Partnerzy raportu

Cyberbezpieczeństwo i AI

Wydawcy raportu

Cyberbezpieczeństwo i AI

Raport przygotowany przez
Centrum Prawa Bankowego i Informacji

Centrum Prawa
Bankowego
i Informacji

Partnerzy raportu:
Biuro Informacji Kredytowej S.A.
Cloudware Polska
Fortinet
ServiceNow
Sii Polska

Warszawa, grudzień 2022
Wydawnictwo Centrum Prawa Bankowego i Informacji

Spis treści

Być gotowym na każde cyberwyzwanie

Postępująca digitalizacja daje wiele nowych możliwości – coraz więcej spraw można dziś załatwić, nie wychodząc z domu. Ale ma także te ciemniejsze strony; spora część przestępców zmigrowała do kanałów zdalnych, a takie hasła jak phishing, DDoS czy ransomware znane są nie tylko ekspertom z dziedziny cyberbezpieczeństwa.

Fot. CPBII

Karol Mórawski

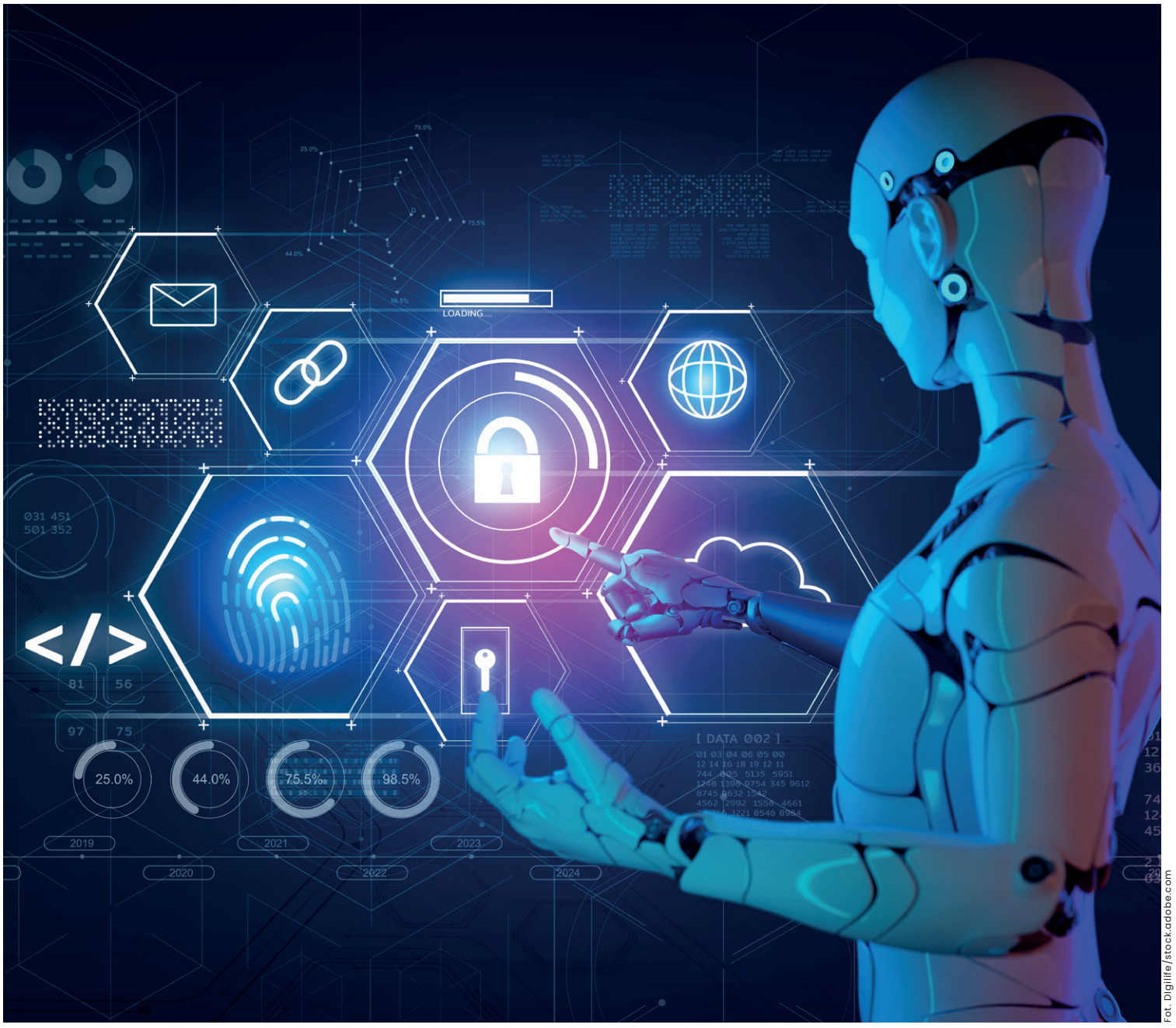
Aktywność sieciowych złodziei, oszustów bądź szantażystów to wyzwanie dla całej gospodarki, jednak instytucje finansowe stają się ich celem częściej niż pozostałe branże. Dzieje się tak z uwagi na status instytucji zaufania publicznego, jaki tradycyjnie już przysługuje bankom. W efekcie ponoszą one odpowiedzialność nie tylko za własne zasoby, ale także za środki powierzone przez deponentów, często niedostatecznie wyedukowanych w zakresie cyberbezpieczeństwa i stanowiących pod tym względem najsłabsze ogniwo obrotu gospodarczego.

Bankowe działy IT mają naprawdę olbrzymie kompetencje w dziedzinie bezpieczeństwa transakcji, zdalnego uwierzytelniania klientów czy wykrywania prób oszukańczych w czasie rzeczywistym, co pozwala na ich błyskawiczną neutralizację. W pełni sprawdza się tu łacińska paremia ***si vis pacem, para bellum*** (chcesz pokoju, szykuj się do wojny), a kolejnymi stopniami zaawansowania technik zabezpieczających jest uwierzytelnianie wieloskładnikowe czy biometria behawioralna. W tym ostatnim przypadku mamy do czynienia ze zmianą nie tylko ilościową, ale i jakościową. Użycie sztucznej inteligencji pozwala wszak nie tylko ograniczyć do minimum ryzyko, związane z nieświadomością użytkowników aplikacji bankowej czy karty płatniczej, ale również znacząco poprawić doświadczenie klienta. Choćby poprzez wyeliminowanie konieczności stosowania haseł, loginów, tokenów, kodów jednorazowych i innych środków, niezbędnych w procesie tradycyjnej autentykacji.

Problematyce szeroko ujętego cyberbezpieczeństwa rynku finansowego poświęcamy najnowszy z raportów technologicznych. Opracowanie w przekrojowy sposób przedstawia poszczególne komponenty spójnej strategii w dziedzinie cyberbezpieczeństwa, jaką powinna wdrażać każda instytucja rynku finansowego. Obok nowoczesnych rozwiązań IT należy do nich właściwa infrastruktura organizacyjna, kultura ryzyka, kompetencje pracowników i obszar prawno-regulacyjny, ze szczególnym uwzględnieniem compliance. W raporcie nie ograniczamy się wyłącznie do bezpośrednich konsekwencji ataku, ale wskazujemy bardziej długofalowe skutki działań przestępczych, jak choćby ryzyko cyfrowego łańcucha tworzenia wartości, immanentnie wpisane w nieunikniony przy tym poziomie zaawansowania technologicznego trend korzystania z zewnętrznych dostawców technologii i rozwiązań as a service.

W tym kontekście szczególnego znaczenia nabiera właściwe ułożenie relacji pomiędzy podmiotem rynku finansowego a firmą technologiczną, tak by bezpieczeństwo nie było jedynie aneksem do umowy, lecz aby – zarówno na etapie uzgodnień, jak i późniejszej realizacji – konsekwentnie stosować zasadę security by design. Szczególnie sporo miejsca w raporcie poświęcono wykorzystaniu sztucznej inteligencji i uczenia maszynowego, i to po obu stronach barykady. Obok opisów konkretnych rozwiązań, pozwalających na poprawę cyfrowej odporności instytucji finansowych, znajdziemy zatem przykłady użycia AI przez zorganizowane grupy przestępcze, a także ryzyk, towarzyszących wdrażaniu cyfrowych pomocników bez odpowiedniego nadzoru ze strony człowieka. Zalicza się do nich choćby niewystarczająca transparentność procedur obsługiwanych przez AI czy wręcz możliwość podejmowania działań dyskryminacyjnych przez – z pozoru tylko – obiektywne boty. To niezwykle cenny zasób wiedzy, nie tylko dla przedstawicieli banków, ale i przeciętnego użytkownika aplikacji internetowych i mobilnych. Ten ostatni, jak mało kto potrzebuje wszakże wiedzy, kto i w jaki sposób stanowi dlań zagrożenie, na ile banki są w stanie odeprzeć atak, a kiedy niezbędne jest zaangażowanie samego klienta. •

Jak bronić się przed atakami poprzez algorytmy i sztuczną inteligencję



Fot. Digilife/stock.adobe.com

Narastające zagrożenia związane z bezpieczeństwem cybernetycznym, przed którym stoi cały świat, a instytucje finansowe w szczególności, to główne dziedziny zainteresowania kierownictw zarówno firm prywatnych, jak i sektora publicznego. Wynika to z rozwoju nowych technologii i postępującej cyfryzacji praktycznie każdej dziedziny życia.

→

Fot. Archiwum prywatne

Prof. zw. dr hab. Stanisław Kasiewicz
SEKRETARZ NAUKOWY ALTERUM OŚRODKA BADAŃ I ANALIZ SYSTEMU FINANSOWEGO
EMERYTOWANY PROFESOR SZKOŁY GŁÓWNEJ HANDLOWEJ W WARSZAWIE

Fot. Archiwum prywatne

Dr hab. Lech Kurkliński prof. SGH
DYREKTOR ALTERUM OŚRODKA BADAŃ I ANALIZ SYSTEMU FINANSOWEGO
KIEROWNIK ZAKŁADU FINANSÓW CYFROWYCH FINTECH W SZKOLE GŁÓWNEJ HANDLOWEJ W WARSZAWIE

Poczucie bezpieczeństwa od zawsze należało do najważniejszych priorytetów człowieka, jednakże gdy zaczyna otaczać go coraz więcej nowych rodzajów ryzyka, to ta potrzeba staje się jeszcze bardziej odczuwana. Intensywniej poszukuje się wtedy metod i sposobów rozwiązania lub chociażby zmniejszenia tego problemu. Pojawiają się innowacje, do których z pewnością należy zastosowanie sztucznej inteligencji i uczenia maszynowego w systemach stojących na straży bezpieczeństwa cybernetycznego. Oczywiście nie należy zapominać, że także sprawcy tych zagrożeń rozwijają lub mają dostęp do nowych technologii, co utrudnia z nimi walkę. Kluczowego znaczenia nabrała informacja (jej masowość, jakość, gromadzenie, przetwarzanie, dostępność, szybkość wykorzystania itd.). Dlatego też właśnie big data w połączeniu ze sztuczną inteligencją oraz uczeniem maszynowym może stanowić przełom w dążeniu do uzyskania zadowalającego poziomu cyberbezpieczeństwa[1].

Sztuczna inteligencja ma sprawiać, aby komputer, sterowany systemowo robot, czy oprogramowanie działały podobnie, jak myślą i postępują ludzie. Dlatego też prowadzi się badania nad sposobem funkcjonowania ludzkiego mózgu, procesem uczenia się, podejmowania decyzji i działaniem, w celu rozwiązania problemu, czy też realizacji określonego zadania. Przy czym pod uwagę bierze się nie tylko czynniki racjonalne, ale też emocjonalne. Wyniki tych prac stanowią podstawę do opracowywania inteligentnego programu i systemów. Inteligencja powszechnie uważana jest za zdolność do gromadzenia wiedzy i rozumowania służącym rozwiązywaniu złożonych problemów. Natomiast uczenie maszynowe stara się replikować rzeczywiste postępowanie człowieka. W niedalekiej przyszłości inteligentne maszyny zastąpią ludzkie możliwości w wielu dziedzinach. Odwołać się tu można do Johna McCarthy'ego, autora terminu „sztuczna inteligencja", który powstał jeszcze w połowie lat 50. XX w., a dotyczył dziedziny informatyki zajmującej się sprawieniem, by komputery zachowywały się jak ludzie[2].

1. Cyberbezpieczeństwo – kluczowa kategoria w zarządzaniu finansami cyfrowymi

Cyberbezpieczeństwo wiąże się z zagrożeniami wynikającymi z wykorzystania technologii cyfrowej. Generalnie mamy do czynienia z niebezpieczeństwami dla różnych interesariuszy instytucji finansowych (przede wszystkim dla nich samych oraz ich klientów, ale też partnerów, czy władz nadzorujących rynek), w postaci zdarzeń wywołanych w sposób intencjonalny lub przypadkowy, jak m.in. iniekcje złośliwego oprogramowania, przełamywanie zabezpieczeń, publikowanie w sieci lub rozsyłanie szkodliwych treści, nielegalne gromadzenie i przetwarzanie informacji, sabotaż komputerowy, ale także wypadki i zdarzenia losowe (zwłaszcza wywołane przez czynnik ludzki)[3]. Pojawia się też pozytywny aspekt, który wiąże się z możliwością uzyskiwania przewagi konkurencyjnej przez podmioty wyróżniające się pod kątem cyberbezpieczeństwa, a dzięki temu oferujące wyższą jakość usług, mające lepszy wizerunek wśród klientów, nadzorców. Organizacje takie częściej i skuteczniej unikają lub ponoszą mniejsze straty finansowe z tytułu tego typu incydentów. Zatem cyberbezpieczeństwo wpisuje się w skumulowane ryzyko prowadzonej transformacji cyfrowej instytucji finansowych. Można więc dokonać zestawienia korzyści i negatywnych aspektów tego zjawiska. Do tej pierwszej kategorii należą przede wszystkim[4]:

1) Doświadczenie użytkownika (*user experience*): postęp cyfryzacji umożliwił instytucjom (w tym finansowym) kompleksową poprawę całej sfery styczności z klientem – doświadczenia użytkownika i udoskonalenie oferowanych usług np. poprzez podejście

1 J. N. Welukar, G. P. Bajoria, *Artificial Intelligence in Cyber Security – A Review*, „International Journal of Scientific Research in Science and Technology", 2021, Volume 8, Issue 6.

2 R. Kumar, *Artificial Intelligence: A Path to Innovation*, „International Journal of Scientific Research in Science and Technology", 2017, Volume 3, Issue 1.

3 G. Strupczewski, *Zagrożenia cybernetyczne instytucji finansowych*, „Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych" nr 24 (2/2017).

4 *5 advantages of digitalisation in the banking sector*, https://softtek.eu/en/corporate-en/5-advantages-of-digitalisation-in-the-banking-sector/

Fot. knssr/stock.adobe.com

omnikanałowe, przy stałej ewolucji w kierunku modelu zorientowanego właśnie na klienta (*be-direction channel*). Oznacza to posiadanie analitycznych rozwiązań technologicznych w celu oferowania produktów i usług dostosowanych (spersonalizowanych) do użytkowników. Służy temu uwzględnienie znajomości ich preferencji, zachowań transakcyjnych, nawyków oraz postaw wobec ryzyka i kondycji finansowej.

2) Wzrost liczby klientów: w obliczu utraty zaufania przez tradycyjne instytucje finansowe oraz wzrostu korzystania z aplikacji mobilnych i usług online przez konsumentów, podmioty nastawione na rozwiązania cyfrowe w ostatnim czasie znacząco zwiększyły liczbę klientów. Wraz z pojawieniem się fintechów w sektorze jasne jest, że tradycjonaliści będą musieli zmienić sposób prowadzenia swojej działalności, aby nie tracić klientów.
3) Większa efektywność procesów: wdrażanie różnych, najnowocześniejszych technologii, takich jak m.in. podpis elektroniczny, trwały nośnik, czy tworzenie aplikacji na smartfony, przyczynia się do poprawy wydajności procesowej i eliminacji czynności manualnych. W ten sposób można np. ograniczyć błędy ludzkie w kontaktach z klientami. Poprawianie tego typu błędów jest zwykle od trzech do czterech razy droższe niż tworzenie procesu cyfrowego.
4) Redukcja kosztów: kolejną zaletą cyfryzacji jest oszczędność kosztów, zarówno dla instytucji, jak i klientów, np. poprzez wykorzystanie nowych środków płatniczych i transakcji bezgotówkowych oraz usprawnienie wielu procesów o charakterze operacyjnym.
5) Lepsze decyzje w oparciu o dane: wraz z postępującą cyfryzacją, dane stają się jednym z najważniejszych aktywów przy podejmowaniu dynamicznych decyzji, opartych na dużych wolumenach dostępnych informacji (np. dotyczące zarządzania ryzykiem). Technologie takie, jak big data pozwalają instytucjom finansowym opierać swoje decyzje lub usprawniać procesy na podstawie szczegółowej analizy dostępnych danych o ich obecnych lub potencjalnych klientach. Jednakże należy pamiętać, że pojawienie się wielkich firm technologicznych staje się dużym wyzwaniem dla dotychczasowych graczy. Bigtechy dysponują w tym zakresie o wiele większymi możliwościami zarówno w odniesieniu do danych, kapitału, jak i technologii.

Natomiast niekorzyści związane z przeprowadzaniem transformacji cyfrowej instytucji finansowych dotyczą (oprócz nieprawidłowego przeprowadzania tego procesu) przede wszystkim kwestii związanych z nieumiejętnym zarządzaniem cyberbezpieczeństwem.

Cyberzagrożenia mimo podejmowanych w instytucjach finansowych wielorakich działań zabezpieczających, nadal znajdują się na czołowych pozycjach w globalnych raportach poświęconych ryzyku i co ważniejsze nie widać tu istotnej zmiany[5]. Za najważniejsze i najniebezpieczniejsze uznaje się ataki ransomware (57% wskazań w badaniach firmy Allianz); naruszenia ochrony danych (57%); luki w pracy zdalnej (34%); zakłócenia w łańcuchach dostaw, technologii chmurowej i usługach świadczonych w ramach platform (33%)[6]. Firma RSA wskazuje na osiem rodzajów ryzyka cyfrowego, a do najważniejszych zalicza: naruszenia ochrony danych (44%), cyberbezpieczeństwa – ataki przestępcze (33%), ryzyko stron trzecich (21%)[7]. Z badań →

5 *Allianz Risk Barometer 2022*. Allianz Global Corporate & Specialty, Report, s. 1, 6, 7.

6 Liczby przedstawiają odsetek odpowiedzi wszystkich uczestników, którzy odpowiedzieli (1153). Liczby nie sumują się do 100%, ponieważ można było wybrać maksymalnie trzy rodzaje ryzyka. Ogólnie oczekiwany wzrost ryzyka cyberzagrożeń w 2022 r. w porównaniu do 2021 r. *Ibid*, s.12.

7 *Managing Digital Risk. 8 Types of Digital Risk and How to Manage Them*. 2019, s. 4.

Schemat 1. Kompleksowe determinanty zapewnienia cyberbezpieczeństwa

Źródło: Opracowanie własne.

respondentów przeprowadzonych przez EY i Institute of International Finance, według działów ryzyka operacyjnego, wynika, że aż 77% z nich uznaje cyberbezpieczeństwo za najważniejsze ryzyko, a dla zarządów te wskazania są tylko nieco mniejsze (57%)[8].

Dla uzyskania większej czytelności podejmowanych działań w celu przystosowania się do warunków środowiska cyfrowego warto analizować cyberbezpieczeństwo w sposób kompleksowy (zob. schemat 1).

Uwarunkowania regulacyjne

Aspekty regulacyjne w bardzo dużym stopniu wpływają na wymogi stawiane systemom informatycznym, ale także rozwiązaniom organizacyjnym o charakterze proceduralnym. Wymuszają znajomość przepisów i ich stosowanie, a w konsekwencji działanie podmiotów regulowanych oraz praktycznie prawie całego rynku. Dotyczy to zarówno bezpośrednio cyberbezpieczeństwa (jak np. wymóg silnego uwierzytelnienia w dyrektywie PSD2), ale także pośrednio, np. konieczności ciągłego poszarzania wiedzy i umiejętności pracowników, czy zastosowania odpowiednich rozwiązań organizacyjnych (np. funkcjonowania komórek audytu i *compliance*).

