chodzi tylko o modernizację maszyn – chodzi o zmianę mentalności, zrozumienie, że technologia to partner, a nie wróg.

Czas na działanie

Na globalnym rynku nie ma miejsca na wahania. Firmy, które wstrzymują się z decyzjami o automatyzacji, ryzykują utratę konkurencyjności. Tymczasem technologie, które jeszcze kilka lat temu wydawały się drogie i niedostępne, stają się coraz bardziej przystępne, również dla małych i średnich przedsiębiorstw. To idealny moment, by postawić na przyszłość i wykorzystać potencjał, jaki daje Przemysł 4.0. W świecie biznesu czekanie rzadko jest dobrą strategią.

Technologie napędzające transformację sektora finansowego

Sektor bankowy i ubezpieczeniowy przechodzą obecnie głęboką transformację technologiczną. Kluczową rolę w tej zmianie odgrywają zaawansowane technologie, takie jak chmura obliczeniowa czy sztuczna inteligencja.

ROBERT CZARNIEWSKI
wiceprezes i CFO w Polcom

Jak wynika z badań Bain & Company, banki, które dynamicznie wdrażają nowoczesne technologie, osiągają znacznie lepsze wyniki finansowe oraz zyskują lojalność klientów. Liderzy cyfrowi notują o 5 pp. wyższe stopy zwrotu dla akcjonariuszy w porównaniu z resztą rynku, a wydatki na technologie stanowią obecnie ok. 16 proc. całkowitych kosztów sektora.

Przyszłość sektora finansowego w technologii

Transformacja technologiczna nie ogranicza się jednak tylko do bankowości. Z raportu Sollers Consulting „Against the Wind", który zawiera prognozy dotyczące rynku ubezpieczeń na 2024 r., wynika, że branża ubezpieczeniowa również staje przed koniecznością automatyzacji procesów. Aby sprostać rosnącym wymaganiom klientów i poprawić wydajność operacyjną, wdrożenie rozwiązań chmurowych oraz rozwój w zakresie zarządzania danymi będą głównymi celami ubezpieczycieli na przyszły rok.

Eksperci przewidują, że AI diametralnie zmieni sektor ubezpieczeniowy, otwierając drzwi do bardziej precyzyjnych i spersonalizowanych usług. Do tego, by w pełni wykorzystać potencjał sztucznej inteligencji, firmy ubezpieczeniowe muszą być jednak odpowiednio przygotowane, oraz zbudować odpowiedni potencjał cyfrowy, związany np. z wdrożeniem odpowiednich systemów IT czy skalowalnej chmury obliczeniowej, które w dalszych krokach umożliwią lepsze zarządzanie danymi oraz automatyzację procesów.

Z kolei wg raportu EY „Generatywna AI w bankowości" motorem wdrażania AI jest potrzeba zwiększenia produktywności (78 proc.), poprawy doświadczeń klientów (60 proc.) oraz redukcji kosztów (59 proc.). W globalnej skali już 45 proc. instytucji finansowych inwestuje w rozwiązania oparte na GenAI, a 52 proc. ma to w planach. Liderzy rynkowi – zarówno w sektorze bankowym, jak i ubezpieczeniowym – coraz częściej tworzą dedykowane zespoły do wdrażania tych technologii.

Ponadto zgodnie z raportem Związku Banków Polskich oraz Centrum Prawa Bankowego i Informacji chmura obliczeniowa staje się kluczowym narzędziem w bankach, umożliwiając szybkie tworzenie, testowanie i wdrażanie nowych rozwiązań. Podobny trend obserwujemy w branży ubezpieczeniowej. Jak wskazuje raport Sollers Consulting, chmura pozwoli ubezpieczycielom poprawić wydajność operacyjną, elastyczność oraz szybkość w dostarczaniu usług.

Cyberbezpieczeństwo priorytetem

Rozwój technologii cyfrowych wiąże się jednak z rosnącymi zagrożeniami, szczególnie w sektorze finansowym i ubezpieczeniowym. Firma Check Point podaje, że w Polsce codziennie dochodzi do ok. 160 cyberataków na instytucje finansowe. Wzrost inwestycji w technologie, takie jak AI i chmura obliczeniowa, powinien iść więc w parze ze wzmocnieniem kompetencji i budową rozwiązań w obszarze cyberbezpieczeństwa firmy.

Nie ulega wątpliwości, że nowoczesne technologie stają się kluczem do budowania długofalowego sukcesu na dynamicznie zmieniającym się rynku, a co za tym idzie – zarówno sektor finansowy, jak i ubezpieczeniowy są w trakcie ogromnych zmian technologicznych. Banki i ubezpieczyciele, którzy zainwestują w chmurę, sztuczną inteligencję i zaawansowane rozwiązania z zakresu cyberbezpieczeństwa, będą w stanie lepiej odpowiadać na zmieniające się potrzeby klientów, poprawić wydajność operacyjną i zyskać przewagę konkurencyjną. Trudno nie zauważyć jednak, że w pierwszym kroku muszą zbudować odpowiednią strategię i przygotować zaplecze cyfrowe, co w przyszłości napędzi cyfrową transformację firmy bez konieczności nadrabiania technologicznych zaległości.

Zrównoważona transformacja cyfrowa w praktyce

W dobie wzmożonej cyfryzacji i rosnących wyzwań związanych z ochroną środowiska przedsiębiorcy powinni poszukiwać rozwiązań i partnerów, pozwalających łączyć rozwój biznesu z odpowiedzialnością ekologiczną.

WOJCIECH STRAMSKI
prezes Beyond.pl, dostawcy usług data center, chmury i Managed Services

Sektor IT ma na tym polu dokonania i może być przykładem dobrych praktyk. Co więcej, może pomóc innym biznesom stać się bardziej niskoemisyjnymi. Jakie praktyczne działania może podjąć firma, aby funkcjonować konkurencyjnie na rynku i kontynuować rozwój w sposób bardziej odpowiedzialny i zrównoważony?

Energia ze źródeł odnawialnych

Jednym z oczywistych kroków w ramach transformacji ekologicznej firmy jest przejście na odnawialne źródła energii. Wybór dostaw energii pochodzącej ze źródeł odnawialnych gwarantowanych certyfikatami pochodzenia znacząco redukuje ślad węglowy przedsiębiorstwa. Wybór OZE wspiera również osiągnięcie celów dotyczących ograniczania emisji gazów cieplarnianych, jeżeli organizacja takowe posiada oraz ma istotne znaczenie w kontekście raportowania niefinansowego.