Infrastruktura technologiczna

Jej zadania wiążą się z zapewnieniem skutecznego zabezpieczania i walki z zagrożeniami cyfrowymi, zwłaszcza szkodliwym oprogramowaniem używanym do ataków na systemy instytucji finansowych. Posiadanie lub dostęp do elastycznej i niezawodnej infrastruktury technologicznej (własnej i partnerów) jest kluczem dla zachowania cyberbezpieczeństwa, szczególnie w warunkach coraz większej otwartości systemów, ich złożoności i wzajemnych powiązań, szybkości, skali oddziaływania oraz pojawiania się coraz nowszych innowacji.

Infrastruktura organizacyjna

Sposób zorganizowana danej instytucji ma znaczący wpływ na zarządzanie ryzykiem, w tym cyfrowym. Komórki organizacyjne (poszczególni pracownicy) winny mieć odpowiednio określone zakresy odpowiedzialności, przy zachowaniu dobrej współpracy

8 *Restore, rationalize and reinvent*. EY, Institute of International Finance. 2017, s. 7.

i partnerstwa z innymi jednostkami wewnętrznymi i zewnętrznymi (np. system komunikacji, dzielenie się informacjami) – chodzi o zapewnienie podejścia zintegrowanego, a nie tak często występującego silosowego. Nie jest to łatwe wobec konieczności utrzymania otwartości na zmieniające się uwarunkowania (technologiczne, regulacyjne, ekonomiczne, społeczne, ekologiczne itd.). Ponadto wszystko to powinno być ukierunkowane na realizację celów strategicznych danego podmiotu.

Kompetencje

Na sukces składa się również posiadanie liderów mających wysokie umiejętności i wiedzę technologiczną, doświadczenie w przeprowadzaniu skutecznej transformacji cyfrowej, podążającej za współczesnymi trendami, ale także pamiętających o konieczności zachowania efektywności podejmowanych działań. Wzrost upodmiotowienia całej kadry wymusza, aby praktycznie wszyscy pracownicy dostosowywali swoje kompetencje do zmieniających się uwarunkowań, wymogów technologii, regulacji, preferencji klientów itd. Oznacza to wzrost oczekiwań dotyczących nie tylko umiejętności twardych (głównie opartych na wiedzy, np. znajomości konkretnego oprogramowania, metod analitycznych), ale też miękkich (np. elastyczności dostosowania się do nagłych zmian otoczenia, kreatywności), co winno prowadzić do poprawnych reakcji na pojawiające się różnego rodzaju ryzyko, na wszystkich szczeblach organizacyjnych, począwszy od szeregowych pracowników, a skończywszy na kierownictwie najwyższego szczebla (zarządu, rady nadzorczej).

Kultura ryzyka/organizacyjna

Ściśle z wyżej wymienionymi elementami powiązana jest kultura organizacyjna danej instytucji i wynikająca stąd kultura ryzyka. Na podstawie przeprowadzonych badań dotyczących różnic kulturowych pomiędzy organizacjami tradycyjnymi, a tymi nastawionymi na innowacje technologiczne, można wskazać główne czynniki sukcesu. Należą do nich cztery cechy związane z kulturą cyfrową: sprawczość, szybkość, otwartość i autonomia. Pierwsza z nich dotyczy przede wszystkim kreowania, a następnie wdrażania innowacji, przy silnej wierze w powodzenie podejmowanych działań. Części z tych innowacji udaje się rewolucjonizować całe branże i wygrywać konkurencję z dotychczasowymi głównymi graczami, którzy nie zmieniają się wystarczająco szybko. Dlatego też druga cecha to właśnie szybkość. Pomaga ona firmom wyprzedzać konkurencję i nadążać za szybko zmieniającymi się oczekiwaniami klientów. Dla cyberbezpieczeństwa niezbędne jest, by w ramach istniejących rygorystycznych procedur bezpieczeństwa zapewnić krytyczną postawę otwartości zorientowaną na kwestionowanie *status quo* i zadawanie pytań (aby identyfikować słabości systemów) lub sformalizowanie i uspójnienie sposobów komunikacji (aby uniknąć niedopowiedzeń i nieporozumień). Nawet najlepiej zaprojektowane systemy informatyczne nie zadziałają prawidłowo, w przypadków ludzkich błędów. Redukowanie ryzyka popełnienia tych błędów możliwe jest w tzw. wysoce odpornych organizacjach, gdzie istnieją czytelne wzorce zachowań wspieranych przez menedżerów i praktykowanych w całej organizacji. Autonomia daje ludziom swobodę robienia tego, co jest właściwe dla firmy i jej klientów, nie czekając na formalne pozwolenia na każdym kroku. Razem wszystkie te wartości mogą wspierać cały zaangażowany personel, gdzie także szeregowi pracownicy czują się osobiście odpowiedzialni za firmę i ciągłą zmianę. Wartości wysoko wydajnych firm cyfrowych kształtują ich podstawowe praktyki: szybkie eksperymentowanie, samoorganizacja, podejmowanie decyzji w oparciu o różnorodne dane oraz obsesja na punkcie klientów i wyników. Wzmacniają się one nawzajem, gdy udaje się je zintegrować, tworząc jednolitą kulturę, która jest skutecznym wyrazem czterech wyżej wymienionych kluczowych wartości cyfrowych[9]. W ten obraz należy wpisać wymogi stawiane wobec cyberzagrożeń, co nie jest łatwe do osiągnięcia. Stąd właśnie sztuczna inteligencja i uczenie maszynowe mogą stać się tu nieocenione.

Świat zmienia się radykalnie poprzez permanentne innowacje. Zatem potrzebne są szybkie, iteracyjne kroki, a nie czekanie na zgromadzenie wszystkich odpowiedzi przed podjęciem działania. Szerokie zaangażowanie, zbieranie danych, materiałów z różnorodnych źródeł, otwarte dzielenie się radami i informacjami stanowi klucz do odpowiedniego zarządzania ryzykiem, zamiast zachowywania wiedzy dla siebie. Należy pozwolić ludziom na wysoki poziom zaufania i delegowania zadań, aby robili to, co należy zrobić, zamiast polegania wyłącznie na formalnie zorganizowanym zarządzaniu i wyznaczonych politykach.

Problematyka cyberbezpieczeństwa stała się centralnym zagadnieniem w zarządzaniu instytucjami finansowymi, w tym bankami. Wdrażają one liczne projekty łączące się z transformacją cyfrową, implementują innowacje finansowe, eksperymentują z systemami zarządzania nowymi rodzajami ryzyka. W tych okolicznościach powstają skomplikowane i skumulowane zagrożenia z tytułu ryzyka cyfrowego. Jego skala →

9 G. Westerman, D. L. Soule, A. Eswaran, *Building Digital-Ready Culture in Traditional Organizations*, MIT Sloan Management Review, Summer 2019; https://sloanreview.mit.edu/article/building-digital-ready-culture-in-traditional-organizations

może być niewspółmierna prawie do wszystkich innych rodzajów ryzyka. Ponadto podlega ono stałej ewolucji i może się pojawić w każdym momencie czasu (np. sposoby działania przestępców tuż przed rozpoczęciem weekendu lub przed dłuższymi świętami). Niebagatelne jest to, że często klienci postępują niefrasobliwie, nie dochowując podstawowych zasad bezpieczeństwa, jednak w przypadku utraty swoich środków, czy udostępnienia wrażliwych informacji, obwiniają za to instytucje finansowe (banki), a przez to podważają przypisywane im zaufanie publiczne.

Zmiany technologiczne i rynkowe wymuszają przeprowadzanie transformacji cyfrowej przez tradycyjne instytucje finansowe. Jednocześnie pojawiają się nowe już całkowicie nastawione na funkcjonowanie w sferze cyfrowej (np. neobanki, fintechy). Ogólnie poziom tej transformacji jest zróżnicowany, jednakże w przypadku banków znajduje się w dojrzałej fazie, w której dominująca część instytucji działających na rynku usług bankowych już dokonała kluczowych zmian (na poziomie ok. 70%) wynikających z napływu fali nowych technologii[10]. Oznacza to, że te banki zaakceptowały nowe reguły konkurencji rynkowej, w dużym stopniu dostosowały strategie i modele biznesowe do ewoluującego otoczenia, dokonują na bieżąco adaptacji do wymogów regulacyjnych, zmieniają infrastrukturę organizacyjną (np. redukują liczbę oddziałów) oraz przyjmują nową kulturę organizacyjną i ryzyka. W konsekwencji tego nieuniknionego procesu każdy bank, jego pracownik i klient niemal codziennie styka się z rozwiązaniami o charakterze cyfrowym, co oznacza ekspozycję na zagrożenia związane z cyberbezpieczeństwem.

2. Współczesne trendy w zarządzaniu cyberbezpieczeństwem – wykorzystanie nowych technologii

Jednym z najważniejszych zagadnień w zarządzaniu cyberbezpieczeństwem jest zapewnienie spójności w opracowanej i wdrażanej strategii, obecnie cechującej się obsesją na punkcie klienta, a wykorzystaniem adekwatnych technologii. Chodzi o technologiczne dopasowanie, umożliwiające szybką rekonfigurację biznesowej struktury i posiadanych zdolności do zaspokojenia obecnych i przyszłych potrzeb oraz oczekiwań klientów[11]. W tym celu należy dokonać powiązania strategii z odpowiednimi fazami modeli informatycznej dojrzałości. Możliwe są tu trzy zasadnicze opcje:

a) Tradycyjne instytucje (jak np. część z banków) stosują znane od lat metody wykorzystania technologii zorientowanej na obniżkę kosztów. W związku z tym dążą do redukcji technologicznego opóźnienia przez działania modernizacyjne, upraszczające, konsolidujące, ale to wszystko dzieje się w ramach dotychczas stosowanych technologii.
b) Instytucje finansowe nawiązują partnerstwo z nowoczesnymi specjalistami od technologii i koncentrują się na biznesie oraz wartości klienta. Natomiast technologiczni partnerzy zwykle proponują zastosowanie rozwiązań chmurowych i prowadzenie działalności w architekturze platformy. Dzieje się to w różnych przekrojach – budowania wartości w obszarze klientów, partnerów i samych organizacji.
c) Usługodawcy w sposób adaptacyjny zaspokajają pojawiający się popyt klientów. Specjaliści cyfrowi (najczęściej zewnętrzni) i komórki zajmujące się biznesem dzielą się odpowiedzialnością za osiągane wyniki. Dzięki elastycznym platformom, które w coraz większym stopniu dostarczają innowacyjni partnerzy, mogą być stosowane praktyki kreacji wartości, przy wykorzystaniu modelu operacyjnego zdominowanego przez technologię zorientowaną na przyszłość. Dzięki temu uzyskuje się elastyczność i zdolność do przyjmowania modeli biznesowych, które likwidują zakłócenia w dotychczasowym funkcjonowaniu danej instytucji.

Przyszłe dostosowanie zdolności i kluczowych generatorów wzrostu wartości dokonuje się głównie poprzez wykorzystanie danych i analityki. W szczególności predykcyjna analityka pozwala odczytywać sygnały i dokonywać analizy doświadczeń, a na tej podstawie budować produkty i usługi, dostosowane do kształtujących się trendów i popytu. Zatem pojawia się możliwość uwalniania wartości z dostępnych danych. Niebagatelną rolę w tej sferze odgrywa sztuczna inteligencja. Dotyka to też obszaru cyberbezpieczeństwa. Wynika to z wysokiego stopnia elastyczności i zaakcentowania podejścia predykcyjnego, którymi cechują się omawiane rozwiązania technologiczne i organizacyjne. Wskazuje na to aż 85% specjalistów biznesowych i technologicznych uważających[12], że pojawiające się problemy cyberbezpieczeństwa i ochrony prywatności zdecydowanie łatwiej mogą być rozwiązywane przy zastosowaniu właśnie takiej,

10 J. Marous, *6 Digital Banking Transformation Trends for 2022. The Finacial Brand's Free Email* NEWSLETTER In 2021, s. 2; Raport RSA już w 2019 r. podawał, że 74% przedstawicieli najwyższego kierownictwa uznawało transformację cyfrową za cel o najwyższym priorytecie. Zob Managing Digital Risk. *8 Types of Digital Risk and How to Manage Them*. RSA 2019, s. 2.

11 B. Cameron, F. Mark and others, *The State of Future Fit Technology Strategy, 2022*. 26 September 2022. Forrester Research, Inc.

12 *Achieving Individual and Organisational Value with AI*. MITSloan Management Review, BCG, Research Report. November 2022, s. 3.

Fot. ipopba/stock.adobe.com

technologicznej strategii. Ważne są także zdolności w obszarze kreatywności i wzmacniania odporności w postaci umiejętności wdrażania innowacji przy utrzymaniu bezpieczeństwa, jednakże w stopniu nie hamującym rozwoju.

Identyfikacja znaczenia przyszłych trendów, które będą miały wpływ na zarządzanie cyberbezpieczeństwem stanowi przedmiot zainteresowań wielu ekonomistów i ośrodków naukowych. Nie ma tu wypracowanego jednolitego stanowiska, ale też nie ma daleko idących rozbieżności[13]. Na uwagę zasługuje raport firmy Gartner *Top Trends in Cybersecurity, 2022*. Do wymienianych tam najważniejszych trendów zaliczamy[14]:

Trend nr 1: Rozszerzanie się „powierzchni" potencjalnego ataku (*attack surface expansion*)

Generalnie 60% pracowników umysłowych pracuje zdalnie, co dotyczy także instytucji finansowych, a co najmniej 18% nie wróci do biura. Zmiany w sposobie pracy, wraz z coraz większym wykorzystaniem rozwiązań chmurowych otworzyły ogromne pole do potencjalnych ataków cyfrowych.

Trend nr 2: Obrona systemu weryfikacji tożsamości (*identity system defense*)

Systemy weryfikacji tożsamości są przedmiotem ciągłych ataków. Niewłaściwe (wyłudzenie, kradzież, zmanipulowanie, ominięcie itd.) użycie poświadczeń (*credentials*) jest obecnie podstawową metodą stosowaną przez atakujących w celu uzyskania dostępu do systemów i osiągnięcia swoich celów.

Trend nr 3: Ryzyko cyfrowego łańcucha tworzenia wartości (*digital supply chain risk*)

Coraz popularniejszą metodą dystrybucji złośliwego oprogramowania przez cyberprzestępców jest atakowanie dostawcy oprogramowania, a następnie dostarczanie złośliwego kodu klientom i innym osobom w łańcuchu dostaw w postaci produktów lub aktualizacji, które na pierwszy rzut oka wydają się prawidłowe. Ryzyko to wzmacnia dość radykalne przyspieszenie odchodzenia przez instytucje finansowe (np. banki) od modeli biznesowo-operacyjnych opartych na samodzielnym wykonywaniu wszystkich funkcji. Proces „rozkooperowania" przyspieszył zwłaszcza wraz z rozpowszechnianiem się rozwiązań chmurowych, takich jak SaaS, PaaS i IaaS, a w sferze bankowej modeli BaaS, BaaP, BaaM, czy zwłaszcza PBaaS. →

13 *On the cusp of a new era?* McKinsey Global Institute. October 2022; Ch. Skinner, *The top technologies for banks now and next year.* October 14, 2022; J. Marous, *Six Retail Banking Technology Trends for 2022*; S. Cocheo, *7 Major Payment Trends that Will Shake Up Banking in 2022.* „The Financial Brand"; BK Kaira, *9 Pivotal Trends that Will Shape Banking Strategies for 2022.* „The Financial Brand".

14 https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Trend nr 4: Konsolidacja dostawców (*vendor consolidation*)

Produkty (rozwiązania) zabezpieczające podlegają procesowi konwergencji. Dostawcy konsolidują funkcje bezpieczeństwa w ramach pojedynczych platform i wprowadzają opcje cenowe i licencyjne, aby uatrakcyjnić swoje rozwiązania pakietowe. Tendencja ta powinna zmniejszać złożoność, przyczyniać się do obniżki kosztów i poprawiania wydajności, w efekcie finalnym prowadząc do poprawy ogólnego bezpieczeństwa.

Trend nr 5: Siatka cyberbezpieczeństwa (*cybersecurity mesh*)

Sieć cyberbezpieczeństwa stanowi nowoczesne, koncepcyjne podejście do architektury bezpieczeństwa, które umożliwia poszczególnym instytucjom wdrażanie i integrowanie swoich zabezpieczeń z własnymi i zewnętrznymi zasobami, niezależnie od tego, czy znajdują się one lokalnie, w centrach danych czy w chmurze. Firma Gartner przewiduje, że do 2024 r. organizacje stosujące architekturę siatki cyberbezpieczeństwa zmniejszą skutki finansowe poszczególnych incydentów związanych z cyberbezpieczeństwem średnio o 90%.

Trend nr 6: Decyzje rozproszone (*distributed decisions*)

Menedżerowie potrzebują szybkiego i sprawnego systemu cyberbezpieczeństwa, aby wspierać cyfrowe priorytety biznesowe, a przede wszystkim ich nie blokować. Jednak wraz z cyfryzacją coraz większej skali działalności, zarządzanie cyberbezpieczeństwem w formule scentralizowanej przez CISO (*Chief Information Security Officer*) staje się coraz bardziej problematyczne. Dlatego też wiodące organizacje budują swoje biura CISO w taki sposób, aby umożliwić rozproszoną ocenę ryzyka cybernetycznego. Nie kwestionując potrzeby scentralizowanego ustalania zasad postępowania z tym rodzajem ryzyka, pojawiają się liderzy cyberbezpieczeństwa, umieszczani w różnych częściach organizacji w celu zdecentralizowania decyzji w tym zakresie.

Trend nr 7: Poza świadomością (*beyond awareness*)

Błąd ludzki nadal przyczynia się do większości problemów łączących się z cyberbezpieczeństwem, co pokazuje, że tradycyjne podejście do szkolenia w zakresie świadomości bezpieczeństwa jest mało skuteczne. Stąd odchodzi się od przestarzałych kampanii uświadamiających, opartych na zgodności. Znaczenia nabierają holistyczne programy zmiany zachowania i kultury, których celem jest wprowadzenie bezpieczniejszych sposobów pracy.

3. Rodzaje, obszary i skala ryzyka związane z cyberzagrożeniami

Ryzyko cyfrowe jest prawie wszędzie i ma tendencję narastającą. Jednakże na szczeblu najwyższego kierownictwa nie zawsze zalicza się do tych, które klasyfikuje się w rankingach w pierwszej piątce. W raporcie Protiviti w 2022 r.[15] ulokowano je na dziewiątej pozycji. Natomiast raport firmy Deloitte wskazuje już, że w okresie najbliższych dwóch lat przesunie się na pozycję drugą[16].

Najważniejsze rodzaje cyberzagrożeń wskazywane w 2022 r. przez różne raporty i badania w pełni wpisują się w wyżej przedstawione trendy. Należą do nich[17]:

1) Oprogramowanie ransomware wymuszające okup. Jest to metoda cyberprzestępczości, w której pliki są szyfrowane, a użytkownicy blokowani, zaś przestępcy żądają pieniędzy za ponowny dostęp do systemu. Organizacje dotknięte atakami ransomware mogą być narażone na to, że ich systemy będą uszkodzone przez dłuższy czas, zwłaszcza jeśli nie mają kopii zapasowych.
2) Ryzyko osób trzecich. Stale rozszerzający się zakres dostawców zewnętrznych – dotyczy to zwłaszcza usług w chmurze i usług płatniczych, wirtualnych sieci dostępowych i oprogramowania – daje cyberprzestępcom większe możliwości przeniknięcia do kluczowych systemów instytucji finansowych.
3) Złośliwe oprogramowanie, e-skimmery i formjacking. Atakujący wykorzystują złośliwy kod poprzez wykorzystywanie różnych platform i procesów płatniczych, w tym formularzy handlu elektronicznego (np. przechwytywanie danych za sprawą wstrzyknięcia złośliwego kodu), a właśnie tam podawane są te najbardziej wrażliwe dane.
4) Przechwytywanie danych uwierzytelniających (credentials). Mamy tu do czynienia z możliwościami przejęcia danych uwierzytelniających zarówno za pomocą metod socjotechnicznych (np. phishing), ale też rozwiązań technologicznych (np. wirusów). Hasła użytkowników, a w szczególności administratorów są jak klucze do królestwa, a po ich zdobyciu brama do działań przestępczych jest otwarta na oścież.
5) Tożsamości syntetyczne. Łącząc legalne i fałszywe dane, cyberprzestępcy testują zdolność organizacji finansowych do wykrywania tego typu procederu. W ten sposób pojawia się możliwość ubiegania o kredyt pod fałszywą tożsamością, a także zastosowanie innych rodzajów oszustw.

---

15 *Executive Perspective on Top Risks*. Protoviti. Global Business Consulting 2022-2031, s. 2.

16 *Global risk management survey*, 12th edition. Deloitte Insights 2021, s. 27.

17 *Top 7 Cyber Threats to the Financial Services Sector in 2022*; https://flashpoint.io/blog/top-7-cyber-threats-to-financial-services-sector-2022

6) DeFi i kryptowaluty. Przede wszystkim przestępcy wykorzystują kryptowaluty do dokonywania transakcji, ze względu na ich anonimowość za pośrednictwem technologii blockchain, co ma utrudniać działanie służb śledczych. Jednakże pod kątem zagrożeń cyfrowych również obejmują one posiadaczy kryptowalut, zwłaszcza dotyczy to oszustw socjotechnicznych (np. podstępne instalowanie „zdalnego pulpitu", który może mieć zastosowanie również w przypadku innych rodzajów transakcji finansowych).
7) Naruszenia danych. Dostęp do informacji poufnych, wrażliwych lub specjalnie chronionych przejmują osoby nieupoważnione. Zwłaszcza w sektorze finansowym cyberprzestępcy próbują „hakować" częściej niż w jakiejkolwiek innej branży, być może z wyjątkiem opieki zdrowotnej.

W innym przekroju, o największych zagrożeniach (2022 r.) związanych z cyberbezpieczeństwem możemy mówić w stosunku do: stosowania danych niezaszyfrowanych, oprogramowaniu typu malware, ryzyku generowanemu przez strony trzecie, spoofingu oraz phishingu. We wszystkich tych przypadkach pomocne okazują się rozwiązania tworzone za pomocą sztucznej inteligencji oraz uczenia maszynowego.

W 2007 r. cyberataki/naruszenia ochrony danych zajmowały 19. pozycję wśród wszystkich badanych ryzyk, ale w 2021 r. wysunęły się na pozycję pierwszą[18]. Ataki ransomware są niezwykle kosztownym ryzykiem, a to one dominują w obszarze cyberbezpieczeństwa. Dla atakujących są one unikalną kombinacją bardzo niskiego ryzyka z bardzo wysoką korzyścią. Zatem nie jest zaskoczeniem, że liczba ataków ransomware prawie podwoiła się w porównaniu z 2021 r., a całkowity ich koszt oszacowano na 20 miliardów USD[19]. Skala tego zjawiska nie jest tak dotkliwa dla polskich banków. Na pytanie: czy w ciągu ostatnich 12 miesięcy Polacy doświadczyli próby kradzieży prywatnych danych za pośrednictwem e-maila lub telefonu padały następujące odpowiedzi[20]: 77% – nie, nic takiego nie miało miejsca, 13% – tak, zdarzyło się kilka razy, 6% – nie pamiętam, 4% – tak, wiele razy. Dane te wskazują na umiarkowany poziom cyberzagrożenia, o czym świadczy także świadomość tego ryzyka (53%)[21].

4. Algorytmy i sztuczna inteligencja jako narzędzia do zwalczania cyberzagrożeń

Poszerzające się „powierzchnie" ataków oraz rosnąca dotkliwość i złożoność cyberzagrożeń pogłębia chroniczny niedobór kadr w dziedzinie cyberbezpieczeństwa. Szacuje się, że zatrudnienie w tej dziedzinie powinno wzrosnąć o ponad 70% (mimo że w 2022 r. przybyło 464 tys. osób), aby wyeliminować globalny niedobór 3,4 miliona specjalistów[22]. Problem ten zwiększa stosunkowa duża ich rotacja, wynosząca od 10 do 25%[23]. Te niedobory, chociażby w części, może wyeliminować sztuczna inteligencja i uczenie maszynowe. Właśnie przyspieszone wykrywanie zagrożeń było jednym z najwcześniejszych zastosowań tych innowacji. Pojawia się szansa na zarządzanie wspomnianą „powierzchnią" ataku, aby redukować szumy i umożliwić relatywnie nielicznym specjalistom skupianie się na najsilniejszych sygnałach i wskaźnikach naruszenia bezpieczeństwa. Kolejną zaletą jest możliwość szybszego podejmowania decyzji i działań, zwłaszcza w strategicznych obszarach. Zaawansowane platformy analityczne i systemy uczenia maszynowego, zgodnie z imperatywem transformacji cyfrowej, działają szybko, przeszukują duże ilości danych, identyfikują odchylenia od normy i nieprawidłowości oraz dokonują ich ocen (kategoryzacji). Wykorzystuje się w tym celu inteligentne platformy zdolne do stałego monitoringu, mapowania (rozpoznawania połączeń) i wizualizacji zasobów, obejmujące w czasie rzeczywistym rozszerzające się „powierzchnie" ataków cyfrowych[24].

Zakłada się, że sztuczna inteligencja winna wspomagać zespoły ds. bezpieczeństwa poprzez automatyzowanie czasochłonnych, rutynowych czynności, a w konsekwencji usprawniać powstrzymywanie ataków i reagowanie na różne incydenty. Wykorzystując uczenie maszynowe, tzw. uczenie głębokie, przetwarzanie języka naturalnego, uczenie ze wzmocnieniem, sztuczne sieci neuronowe i inne podejścia do sztucznej inteligencji, pojawiają się możliwości zautomatyzowanej oceny i podejmowania decyzji. →

18 *Global Risk Management Survey*. Report AON 2021, s. 22.
19 *Report: Ransomware Attacks and the True Cost to Business 2022*. Cybereason, June 7, 2022.
20 *Cyberbezpieczny portfel*, Raport ZBP, styczeń 2021, s. 11.
21 Ibid, s. 14.
22 *(ISC)² Research Reveals the Cybersecurity Profession Needs to Grow by 3.4 Million People to Close Global Workforce Gap*; https://www.isc2.org/News-and-Events/Press-Room/Posts/2022/10/20/ISC2-Research-Reveals-the-Cybersecurity-Profession-Must-Grow-by-3-4-Mil-to-Close-Workforce-Gap
23 *Critical Start, The impact of security alert overload*, Report, November 17, 2021.
24 C. Aubley i inni, *Cyber AI: Real defense Augmenting security teams with data and machine intelligence* [w:] *Tech Trends* 2022, Deloitte Insights, 2022, s. 82–83, https://www2.deloitte.com/pl/pl/pages/technology/articles/Raport-Deloitte-Trendy-Technologiczne-2022.html

Wzmacnia to zdolność do zarządzania rosnącą liczbą coraz bardziej złożonych zagrożeń bezpieczeństwa i osiąganie efektów skali. Kluczem staje się skrócenie czasu między wykryciem a naprawą. Niebagatelne znaczenie ma szybkość blokowania dostępu do określonych danych, dająca czas na bardziej zaawansowane oceny dokonywane już przez człowieka. Szczególnie sprawdzają się rozwiązania do zarządzania interfejsami API, kontrolują cały ruch z nimi związany, aby wykrywać anomalie, zgłaszać je i reagować w czasie rzeczywistym.

Sztuczna inteligencja pozwala też na proaktywną postawę bezpieczeństwa. Wykorzystuje się w tym celu kontekstową analizę zachowań użytkowników, która wraz z algorytmami uczenia maszynowego automatycznie bada ich działania, rozpoznaje typowe wzorce aktywności sieciowej lub dostępu do danych, identyfikuje, ocenia i oznacza anomalie. Ważna jest również umiejętność ignorowania fałszywych alarmów, czyli zdolność do podjęcia decyzji, czy reakcja lub interwencja jest uzasadniona. Właśnie jednym z największych problemów jest zbyt duża liczba alertów, na co wskazują specjaliści od spraw cyberbezpieczeństwa. W tej sytuacji pojawiają się problemy z określeniem, którym alertom należy nadać priorytet przy reagowaniu na incydenty[25]. Sztuczna inteligencja wkracza również w sferę zbierania i przetwarzania danych wywiadowczych, co dodatkowo wzmacnia proaktywne polowanie na zagrożenia[26].

Instytucje finansowe mogą wykorzystywać sztuczną inteligencję i uczenie maszynowe do automatyzacji obszarów, takich jak konfiguracja zasad bezpieczeństwa, monitorowanie zgodności oraz wykrywanie zagrożeń i luk w zabezpieczeniach oraz reagowanie na nie. Na przykład oparte na uczeniu maszynowym platformy zarządzania dostępem uprzywilejowanym mogą rozróżniać prawidłowe i złośliwe połączenia oraz wydawać zalecenia dotyczące segmentacji sieci w celu ochrony aplikacji i obciążeń. Łącząc analizę podatności i wzmocnione uczenie, generuje się wykresy ataków, które modelują strukturę złożonych sieci i ujawniają optymalne trasy ataku, co skutkuje lepszym zrozumieniem podatności sieci i zmniejszeniem liczby personelu wymaganego do przeprowadzenia testów. Podobnie narzędzia do symulacji cyberataków mogą stale naśladować taktyki i procedury zaawansowanych zagrożeń, aby uwypuklić luki w zabezpieczeniach infrastruktury. Należy jednak pamiętać, że sztuczna inteligencja nie może zastąpić specjalistów ds. bezpieczeństwa, ale za to usprawnić ich pracę. Przyczynia się do eliminowania żmudnych czynności analityków oceniających napływające dane i decydujących o eskalacji problemów. Wspomaga proces rejestrowania problemów, oceny każdego zagrożenia, określania potrzebnych reakcji i działań naprawczych, a w razie konieczności dalej eskaluje problem. Dzięki temu odciążeniu można się bardziej skupiać na obszarach o znaczeniu strategicznym, walce z najtrudniejszymi wyzwaniami związanymi z bezpieczeństwem oraz na proaktywnym monitorowaniu zagrożeń i słabych punktów[27].

Fot. Blue Planet Studio/stock.adobe.com

Niestety sztuczna inteligencja jest bronią obusieczną. Szybka analiza danych, przetwarzanie zdarzeń, wykrywanie luk, ciągłe uczenie się i inteligencja predykcyjna mogą być również wykorzystywane przez przestępców do opracowywania nowych lub skuteczniejszych ataków. Za przykład posłużyć może wykorzystanie generatywnych sieci kontradyktoryjnych – np. stworzenie sieci neuronowych, które konkurują ze sobą w tworzeniu zestawów danych podobnych – aby skutecznie łamać hasła dostępowe[28].

25 Palo Alto Networks, *The state of incident response 2017*; https://www.paloaltonetworks.com/resources/research/the-state-of-incident-response-2017

26 C. Aubley... op. cit.

27 Ibid.

28 M. Hutson, *Artificial intelligence just made guessing your password a whole lot easier*, „Science", 5.09.2017.

Podobnie model języka głębokiego uczenia się może rozpoznawać niuanse zachowania i specyfikę języka. W ręku cyberprzestępców prowadzi to do podszywania się pod zaufanych użytkowników i prawie uniemożliwia odróżnienie prawdziwej i fałszywej wiadomości np. w e-mailach oraz innej formie komunikacji[29]. Dlatego też ataki typu phishing mogą stać się znacznie bardziej kontekstowe i wiarygodne. Wzrasta też zagrożenie infiltracją sieci i utrzymywaniem długoterminowej obecności w ukryciu, przy powolnym i dyskretnym poruszaniu się po penetrowanych systemach[30]. Po drugiej stronie natomiast specjaliści ds. bezpieczeństwa mogą posługiwać się tą samą techniką, która jest wykorzystywana do łamania haseł, do pomiaru ich siły lub generowania fałszywych, aby pomóc w wykrywaniu naruszeń[31]. Kontekstowe uczenie maszynowe może być wykorzystywane do zrozumienia zachowań, relacji i wzorców postępowania użytkowników np. poczty e-mail – pory jej odbierania, odpisywania itd., w celu dynamicznego wykrywania nieprawidłowych lub ryzykownych zachowań[32].

Systematycznie wzrasta wprzęgnięcie sztucznej inteligencji do wykrywania naruszeń i zapobiegania im, chociaż wiele organizacji wciąż znajduje się na wczesnym etapie w tym zakresie. Ponieważ jednak powierzchnie ataków stale rosną, oczekiwania wobec sztucznej inteligencji także się zwiększają. Napędza to innowatorów w stosowaniu uczenia maszynowego, przetwarzania języka naturalnego, zastosowania sieci neuronowych przede wszystkim w odróżnianiu sygnału od szumu w sferze bezpieczeństwa. Wykorzystując rozpoznawanie wzorców, algorytmy uczenia maszynowego oraz analizy predykcyjne i behawioralne, sztuczna inteligencja może pomóc w identyfikowaniu i odpieraniu ataków oraz automatycznie wykrywać nieprawidłowe zachowania użytkowników. AI wykorzystuje się do zabezpieczania zarówno architektury lokalnej, jak i usług chmurowych, chociaż paradoksalnie zabezpieczanie obciążeń i zasobów w chmurze jest zazwyczaj mniejszym wyzwaniem niż w starszych środowiskach lokalnych.

Sama sztuczna inteligencja (ani żadna inna technologia) nie rozwiąże dzisiejszych lub przyszłych złożonych wyzwań związanych z bezpieczeństwem. Zdolność AI do identyfikowania wzorców i adaptacyjnego uczenia się w czasie rzeczywistym, gdy wymagają tego zdarzenia, może przyspieszyć wykrywanie, powstrzymywanie i reagowanie na incydenty. Powinna pomóc także zmniejszyć obciążenie analityków działaniami rutynowymi i umożliwić im bardziej proaktywne postępowanie. Chociaż specjaliści od cyberbezpieczeństwa prawdopodobnie nadal będą bardzo poszukiwani, to sztuczna inteligencja zmieni ich role. Pojawi się potrzeba przekwalifikowania, aby zmienić punkt ciężkości ze zbierania i segregowania alertów, na wyższe potrzeby analityczne oraz adekwatne do wielkości zagrożeń sposoby postępowania[33].

5. Etyczne i regulacyjne aspekty implementacji sztucznej inteligencji

Sztuczna inteligencja wraz z big data, analityką i algorytmami jest uznawana za najważniejsze narzędzie konkurowania instytucji finansowych w środowisku cyfrowym. Dlatego podejmowane są inicjatywy regulacyjne, aby stworzyć przepisy dla rozwoju i implementacji tych innowacji, które generowałyby pożądane korzyści dla instytucji finansowych, klientów i społeczeństwa, zapewniając jednocześnie wysoki poziom bezpieczeństwa[34]. Mimo prowadzonych prac w tym zakresie trudno jest jednak stwierdzić, że w odniesieniu do rynku usług finansowych sfera ta jest uregulowana. W 2021 r. Komisja Europejska przedłożyła projekt rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące AI[35], który zakłada jednolite unormowanie kwestii opracowywania, wprowadzania do obrotu i wykorzystywania systemów sztucznej inteligencji na obszarze UE. Projekt ten oparto na rezultatach wcześniejszych, kompleksowych przygotowań. Zaliczyć do nich można opublikowaną jeszcze w 2018 r. strategię „Sztuczna inteligencja dla Europy"[36], a następnie opracowanie z 2019 r. dotyczące wytycznych na temat wiarygodności AI[37], oraz białą księgę w tej sprawie z 2020 r.[38]. Natomiast wraz z projektem →

29 L.H. Newman, *AI wrote better phishing emails than humans in a recent test*, „Wired", 20.07.2021.

30 W. Dixon, N. Eagan, 3 ways AI will change the nature of cyber-attacks. World Economic Forum, 19.06.2019.

31 M. Hutson, Artificial intelligence ... op. cit.

32 T. Pepper, *Why contextual machine learning is the fix that zero-trust email security needs*, „Help Net Security", 16.02.2021.

33 C. Aubley ... s. 82–86.

34 M. Więckowska, *Akt w sprawie sztucznej inteligencji – nowe wyzwania dla prawników*. Temidium.pl, 19.07.2022.

35 *Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji*, 21.4.2021.

36 *Sztuczna inteligencja dla Europy*, Komunikat Komisji Europejskiej, 25.4.2018.

37 *Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, 8.4.2019.

38 *Biała księga w sprawie sztucznej inteligencji, Europejskie podejście do doskonałości i zaufania*, Komisja Europejska, 19.2.2020.

rozporządzenia ogłoszono również nowy, przygotowany we współpracy z państwami członkowskimi, skoordynowany plan działania[39]. Mimo braku sfinalizowania prac legislacyjnych, przyjęte inicjatywy, jak i próby unormowania rynku cyfrowego skłaniają do uznania UE za lidera regulacji rynku cyfrowego. Proponowane ramy prawne dla sztucznej inteligencji zakładają wyodrębnienie czterech poziomów ryzyka, jakie stwarza jej zastosowanie. Ponadto projekt, poza wymogami RODO, wprowadza dalsze lub uzupełniające obowiązki, w szczególności w zakresie: zarządzania ryzykiem i danymi, dokumentacji technicznej, prowadzenia rejestrów, przejrzystości przekazywania informacji użytkownikom, nadzoru ludzkiego, dokładności i solidności oraz cyberbezpieczeństwa[40]. Wynikające stąd konkluzje prowadzą do tego, że instytucje finansowe powinny skupić się przede wszystkim na[41]:

1) uwzględnieniu wymogów regulacyjnych w zakresie AI już na wczesnym etapie przygotowywania i wdrażania ich systemów lub narzędzi;
2) przeprowadzaniu oceny luk we wszystkich istniejących systemach w obszarze zautomatyzowanego podejmowania decyzji i próbie określania ich zgodności z obowiązującymi, a nawet projektowanymi przepisami;
3) zwróceniu uwagi na rzetelne dokumentowanie wyników przeprowadzanych ocen zastosowania AI.

Instytucje finansowe technologię sztucznej inteligencji mogą wykorzystywać niemal we wszystkich obszarach działalności, w tym w komórkach front and back office. Jednak ze względu na wczesny etap wdrażania AI w gospodarce oraz jej innowacyjny charakter nie wiadomo jeszcze, jakie efekty finansowo-ekonomiczne ona przyniesie. Należy też zastanowić się, jaka rola w już przyjmowanych strategiach cyfrowych przypada właśnie sztucznej inteligencji (cele, horyzont, kompleksowość, spójność, posiadane zasoby). Ogromne znaczenie będzie miało tu wsparcie (lub jego brak) agend rządowych i współpraca na poziomie całej UE (np. biorąc pod uwagę dostęp do systemów i publicznych baz danych). Priorytetowość tego obszaru dla władz polskich budzi poważne zastrzeżenia, chociażby w kontekście dotychczasowego braku wykorzystania przez Polskę środków z Krajowego Planu Odbudowy, gdzie cyfryzacja należy do jednego z głównych kierunków inwestycyjnych tego programu.

O jakości opracowanych strategii cyfrowych, a w ich ramach sztucznej inteligencji, w dużym stopniu decyduje znajomość trendów rozwoju tej technologii. Informacje na ten temat zawiera cykl rozwoju AI zbudowany przez firmę analityczno-badawczą Gartner (patrz wykres 1).

Z tego wykresu wynika szeroki zakres potencjalnych technologii związanych z AI, co skłania do implementacji realistycznej strategii krajowej, stałego śledzenia trendów technologicznych i priorytyzacji, aby wysiłki instytucji finansowych i ponoszone nakłady inwestycyjne nie okazały się nieefektywne.