Warto wspomnieć, że ograniczenie emisji CO_2 można realizować również poprzez wybieranie takich partnerów, którzy sami stawiają na „zieloną" energię. Przykład? Jeśli firma potrzebuje wsparcia w postaci utrzymania infrastruktury IT w zewnętrznym centrum danych, powinna zdecydować się na operatora, który zasila swoje obiekty energią ze źródeł odnawialnych. Przeniesienie zasobów IT do takiego centrum danych redukuje ślad węglowy utrzymywanej infrastruktury IT. Używając dedykowanych kalkulatorów bardzo łatwo samodzielnie sprawdzić, o ile można zredukować ślad węglowy firmowej infrastruktury IT, utrzymując ją samodzielnie vs. u wyspecjalizowanego dostawcy kolokacji.

Optymalizowanie zużycia zasobów

Aby skutecznie realizować cele związane z ochroną środowiska, przedsiębiorstwa powinny regularnie monitorować swoje zużycie energii. W branży IT i centrów danych istotnym wskaźnikiem jest efektywność energetyczna, tzw. PUE (power usage effectiveness). Im niższy wskaźnik, tym bardziej efektywnie wykorzystywana jest energia w obiekcie. W naszym przypadku, m.in. dzięki zaawansowanym technologiom chłodzenia, osiągamy wskaźnik PUE 1.2, co stanowi jeden z najkorzystniejszych wskaźników w Polsce i regionie, podczas gdy większość europejskich centrów danych osiąga PUE 1.5-1.8. Oprócz optymalizacji zużycia energii warto również monitorować efektywność zużycia wody. Wskaźnik WUE (water usage effectiveness) pozwala ocenić, jak efektywnie zarządza się wodą w centrum danych, która używana jest m.in. do systemów chłodzenia.

Warto również poszukiwać nowych, kreatywnych sposobów na gospodarowanie zasobami, które powstają np. jako skutek uboczny prowadzonej działalności. W przypadku centrów danych takim zasobem jest ciepło powstające w wyniku pracy serwerów, które może być z powodzeniem wykorzystywane do ogrzewania budynków lub wody użytkowej. Jako Beyond.pl mamy doświadczenie w odzysku ciepła na własne potrzeby – od uruchomienia obiektu Data Center 2 w 2016 r. ciepło generowane w komorach serwerowych jest wykorzystywane do ogrzewania budynku biurowego zlokalizowanego na terenie kampusu.

Certyfikaty, normy i działania uzupełniające

Dbałość o środowisko może być potwierdzona certyfikatami i normami, które są uznawane na całym świecie. Przykładem jest norma ISO 14 001, która certyfikuje system zarządzania środowiskowego w firmie. Posiadanie takiego certyfikatu świadczy o wdrożeniu w przedsiębiorstwie procesów, które minimalizują negatywny wpływ działalności firmy na środowisko naturalne. Wprowadzenie systemów zarządzania środowiskowego zgodnych z międzynarodowymi standardami powinno być jednym z głównych celów dla firm dążących do zrównoważonego rozwoju.

Zwróć uwagę na partnerów

Firmy wdrażające strategię ESG powinny współpracować z partnerami podzielającymi filozofię prowadzenia biznesu w oparciu o modele odpowiedzialne i zrównoważone, i w ten sposób tworzyć łańcuch wartości, który będzie skutecznie wspierał zrównoważoną transformację. Wybór dostawców, którzy także kierują się zasadami zrównoważonego rozwoju, może znacząco przyczynić się do realizacji celów ESG. Przedsiębiorstwa korzystające z usług chmurowych lub centrodanowych powinny np. zwracać uwagę na to, czy ich dostawcy korzystają z energii odnawialnej i wdrażają projekty wspierające zrównoważoną transformację.

Działanie na rzecz ochrony środowiska i klimatu nie jest trendem, ale koniecznością, którą współczesne przedsiębiorstwa muszą uwzględnić w swojej działalności. Ważnym aspektem jest również rosnąca liczba regulacji prawnych tworzących nowe standardy – dotyczących raportowania pozafinansowego czy efektywności energetycznej. Zmniejszenie śladu węglowego, efektywne zarządzanie zasobami oraz współpraca z odpowiedzialnymi partnerami to fundamenty, na których można budować zrównoważony rozwój, niezależnie od branży, w której się funkcjonuje.

Wyścig zbrojeń w cybersecurity

Mamy wyścig zbrojeń w cybersecurity. Wojna czerwonych z niebieskimi, jasnej strony z ciemną. Trwa już od dawna i warto się mu przyjrzeć, żeby lepiej zrozumieć sytuację, w jakiej dzisiaj jesteśmy. Sprawa wygląda tak, że bezpieczeństwo cyfrowe nigdy nie było tak ważne i tak doceniane, jak jest teraz. Zbudujmy sobie odpowiedni kontekst, przechodząc przez najważniejsze etapy tytułowego wyścigu zbrojeń. Zobaczymy, jak rozwijały się metody ataku, a jak ochrony, a później zobaczymy, jak sprawa ma się dzisiaj i będzie miała w przyszłości.

BARTŁOMIEJ SKOWRONEK
Cybersecurity Offering Lead, Ideas Accelerator Lead and Architect w GFT Poland

Tour de security

Przeskoczymy czasy zimnej wojny – pojęcia bezpieczeństwa cyfrowego sprowadzały się głównie do szyfrowania wiadomości i ochrony fizycznej: sprzętu używanego do tego celu, jak i ludzi mających czy to wiedzę, czy będących kurierami, szpiegami. Nie chcę tutaj zagłębiać się w niuanse, bo daleko mi w tym do Wołoszańskiego, ale istotne jest, że taki stan (przynajmniej w Polsce) utrzymywał się do lat 90.

Lata transformacji ustrojowej to etap, kiedy komputery poważnie zagościły w polskich firmach, organizacjach i urzędach. Wraz z dość swobodną dystrybucją oprogramowania pojawiły się pierwsze wirusy. Na początku były to proste aplikacje doklejające się do plików wykonywalnych czy odpowiednich miejsc na dyskietkach, programy rezydentne (skuteczniej rozprzestrzeniające się). Szybko ewoluowały z programów, które nieco uprzykrzały życie (np. grając w tle na PC Speakerku melodię Yankee Doodle-a) do wersji niszczącej dane. Jednocześnie rozwinęły się też ataki na sieci telekomunikacyjne: od 2600 Hz i dialerów do masowego klonowania kart magnetycznych umożliwiających „darmowe" rozmowy telefoniczne z budek. W USA to czas, gdy Kevin Mitnick pokazuje, jak skuteczna jest inżynieria socjalna połączona ze znajomością podatności sieci telefonicznych i procesów autoryzacji. Obrona to jednak nadal głównie ochrona dostępu fizycznego, choć pojawiają się programy antywirusowe. Mamy świetny polski akcent w postaci bardzo dobrego programu antywirusowego autorstwa śp. Marka Sella: MkS_Vir.