Biorąc pod uwagę strategiczne znaczenie nowych technologii, należy także pamiętać o etycznych aspektach ich skutków. Zgodzić się trzeba z poglądem Ally MacDonald, że „jednocześnie tempo zmian, zwiększona niepewność i rosnące zapotrzebowanie spowodowało, że instytucje finansowe musiały zająć się wyzwaniami społecznymi i popchnęły kwestię etyki oraz zaufania do nowych technologii na szczyt ich agendy wykonawczej"[42]. Waga tych kwestii wynika z wielu przyczyn. Warto wspomnieć o kilku z nich.

Po pierwsze, AI używa powszechnie algorytmów, których cechą jest to, że ich działanie nie jest w pełni transparentne, w tym także dla instytucji nadzorczych[43]. Rozpoznanie działania algorytmów z zewnątrz, a właściwie na jakich przesłankach podejmowane są decyzje, jest zadaniem wyjątkowo złożonym i trudnym. W istocie stanowią czarną skrzynkę (black box), a często też niewidoczną (ukrytą) skrzynkę, której zasady działania obejmowane są tajemnicą handlową.

Po drugie, jednym z najważniejszych narzędzi w konkurencji cyfrowej okazały się platformy i ekosystemy. Organizacje tego typu mogą pełnić funkcje strażników dostępu (gate keepers), które określają niezależne reguły gry rynkowej w granicach zasięgu ich działania. Stając się samodzielnym regulatorem, mogą więc ustalać zasady korzystania z usług finansowych dla graczy rynkowych, które preferują ich cele i pozwalają na nadużywanie posiadanej silnej i uprzywilejowanej pozycji.

39 *Promowanie europejskiego podejścia do sztucznej inteligencji*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, 21.4.2021.

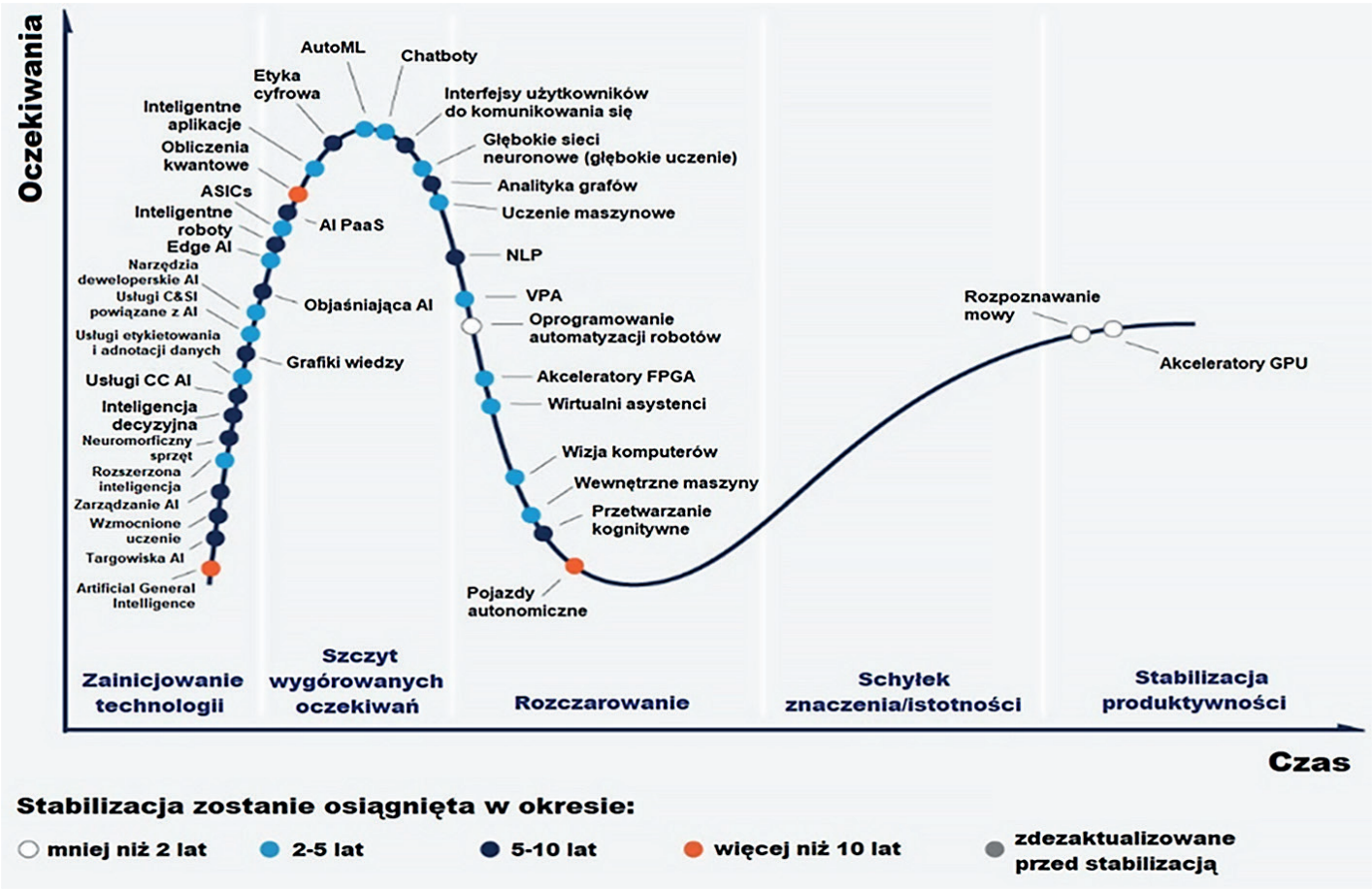
40 *Draft Regulation on Artificial Intelligence*. EY Switzerland Global, Switzerland, 19.08.2022.

41 Ibid.

42 A. MacDonald, *A New Business Mandate for Ethical Technology*, [in:] *Developing an Ethical Technology Mindset*. MIT Sloan, Deloitte, Fall 2021, s. 1.

43 *Komisja Europejska tworzy nowe Europejskie Centrum Przejrzystości Algorytmicznej*. Komunikat prasowy, 22.11.2022, Strasburg.

Wykres 1. Predykcja cyklu rozwoju technologii sztucznej inteligencji.



Źródło: P. Beńke, Artificial Intelligence fashion or necessity? Digital Banking Academy 2020.

Po trzecie, konkurencja cyfrowa na rynku usług finansowych, zwłaszcza wspomagana przez takie narzędzie, jak nietransparentna sztuczna inteligencja, jest podatna na monopolizację, co może zagrażać równej, uczciwej i sprawiedliwej rywalizacji.

Po czwarte, akceleratory napędzające konkurencję stanowią duże zbiory danych, pozyskiwanych od klientów, stąd ich ochrona należy do kluczowych zadań, które silnie wspomagać może właśnie sztuczna inteligencja.

Po piąte, cyberbezpieczeństwo i wykorzystanie w tym celu słabo kontrolowanej sztucznej inteligencji może łatwo stać się pretekstem do ograniczania prywatności w stopniu nieuzasadnionym zagrożeniami. Zatem otwarte pozostaje pytanie, jak winni działać regulatorzy, aby dane były dobrej jakości, dostępne, transparentnie przetwarzane, a w ostateczności, jak mają być chronieni klienci.

UE przywiązuje dużą wagę do wypracowania skutecznych i efektywnych przepisów w zakresie wykorzystania sztucznej inteligencji w sposób nie budzący wątpliwości od strony etycznej. Świadczy o tym programowa deklaracja z 2020 r.[44], czy rozporządzenie Parlamentu Europejskiego z 2021 r.[45]. W pierwszym dokumencie przedstawia się osiem kluczowych wymogów, których powinny przestrzegać twórcy AI:

- podmiotowość człowieka i nadzór ludzki,
- odporność techniczna i bezpieczeństwo, →

44 *On Artificial Intelligence – A European approach to excellence and trust*. WHITE PAPER. Brussels, 19.2.2020.

45 *Rozporządzenie Parlamentu Europejskiego i Rady. Ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji. (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii*. Bruksela, 21.04.2021.

- ochrona prywatności i zarządzanie danymi,
- transparentność,
- różnorodność,
- podejście niedyskryminacyjne i sprawiedliwość,
- dobrostan społeczny i środowiskowy,
- odpowiedzialność.

Ponadto grupa ekspertów pracująca na zlecenie UE rekomenduje cztery zasady etyczne dotyczące stosowania godnej zaufania sztucznej inteligencji[46]. Zasady te, spełniające wyżej wymienione postulaty, to: poszanowanie autonomii człowieka; zapobieganie szkodom; sprawiedliwość; możliwość wyjaśnienia. Ta ostania zasada wymaga, aby procesy były transparentne, a zakres działania i cele systemów AI otwarcie komunikowane, a decyzje w jak największym stopniu możliwe do wyjaśnienia osobom, na które mają bezpośredni i pośredni wpływ[47].

Zakończenie

Zainteresowane instytucji finansowych zarządzaniem cyberbezpieczeństwem jest oczywiste. Raport poświęcony tej tematyce wpisuje się też w aktywną działalność agend Związku Banków Polskich w zakresie edukowania klientów i pracowników instytucji finansowych, w tym banków, w związku z przeprowadzaną transformacją cyfrową usług finansowych oraz propagowaniem świadomego i racjonalnego wykorzystania nowych technologii.

Wymogi cyberbezpieczeństwa zmuszają do przyjmowania coraz nowocześniejszych metod i narzędzi walki w tym zakresie. Niewątpliwie należy do nich zastosowanie sztucznej inteligencji i uczenia maszynowego. Apetyt na efekty jest ogromny, gdyż bariery związane z tego rodzaju zagrożeniami są najistotniejsze dla rozwoju cyfrowych usług finansowych. Dlatego też koszty walki z cyberprzestępczością stają się coraz większe. Na koniec 2021 r. przewidywano podwojenie nakładów na ten cel w stosunku do 2015 r. na poziomie 6 bilionów USD, a do 2025 r. osiągnięcie pułapu ponad 10 bilionów USD[48]. W tych warunkach zapewnienie cyberbezpieczeństwa należy do głównych czynników decydujących o konkurencyjności w dobie usług cyfrowych. Sprawna obrona przed zagrożeniami, przy tym o wysokim stopniu skuteczności, stała się koniecznością. Wymagające kryteria jej sprawności (m.in. wyprzedzające działanie, natychmiastowość itd.) zmuszają do sięgnięcia do rozwiązań technologicznych. Konieczne jest redefiniowanie roli człowieka w tych procesach (np. lawinowy wzrost zapotrzebowania na armie specjalistów, o wysokich kompetencjach, posługujących się nowoczesnymi narzędziami). Nadzieją w tej materii stała się właśnie sztuczna inteligencja i uczenie maszynowe. Jednak przy nieocenionych korzyściach, niesie ze sobą również określone rodzaje ryzyka w duchu zasady, że „nie ma nic za darmo". Oprócz kosztów finansowych, narzędzia te wykorzystywane są przez cyberprzestępców. Stąd obok ewidentnych korzyści zastosowania AI, należy pamiętać o słabościach i niekorzyściach powstających przy jej implementacji. Zaliczamy do nich przykładanie niedostatecznej wagi do opracowania i wdrażania całościowych strategii cyfrowych, które winny być oparte na podejściu zintegrowanym, a nie silosowym. Problemy wiąże się też z nieuregulowanym od strony prawnej statusem funkcjonowania sztucznej inteligencji, niedocenianiem znaczenia kultury organizacyjnej/ryzyka, słabościami natury etycznej, ale także analizami od strony oceny efektywności realizowanych projektów.

Z perspektywy czytelnika, niniejszy raport może stanowić impuls do oceny, w jakim stopniu moja organizacja jest przygotowana do wdrożenia omawianych najnowocześniejszych rozwiązań technologicznych. Dotyczy to zarówno aspektów technicznych, jak też organizacyjnych oraz ludzkich. Jesteśmy bowiem w pełni przekonani, że sukces w zarządzaniu cyberbezpieczeństwem zależy w równym stopniu nie tylko od technologii, ale również od decyzji profesjonalnych zarządów oraz kompetencji i zaangażowania ze strony wszystkich pracowników. Monitorowanie i kontrola ryzyka związanego z cyberbezpieczeństwem nie może być dokonywana okresowo, czy tylko w godzinach pracy. Dlatego też zastosowanie sztucznej inteligencji staje się pilną koniecznością. Nawet gdy ogólny poziom bezpieczeństwa danej instytucji uznaje się za dostatecznie wysoki, nie oznacza to całkowitego wyeliminowania tego rodzaju ryzyka. Szczególnie w sferze cyfrowej zagrożenia mogą się kumulować, wzrasta ich złożoność, umiejętność ukrywania się oraz stała ewolucja. Jednak należy pamiętać, że te instytucje, które liderują w obszarze cyberbezpieczeństwa osiągają zdecydowanie lepsze wyniki finansowe, wykazują większą stabilność finansową oraz wyższy poziom reputacji. •

46 *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji.* Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji. Komisja Europejska, Bruksela 10 kwietnia 2019 r., s. 14.

47 *What AI Reveals About Trust in the World's Largest Companies.* BCG Henderson Institute, Boston, May 2022; S. Kasiewicz, *Etyczne i kulturowe aspekty zarządzania ryzykiem AI w bankowości*, Zeszyty Naukowe TNP. „Prakseologia i Zarządzanie". 2022 Nr 1.

48 Steve Morgan, „Cybercrime to cost the world $10.5 trillion annually by 2025," Cybersecurity Ventures, 13.11.2020.

Cyberbezpieczeństwo. Czy przestępcy mogą pokonać instytucje finansowe?

Fot. Gbor/stock.adobe.com

Coraz bardziej zaawansowane roboty dzwonią i piszą do klientów banków, algorytmy uczące się maszynowo próbują atakować zarówno serwery dużych organizacji, jak i konsumentów. Cyberprzestępcy sięgają po coraz bardziej wyrafinowane sposoby, aby kraść. Mimo że zmienia się techniczna strona przestępczych metod, to – paradoksalnie – bazują one od lat na tym samym: ludzkich emocjach i słabościach.

→

Andrzej Karpiński
DYREKTOR DEPARTAMENTU BEZPIECZEŃSTWA, GRUPA BIK
OD PONAD 20 LAT DZIELI SIĘ SWOIM DOŚWIADCZENIEM, WIEDZĄ I PASJĄ Z ZAKRESU SIECI I BEZPIECZEŃSTWA. PRACOWAŁ M.IN. W NAJWIĘKSZYCH FIRMACH TELEKOMUNIKACYJNYCH W POLSCE ORAZ ZA GRANICĄ (NP. ORANGE, ATMAN, ASIACELL), JAKO KOORDYNATOR JEDNEJ Z NAJWIĘKSZYCH NA ŚWIECIE SIECI IRC (EFNET), JAKO EKSPERT GRUPY ROBOCZEJ IOT PRZY MINISTERSTWIE CYFRYZACJI. EKSPERT W ZAKRESIE ZARZĄDZANIA ZESPOŁAMI BEZPIECZEŃSTWA SIECI, TWORZENIA ARCHITEKTURY ZABEZPIECZEŃ TELEINFORMATYCZNYCH, TELEMEDYCZNYCH I ROZWOJU STRATEGII BEZPIECZEŃSTWA ORGANIZACJI. W GRUPIE BIK ZARZĄDZA SYSTEMEM BEZPIECZEŃSTWA INFORMACJI BIURA INFORMACJI KREDYTOWEJ I SPÓŁEK ZALEŻNYCH REJESTRU DŁUŻNIKÓW BIG INFOMONITOR ORAZ DIGITAL FINGERPRINTS.

Wielkie zbiory danych gromadzone przez duże instytucje są zwykle świetnie chronione. Im cenniejsze dane, tym większe środki przeznacza się na ich bezpieczeństwo. Gra toczy się o olbrzymią stawkę – zaufanie klientów oraz kontrahentów.

Do tego należy dodać aspekt otoczenia prawnego – zapewnienia bezpieczeństwa wymagają od instytucji finansowych m.in. Komisja Nadzoru Finansowego, a od wszystkich Urząd Ochrony Danych Osobowych. Jednak, gdyby wszystkie zabezpieczenia dawały 100-procentową pewność, przestępcy nie próbowaliby ataków. Oni też ponoszą koszty, a biznes przestępczy rządzi się takimi samymi zasadami, co legalny – przychody muszą przewyższać koszty.

Trwa więc swoisty cyberwyścig – im bardziej wyrafinowani są złodzieje, tym bardziej skuteczne zabezpieczenia stosują właściciele pożądanych dóbr. Im lepszą ochronę stosują organizacje, tym większą kreatywnością wykazują się hakerzy.

Po co wyważać drzwi, skoro można wejść oknem

Niewiele ataków na świetnie chronione systemy rządowe czy dużych instytucji finansowych jest ujawnianych. Do wiadomości publicznej zazwyczaj docierają informacje o tych, którym celem była ambicja hakera i on sam się pochwalił sukcesem. O tym, co ukradł (i czy w ogóle cokolwiek), żadna ze stron nie informuje. Ewentualnie do publicznej wiadomości podawane są informacje po upływie czasu potrzebnego do załatania luk w bezpieczeństwie nie tylko okradzionej instytucji, ale również wszystkich innych stosujących analogiczne zabezpieczenia. Na końcu i tak do odbiorców dociera uspokajający (choć nie zawsze prawdziwy) komunikat, że żadne dane wrażliwe nie znalazły się w niepowołanych rękach.

Inną kategorią jest przejęcie danych osobowych, o czym instytucja, która je utraciła, musi poinformować UODO. Zobowiązana jest również ostrzec osoby, których dane wyciekły, czyli najczęściej swoich klientów.

Jednak zdecydowana większość ataków nie jest skierowana przeciw systemom bezpieczeństwa, które w dużych organizacjach są bardzo skuteczne, ale na ich omijanie. Owszem, w ostatnich dekadach można było przeczytać o włamaniu do systemów wojskowych czy wielkich międzynarodowych korporacji – i to tkwi w świadomości ludzi – ale były to właśnie ataki polegające na ominięciu zaawansowanych systemów bezpieczeństwa.

Ominięcie, a nie złamanie zabezpieczeń, nie umniejsza inwencji, inteligencji, sprytu i konsekwencji działania przestępców. Wręcz przeciwnie. Tylko tępy złodziej będzie godzinami forsował antywłamaniowe drzwi, ściągając na siebie uwagę sąsiadów, przechodniów, aż wreszcie policji. Sprytny włamywacz w takiej sytuacji wejdzie do domu przez otwarte okno w piwnicy.

W przeszłości skuteczne ataki były możliwe np. przez kosz w komputerze. Dostanie się do niewinnego katalogu z usuniętymi plikami umożliwiało wejście do systemu. Natomiast rozwiązania chmurowe oferowanych przez renomowanych dostawców są bardzo dobrze strzeżone, a jednak wyciekły intymne zdjęcia jednej z celebrytek, która tam je przechowywała. Jak to możliwe? Nikt nie złamał zabezpieczeń znanego producenta sprzętu i dostawcy chmury. Po prostu użytkowniczka smartfonu, którym robiła rzeczone ujęcia, nie zabezpieczyła go należycie. Banalne hasło haker odkrył i wszedł do jej chmury tak, jakby ona to zrobiła.

Ofiary często pomagają przestępcom

Specjalista do spraw bezpieczeństwa jednej z firm z branży internetowej zwierzył się z początków swojej kariery. W latach licealnych dla zabawy włamywał się do skrzynek pocztowych. Bez używania wyrafinowanych technologii. Były to początki mediów społecznościowych, wiele osób obnażało się na Naszej Klasie, tak jak dziś np. na Facebooku. Śledząc profil zdobywał od swojej ofiary wskazówki. Następnie próbował się zalogować przez stronę WWW na pocztę wybranej osoby. Nie znał hasła, więc klikał w link *„przypomnij hasło”*. Jeśli pytanie pomocnicze było *„imię chłopaka”*, *„jak wabi się Twój pies”*, wpisywał w formularz informacje z mediów społecznościowych i z reguły trafiał.