Gdy tylko zaczęliśmy podłączać komputery do sieci, pojawiły się zagrożenia związane ze zdalnym dostępem. Wspomnę tu suchar o Internet Explorerze: służył do przeglądania internetu z komputera i vice versa. Usługi ActiveX, VBS czy rozwiązania od Macromedia szybko nam pokazały, jak można wykradać dane i infekować komputery, używając podatności platform. Same wirusy uzyskały zdolność polimorfizmu, więc gdy social engineering przesiadł się na IRCa, ICQ, Gadu-Gadu oraz strony z oprogramowaniem (gratis zainfekowane instalatory) – problemy z utratą danych, niedziałającymi Windowsami stały się zmorą w firmach i naszych domach. Do tego pojawił się spam. Dużo spamu. Na to wszystko odpowiedzią były pierwsze firewalle (Linuxowe iptables -j DROP, jak i rozwiązania dla Windows), antywirusy otrzymały heurestykę, a filtry antyspamowe skuteczne uczenie maszynowe w postaci klasyfikatorów Bayes'a.

Szybko się to rozwinęło w latach dwutysięcznych. Szczególnie, że organizacje poruszały się w bardzo różnych światach technologicznie. Ataki drive-by zaczęły być powszechne i skuteczne, podatności usług powodowały wycieki danych i przejęcia kontroli (wspomnę tylko o SMB i SNMP), zostaliśmy zaznajomieni z pojęciem zero-day. Zmieniła się sieć telekomunikacyjna: komórki spowszechniały, więc pojawiły się ataki na nie (np. zatrute SMSy), a klonowanie kart SIM stało się poważnym problemem dla polskich banków. Ataki skutecznie wykorzystywały podatności wszystkich warstw: od platform, przez usługi (np. bazy danych) i OS, do warstwy sieciowej i sprzętowej. Do obrony wystawiliśmy skuteczne filtry antyspamowe i black/white listy, firewalle – tym razem już jako sprzętowy appliance (np. od Cisco i F5), VPNy, rezydentne antywirusy (w tym także darmowe i open-source). Temat bezpieczeństwa systemów operacyjnych wzięliśmy na poważnie, tworząc SELinuxa oraz zabezpieczając (wreszcie) Windowsa. Szyfrowanie zaczęło być wymogiem, a nie ciekawostką (HTTPS everywhere, Tor).

Wkrótce później ransomware „nauczył się" szyfrować stacje robocze i kopie zapasowe, zwalając z nóg wiele firm, np. Norsk Hydro w 2019 r. Ataki DoS dostały dodatkową literkę D, dzięki powszechnym botnetom. Nasze komórki zrobiły się „smart", ale nie na tyle, żeby uniknąć ataków na ich systemy operacyjne i masy złośliwych, szkodliwych aplikacji. Ataki stały się wielowektorowe, z zaawansowanym zapleczem social engineering. Przestępstwa stały się usługą przemysłową. Crime-as-a-Service doszedł do poziomu, gdzie powstały zarówno przedsiębiorstwa zajmujące się internetowym scamem, jak i sklepy internetowe oferujące pakiety numerów kart kredytowych z gwarancją minimum 15 proc. dobrych CVC lub zwrot pieniędzy. Więc wymyśliliśmy Web Application Firewalle do ochrony naszych aplikacji webowych. Zaczęliśmy stosować sandboxing i skuteczną ochronę w czasie rzeczywistym. Zaczęliśmy używać wieloetapowego uwierzytelniania i rozwiązań sprzętowych do generowania haseł jednorazowych (RSA, YubiKey), a samo uwierzytelnianie zaczęło wykorzystywać analizę behawioralną. Systemy operacyjne i usługi zyskały na bezpieczeństwie poprzez hardeningi.

Usług zrobiło się więcej – skala rozwinęła się wraz z erą chmury, mobile i IoT. Ataki na podatności usług, bezwzględne wykorzystanie luk zarówno w ich domyślnych zabezpieczeniach, jak i w domyślnych ustawieniach sprzętu (czytaj: podłączonych do Internetu komputerów) zostały „wzbogacone" o ataki na popularne biblioteki (log4j, ssh, xz...) i sieci bezprzewodowe (cały alfabet: od Bluetootha, przez GSM i Tetra po WEP, WPA). Do tego doszły wycieki danych, aplikacje agresywnie zbierające dane i sprzęt, w tym taki, po którym nie spodziewamy się tak drastycznych naruszeń prywatności (raport 'Privacy Nightmare on Wheels': Every Car Brand Reviewed By Mozilla).

Chronimy się jeszcze bardziej zaawansowanym hardeningiem, oprogramowaniem monitorującym, zmianą protokołów i szyfrowaniem (teraz już wszędzie i zawsze). Hashtagi #zerotrust #zeroknowledge #securitybydesign #SecureSDLC mamy wygrawerowane na ścianach („writing is on the wall").

Kolejny ważny etap to ataki celowane, szczególnie takie z zapleczem rządowym. Nastąpiło połączenie pracy operacyjnej (szpiegowskiej) z wieloetapowymi atakami, gdzie pokonanie ochrony zasobów cyfrowych było ważnym elementem. Dla mnie tym przełomowym, bo i głośnym, i skutecznym, i szokująco zaawansowanym był atak na irańską placówkę wzbogacania uranu – Stuxnet w 2010 r. Takie ataki – niestety – trwają, co pokazują ostanie wydarzenia: wybuchające pagery i walkie-talkie (znów Iran), tym razem z wieloma ofiarami... To także multum ataków, o których nie słyszymy – w tym na polską infrastrukturę i firmy, oraz takie, które giną w natłoku informacji – jak np. tegoroczny atak na przepompownię wody w małym teksańskim miasteczku. Te wydarzenia pokazują, że bezpieczeństwo cyfrowe stało się istotne na co dzień, ale także – co bardzo znaczące – że drużyna „niebieska" zaczęła odpowiadać nie tylko za ochronę dóbr materialnych, ale też za ochronę zdrowia i życia... To daleka droga: od „pana Mietka od komputerów", przez „Dział IT" przeszliśmy szybko do zespołów i jednostek wojskowych cyberse-

> Cała branża cybersecurity rośnie i będzie rosła w najbliższych latach – to pewnik, więc i zastosowania AI będą się rozszerzały.

> Oprócz raportowania poincydentowego równie ważna w organizacjach jest zgodność z wymogami formalnymi i standardami i politykami. Tutaj także sztuczna inteligencja nas odciąża i szybko, dokładnie przeanalizuje środowisko i porówna z wymaganiami.

curity. Tutaj jeszcze jedna ważna zmiana: od tego roku mamy w Polsce nową domenę wojny: wojska ochrony cyberprzestrzeni dołączyły do wojsk lądowych, powietrznych i morskich.

Etap AI

Możemy popatrzeć na sztuczną inteligencję jako następny poziom rozwoju automatyzacji, czyli inteligentnego następcę regułek i „logiki biznesowej", ale to wypłyca zmianę, jaka się teraz rozpoczęła. Spróbujmy, w tej części artykułu, przyjrzeć się, jak sztuczną inteligencję wykorzystują obie strony i pomyślmy, jakie to może mieć konsekwencje.

Ciemna strona + AI

Zacznijmy od malware-u wspomaganego AI. Można pomyśleć, że to ewolucja polimorfizmu, który już znamy, ale patrząc na Emotet, to już kilka lat temu mieliśmy malware, który skutecznie i sprytnie (inteligentnie?) unikał wykrycia, będąc platformą (Crime-as-a-Service...) do ataków ransomware. Czyli techniki unikania wykrycia też się poprawiają z AI (vide Zeus), rozpoznają wzorce alarmów, ruchu sieciowego i to pozostając poniżej progu detekcji. Lepiej działający malware oznacza, że liczba ataków będzie rosła, a zastosowana sztuczna inteligencja – że oprogramowanie będzie się (samodzielnie i w sposób nadzorowany) uczyło na poprzednich atakach. Będzie też potrafiło wykorzystać informacje zdobyte z innych części organizacji (np. godziny zmian i dane osób pracujących z ataku na system kadrowy).

Ataki DDoS stały się bardziej dopasowane, ale też adaptują swoje techniki szybciej, w czasie rzeczywistym. Skala i łatwość koordynacji ataków, gdy używamy AI, rośnie diametralnie, więc czeka nas dalsza industrializacja ataków, a przy tym równoczesne, innego typu ataki na dostawców, usługodawców czy organizacje powiązane. Narzędzia do obrony, które nie będą umieć skutecznie rozpoznać ataku (nie nauczą się nowych, dynamicznych metod) znikną z rynku, a dobrze uczące się AI w systemach obronnych to twarde wymaganie, szczególnie przy atakach celowanych.

Samo uczenie maszynowe, w tym modele LLM też są mocno atakowane. Celem jest tutaj zarówno oszukanie broniących (ukrywanie się), jak i doprowadzenie AI do wykonania (nie)pożądanych akcji. Mówimy o atakach, w których zatrucie danych wejściowych spowoduje np., że nasz samochód zinterpretuje znak stopu jako pierwszeństwo, ale też, że nasze AI się nauczy, że wyciekające z firmy dane to norma. Do tego dochodzą ataki na biblioteki (np. phasing dążący do DoS), na interfejsy (nota bene tu też wpada prompt engineering). Pamiętajmy, że nadal mamy pod spodem wszystkie klasyczne elementy i warstwy do ochrony. Czyli wiarygodne źródła danych uczących będą coraz bardziej pożądane, a co za tym idzie – certyfikowane, nadzorowane, czyli drogie. Modele AI będzie zaś trzeba skutecznie zabezpieczyć przed nowymi technikami i metodami ataków – powstaje kolejna specjalizacja w cybersecurity.

Pozyskiwanie wiedzy wspomagane AI jest też łatwiejsze. Social engineering, a w szczególności biały wywiad, robi się superprosty, a pozyskane informacje są coraz szybciej (automatyzacja...) wykorzystywane np. do spear phishingu czy whalingu. Przykłady już mieliśmy przy atakach na CxO (Pathe), ale użycie AI dodaje przekonujących szczegółów i spersonalizowane ataki zaczną być powszechne. Pożegnajmy nigeryjskiego księcia. Teraz do nas zadzwoni „kuzyn" albo „mama" w potrzebie. Generatywne AI wkrótce będzie umiało wstawić sztucznych (aktywnych!) uczestników do telekonferencji i wyciągać w ten sposób wrażliwe dane. Skutek taki, że uwierzytelnianie nie tylko będzie potrzebne silne, ale też stałe – działające w tle, wspomagane AI. Zwiększy się nacisk na ochronę danych – firmowych i prywatnych – ponieważ wszelkie naruszenia będą miały większe i szybsze konsekwencje. Z drugiej strony kwestia zapomnienia w sieci, usuwania danych, zyska na znaczeniu – może warto kupić akcje firm oferujących takie usługi.

SolarWinds pokazał z kolei, że można bardzo łatwo zaatakować przez dostawców. Ataki na biblioteki, że wykorzystanie podatności może być powszechne (log4j, ssh), a celowo ukryte – trudne do wykrycia (patrz: wielomiesięczne implantowanie backdoora w xz). AI tutaj pozwoli na szybkie sprawdzenie zabezpieczeń całego naszego łańcucha dostaw, równie szybkie wykorzystanie wszelkich znalezionych podatności. Celowany atak na firmę A będzie oznaczał atak na wszystkich z nią związanych. Urosną wymagania, w tym dla małych dostawców, co podniesie próg wejścia na rynek, ale też wymusi #securebydesign i #SecureSDLC. Czekam na rankingi bezpieczeństwa bibliotek i frameworków. Tak samo jak teraz czytamy, który framework webowy jest najszybszy – tak będziemy śledzili, który jest najbezpieczniejszy.

Postępuje automatyzacja narzędzi, które – choć niekoniecznie służące do złych celów (Sniper czy Autosploit) – pokazują, że z AI lepiej zoptymalizowany jest cały proces ataku: identyfikacja, priorytetyzacja i wykorzystanie. To już nie statyczna i dynamiczna analiza kodu – to wspomagane AI wykrywanie podatności, napisanie exploita i jego uruchomienie na znalezione słabiej zabezpieczone cele. W komercyjnej przestępczości idzie to w kierunku usług „click'n'play": wybierasz cel, płacisz, twój cel automatycznie zostanie przeanalizowany i zaatakowany z użyciem znalezionej podatności zero-day. Każda świeżo opublikowana usługa czy aplikacja natrafi na tak AI-zautomatyzowany atak.

> Lepiej zaczęliśmy rozumieć znaczenie i wagę danych, procesów i rozwiązań IT, które mamy i od których tak bardzo jesteśmy zależni.