Robił to dla żartów, choć niektóre żarty mogą mieć przykre – choćby towarzyskie – konsekwencje dla ofiary. Niekiedy łatwo można się włamać do sieci Wi-Fi sąsiadów, aby za darmo korzystać z internetu, a można – również przykład z życia – puścić na drukarkę sąsiada spreparowane wezwanie do zapłaty za nieuregulowany rachunek z klubu nocnego wystawione na pana

domu. Żart tylko z pozoru przedni, bo nie wiadomo, na ile wystarczy poczucia humoru pani domu.

Te przykłady pokazują, że niefrasobliwość użytkowników urządzeń cyfrowych może być bardzo niebezpieczna, zarówno dla ciepła ogniska domowego, jak i bezpieczeństwa kluczowych danych organizacji.

Przestępcy bowiem posługują się czasem dość prymitywnymi metodami, wymagającymi jednak od nich sporego samozaparcia. Sprawdzały się one znacznie lepiej przed erą biometrii. W dobrze chronionych systemach od użytkowników wymagana jest częsta zmiana haseł oraz to, aby były one dość skomplikowane. Do każdej aplikacji użytkownik musi posiadać inne zabezpieczenie. Można z takimi rozwiązaniami przedobrzyć, bo przekracza to możliwości pamięci przeciętnego człowieka. Wtedy uzasadnienie ma branżowy żart: po czym poznać, że systemy organizacji są dobrze chronione? Po tym, że każdy użytkownik ma monitor obklejony karteczkami, na których zapisane są hasła.

Dlatego też włamywacze nie są genialnymi informatykami, za to charakteryzują się sprytem i inteligencją oraz oczywiście, co jest niezbędne, wiedzą z zakresu IT. Potrafią przeszukiwać kubły, do których trafiają śmieci z interesującej ich instytucji w poszukiwaniu właśnie tych karteczek z hasłami. W końcu trafią na aktywne hasło, albo po pewnym czasie potrafią wywnioskować, jakie jest aktualne hasło danego użytkownika na podstawie dotychczasowych.

Takie działania nie mają wiele wspólnego z utrwalonym przez kinematografię stereotypem cybermaniaka siedzącego przed wielkim komputerem z kilkoma monitorami, który podgryza zimną pizzę, popijając ją siódmym energetykiem i łamie systemy zabezpieczeń tak, jakby przechodził kolejne poziomy w grze zręcznościowej. Konsekwentne grzebanie w śmieciach bywało skuteczniejszą techniką.

Reklama dźwignią przestępczości

Coraz częściej wykorzystywane uczenie maszynowe – machine learning – potocznie i na wyrost nazywane sztuczną inteligencją, przynosi przestępcom realne zyski. Jednak rzadko mowa o atakach na dobrze zabezpieczoną sieć czy serwery. Zaawansowane technologie – choć coraz bardziej dostępne i tańsze – znów bazują na najsłabszym ogniwie w systemie zabezpieczeń: człowieku.

Aplikacja może się nauczyć mówić dowolnym głosem, zachowując intonację, używając ulubionych zwrotów czy przerywników dowolnej osoby. Na przykład dyrektora finansowego, który awaryjnie, telefonicznie, zleca wykonanie dużego przelewu. Takie przestępstwo się udało. Tak, chatbot może ukraść pieniądze – ściślej, przestępcy przy odpowiednim użyciu tej technologii.

Uczenie maszynowe wykorzystywane jest też do formułowania spersonalizowanych maili phishingowych. Odbiorcy są coraz bardziej czujni, więc należy do nich podchodzić w sposób bardziej wyrafinowany. Taniej jest zaprząc technologię, niż zatrudnić ludzi do napisania kilku tysięcy wersji wiadomości. Phishing jest często stosowany właśnie ze względu na niskie koszty. Odzew na taki atak jest znikomy, ale ekonomiczny rachunek jest na plusie, jeśli na milion rozesłanych wiadomości w link kliknie 0,01% odbiorców.

Tego typu ataki są skuteczne właśnie dzięki temu, że są prowadzone na masową skalę. Z branżowego zespołu bezpieczeństwa działającego przy KNF mamy informacje, że przestępcy dzwonią do miliona osób miesięcznie z numeru podszywającego się pod numer banku. To 12 mln połączeń rocznie. Statystycznie co trzeci Polak, wliczając dzieci, taki telefon powinien raz w roku otrzymać.

Wielkim zagrożeniem są również reklamy, które obiecują wygraną, albo zachęcają do udziału w ankiecie inwestycyjnej. W formularzu ofiary podają dane dotyczące swojej sytuacji finansowej, a nawet bardziej szczegółowe informacje, w jakiej formie, gdzie i w jakiej wysokości mają ulokowane oszczędności oraz w jakich bankach mają rachunki. Taki komplet informacji otwiera furtkę do kradzieży.

Bardzo niepokoi bierność wielkich graczy na rynku reklamowym. Nie weryfikują emitowanych treści. Skala zjawiska jest olbrzymia, mowa tu bowiem o 2,4 tys. wykrytych i zablokowanych reklamach tylko w październiku tego roku. I to na dużych, renomowanych stronach. Takie media budzą zaufanie, bo są globalnymi graczami, co dodatkowo usypia czujność odbiorców.

Maszyny służą obu stronom

Z wyrafinowanymi atakami w wykonaniu grupy informatycznych geniuszy mamy niezwykle rzadko do czynienia. Metody przestępców są dość prymitywne i bazują na ludzkich emocjach czy wręcz słabościach, takich jak strach, nerwowość czy chciwość.

Dekady temu autorami ataków rzeczywiście byli osobnicy, których można nazwać protoplastami hakerów z filmów. Zdolni licealiści, studenci, samotni informatycy łamiący zabezpieczenia. Dziś natomiast to są przedsiębiorstwa. Firmy, które zatrudniają wiele osób, w tym do obsługi swoistego call center, z którego obdzwaniane są potencjalne ofiary. Oczywiście to biznes nielegalny, podziemny, ale dobrze rozwinięty.

Należy też mieć na uwadze, że te organizacje przestępcze mają środki na kupowanie danych od pracowników instytucji finansowych czy wręcz „delegowanie" ludzi do pracy w nich. Dbający o standardy bezpieczeństwa podmiot →

Fot. Blue Planet Studio/stock.adobe.com

nie ma nawet świadomości, że zatrudnia członka organizacji przestępczej.

Działaniom nieuczciwych pracowników da się zapobiegać, a przynajmniej w porę interweniować. Bankowe systemy – zresztą nie tylko bankowe, bo wykorzystują je organizacje przetwarzające duże bazy z danymi osobowymi – wykrywają nietypowe zachowania pochodzące nie tylko z zewnątrz, ale również wewnątrz instytucji. Działają na zasadzie alarmów. Dobrze skonfigurowany system bezpieczeństwa wykorzystujący machine learning alarmuje, gdy dzieje się coś, co odstaje od standardu. Wtedy do gry wchodzi człowiek, specjalista ds. bezpieczeństwa i weryfikuje alarm. Może być fałszywy, to znaczy, że system zareagował na niewinną, choć mniej typową operację, może jednak zmusić do reakcji, zablokowania podejrzanego działania (albo odblokowania, gdy system sam je zablokował).

W ten sposób wykrywane są próby hakerskich ataków, ale też kopiowanie baz danych przez nieupoważnionych pracowników, którzy zgodnie z procedurą nie mogą tego robić. Specjaliści ds. bezpieczeństwa od razu widzą, kto wykonuje taką operację. Może się okazać, że upoważniona osoba robi coś bardzo nietypowego, wykonując polecenie, musi bowiem przygotować specjalne opracowanie czy analizę na potrzeby organizacji. Może jednak próbować wykraść dane, aby je sprzedać.

Atak psychologiczny

Wśród ofiar przestępstw często następuje dość szybko refleksja: *„jak ja mogłem/mogłam się na to nabrać?”*. *„To było grubymi nićmi szyte!”*. Jednak nabrali się, bo oszukali ich profesjonaliści, wykorzystując odpowiedni moment plus silną emocję: strach.

Większość ludzi jest rano dość spiętych. Dziecko pobrudziło się podczas śniadania, trzeba je przebrać, a już jesteśmy spóźnieni, po drodze korek większy niż zwykle albo autobus spóźniony, a tu telefon z *„banku”*, że właśnie ktoś się włamał na nasze konto i próbuje nas okraść, trzeba szybko działać, aby zapobiec utracie wszystkich pieniędzy. Proszę podać hasło, to zablokujemy konto i karty, i tak dalej.

Presja czasu, zaskoczenie, konieczność kontrolowania niesprzyjającego nam tego ranka otoczenia i robimy, co złodziej chce. Mimo że dobrze wiemy, iż bank nigdy nie prosi o hasło, albo przesłanie jednorazowego kodu. W zwykłych okolicznościach średnio świadomy klient banku nie pozwoliłby się okraść, ale przestępcy stosują psychologiczne sztuczki. To tańsze niż pisanie zaawansowanych programów włamujących się na konta klientów.

O ile organizacje przechowujące dane wrażliwe są zobowiązane stosować adekwatną ochronę przed ich kradzieżą, to przestępcy stosują adekwatne do spodziewanego zysku techniki kradzieży.

Bank chroniący miliony, jest skłonny wydać setki tysięcy na zabezpieczenia. To tak, jak w analogowym świecie z ochroną transportu pieniędzy. Nikt nie wynajmuje za dwa tysiące złotych firmy ochroniarskiej, aby konwojowała tysiąc złotych utargu. Robi to, aby zabezpieczyć 100 tys. zł. To działa również w drugą stronę. Złodziej nie zainwestuje dwóch tysięcy, aby ukraść tysiąc.

Bogata organizacja przestępcza mogłaby zainwestować miliony, aby ukraść setki milionów z banku. Musiałaby mieć jednak przeko-

nanie, że jej się to uda. Ryzyko niepowodzenia takiej operacji musiałaby ocenić jako niewielkie. Oczywiście nie wystarczy ukraść, wyczyścić konta, ale też trzeba przetransferować te pieniądze, a takie operacje na wielkie kwoty nie mogą przejść niezauważone. To brawurowy scenariusz. Znacznie taniej i jak się okazuje skuteczniej jest polować na klientów i niewielkim kosztem czyścić konta z paru tysięcy złotych, za to wiele kont.

Znając mechanizmy psychologiczne, łatwo także uśpić czujność ofiary obietnicą dużego zarobku. Np. inwestycją ze stopą zwrotu na poziomie kilkudziesięciu procent. Ulegają temu zarówno drobni ciułacze, jak i majętne osoby. Niemałą rolę odgrywa tu chciwość. Przy tak wysokiej inflacji każda inwestycja oferująca kilkunastoprocentowy zysk zaledwie chroni kapitał przed utratą wartości. Zarobić pozwala przedsięwzięcie dające 20, 30 czy 40% Jeśli dodamy do tego, że decyzję należy podjąć szybko, bo za dwadzieścia minut kończą się zapisy inwestorów do inwestycyjnego funduszu zamkniętego, to górę wezmą emocje, a nie zdrowy rozsądek, który powinien zadać pytania, jak możliwa jest taka wysoka stopa zwrotu, dlaczego nie znam nazwy instytucji oferującej taka inwestycję?

Biometria chroni nas przed... nami

Ze sposobu działania cyberprzestępców jasno wynika, że bezpieczeństwo danych oraz pieniędzy zależy w dużej mierze od klientów-konsumentów. Oczywiście zrzucenie na nich odpowiedzialności byłoby niewłaściwe. Instytucje finansowe powinny dawać im narzędzia, które pomagają chronić ich przed nimi samymi. Banki muszą też akceptować i promować rozwiązania technologiczne, które dla swojego dobra powinni stosować klienci. Do tego ważna jest edukacja na każdym możliwym kroku.

Wiele niezdrowych emocji budzi biometria. Część osób wzbrania się przed jej stosowaniem przez instytucje państwowe czy banki. Jednocześnie swoje dane biometryczne bezkrytycznie przekazuje np. firmie Google, Microsoft czy Apple, logując się do swojego smartfonu czy laptopa odciskiem palca, zezwalając na rozpoznawanie twarzy. Firmy hi-tech zbierają za zgodą użytkowników setki informacji – i to nie tylko te wielkie, ale również mało znani wydawcy aplikacji, które są masowo instalowane i zapewne nikt nie czyta, na zbieranie jakich danych się zgadza, co się będzie z nimi działo, komu mogą być udostępniane czy sprzedawane.

Przy tym wszystkim opór przed dowodem osobistym z warstwą biometryczną (najnowsze wydawane dowody osobiste w Polsce) wydaje się zabawny. A taki dokument jest na dziś niepodrabialny. Jeśli ktokolwiek udzieli złodziejowi kredytu na podrobiony dowód biometryczny, to znaczy że nie dochował należytej staranności przy weryfikacji kredytobiorcy. Wtedy okradziona osoba ma w sądzie sprawę bezproblemowo wygraną.

Technologia sprzyja bezpieczeństwu transakcji na wiele różnych sposobów. Weryfikacja płatności za pomocą tęczówki czy odcisku palca daje niespotykaną nigdy wcześniej gwarancję bezpieczeństwa. Podobnie jak biometria behawioralna. Technologię opracowała polska firma (obecnie należąca do Grupy BIK), która stworzyła jedno z najnowocześniejszych i najskuteczniejszych rozwiązań cyberbezpieczeństwa.

Ciekawym przykładem rozwiązań wprowadzonych przez Digital Fingerprints jest ochrona aplikacji mobilnych. Chroni ono aplikacje (np. bankowe) zainstalowane na smartfonach przed nieautoryzowanym użyciem. Technologia ta analizuje zachowania właściciela urządzenia i rozwija jego model behawioralny. Wie, jak konkretny człowiek używa smartfon, jak pisze na klawiaturze itd.

W sytuacji utraty urządzenia, gdy analogiczne operacje wykonuje ktoś inny, system opracowany przez DFP alarmuje o tym. W połączeniu z aplikacją banku nie pozwoli użytkownikowi nieodpowiadającemu stworzonemu modelowi behawioralnemu kupić za 100 tys. zł oszczędności zbieranych przez lata kryptowaluty na giełdzie działającej na Bahamach. Rozwiązanie to ma jedną słabość – jesteśmy nią my sami – musimy zgodzić się na korzystanie z takiego zabezpieczenia.

Działają też oczywiście prostsze metody, znane powszechnie w świecie finansów, jak alerty BIK. Osoby korzystające z nich są informowane o każdym ich sprawdzeniu w bazie BIK – jeśli kredytu nie zaciąga sam zainteresowany, jest czas na reakcję i zapobieżenie transakcji.

Mniej popularne, ale skuteczne w swej prostocie, jest zastosowanie zastrzeżenia kredytowego. Instytucja finansowa wysyłająca zapytanie otrzymuje odpowiedź, że klient nie jest zainteresowany zaciąganiem żadnych kredytów. Ta blokada jest bardzo prosta do zdjęcia przez użytkownika, gdy zapomni o niej albo gdy jednak zdecyduje się kupić pralkę na raty. Może w sklepie ją dezaktywować, a po przejściu procedury kredytowej ponownie aktywować.

Szeroko pojmowane cyberbezpieczeństwo kładzie obecnie duży nacisk na to, aby klienci mogli się ochronić (z pomocą instytucji, z której usług korzystają), przed chwilą własnej słabości czy niefrasobliwości. Najlepsze, najdroższe zabezpieczenia stosowane przez banki nie są w stanie w pełni przeciwdziałać sytuacji, kiedy klient – mówiąc brutalnie – sam podaje swoje dane osobowe przestępcy.

Czy przestępcy mogą pokonać zabezpieczenia instytucji finansowych? Teoretycznie mogą. Jednak nie opłaca im się próbować. Bardziej lukratywne i skuteczniejsze jest okradanie bezpośrednio klientów tych instytucji, którzy nieświadomie w tym pomagają. •

Identity Governance Administration (IGA)

– zyskaj lepszą kontrolę nad procesami w przedsiębiorstwie!

Identity Governance Administration (IGA) wspiera organizacje w zarządzaniu tożsamością oraz dostępami.

Działanie to zapewnia nadanie odpowiedniego dostępu, w ramach pełnionych przez pracownika obowiązków w przedsiębiorstwie.

- Cykliczna weryfikacja uprawnień użytkowników
- Usprawnienie efektywności procesów
- Redukcja ryzyka związanego z dostępami
- Automatyczny nadzór nad cyklem życia organizacji

- Procesy kadrowe
- Konta, dostępy i uprawnienia
- Wnioskowanie i akceptacja
- Recertyfikacja i weryfikacja
- Zgodność i raporty
- Automatyzacja zarządzania uprawnieniami

60%

przypadków naruszenia danych pochodzi od osób posiadających dostęp do danych poufnych

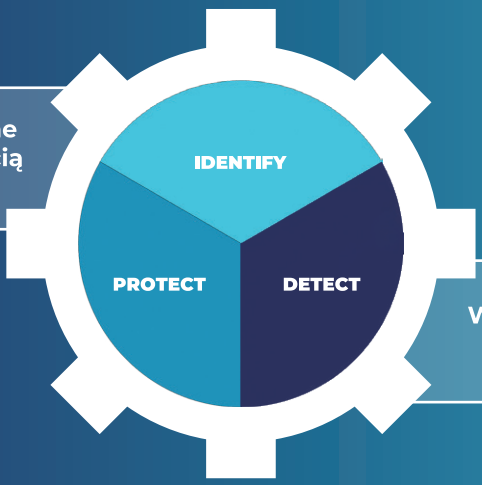
$14.8m

średni koszt kar dla organizacji, z powodu niespełnienia wymogów regulacyjnych

$3.9m

średni koszt całkowity związany z naruszeniem dostępu do danych

Zabezpiecz swoje poufne dane i miej kontrolę nad tożsamością pracowników



Wykryj potencjalne ryzyko i bądź o krok przed zagrożeniem

cloudware

Platinum Business Partner IBM

W czym **Identity Governance Administration (IGA)** może pomóc Twojej firmie?

- Możliwość konfiguracji zaawansowanych zasad udostępniania oraz nadawania uprawnień
- Modelowanie ryzyka opartego na czynnościach biznesowych w celu wykrycia potencjalnego zagrożenia
- Analiza ryzyka wrażliwego dostępu i rozdziału obowiązków z wykorzystaniem wizualizacji i kontroli zmian
- Możliwość wdrożenia w dowolnej infrastrukturze: chmurze prywatnej, on-premise, chmurze publicznej oraz hybrydowej

80%
pracowników posiada nadmiarowe uprawnienia

60%
kont specjalistów IT nie jest blokowanych bądź usuwanych po ich odejściu z organizacji

30%
kont w organizacjach nie posiada przypisania do tożsamości

Korzyści z zastosowania **IGA**:

1. Redukcja kosztów w organizacji
2. Zwiększenie oraz ulepszenie automatyzacji
3. Pełny nadzór nad nadawaniem uprawnień
4. Zmniejszenie ryzyka wynikającego z konfliktu uprawnień
5. Możliwość podejmowania lepszych decyzji dzięki przejrzystości danych

Skontaktuj się z nami! Odpowiemy na wszystkie Twoje pytania.

Grzegorz Gołda / Sales Director

cloudware | Platinum Business Partner IBM

Odpowiedź na nowe wyzwania cyberbezpieczeństwa

Rozmowa z ŁUKASZEM KUFLEWSKIM,
Identity Management Architect w Cloudware Polska.