Jestem Edgar, jestem AI i chronię to miejsce

Żeby nie było tak czarno, to popatrzmy na „jasną stronę mocy", gdzie sztuczna inteligencja pomaga, ułatwiając nam zadania obronne, jak i wspomagając naszą codzienną pracę. Zobrazujmy to na przykładzie cyklu życia incydentu security. Wiemy już, że wykrycie naruszeń chronionej infrastruktury robi się trudniejsze, ale dzisiejsze systemy monitorujące potrafią przetworzyć nadludzką ilość spływających logów i zdarzeń. Co więcej, uczą się, jak wygląda nasza infrastruktura, które komponenty ze sobą rozmawiają (i jak dużo informacji przesyłają), kiedy to się dzieje, ale także kiedy my pracujemy, na czym i skąd. Na bazie takiego szerokiego i szczegółowego zestawu informacji obronna sztuczna inteligencja dużo łatwiej i sprawniej wykrywa nietypowe zachowania, zdarzenia – co zarówno nas odciąża od stałego śledzenia skomplikowanych aplikacji oraz priorytetyzuje dla nas zdarzenia. Po takim automatycznym triage w reakcji na ataki systemy z AI wskażą nam źródło ataku, jego przebieg, zasugerują rozwiązania lub samodzielnie podejmą akcje. Ponadto już po ataku mamy od razu zebrane i przeanalizowane informacje przygotowane w formie raportu. To nie przyszłość: rozwiązania CNAPPowe Laceworka, Sentinela, Palo Alto czy firewalle next-gen opierają się na AI i dzięki temu są dużo skuteczniejsze. Oprócz raportowania poincydentowego równie ważna w organizacjach jest zgodność z wymogami formalnymi i standardami i politykami. Tutaj także sztuczna inteligencja nas odciąża i szybko, dokładnie przeanalizuje środowisko i porówna z wymaganiami. A jeśli pozwolimy, to także samodzielnie naprawi źle skonfigurowane usługi, usunie podatności.

Takie wykorzystanie AI dąży do poziomu, w którym nasz system obronny będzie dobrze rozumiał także, co chroni – jak ważne dane są chronione, jakie procesy biznesowe są chronione. W przypadku ataku chroni kluczowe elementy, uniemożliwiając utratę danych, ale także zachowując zdolności biznesowe.

A mamy co chronić: coraz więcej danych zbieramy i generujemy, a także rośnie świadomość ich roli, i co za tym idzie, także wymagania formalno-prawne. Dlatego AI wykorzystujemy w szerokim zakresie: od automatycznej klasyfikacji danych, przez ochronę generatywnego AI, po wykrywanie szarego IT. Tutaj mówimy o systemach Data Loss Prevention, antyransomware i inteligentnych firewallach potrafiących zablokować wykryty wyciek danych (np. przesyłanie dużej paczki danych z miejsca, które do tej pory tego nigdy nie robiło).

Według mnie pójdzie to dalej, w stronę systemów wręcz cenzorskich, które będą umieć wyciąć kawałek rozmowy na telekonferencji, wyczernić kawałek ekranu, żeby zapobiec wyciekowi danych. Przede wszystkim jednak te systemy będą zasilały wiedzę głównego obronnego AI. W ten sposób dochodzimy do tego zastosowania, które jest najjaskrawsze w tej chwili – AI, z którym możemy porozmawiać.

Takie główne AI wspomaga nas na wszystkich etapach: wyszukuje, analizuje, śledzi zdarzenia, pomaga zrozumieć, odsiać, ale także podsumować, zasugerować rozwiązanie i zareagować, czyli wymusić zmiany. Ponadto doskonale zdaje egzamin, unifikując dostęp do wielu zintegrowanych narzędzi, które mamy pod spodem, włączając w to narzędzia operacyjne. Zyskujemy asystenta, który potrafi rozmawiać we wszystkich nastu- (-dziesięciu?) odmianach i językach kwerend, CLI i API, jakie mamy w dzisiejszym środowisku. W różnym stopniu zaawansowania mamy to już dzisiaj, a rozwinie się to albo w kierunku omnipotencjalnego obronnego AI (mi się tutaj pojawia w głowie Edgar z hotelu w Altered Carbon, stąd śródtytuł), albo „prompt hell" – gdzie dostaniemy mnóstwo bardzo rozmownych AI, z którymi porozumienie będzie koszmarem.

> Możemy popatrzeć na sztuczną inteligencję jako następny poziom rozwoju automatyzacji, czyli inteligentnego następcę regułek i „logiki biznesowej", ale to wypłyca zmianę, jaka się teraz rozpoczęła.

Hype na AI, czyli kto prowadzi w wyścigu

Przy szukaniu materiałów łatwiej mi było znaleźć przykłady, gdzie AI jest wykorzystywane do ataku, niż konkrety przy użyciu AI w rozwiązaniach do obrony. Takie skrzywienie potwierdza raport Splunka (State of Security 2024), gdzie na pytanie „Komu bardziej pomoże AI?" większość respondentów odpowiedziała, że atakującym (45 proc. atakującym, 43 proc. broniącym, 12 proc. zrównoważą się). Z drugiej strony może to tylko wrażenie, ponieważ łatwiej mówić o przeszłych zdarzeniach (dokonane ataki), niż o przyszłości (możliwościach, jakie daje AI w obronie). Więc może AI to hype? Lubię Gartnerowski hype-cycle jako narzędzie do zobrazowania etapu, na którym jest dana technologia, i tak dla sztucznej inteligencji conversational AI jest na, albo już za pierwszą górką (hype). Za to rozwiązania używające AI w systemach cybersecurity na pewno są na pierwszej fali wznoszącej. Cała branża cybersecurity rośnie i będzie rosła w najbliższych latach – to pewnik, więc i zastosowania AI będą się rozszerzały.

Patrząc na cały rys historyczny, który prześledziliśmy w artykule, można się też zastanawiać, gdzie prowadzi wyścig zbrojeń, czy robi się coraz gorzej i trudniej. Na pewno zmieniła się skala, więc też „głośniej" i częściej słyszymy o atakach. Przede wszystkim jednak lepiej zaczęliśmy rozumieć znaczenie i wagę danych, procesów i rozwiązań IT, które mamy i od których tak bardzo jesteśmy zależni. To mocne nawiązanie do tego, o czym pisałem wcześniej – od bezpieczeństwa cyfrowego zaczęło też zależeć bezpośrednio zdrowie i życie. Więc nie jest gorzej – bezpieczeństwo cyfrowe stało się dla nas ważniejsze. Myślę też, że poradzimy sobie z kolejnymi etapami wyścigu, nowymi metodami ataków, włączając w to te wspomagane AI – z przekonania, że zawsze dawaliśmy radę w tym wyścigu, a także w momentalnej, sprawnej reakcji na nowe możliwości ze sztuczną inteligencją.

Zresztą kto ma dać radę, jak nie my?

Automatyzacja procesów rekrutacyjnych – narzędzia ATS (Applicant Tracking Systems)

Znam wiele osób, które zmieniły Excela na ATS, ale nikogo, kto po rozpoczęciu korzystania z systemu ATS wrócił do rekrutowania bez takiego narzędzia. To chyba najlepszy argument dla tych, którzy rekrutują i dopiero rozważają wdrożenie systemu ATS.

ANNA SYKUT
Product Marketing Manager w Traffit

Czym jest system ATS?
Zacznijmy od rozwinięcia enigmatycznego skrótu ATS – nazwa ta pochodzi z języka angielskiego i oznacza applicant tracking system (czyli system śledzenia aplikacji).
Z założenia system ATS służy więc do zbierania i zarządzania aplikacjami w prowadzonych procesach rekrutacyjnych. Jest to też nadal kluczowa funkcja każdego takiego systemu.
Pierwsze ATS-y pojawiły się w latach 90. i od tamtego czasu zakres ich możliwości znacznie się rozszerzył. Dlatego dziś nie nazwałabym ich systemami śledzenia aplikacji, a bardziej „systemami zarządzania relacjami z kandydatami" lub „systemami do budowania i zarządzania bazą kandydatów". Ich wszechstronność jest więc imponująca, pomimo że skupiają się tylko na wycinku aktywności HR-owych – tych związanych z rekrutacją.
Na świecie funkcjonuje aż kilkaset dostawców systemów ATS – tylko w samej Polsce jest ich kilka. Polskie działy rekrutacyjne chętnie wybierają rodzime ATS-y, ponieważ są one dostosowane do polskiego prawa pracy oraz RODO. Na całym świecie zaś z systemów ATS korzysta 66 proc. dużych i 35 proc. małych firm (dane z 2023 r.1).

Kto korzysta z systemów ATS?
Na początku istnienia systemów ATS ich użytkownikami byli zwykle pracownicy dużych organizacji. Dzisiaj, dzięki dostępności rozwiązań chmurowych i rozliczanych w modelu subskrypcyjnym (comiesięczna opłata za dostęp do narzędzia) system rekrutacyjny ATS może kupić i używać każdy, kto rekrutuje – niezależnie od skali.
Systemy ATS są wdrażane nie tylko w wewnętrznych działach HR w firmach, ale także przez agencje rekrutacyjne, instytucje publiczne czy nawet freelancerów obsługujących rekrutacje dla swoich klientów.

> Mając na uwadze spektrum funkcji, jakie posiadają systemy ATS, nie są one tylko miłym dodatkiem ułatwiającym pracę, ale praktycznie podstawowym narzędziem pracy zespołów rekrutacyjnych.

Dlaczego firmy inwestują w system ATS?
Powodów, dla których firmy inwestują w systemy ATS jest kilka i w każdej z nich motywacja może być inna. Jednak gdybym miała wymienić te najbardziej popularne, byłyby to:
• Sprawne zarządzanie aplikacjami: w przypadku dużej liczby aplikacji, którymi muszą zaopiekować się zespoły rekrutacyjne niezbędne jest im narzędzie, które pozwoli zbierać je w jednym miejscu, łatwo przeglądać, oceniać i przesuwać na kolejne etapy procesu. Konto w systemie ATS mogą mieć nie tylko osoby rekrutujące, ale też Hiring Managerowie, czyli osoby zaangażowane w proces, np. przyszli managerowie nowo zatrudnianej osoby, czy też weryfikujące wiedzę techniczną lub językową aplikujących. Dzięki wspólnemu i równemu dostępowi do danych obieg informacji jest szybszy i wygodniejszy.
• Dbanie o doświadczenia kandydatów: systemy ATS pozwalają na zadbanie o tzw. „candidate experience", czyli doświadczenia kandydatów. Firmy już dawno zrozumiały, że to, co mówią o nich kandydaci jest niemal tak samo ważne dla jej wizerunku, jak to, co mówią jej klienci. Chcą więc zbudować relacje od pierwszego kontaktu i zagwarantować kandydatom feedback. ATS pozwala zaprojektować proces, zadbać o stronę wizualną oferty (ogłoszenie i formularz aplikacyjny) oraz sprawną komunikację z kandydatami. Jedną z funkcji systemów ATS, które to wspierają jest np. automatyzacja komunikacji e-mail. Wiadomości wysyłane po aplikacji (potwierdzenie wpłynięcia aplikacji), po przeniesieniu na kolejny etap czy np. z linkiem do wybrania terminu rozmowy rekrutacyjnej mogą być wysyłane przez system automatycznie. ATS wykorzysta przygotowany wcześniej szablon e-mail, wyśle wiadomość ze skrzynki rekrutera, a nawet spersonalizuje jego treść!
• Optymalizacja (kosztów i czasu): dobry system ATS pozwala monitorować obciążenie zespołu rekrutacyjnego, automatyzować powtarzalne zadania oraz lepiej zrozumieć, które źródła aplikacji są najbardziej skuteczne. Przy niemałych kosztach publikacji na portalach pracy jest to wiedza na wagę złota. Tutaj warto też wspomnieć o budowaniu własnej bazy kandydatów, czyli zbieraniu zgód na poczet przyszłych procesów i czerpanie z niej, gdy otwiera się nowy wakat.
• Bezpieczeństwo danych: na administratorze danych kandydatów, którym w przypadku rekrutacji jest przyszły pracodawca, spoczywa obowiązek przetwarzania ich zgodnie z RODO. Kandydaci powinni być informowani o tym, kto jest administratorem ich danych (spełniać obowiązek informacyjny), wyrazić stosowne zgody i mieć możliwość ich wycofania. Systemy ATS znacząco ułatwiają spełnienie tych wszystkich obowiązków. Mogłoby się wydawać, że niektóre firmy nie potrzebują systemu ATS, np. małe firmy, które rekrutują głównie offline. Takie firmy często zbierają dane kandydatów w formie papierowej i w plikach Excel. Jednak na każdym, w równym stopniu ciąży obowiązek dbania o prawidłowe procesowanie danych. System ATS umożliwia dodanie skanów dokumentów aplikacyjnych lub wygenerowanie linku do formularza aplikacyjnego, który następnie można umieścić na ulotkach i rozdawać na targach pracy. Działania offline nie wykluczają możliwości korzystania z rozwiązań chmurowych do zbierania i przetwarzania danych. A danych w chmurze nie da się tak łatwo zgubić lub zniszczyć.

> Podstawową funkcją każdego systemu ATS na świecie jest tworzenie rekrutacji, ogłoszeń rekrutacyjnych oraz formularzy aplikacyjnych, a także zarządzanie aplikacjami w procesie.