Fot. ipopba/stock.adobe.com

Przed jakimi wyzwaniami, jeśli chodzi o bezpieczeństwo, stają dziś organizacje migrujące w ramach transformacji cyfrowej do chmury?
– Transformacja cyfrowa do chmury wprowadza konieczność holistycznego spojrzenia na bezpieczeństwo w ramach środowisk. Musimy pamiętać, że korzystając z chmur publicznych lub hybrydowych, narażamy nasze systemy, aplikacje oraz cenne dane na większą skalę ataków z zewnątrz. Nie wystarczy tylko odpowiednie zabezpieczenie samej warstwy sieciowej. Należy również zadbać o kontrolę nad dostępem, uprawnieniami i zabezpieczeniem danych. Jak pokazują najnowsze badania, 51% podmiotów udostępniło przynajmniej jedną usługę danych w chmurze, przy czym tylko 7% z nich ma wiedzę, gdzie dokładnie dane fizycznie przechowują i przetwarzają, a jest to wiedza krytyczna z punktu widzenia bezpieczeństwa. Co więcej, 49% baz danych nie jest w ogóle szyfrowanych. Brak zabezpieczeń tego typu sprawia, że firmy same tak naprawdę proszą się o kłopoty. Kolejną istotną kwestią jest dbanie o kontrolę dostępów – aż 73% organizacji nie ma wdrożonych rozwiązań z zakresu zarządzania tożsamością uprzywilejowaną dla zespołów DevOps. Co przekłada się na fakt,

że w przypadku 80% naruszeń dostępu do danych, wykorzystywane są poświadczenia zdobyte w sposób nieautoryzowany.

Jak zmieniało się bezpieczeństwo w sieci i jakie strategie związane z bezpieczeństwem są dziś skuteczne?

– Pierwotnie skupiano się na narzędziach klasy SIEM, które zbierają informacje z logów urządzeń i systemów, analizują ruch w sieci itp. Korelując, filtrując i normalizując wszystkie zebrane dane, dostarczają informacje oraz ostrzegają o podejrzanym ruchu, który ma miejsce w sieci. Na kolejnym etapie systemy SIEM zostały wzbogacone o rozwiązania klasy SOAR (Security Orchestration, Automation and Response), których zadaniem jest automatyzacja procesów reagowania na podstawie tzw. playbooków oraz wzbogacanie informacji agregowanych przez SIEM-y, wykorzystując do tego integracje ze źródłami danych o zagrożeniach. Obecnie rozwiązania dedykowane bezpieczeństwu działają, wykorzystując zasadę: przewiduj, zapobiegaj i reaguj. Do skutecznego działania rozwiązań tego typu została wykorzystana sztuczna inteligencja, której zadaniem jest automatyczne wykrywanie oraz cykliczna analiza zachowań użytkowników. Dodatkowo, w ramach ery transformacji cyfrowej do chmury istotne jest, aby uwzględnić nie tylko środowisko on-premise, ale również te elementy, które są wystawione do chmury. Tutaj IBM oferuje narzędzie, takie jak IBM Cloud Pak for Security, które pozwala na pełną integrację i centralizację danych oraz zarządzanie informacjami dotyczącymi bezpieczeństwa zarówno z lokalnego środowiska, jak i środowisk chmurowych.

Czym są rozwiązania Security Software, takie jak Guardium Data Protection i Guardium Insights firmy IBM?

– To rozwiązania przeznaczone do kontroli, monitorowania oraz zabezpieczania danych. Jak wcześniej wspomniałem, niemal połowa organizacji nie posiada rozwiązań z zakresu szyfrowania danych, a nie tylko te są nam potrzebne. Ważna jest również wiedza o tym, jakie mamy dane, gdzie są przechowywane i kto, kiedy i w jaki sposób z nich korzysta. Tu z pomocą przychodzi rodzina rozwiązań IBM Security Guardium. Data Protection pozwala na skanowanie i klasyfikowanie danych wrażliwych. Dodatkowo, w czasie rzeczywistym monitoruje aktywność wykorzystania danych oraz dostarcza analizy zachowań użytkowników, by rozpoznawać nietypowe aktywności. Pomaga też spełnić wymagania i regulacje dotyczące gromadzonych i przetwarzanych danych. IBM Security Guardium Insigths daje natomiast możliwość egzekwowania zasad, polityk oraz korelacji zdarzeń, czyli centralizuje wszystkie informacje zarówno ze środowisk lokalnych, jak i chmurowych. Rozwiązanie może być wykorzystane jako element wzbogacający dane z Data Protection bądź może znaleźć zastosowanie jako osobne narzędzie. Platforma IBM Security Guardium to jeszcze więcej rozwiązań wspierających bezpieczeństwo w organizacji: szyfrowanie danych i ich anonimizacja, skanowanie oraz usuwanie luk w zabezpieczeniach, analiza ryzyka oraz centralizacja zarządzania kluczami szyfrującymi. Podsumowując, jest to platforma pozwalająca wdrożyć kompleksowe rozwiązanie zabezpieczające wrażliwe oraz cenne dane w przedsiębiorstwie.

Jak w środowiskach hybrydowych skutecznie zabezpieczyć się przed naruszeniem danych uwierzytelniających?

– Ważne jest dbanie o właściwy stan uprawnień oraz odpowiednią weryfikację dostępu. Przez właściwy stan uprawnień rozumiem strategię polegającą na tym, że uprawnienia i dostępy powinny być tylko takie, jakie są niezbędne do wykonywania konkretnych obowiązków pracowników. To koniec z nadmiarowymi uprawnieniami, które zwykle wnoszą więcej problemów niż realnych korzyści. Kolejną ważną kwestią jest zarządzanie tożsamością uprzywilejowaną i kontami/dostępami współdzielonymi. W każdym środowisku będą tego typu dostępy i siłą rzeczy mają one zwykle podwyższone uprawnienia. Kontrola i rozliczalność w tym obszarze to podstawa. Człowiek jest najsłabszym ogniwem w tej układance i kontrola dostępu to priorytet. Narzędzia umożliwiające centralizację oraz wieloskładnikowe i kontekstowe uwierzytelnianie są istotnym elementem całego systemu bezpieczeństwa. Systemy, takie jak IBM Guardium, mają moduły przeznaczone do analizy zachowań użytkowników i w ten sposób uzupełniają całość, bo nawet w przypadku, gdy ktoś przedostanie się przez system weryfikacji, mogą to wykryć i zablokować nienaturalną aktywność takiego użytkownika. →

> ***49% baz danych nie jest w ogóle szyfrowanych. Brak zabezpieczeń tego typu sprawia, że firmy same tak naprawdę proszą się o kłopoty. Co więcej – aż 73% organizacji nie ma wdrożonych rozwiązań z zakresu zarządzania tożsamością uprzywilejowaną dla zespołów DevOps. Co przekłada się na fakt, że w przypadku 80% naruszeń dostępu do danych, wykorzystywane są poświadczenia zdobyte w sposób nieautoryzowany.***

Fot. tippapatt/stock.adobe.com

Coraz częściej mówi się o nowoczesnym zarządzaniu tożsamością i dostępem (IAM). Jakie ono powinno być?

– Nowoczesne zarządzanie tożsamością i dostępem to nie tylko systemy, które centralizują informacje o tożsamościach, kontach i uprawnieniach. Ich zadaniem jest również stała kontrola i zapewnienie, że użytkownicy mają tylko taki dostęp, jaki jest im potrzebny do wykonywania obowiązków, poprzez wykorzystanie procesów cyklicznej recertyfikacji uprawnień. Dodatkowo pozwalają na kategoryzację uprawnień pod względem ryzyka (np. dostępy do danych wrażliwych i tajnych). Kolejnym istotnym elementem jest kontrola rozdzielności obowiązków (SoD – Segregation of Duties), której zadaniem jest eliminacja posiadania uprawnień przez jednego użytkownika, które wzajemnie się wykluczają. Idąc dalej, ważnymi elementami, które adresowane są przez systemy IAM, to kontrola kont i uprawnień uprzywilejowanych, nie zapominająca przy tym o zarządzaniu urządzeniami. Z kolei uwierzytelnianie użytkowników powinno odbywać się wieloskładnikowo z wykorzystaniem kontekstu, czyli np. skąd się on łączy, z jakiego urządzenia (zaufanego bądź nie) itp.

Co tak naprawdę znaczy Zero Trust Security?

– Zero Trust to podejście, które zakłada, że nawet najbardziej złożone zabezpieczenia zawsze są narażone na zagrożenia zewnętrzne i wewnętrzne. Główne założenia tego podejścia to: nadawaj uprawnienia umożliwiające najmniejszy dostęp, nie ufaj nikomu i niczemu, zawsze kontroluj oraz zawsze zakładaj ryzyko ataku. Nie ma się co oszukiwać, im więcej powstaje zabezpieczeń, tym bardziej chcą je złamać hakerzy. W skład środowiska realizującego tę strategię wchodzą narzędzia z zakresu detekcji i reagowania na zagrożenia (IBM Security QRadar, IBM Security Cloud Pak for Security, IBM Security Guardium), zarządzania tożsamością oraz dostępem uprzywilejowanym (IBM Security Verify) oraz zarządzanie urządzeniami (MaaS360 with Watson).

Dlaczego warto przy wdrożeniach tych systemów korzystać z pomocy wyspecjalizowanych w outsourcingu IT firm, takich jak Cloudware Polska?

– Mamy w tym doświadczenie. Od lat dzielimy się wiedzą z naszymi klientami i wdrażamy rozwiązania m.in. z dziedziny bezpieczeństwa. Mamy szerokie portfolio klientów, którzy nam zaufali i konsekwentnie z nami współpracują, budując rozwiązania oraz podnosząc poziom bezpieczeństwa w swoich organizacjach. Dodatkowo mamy najwyższy poziom partnerstwa, jakie przyznaje IBM, co umożliwia nam oferowanie rozwiązań najwyższej klasy w najbardziej konkurencyjnych cenach.

Jak może wyglądać przykładowe wdrożenie?

– Jeden z naszych klientów z sektora bankowego zgłosił się do nas z potrzebą zorganizowania skutecznego zarządzania nadzorem i uprawnieniami. Wiedział, jak jest to ważne i miał konkretne wymagania. Chciał zbudować katalog uprawnień, w celu wdrożenia modelu RBAC (Role Based Access Control), cyklicznej weryfikacji uprawnień oraz klasyfikacji ryzyka związanego z uprawnieniami, oraz implementacji procesu delegacji uprawnień w ramach oddziałów. Wszystko to oczywiście z wykorzystaniem pełnej automatyzacji w celu zminimalizowania czynnika błędu ludzkiego. Zaproponowaliśmy i z sukcesem wdrożyliśmy rozwiązanie IBM Verify Governance, które bardzo dobrze spełniło te konkretne założenia. Nasz klient otrzymał rozwiązanie obsługujące całą organizację i podnoszące poziom bezpieczeństwa. Osiągnięto to dzięki: centralizacji, zapewnieniu spójności polityk, uruchomieniu procesów cyklicznej weryfikacji uprawnień w tym uprawnień nadanych poza systemem zarządzania tożsamością, wdrożeniu reguł rozdzielności obowiązków oraz ujednoliceniu zarządzania poprzez przejście na model korzystający z ról. Od momentu wdrożenia zarządzanie, przygotowanie oraz przejście audytów nie stanowi już dla niego żadnego problemu. •

Bazujące na sztucznej inteligencji rozwiązania cyberbezpieczeństwa dla branży finansowej

Fot. Blue Planet Studio/stock.adobe.com

W ostatnich latach sztuczna inteligencja (AI) i uczenie maszynowe (ML) zaczęły odgrywać coraz większą rolę w codziennym życiu. W domu inteligentne urządzenia decydują o tym, o której godzinie włączyć grzejniki i światła. Media społecznościowe wykorzystują złożone algorytmy, aby wybrać wiadomości, które mają trafić do konkretnych odbiorców. Mapy Google nawigują kierowców, dobierając drogę, która spowoduje najniższą emisję dwutlenku węgla. Banki obsługują klientów za pomocą chatbotów. Z dobrodziejstw AI i ML korzystają przedsiębiorstwa z różnych branż, stały się one również niezbędnym elementem skutecznej architektury cyberbezpieczeństwa. →

Fot. Fortinet

Wojciech Ciesielski
MENEDŻER FORTINET
DS. SEKTORA FINANSOWEGO

Sztuczna inteligencja na dobre zagościła w codziennym życiu. Warto wiedzieć, na czym polega jej działanie, bo nie służy ona wyłącznie jako mózg autonomicznych robotów. Z AI nierozerwalnie związane jest pojęcie uczenia maszynowego. Polega ono na umożliwieniu cyfrowym urządzeniom oraz obsługiwanym przez nie algorytmom nauczenia się, jak zrobić coś bez konieczności programowania ich przez ludzi. Uczenie maszynowe wymaga dostarczania informacji wejściowych, którymi mogą być dane czy też wiedza gromadzona przez przedsiębiorstwo. W efekcie pracy narzędzia wyposażonego w AI decydenci mogą zyskać wskazówki, co należy zrobić w celu poprawy procesów biznesowych. Na przykład, gdy mechanizm uczenia maszynowego analizuje różne parametry, które mogą wpływać na tempo sprzedaży w przedsiębiorstwie, menedżerowie sprzedaży mogą poświęcać odzyskany w ten sposób czas na bardziej intensywną współpracę z przedstawicielami handlowymi.

Dzięki analizie odpowiednich zbiorów danych, mechanizm uczenia maszynowego dokonuje różnych obserwacji, które mogą umknąć uwadze człowieka. Z kolei sztuczna inteligencja wykorzystuje uzyskaną przez uczenie maszynowe wiedzę. AI próbuje rozwiązywać problemy biznesowe lub techniczne, bazując na danych, pomagając użytkownikom w procesie podejmowania decyzji lub samodzielnie dokonując osądu – dlatego często kojarzona jest z *„autonomiczną formą życia”*. W razie potrzeby AI może być wykorzystana do szybkiej analizy dużych zbiorów danych, których żaden ludzki umysł nie byłby w stanie przetworzyć w racjonalnym czasie i może wspomagać podejmowanie decyzji.

Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie

Rozwój sztucznej inteligencji na dobre zmienił sposób, w jaki korzysta się z technicznych rozwiązań. Przemiana nie ominęła również branży cyberbezpieczeństwa, która odpowiada za ochranianie często najbardziej wrażliwych danych. Dzięki AI można szybciej i dokładniej reagować na pojawiające się nieustannie nowe cyberzagrożenia, ograniczając tym samym negatywne skutki naruszeń bezpieczeństwa oraz minimalizując ilość informacji przedostających się w niepowołane ręce. Działy IT przekazują sztucznej inteligencji coraz więcej zadań wykonywanych dotychczas przez ludzi, co w znacznym stopniu przyczynia się do polepszenia jakości informacji o zagrożeniach.

Ważną rolę w tej dziedzinie już teraz odgrywa uczenie maszynowe. Jego zdolności predykcyjne oraz dotyczące rozpoznawania wzorców zachowań sprawiają, że jest to idealne narzędzie do sprostania wielu wyzwaniom związanym z bezpieczeństwem IT. Mechanizmy uczenia maszynowego mogą gromadzić, strukturyzować i organizować dane, a następnie znajdować wzorce pomocne przy podejmowaniu bardziej świadomych decyzji dotyczących reagowania na cyberatak oraz ogólnego planu ochrony przedsiębiorstwa. Zasilane są one obecnie bardzo dużymi ilościami danych gromadzonymi przez urządzenia internetu rzeczy (*Internet of Things, IoT*), które wykorzystywane są przez aplikacje przewidujące wszelkie potencjalnie niebezpieczne zdarzenia w sieci. Informacje te zawierają jednak dziś dużo fałszywych sygnałów w wyniku zmiennej natury IoT. Cyfrowe zagrożenia charakteryzują się znaczną dynamiką: urządzenie może być czyste w jednym momencie, by następnie zostać zainfekowane i ponownie uzdrowione w ciągu kilku sekund. Należy jednak zachować ostrożność. Nie można przekazywać pełnej kontroli maszynom i trzeba wypracować optymalny model równowagi operacyjnej. Dzięki właśnie tej współpracy pomiędzy ludźmi a zaawansowanymi systemami rozwiązania nowej generacji staną się prawdziwie efektywne.

Zastosowanie sztucznej inteligencji i uczenia maszynowego w rozwiązaniach cyberbezpieczeństwa przekłada się także na minimalizowanie błędów ludzkich. Często zdarza się, że zanim administratorzy sieci odkryją zagrożenie, jest już zbyt późno i cyberprzestępcy zaczną siać spustoszenie w systemach. Ten problem można rozwiązać poprzez automatyczną wymianę informacji pomiędzy rozwiązaniami wykrywającymi a prewencyjnymi. Pomocne może też być użycie wspieranej neutralizacji zagrożenia, będącej połączeniem działań ludzi i rozwiązań technicznych. Automatyzacja pozwala również zespołom IT poświęcać więcej czasu na analizę zdarzeń w celu lepszej organizacji działań prewencyjnych. Systemy cyberbezpieczeństwa bazujące na sztucznej inteligencji będą się stale dostosowywać do nieustannie pojawiających się nowych rodzajów ataków,

a w przyszłości będą mogły samodzielnie podejmować wiele skomplikowanych decyzji.

Warto jednak zauważyć, że z osiągnięć sztucznej inteligencji chętnie korzystają także sami cyberprzestępcy. W ich rękach stanowi ona coraz większe zagrożenie dla bezpieczeństwa sieci i danych. Sytuację pogarsza możliwość wykorzystania przez nich tzw. inteligentnych rojów botów oraz tworzenia zautomatyzowanych i bazujących na skryptach zagrożeń. To wszystko w zawrotnym tempie zwiększa szybkość i skalę cyberataków. Warto więc zwalczać ogień ogniem, a więc odpowiadać na działania cyberprzestępców ich własną bronią. Wyrównanie szans w walce z przestępcami będzie możliwe tylko wtedy, gdy do ich taktyki zostanie przystosowana metodyka działań ochronnych – jest to istotne zwłaszcza w sytuacji niedoboru specjalistów na tym rynku. Wykorzystanie potencjału sztucznej inteligencji może usprawnić pracę zespołów ds. bezpieczeństwa i zmniejszyć odczuwanie negatywnych skutków luki kompetencyjnej.

Rozwiązania ochronne Fortinet dla branży finansowej

Bardzo wiele informacji, które nieustannie przyciągają uwagę cyberprzestępców, przechowywanych jest w instytucjach finansowych. Wrażliwe dane osobowe, dające nie tylko dostęp do pieniędzy, ale umożliwiające również podejmowanie innych negatywnych działań, jak ich sprzedaż na czarnym rynku, są niezwykle atrakcyjnym łupem dla przestępców. Ryzyko związane z występowaniem cyberataków w instytucjach finansowych rośnie wraz z procesem cyfryzacji i zwiększaniem ich uzależnienia od rozwiązań technicznych. Instytucje finansowe są uważane za elementy infrastruktury krytycznej państw, a jakiekolwiek problemy w ich funkcjonowaniu byłyby bardzo szkodliwe dla gospodarek.

Tymczasem wyzwań, z którymi branża finansowa musi się mierzyć, ciągle przybywa. Przede wszystkim klienci wymagają, a może nawet uznają to za oczywiste, aby ich dostawcy usług finansowych zapewniali im bezproblemowe korzystanie z produktów w trybie online. Obejmuje to bankowość elektroniczną, zarządzanie finansami za pośrednictwem aplikacji mobilnych, bardziej elastyczną i skuteczną – zarówno w aspekcie ludzkim, jak i cyfrowym – obsługę klienta, jak też oferty bazujące na danych, pomagające im lepiej analizować sytuację finansową i planować przyszłość.