Jakie funkcje mają systemy ATS?
Podstawową funkcją każdego systemu ATS na świecie jest tworzenie rekrutacji, ogłoszeń rekrutacyjnych oraz formularzy aplikacyjnych, a także zarządzanie aplikacjami w procesie.
Użytkownicy takiego systemu mogą zwykle zobaczyć listę kandydatów w danej rekrutacji, przypisać im słowa kluczowe, zostawić notatkę czy odnotować jakąś aktywność związaną z osobą aplikującą. Analogicznie, jak sprzedawcy robią to z klientami w systemach CRM.
Systemy ATS umożliwiają też integrację ze stroną Kariera, łatwą publikację ogłoszeń rekrutacyjnych w social mediach czy na portalach pracy. Mogą być też zintegrowane z innymi niezbędnymi narzędziami rekrutera, np. z kalendarzem, skrzynką e-mail czy systemem do wysyłki SMS. Tym samym stają się swoistym centrum dowodzenia prowadzonymi rekrutacjami.
Nowoczesne systemy ATS nie przespały też boomu na sztuczną inteligencję i wdrożyły funkcje na nim oparte, np. pisanie ogłoszeń rekrutacyjnych czy analiza danych.

Słowem zakończenia
Mając na uwadze spektrum funkcji, jakie posiadają systemy ATS, nie są one tylko miłym dodatkiem ułatwiającym pracę, ale praktycznie podstawowym narzędziem pracy zespołów rekrutacyjnych.
Znam wiele osób, które zmieniły Excela na ATS, ale nikogo, kto po rozpoczęciu korzystania z systemu ATS wrócił do rekrutowania bez takiego narzędzia. To chyba najlepszy argument dla tych, którzy rekrutują i dopiero rozważają wdrożenie systemu ATS.

1. *https://gohire.io/blog/how-many-companies-use-applicant-tracking*

Cyberbezpieczeństwo to nie Yeti

Cyberzagrożenia to zjawiska często niewidoczne dla przeciętnego użytkownika. Ataki z zasady przebiegają w tle, a ich efekty mogą być odczuwalne dopiero po pewnym czasie, gdy ofiary tracą dostęp do zasobów finansowych czy cyfrowych. Mimo że pozornie niedostrzegalne, skutki cyberzagrożeń są mierzone w milionach złotych.

KRZYSZTOF SZCZEPAŃSKI
dyrektor Departamentu Bezpieczeństwa i Ryzyka w KIR

Z badania „Global Data Protection Index 2023" firmy Dell Technologies wynika, że w ubiegłym roku ponad połowa firm (54 proc.) padła ofiarą cyberataku lub incydentu, który uniemożliwił dostęp do danych. Z kolei ich koszty sięgnęły 1,41 mln dol., co oznacza dwukrotny wzrost w porównaniu z 2022 r. (0,66 mln dol.).

Cyfrowa transformacja napędza zagrożenia

Wkraczamy już w czwartą dekadę rozszerzającej się powszechnej dostępności technologii cyfrowej, która dzisiaj kształtuje obraz współczesnej gospodarki. Praktycznie w każdym aspekcie naszego życia stosujemy już rozwiązania cyfrowe, które wspierają pracę, zapewniają rozrywkę czy po prostu pomagają w codziennym życiu.

Cyberbezpieczeństwo odzwierciedla te przemiany. Kiedyś – jeszcze jako bezpieczeństwo IT – polegało na ochronie zasobów informatycznych. Dziś skupia się na zabezpieczaniu procesów i danych, ze szczególnym naciskiem na przetwarzane w systemach dane użytkowników.

Zmieniające się otoczenie wymusza bardziej proaktywne podejście do cyberbezpieczeństwa. Sieć staje się bowiem areną coraz bardziej zaawansowanych ataków cybernetycznych. Przestępcy nadal sprawnie posługują się socjotechniką, wykorzystują ludzką ciekawość, lęki czy chęć zysku, podszywają się pod firmy i instytucje, by wyłudzić dane i środki finansowe. Problem w tym, że skala zagrożeń rośnie i zwiększa się też powierzchnia możliwych do przeprowadzenia ataków. W pandemii nowe możliwości dla cyberprzestępców otworzyło przejście na pracę zdalną i hybrydową. Biorąc pod uwagę zmiany geopolityczne i nowe scenariusze wojny hybrydowej – rozumianej również jako rozszerzenie pola walki na cyberprzestrzeń – należy się spodziewać, że w przyszłości najistotniejsze zagrożenia będą płynęły z łańcucha dostaw i zależności od zaawansowanych komponentów technologicznych.

Rośnie kreatywność cyberprzestępców

W dobie popularyzacji technologii sztucznej inteligencji trzeba się też przygotować na coraz więcej ataków przygotowanych na podstawie zaawansowanych algorytmów AI, np. wykorzystujących narzędzia deepfake.

Jak wynika z „Microsoft Digital Defense Report", o ile incydenty cyberbezpieczeństwa odnotowywane w 2022 r. często miały na celu osiągnięcie korzyści finansowych za pomocą oprogramowania ransomware, to w 2023 r. największą motywacją cyberprzestępców była kradzież informacji, potajemne monitorowanie komunikacji lub manipulowanie opinią społeczną.

Widać dokładnie transformację mającą zagwarantować atakującym możliwie najszerszy dostęp i możliwość wpływu na szerokie grono odbiorców, pozwalające na chirurgiczną precyzję w realizowaniu swoich celów. Zagrożenia związane z wyłudzeniami czy ransomware nie przestaną występować – po prostu te nowe, bardziej zaawansowane, staną się istotniejsze.

> Systemowe uporządkowanie kwestii cyberbezpieczeństwa podejmowane jest na poziomie regulacyjnym.

Niewidoczne działania, bolesne skutki

Ataki w cyberprzestrzeni mogą spowodować wyciek poufnych informacji, ogromne straty finansowe i finalnie – utratę reputacji organizacji. Firmy przechowują ogromne ilości danych klientów, pracowników i partnerów biznesowych, a zabezpieczenie ich stanowi kluczowy aspekt działalności i ochrony interesów każdego przedsiębiorcy. Rosnąca ilość informacji podlegających przetwarzaniu zwiększa ekspozycję na ryzyko, które trzeba właściwie ocenić.

Współczesne państwa również są coraz bardziej uzależnione od infrastruktury cyfrowej. Ataki na systemy krytycznej infrastruktury, takie jak elektrownie, sieci energetyczne czy systemy obronne, mogą mieć poważne konsekwencje dla bezpieczeństwa narodowego, prowadzić do awarii systemów informatycznych, co może zakłócić działanie firm, instytucji publicznych i innych organizacji.