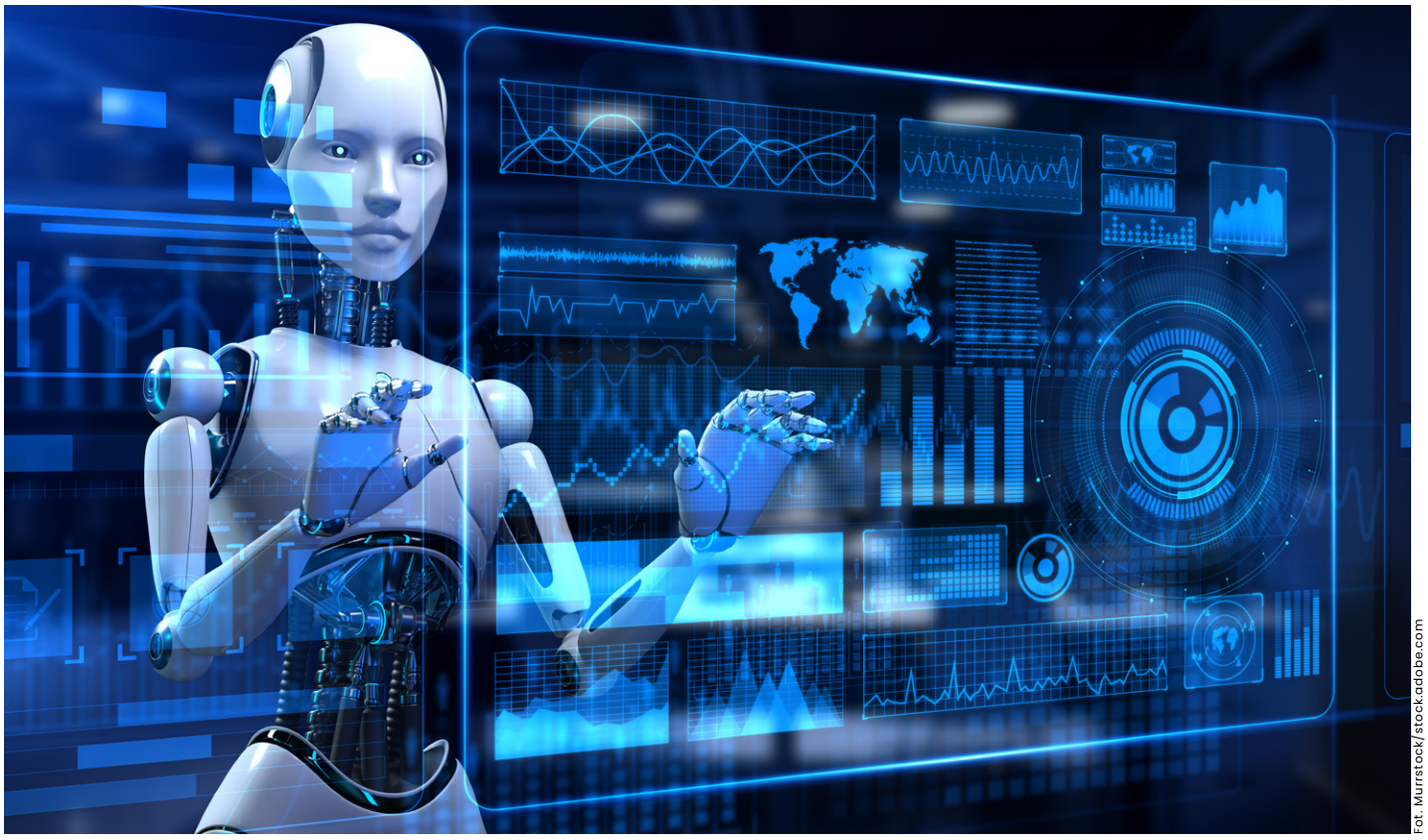
Jednak wraz z wprowadzaniem na rynek coraz większej liczby usług cyfrowych rośnie ryzyko cyberataku. Dostawcy usług finansowych muszą bronić się przed naruszeniami danych, złośliwym oprogramowaniem, phishingiem i innymi atakami socjotechnicznymi, których stopień zaawansowania, częstotliwość i intensywność rośnie. Instytucje finansowe muszą sprostać wszystkim wymaganiom klientów i zagrożeniom bezpieczeństwa, jednocześnie spełniając nowe, bardziej rygorystyczne wymagania, w tym prawne, dotyczące prywatności i ochrony danych w ramach rozległej infrastruktury IT.

Automatyczne wykrywanie cyberzagrożeń oraz reagowanie na nie może być najskuteczniejsze dzięki przyjęciu przez przedsiębiorstwa zintegrowanej architektury ochronnej, jakiej przykładem jest Fortinet Security Fabric. Kiedy wszystkie elementy ekosystemu cyberbezpieczeństwa są połączone i mogą się ze sobą komunikować, pozwala to na zautomatyzowanie procesów kontrolnych bazujących na zdefiniowanych wcześniej politykach bezpieczeństwa. Dzięki temu zadania wcześniej realizowane ręcznie zostają zastąpione zautomatyzowanymi procesami, aby zmniejszyć obciążenie personelu. Zintegrowana platforma ochronna zapewnia również system wymiany danych w czasie rzeczywistym, które mogą zasilać dedykowane lub obszarowe aplikacje ochronne bazujące na sztucznej inteligencji i uczeniu maszynowym.

Kiedyś zespoły IT pracowały oddzielnie – różne grupy zajmowały się aplikacjami, serwerami, routerami i przełącznikami oraz zaporami sieciowymi. Teraz wszyscy mogą się ze sobą komunikować, wykonując swoją pracę w ramach ujednoliconych zautomatyzowanych mechanizmów, które integrują cały cykl wdrażania rozwiązań ochronnych i utrzymują odpowiedni poziom bezpieczeństwa. Dzięki temu klienci z branży usług finansowych, korzystający ze zautomatyzowanych rozwiązań Fortinet, wdrażają aplikacje w ciągu minut, a nie dni.

Narzędzia automatyzujące firmy Fortinet umożliwiają zespołom szybkie wdrażanie bezpiecznej infrastruktury sieciowej i aplikacji, natomiast usługa ponownej rekonfiguracji środowiska IT (*reprovision)* umożliwia usunięcie istniejących ustawień konfiguracyjnych i szybkie ich odbudowanie na podstawie wzorca przechowywanego w bazie danych. Jest to swego rodzaju przycisk resetowania dla całej infrastruktury, której ustawienia mogły być zmienione przez włamywacza podczas ataku, złośliwe oprogramowanie, awarię lub inne nieprzewidziane zdarzenia.

Przedsiębiorstwa ze wszystkich branż, także finansowej, potrzebują narzędzia, które pomoże wdrażać nowe urządzenia ochronne w ich sieciach i jednocześnie eliminować występowanie błędów ludzkich. Przykładem takiego rozwiązania jest FortiManager, w którym zastosowano mechanizmy umożliwiające automatyzację powtarzalnych, ale kluczowych zadań związanych z bezpieczeństwem. Spełnia ono wszelkie wymagane standardy bezpieczeństwa, bez uszczerbku dla szybkości wprowadzania produktów na rynek. →



Fot. Murrstock/stock.adobe.com

Automatyzacja pomaga też lepiej i łatwiej zarządzać bardzo rozległym systemem zabezpieczeń. Równie istotne jest odpowiednie reagowanie oraz – przede wszystkim – zapobieganie wszelkim naruszeniom bezpieczeństwa sieci. Jednym z rozwiązań, które zapewnia kompleksowe zarządzanie obsługą incydentów, od ich rozpoznania do zniwelowania, jest system NDR *(Network Detection and Response)*, wykorzystujący sztuczną inteligencję i inne mechanizmy analizy do identyfikacji podejrzanej aktywności sieciowej, która może być wskaźnikiem trwającego cyberataku. Systemy NDR są szkolone do modelowania wzorców normalnego ruchu sieciowego, co ułatwia późniejsze zidentyfikowanie nietypowej, prawdopodobnie złośliwej aktywności.

Przedsiębiorstwa potrzebują również narzędzi, które zapewniają kompleksową ochronę sieci, a także wykrywanie incydentów i reagowanie na nie. Konieczne przy tym jest nie tylko zabezpieczenie ruchu sieciowego, ale też analiza plików, wraz z identyfikacją źródłowej przyczyny incydentu. Z pomocą przychodzi tu FortiNDR. Jest to rozwiązanie, które zostało wstępnie przeszkolone – zaimplementowano w nim ponad 6 milionów wzorców ułatwiających zidentyfikowanie złośliwego kodu w środowiskach IT i OT, a także zaklasyfikowanie go do odpowiedniej kategorii zagrożeń. Funkcje te mogą również precyzyjnie wskazać źródło problemu i poprzez analizę całego ruchu stwierdzić, czy malware nadal rozprzestrzenia się w systemie.

Współczesne zagrożenia muszą zostać zneutralizowane w bardzo krótkim czasie, a żeby tego dokonać, potrzebne są urządzenia ochronne bazujące na sztucznej inteligencji i wykorzystujące automatyzację procesów. Możliwości te zapewnia rozwiązanie FortiXDR (*eXtended Detection and Response)* zaprojektowane w celu rozszerzenia możliwości, jakie daje architektura Fortinet Security Fabric. Zastosowany w nim silnik Dynamic Control Flow Engine na bieżąco zasilany jest informacjami o nowych zagrożeniach przez zespół specjalistów FortiGuard Labs oraz ekspertów odpowiedzialnych za cyberbezpieczeństwo w danej instytucji. FortiXDR rozpoczyna działanie od analizy incydentów, aby następnie potwierdzić, czy odbiegające od normy zjawisko to rzeczywiście cyberatak. Następnie jest ono dokładnie badane przez mechanizm sztucznej inteligencji, który ma za zadanie sklasyfikować zagrożenie i ocenić jego skalę. Proces ten kończy się wyborem najlepszego sposobu reagowania, który wdrażany jest automatycznie w celu natychmiastowej neutralizacji niebezpiecznej sytuacji.

Przykład wdrożenia rozwiązań ochronnych Fortinet

Branża finansowa jest kluczowym celem cyberprzestępców, którzy stają się coraz bardziej wyrafinowani w swoich próbach szyfrowania danych (a następnie żądania okupu za ich odszyfrowanie) lub kradzieży informacji z groźbą ich upublicznienia. Skuteczny cyberatak może skutkować zniszczeniem marki oraz karami finansowymi za nieodpowiednie zabezpieczenie poufnych danych.

Współczesne oddziały banków są pełne urządzeń końcowych, a więc laptopów, smartfonów, drukarek, serwerów czy kamer. Niestety, wzrostowi ich liczby towarzyszy wzrost ryzyka wystąpienia cyberzagrożeń, w tym niezwykle groźnego i często wykorzystywanego w ostatnich latach oprogramowania ransomware.

Użytkownikom takich rozproszonych urządzeń końcowych często doskwiera brak zintegrowanych rozwiązań ochronnych. Przyjęcie bardziej spójnego podejścia do ich ochrony powinno być priorytetem dla osób odpowiedzialnych za cyberbezpieczeństwo, aby uniknąć niepotrzebnego ryzyka.

Przykładem implementacji zabezpieczeń urządzeń końcowych była sytuacja, w której przedsiębiorstwo poprosiło Fortinet o przedstawienie wersji demonstracyjnej rozwiązania FortiEDR, które bazuje na sztucznej inteligencji i zapewnia odpowiedni poziom widzialności takiego sprzętu oraz analizę i neutralizację występujących w nim zagrożeń w czasie rzeczywistym. Okazało się, że możliwości narzędzia Fortinet wykraczają poza te oferowane przez inne rozwiązania tego rodzaju.

Po rozważeniu różnych opcji firma wybrała FortiEDR, który miał być świadczony jako zarządzana usługa wykrywania incydentów i reagowania na nie (MDR) na 800 urządzeniach końcowych. Przyjęcie podejścia typu MDR oznacza, że Fortinet zajmuje się monitorowaniem sprzętu i wymaganiami dotyczącymi reagowania na zagrożenia w imieniu klienta. Model ten zapewnia znaczne korzyści dla firmy, która nie musi prowadzić własnego centrum operacji bezpieczeństwa (SOC). Dzięki temu, że Fortinet zarządza bezpieczeństwem urządzeń końcowych, pracownicy klienta odpowiedzialni za IT mogą skupić się na innych obowiązkach.

Chociaż bezpośrednim celem klienta była lepsza ochrona urządzeń końcowych, to rozwiązania Fortinet zostały wybrane także z innych powodów. Producent oferuje platformę Security Fabric, w ramach której użytkownicy mogą konsolidować swoje rozwiązania sieciowe, aby wyeliminować luki w infrastrukturze ochronnej. W branży usług finansowych jest to kluczowy wyróżnik Fortinet, dzięki któremu instytucje w niej działające mogą nadal poprawiać stan bezpieczeństwa sieci i danych, w reakcji na stale zmieniający się krajobraz zagrożeń.

Fortinet Security Fabric nie tylko zwiększa poziom bezpieczeństwa przedsiębiorstwa, ale także zmniejsza złożoność procesów zarządzania infrastrukturą IT. Są one intuicyjne, zasilane przez zautomatyzowane i zarządzane usługi bazujące na sztucznej inteligencji i uczeniu maszynowym. W porównaniu ze złożonym zbiorem dostawców zabezpieczeń, do którego firma była przyzwyczajona, Fortinet pokazał również, że może dostarczyć skonsolidowaną, wydajną i skuteczną platformę cyberbezpieczeństwa typu mesh. Rewolucja cyfrowa stwarza wiele możliwości dla instytucji finansowych w zakresie wprowadzania innowacji i świadczenia szeregu nowych usług dla klientów. W miarę postępu tego procesu cyberbezpieczeństwo będzie miało kluczowe znaczenie, jeśli banki i inne instytucje mają utrzymać odpowiedni poziom bezpieczeństwa swoich systemów i obiektów. Oznacza to przyjęcie holistycznego podejścia do cyberbezpieczeństwa z wykorzystaniem najnowszych zdobyczy technologii, w tym AI oraz ML.

(Sztuczna) inteligencja przyszłości

Zastosowanie sztucznej inteligencji (AI) oraz uczenia maszynowego (ML) jest obecnie konieczne przede wszystkim tam, gdzie występują nieznane zagrożenia – AI jest odpowiedzialna za działanie, natomiast ML – za uczenie się. Jednak uczenie maszynowe wykorzystywane przeciwko zagrożeniom internetowym jest stworzone w zupełnie innym modelu niż to używane do wykrywania luk typu zero-day. Dlatego podmioty z branży finansowej muszą być w stanie umiejętnie połączyć wszystkie sposoby wykorzystania ML, aby skutecznie zabezpieczyć się przed różnymi rodzajami ataków oraz chronić swoje cenne dane i zasoby finansowe.

Wykorzystując nowoczesne rozwiązania, w tym uczenie maszynowe i sztuczną inteligencję, w znaczącym stopniu można obniżyć ryzyko poniesienia poważnych strat. W branży usług finansowych mogą one prowadzić również do utraty zaufania klientów i dalszych konsekwencji prawnych, np. w związku z przepisami RODO w przypadku wycieku danych osobowych. Korzystanie z nowatorskich mechanizmów automatyzacji i AI pozwala na niwelowanie skutków istniejącej na rynku luki kompetencyjnej, co przyczynia się do obniżenia kosztów związanych z zabezpieczaniem przedsiębiorstwa i ułatwia zespołom odpowiedzialnym za cyberbezpieczeństwo radzenie sobie z codziennymi zadaniami.

Z rozwiązań bazujących na sztucznej inteligencji i uczeniu maszynowym, służących do wykrywania znanych i nieznanych zagrożeń, może skorzystać każda firma. Ale tym, co wyróżnia najbardziej innowacyjne z nich, jest zastosowanie ich mechanizmów do szybkiego podejmowania decyzji dotyczących bezpieczeństwa, co ma znaczenie dla całości funkcjonowania biznesu. •

Zwinne rozwiązania w kontekście bezpieczeństwa informacji

Jak zapewnić bezpieczeństwo w instytucjach świadczących usługi finansowe

Od 2017 r. cyberataki na instytucje świadczące usługi finansowe wzrosły o ponad 70%[1]. Czas do skutecznego naruszenia bezpieczeństwa (*Time-to-compromise*) obecnie jest już mierzony w minutach, a eksfiltracja danych następuje w ciągu kilku dni[2]. To oznacza, że przed branżą usług finansowych stoją poważne wyzwania.

Fot. ServiceNow

Maciej Ostrowski
COUNTRY SALES DIRECTOR, POLAND, SERVICENOW

Koszty cyberataków są niezwykle wysokie dla każdej organizacji. Średni koszt naruszenia bezpieczeństwa informacji wynosi obecnie 3,92 mln dolarów – to 12% więcej niż pięć lat temu[3]. Opóźnione reagowanie oznacza ryzyko ujawnienia cennych danych i poufnych informacji. Proces naprawczy również może być niezwykle kosztowny, a utratę reputacji trudno wręcz wycenić. Dlaczego więc identyfikowanie zagrożeń i reagowanie na nie wciąż zajmuje organizacjom tak dużo czasu?

Specjaliści ds. bezpieczeństwa informacji i IT jednogłośnie widzą źródło problemu w **niekompatybilności pomiędzy narzędziami bezpieczeństwa a narzędziami informatycznymi**. Nie wynika ona z braku rozwiązań technologicznych, lecz z tradycyjnego podejścia firm do kwestii związanych z bezpieczeństwem – np. z inwestycji w liczne, rozproszone narzędzia, które łącznie generują tysiące powiadomień bez nadawania im priorytetów. Druga przyczyna to brak automatyzacji, czyli postawienie na ręczną realizację procesów w firmie. Przy braku przejrzystości organizacyjnej dodatkowo wiąże się to z trudnościami w identyfikacji odpowiednich osób kontaktowych powiązanych z procesem.

Trzecia sprawa to wielość niezabezpieczonych zbiorów danych i procedur dotyczących bezpieczeństwa informacji (księga procedur). Ten brak precyzji sprawia, że nie ma gwarancji, że wszyscy w firmie stosują się do tych samych zasad.

Niezautomatyzowane procesy typowe dla tradycyjnego reagowania na zagrożenia bezpieczeństwa informacji skutkują więc niską efektywnością: listy przygotowane w arkuszach kalkulacyjnych szybko się dezaktualizują, a wiadomości e-mail często trafiają do niewłaściwych skrzynek; definiowanie i monitorowanie wskaźników efektywności działania staje się trudne, a wysoko wykwalifikowani pracownicy są zmuszeni do skupiania się na zadaniach niskiego poziomu – to powoduje wysoką rotację kadr.

Koordynacja reagowania na incydenty w całej organizacji stanowi największe wyzwanie dla większości przedsiębiorstw[4].

W POSZUKIWANIU OPTYMALNEGO ROZWIĄZANIA

Rozwiązanie, które można by uznać za optymalne dla firmy, **umożliwia skuteczne reagowanie** na incydenty i podatności związane z bezpieczeństwem informacji**; pozwala powiązać zespoły** ds. IT i bezpieczeństwa; umożliwia **przejrzystą wizualizację stanu** bezpieczeństwa przedsiębiorstwa. Dla dyrektora ds. bezpieczeństwa informacji (CISO) i zespołu ds. bezpieczeństwa to na dziś **zintegrowana platforma służąca orkiestracji, automatyzacji i reagowaniu**, która pozwala odpowiedzieć na pytanie: „Czy jesteśmy bezpieczni?".

Takim rozwiązaniem są **systemy bezpieczeństwa informacji, które korzystają z jednego źródła obejmującego zarówno bezpieczeństwo informacji, jak i IT**. Dzięki temu wszystkie osoby zaangażowane w reagowanie mają dostęp do najbardziej aktualnych danych. Ponadto współużytkowany system pozwala zespołom ds. bezpieczeństwa informacji i IT na koordynowanie reagowania.

Systemy te dodatkowo są zintegrowane z bazą danych zarządzania konfiguracją (CMDB). Dzięki temu analitycy mogą **szybko zidentyfikować** obszary dotknięte lub zagrożone, ich lokalizacje i podatność na kolejne ataki. Ważne jest również **automatyczne nadawanie priorytetów** wszystkim incydentom i podatnościom w zakresie bezpieczeństwa danych, uwzględniające potencjalny wpływ sygnalizowanych wydarzeń na organizację. Pozwala to skutecznie reagować na zagrożenia, bo analitycy otrzymują krytyczne informacje w kilka sekund. Reakcja na naruszenie bezpieczeństwa jest też szybka i efektywna w wyniku wdrożonej orkiestracji – gdyż działania podejmowane są z jednej konsoli, która współdziała z innymi narzędziami bezpieczeństwa.