Bez edukacji, prawa i technologii nie ma cyberbezpieczeństwa

Systemowe uporządkowanie kwestii cyberbezpieczeństwa podejmowane jest na poziomie regulacyjnym. Unijny akt o odporności cybernetycznej (CRA) czy dyrektywa NIS2 wymagają proaktywnego podejścia do bezpieczeństwa, wdrożenia procesów zarządzania ryzykiem i opracowania planów reagowania.

Niezależnie od wymagań regulacyjnych wszystkie organizacje i każdy użytkownik z osobna powinni jednak zweryfikować swoje zachowania w cyberprzestrzeni w kontekście ewolucji zagrożeń. Kluczowe jest ograniczone zaufanie i bardzo krytyczna postawa do wszelkich informacji – zwłaszcza takich, które nakłaniają do wykonania wcześniej nieplanowanych działań lub mających na celu zmianę opinii.

Droga do zminimalizowania skutków ataków musi jednak w pierwszej kolejności prowadzić przez stosowanie mechanizmów technologicznych, narzędzi i środków organizacyjnych opartych na świadomości ludzi korzystających z dobrodziejstw ery cyfrowej.

W miarę jak technologia staje się bardziej powszechna, edukacja na temat bezpieczeństwa cyfrowego również się rozwija. Coraz więcej osób rozumie, że korzystanie z internetu i urządzeń elektronicznych wiąże się z pewnym ryzykiem. Użytkownicy są bardziej ostrożni w zakresie stosowania haseł i bezpiecznych zachowań w sieci (np. klikanie podejrzanych linków). Organizacje rządowe, instytucje edukacyjne i firmy prowadzą kampanie informacyjne na temat cyberbezpieczeństwa. To pomaga podnieść świadomość i zachęca do stosowania dobrych praktyk.

Coraz większa świadomość cyberbezpieczeństwa, stosowanie zaawansowanych technologii zabezpieczeń, a także wymiana informacji przyczynią się do wzrostu odporności całych sektorów gospodarki, a w tej perspektywie – całego społeczeństwa. Spierając się o to, czy cyberbezpieczeństwo jest jak Yeti, chyba najlepiej, by było prawdziwe, ale niewidoczne dla nas.

Intuicyjne interfejsy w przemyśle 4.0 – klucz do wydajnej współpracy człowieka z maszyną

Jak wynika z raportu „World Robotics Report", instalacja robotów przemysłowych w Europie wrosła w 2023 r. o 9 proc., do poziomu 92 393 jednostek.

JACEK ZARZYCKI
Business Development Manager w Eaton

Dynamiczny rozwój automatyzacji w regionie napędza głównie przemysł samochodowy, który od lat stawia na innowacyjne technologie. Sukces nowoczesnego przemysłu nie zależy jednak wyłącznie od zaawansowanych funkcji wykorzystywanych maszyn. Kluczowe jest także zapewnienie prostoty ich obsługi, dostosowanej do potrzeb nowej generacji operatorów.

W przeszłości opanowanie obsługi maszyn wymagało lat praktyki. Dziś firmy muszą zapewnić, że nowe technologie będą zrozumiałe i łatwe w obsłudze od pierwszego dnia. Intuicyjne interfejsy pozwalają na szybkie wdrażanie pracowników i redukcję błędów operacyjnych, co ma kluczowe znaczenie w obliczu niedoboru wykwalifikowanej kadry oraz dużej rotacji wśród operatorów.

Łatwość użytkowania jako fundament wydajności

Intuicyjny interfejs użytkownika to harmonijne połączenie sprzętu i oprogramowania, które wspiera naturalną interakcję człowieka z maszyną. Aby spełniał swoją funkcję, powinien być prosty do nauki, wygodny w obsłudze i łatwy do zapamiętania. Dzięki temu nie tylko ułatwia komunikację, ale także skraca czas szkolenia, minimalizuje ryzyko błędów i zwiększa elastyczność w pracy. Ostatecznie przekłada się to na wyższą produktywność, lepszą jakość procesów oraz większe bezpieczeństwo użytkownika.

Nowoczesne maszyny wyposażone w inteligentne komponenty wspierają produkcję na wielu poziomach. Umożliwiają predykcyjną konserwację, co znacząco zmniejsza ryzyko przestojów i pozwala na bardziej efektywne zarządzanie czasem pracy urządzeń. Mogą usprawniać proces instalacji i uruchamiania, skracając czas potrzebny na wdrożenie nowych maszyn. Wreszcie, ich zdolność do przetwarzania dużych ilości danych w czasie rzeczywistym pozwala na optymalizację procesów produkcyjnych i zmniejszenie kosztów operacyjnych.

Kluczowe aspekty projektowania nowoczesnych interfejsów przemysłowych

Jednym z najważniejszych wyzwań w projektowaniu nowoczesnych interfejsów typu człowiek-maszyna (HMI) jest znalezienie równowagi między rosnącą złożonością technologii a jej dostępnością dla użytkowników. Aby interfejs spełniał swoje funkcje, musi zapewniać przejrzysty wgląd w kluczowe informacje oraz umożliwiać podejmowanie szybkich i trafnych decyzji w czasie rzeczywistym. Dodatkowo współczesne interfejsy powinny być uniwersalne, dostosowane do różnych poziomów doświadczenia operatorów. Równie istotne jest wbudowanie funkcji zabezpieczających, które minimalizują ryzyko błędów operacyjnych i wspierają rozwiązywanie problemów. W efekcie dobrze zaprojektowany interfejs staje się narzędziem wspierającym operatorów w codziennej pracy, maksymalizując wykorzystanie potencjału maszyn bez zwiększania obciążenia poznawczego.

Przyszłość współpracy na linii człowiek-maszyna

Kierunki rozwoju technologii w przemyśle wskazują na dalszą integrację systemów IT i OT, co pozwoli na skuteczniejsze wykorzystanie danych produkcyjnych do optymalizacji procesów. Coraz większe znaczenie mają również technologie immersyjne, takie jak rzeczywistość rozszerzona (AR) i wirtualna (VR), które wspierają szkolenia i symulacje pracy. Jednocześnie nowe modalności interakcji, takie jak sterowanie głosem czy gestami, otwierają możliwości bardziej naturalnej i intuicyjnej współpracy z maszynami.

Rosnącą popularnością cieszą się także roboty współpracujące z ludźmi, tzw. coboty, które wymagają nowego podejścia do projektowania interfejsów. Intuicyjne i łatwe w obsłudze narzędzia stają się fundamentem harmonijnej współpracy człowieka z maszyną, co stanowi centralny element nadchodzącej ery Przemysłu 5.0.

Źródła:
https://www.therobotreport.com/ifr-4-million-robots-operating-globally-world-robotics-report/