Prócz rozwiązań technologicznych odpowiedni poziom bezpieczeństwa i reakcji na cyberatak zapewnia przestrzeganie procedur dotyczących bezpieczeństwa informacji – kluczowe znaczenie mają workflow'y. **Scenariusz definiujący zasady bezpieczeństwa** informacji umożliwia pracownikom niższego szczebla realizowanie konkretnych zadań związanych z bezpieczeństwem, podczas gdy bardziej doświadczeni specjaliści ds. bezpieczeństwa informacji koncentrują się na tropieniu złożonych zagrożeń. Pozwala on również na łatwą identyfikację osób uprawnionych do zatwierdzania proponowanych działań i ekspertów. Powinien być też skorelowany z narzędziami umożliwiającymi monitorowanie wyników osiąganych przez zespół i zbieranie danych do ewaluacji, tak aby móc doskonalić procesy.

STARE I NOWE ŚCIEŻKI REAGOWANIA

Wraz ze wzrostem liczby cyberataków konieczne i szybkie naprawianie luk w zabezpieczeniach jest coraz trudniejsze. Głównymi problemami instytucji świadczących usługi finansowe są: brak wspólnego spojrzenia na aplikacje i aktywa w zespołach ds. bezpieczeństwa informacji i IT (82%) oraz trudności z ustaleniem priorytetów w kwestii działań naprawczych (70%).[5]

W przypadku pojawienia się ważnego i widocznego zagrożenia czy podatności na cyberatak przedsiębiorstwo może dziś zareagować na kilka sposobów.

Przy podejściu tradycyjnym, gdy zagrożenie zostaje wykryte, zespół ds. bezpieczeństwa zaczyna działać, aby zaradzić sytuacji. W tym czasie dyrektor ds. bezpieczeństwa informacji (CISO) dowiaduje się o incydencie i chce wiedzieć, czy i w jaki sposób dotyczy to danej organizacji. Zespół rzuca się do oceny systemów, próbując także ustalić, kto musi zatwierdzić wszelkie awaryjne poprawki w trwającej →

sytuacji kryzysowej. Ręczna koordynacja między zespołami może trwać nawet kilka dni, co zwiększa podatność krytycznych systemów i naraża firmę na ryzyko naruszenia danych.

Przy podejściu nowoczesnym instytucja korzystająca z orkiestracji bezpieczeństwa, automatyzacji i platformy reagowania może natychmiast zareagować na wykrytą podatność w zabezpieczeniach. Szybko podejmuje następujące działania w z góry zdefiniowanej kolejności:

- **Ocena:** dane skanowania są automatycznie pobierane z systemu zarządzania podatnościami. Jest to skorelowane z zewnętrznymi źródłami, takimi jak zewnętrzna baza danych o podatności na zagrożenia i wewnątrzorganizacyjna baza aktywów, aby nadać priorytet podatnościom zarówno z punktu widzenia ryzyka samej podatności, jak i jej wpływu na usługi firmy.
- **Powiadomienie:** zdefiniowany wcześniej workflow powiadamia zespół ds. bezpieczeństwa o krytycznej luce mającej wpływ na aktywa o wysokim priorytecie. Analitycy mogą zapoznać się z informacjami o danej podatności i zagrożonych elementach, korzystając z jednej konsoli.
- **Reagowanie:** zgodnie z przygotowanym wcześniej workflow rozpoczyna się proces reagowania na zagrożenie. System automatycznie wnioskuje o zatwierdzenie awaryjnych działań naprawczych w odniesieniu do krytycznych elementów podatnych na dane zagrożenie. Po wprowadzeniu poprawek, przed oznaczeniem luki jako zamkniętej, przeprowadza się dodatkowe skanowanie weryfikujące poprawki.
- **Mitygacja:** po naprawie kluczowych aktywów zespoły ds. bezpieczeństwa i IT mogą opracować plan naprawczy dla pozostałych podatnych elementów, korzystając z jednolitej platformy reagowania. Wnioski o zaakceptowanie zmian są automatycznie kierowane do odpowiednich osób w zespole IT, eliminując konieczność uczenia się struktury organizacyjnej na pamięć. Współdzielona platforma gwarantuje także udostępnianie informacji na bezpiecznych zasadach „wiedzy koniecznej".
Raportowanie: na tym etapie dyrektor ds. bezpieczeństwa otrzymuje wstępny raport, a system bezpieczeństwa automatycznie generuje ewaluację po incydencie z dokładnymi miarami.

BEZPIECZEŃSTWO ZBUDOWANE DZIĘKI AI

Nowoczesne systemy bezpieczeństwa wygrywają z tradycyjnym podejściem m.in. dlatego, że są tworzone w oparciu o rozwiązania sztucznej inteligencji, która szybko i skutecznie rozpoznaje i reaguje na zagrożenia, a także umożliwia ich prze-

NAJWAŻNIEJSZE MOŻLIWOŚCI SZTUCZNEJ INTELIGENCJI TO M.IN.:

Uczenie się: trening sztucznej inteligencji odbywa się poprzez wprowadzanie do systemu dużych ilości danych, zarówno uporządkowanych, jak i nieuporządkowanych. W procesie uczenia maszynowego i głębokiego sztuczna inteligencja uczy się rozumieć cyberbezpieczeństwo i cyberzagrożenia. Nieuporządkowane dane, takie jak dane z rozpoznawania twarzy czy analizy materiałów dźwiękowych i filmowych, stanowią obiecujący obszar, w którym sztuczna inteligencja może przewyższyć możliwości człowieka i zaoferować skuteczniejsze od tradycyjnie stosowanych narzędzia.

Rozumowanie: sztuczna inteligencja dokonuje spostrzeżeń i poprzez zaawansowane analizy szuka związków pomiędzy różnymi atrybutami. Na przykład może szukać powiązań pomiędzy złośliwymi plikami, informatorami i adresami IP oraz wzbogacać swoje ustalenia o informacje behawioralne i historyczne. Analizy takie pozwalają na coraz szybsze podejmowanie decyzji w miarę zdobywania przez sztuczną inteligencję nowych doświadczeń, na podstawie których dokonuje spostrzeżeń.

Automatyzacja: przedsiębiorstwa i instytucje mogą zoptymalizować swoje działania w zakresie automatyzacji przez połączenie ich z innowacjami w zakresie sztucznej inteligencji. Zautomatyzowane procesy gromadzą istotne dane, a sztuczna inteligencja analizuje je za pomocą modeli, w wyniku czego otrzymujemy bardziej wartościowe informacje analityczne.

Powinny one również rozumieć, jak działają rozmaite procesy i narzędzia, z których korzystają, a także jakie mają konsekwencje dla ich bezpieczeństwa. Sztuczna inteligencja może zwiększyć skuteczność oceny danych kontrolnych, a także pomóc w analizie mocnych i słabych punktów w działaniu narzędzi i procesów.

widywanie. W porównaniu do wielu innych rodzajów zabezpieczeń takie rozwiązanie wymaga też mniej nadzoru ze strony człowieka. W miarę jak modele sztucznej inteligencji dojrzewają, a użytkownicy coraz śmielej stosują tę technologię, pojawia się możliwość łączenia poszczególnych zadań w skoordynowane sekwencje.

Współczesne rozwiązania w zakresie bezpieczeństwa są najefektywniejsze, gdy stosuje się je w konkretnych przypadkach, takich jak wysoce niezawodne wykrywanie i unieszkodliwianie na urządzeniach końcowych ataków phishingowych, spamu lub wyrachowanych ataków z użyciem złośliwego oprogramowania. Sztuczna inteligencja musi mieć zdolność uczenia się na podstawie takich zdarzeń, gromadzenia spostrzeżeń i wyciągania wniosków, tak aby z czasem móc zwiększać swoje możliwości.

STRATEGIA NA PRZYSZŁOŚĆ

Branża usług finansowych na pewno będzie przyspieszała swoją transformację cyfrową – będzie udostępniać coraz więcej usług za pośrednictwem internetu i wykorzystywać technologię, by zwiększyć elastyczności swych działań. Zmiany te oznaczają coraz większą podatność na zagrożenia bezpieczeństwa informacji i coraz większą konieczność przeciwdziałania. Należy zatem przewidywać, że branża postawi na sprawne i skuteczne reagowanie. Dużą szansę na rozwój ma w związku z tym popularyzacja innowacyjnych platform orkiestracji bezpieczeństwa, automatyzacji i reagowania.

PLATFORMA W PRAKTYCE

Zbudowana na bazie Now Platform™ platforma Security Operations wykorzystuje inteligentne workflow'y, automatyzację i koordynację z IT na wysokim poziomie, aby usprawnić reagowanie w zakresie bezpieczeństwa. Dzięki orkiestracji procesów związanych z bezpieczeństwem, automatyzacji i rozwiązaniom w zakresie reagowania identyfikacja zagrożeń i podatności, także działania naprawcze i koordynacyjne są bardzo skuteczne.

1 HTF Market Intelligence, „Global Cybersecurity in Financial Services Market (2018- 2023)"; 2019.
2 Verizon, „2018 Data Breach Investigations Report", 2018.
3 IBM Security and Ponemon Institute, „2019 Cost of a Data Breach Report", 2019.
4 Enterprise Strategy Group, „Status Quo Crees Security Risk: The State of Incident Response", 2020.
5 ServiceNow „The State of Vulnerability Response in Healthcare: Patch Work Requires Attention", 2019.

CASE STUDY: INNOWACYJNE ROZWIĄZANIA SERVICENOW W DANSKE BANK

Danske Bank został założony 150 lat temu w Danii. Obecnie działa w ośmiu krajach i zatrudnia ponad 21 600 pracowników na całym świecie. Danske Bank zajmuje się obsługą ponad 3,3 mln klientów – indywidualnych i z sektora MŚP – oraz ponad 2 tys. instytucjonalnych.

Jedną z głównych wartości Danske Bank jest świadczenie konkurencyjnych usług finansowych dzięki wykorzystaniu szerokiej wiedzy, umiejętności i technologii, a także ciągłe poszukiwanie i wdrażanie innowacyjnych rozwiązań, które podnoszą efektywność pracy i ulepszają procedury oraz działania biznesowe.

U podstaw strategii Danske Bank leży nieprzerwana innowacyjność w zakresie produktów i usług oferowanych klientom. Danske Bank zdecydował się na kompleksowe wdrożenie skalowanej i elastycznej platformy firmy ServiceNow z myślą o dalszym rozwoju firmy. Wdrożone rozwiązania stały się istotnym wsparciem bieżących działań biznesowych banku.

Jednym z głównych obszarów wdrożenia platformy ServiceNow było bezpieczeństwo. Danske Bank skoncentrował się na konsolidacji danych i procesów w jednym środowisku. Platforma ServiceNow umożliwiła automatyczne unieszkodliwianie zagrożeń, a także pozwoliła na precyzyjne oszacowanie wydajności procesów bezpieczeństwa. Powiązanie ich z procesami operacyjnymi umożliwiło lepszą współpracę we wszystkich departamentach i filiach banku. Ponadto dzięki wdrożonym rozwiązaniom Danske Bank zanotował 93% mniej zdarzeń o wysokim priorytecie bezpieczeństwa i aż sześciokrotnie krótszy czas przywrócenia usług.

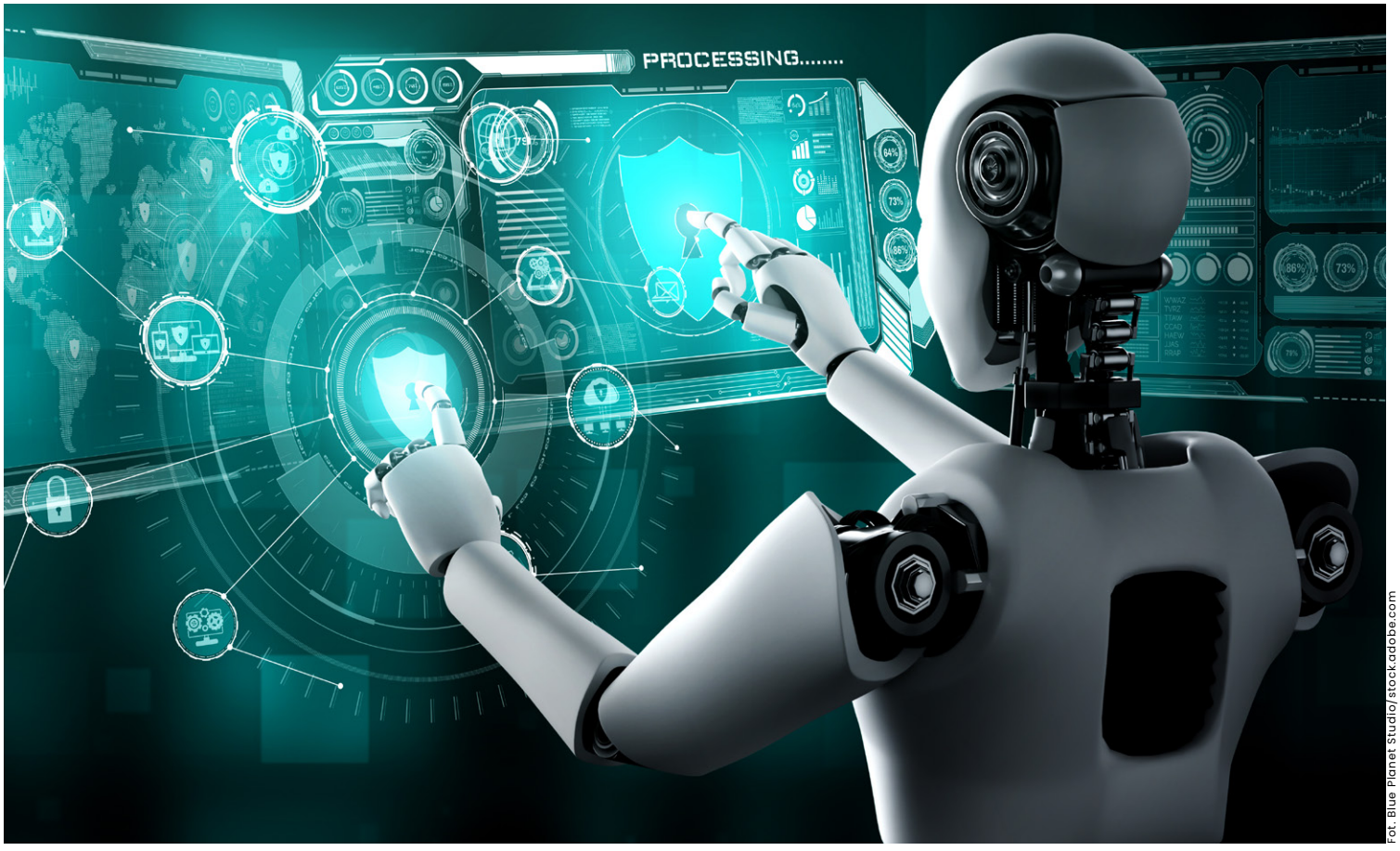
Od czasu wprowadzenia platformy ServiceNow stała się ona strategiczną częścią działalności Danske Bank, umożliwiła bowiem bankowi wydajne zarządzanie danymi, usługami i ryzykiem, a jednocześnie ułatwiła życie jego pracownikom.

Platforma ServiceNow obecnie stanowi podstawę działalności Danske Bank, a także bazę dla wszystkich przyszłych wdrożeń, integracji i innowacji. Bank ma w planach dalszą integrację systemu z działem HR, a także analizuje możliwość wdrożenia kolejnych aplikacji z portfolio ServiceNow.

SZTUCZNA INTELIGENCJA JAKO WSPARCIE W PROCESIE ZARZĄDZANIA INCYDENTAMI BEZPIECZEŃSTWA

Bezpieczeństwo organizacji

Każda firma musi zadbać o bezpieczeństwo swoich danych i systemów informatycznych. Współpracujący z nią klient liczy na poufność przekazanych danych wrażliwych, kontraktów i innych informacji, których ujawnienie mogłoby przynieść szkodę. Wyciek takich danych może być katastrofalny w skutkach. Samo GDPR nakłada karę w wysokości 20 mln euro lub 4% rocznego przychodu – w zależności od tego, która kwota jest większa – za każdy udowodniony wyciek danych.



Fot. Blue Planet Studio/stock.adobe.com

Fot. Sii Polska

Dawid Jankowski
OD PODSTAW ZBUDOWAŁ I PROWADZI CENTRUM KOMPETENCYJNE CYBERSECURITY W SII. POSIADA 16-LETNIE DOŚWIADCZENIE W TWORZENIU I ZABEZPIECZANIU SYSTEMÓW IT.

Dochodzi również do utraty wizerunku, przerwania produkcji i potencjalnego bankructwa. Od czasu wybuchu pandemii COVID-19, kiedy większość biznesu przestawiła się na zdalny tryb pracy, częstotliwość cyberataków znacznie się zwiększyła. Wzrost ten szacowany jest na 600%, a roczne straty w gospodarce z tytułu cyberataków mogą wynosić już 6 bilionów USD. Co więcej, trend nieustannie wykazuje wzrost. Szacuje się, że do roku 2025 liczby te ulegną podwojeniu. Same ataki typu ransomware (szyfrowanie komputera i wymuszanie okupu w celu odzyskania danych) są obecnie kilkadziesiąt razy bardziej szkodliwe niż w 2015 roku.

Dodatkowym elementem, który w ostatnich latach pojawił się na szachownicy cyberbezpieczeństwa jest sztuczna inteligencja. Jest ona coraz częściej wykorzystywana zarówno przez cyberprzestępców, jak i zespoły chroniące organizacje.

Na łamach tego artykułu skupimy się na wykorzystaniu sztucznej inteligencji do wykrywania i obsługi incydentów bezpieczeństwa.

Wykorzystanie sztucznej inteligencji i automatyzacji w zakresie bezpieczeństwa wzrosło o prawie jedną piątą w ciągu dwóch lat, z 59% w 2020 roku do 70% w 2022 roku.

Źródła: https://www.ibm.com/reports/data-breach

Security Operations Center

Detekcją i obsługą incydentów bezpieczeństwa zajmują się dedykowane jednostki w organizacji, czyli CSIRT (*Computer Security Incident Response Team*) lub SOC (*Security Operations Center*).

Organizacja może posiadać wewnętrzny zespół SOC lub skorzystać ze wsparcia strony trzeciej, korzystając z usługi *SOC-as-a-Service* (SOCaaS). Taka usługa zewnętrzna ma sens, gdy firma ma duże potrzeby w zakresie bezpieczeństwa, a jednocześnie ma ograniczony budżet na ten cel. Wówczas SOCaaS realizowany przez zewnętrznego dostawcę umożliwia dostęp do wiedzy eksperckiej i narzędzi branżowych bez konieczności ich zakupu na wyłączność, co pozwala uniknąć dużych nakładów finansowych. Dodatkowo, parametry takiej usługi mogą być na bieżąco dostosowywane, zapewniając pożądaną elastyczność.

SOC-as-a-Service to swego rodzaju naturalna ewolucja cyberbezpieczeństwa firmy. Świat zmierza wielkimi krokami w kierunku rozwiązań chmurowych, a SOCaaS jest odpowiedzią na rosnące zagrożenia związane z atakami na małe i średnie firmy posiadające dane właśnie w chmurze.

Można wskazać cztery główne korzyści rozwiązań SOCaaS:

1. **Znacznie zmniejszone ryzyko ataku**. Za naszymi plecami stoją eksperci w zakresie cyberbezpieczeństwa, którzy każdą sprawę rozpatrują indywidualnie i stale monitorują systemy bezpieczeństwa. Ryzyko wycieku danych lub przerwania produkcji jest zatem istotnie zredukowane.
2. **Szybsza detekcja i działania zapobiegawcze**. Podczas ataku czas odgrywa kluczową rolę – kiedy maszyna zostanie zainfekowana, trzeba ją natychmiast odizolować od reszty, natomiast gdy konto użytkownika zostanie przechwycone, należy natychmiast zresetować hasło. Nasze zespoły SOC mają sprawdzone, predefiniowane automatyzacje, które pozwalają szybko i dokładnie reagować na cyberzagrożenia. Przywracanie może być na tyle sprawne, że użytkownicy końcowi w ogóle nie zauważą przerwy w dostępności lub wydajności usług.
3. **Skalowalność**. Kiedy organizacja się rozwija, SOCaaS rośnie razem z nią. Dla dostawcy SOCaaS, takiego jak Sii, podwojenie SOC nie stanowi problemu, ponieważ dysponujemy ogromną liczbą ekspertów gotowych do pracy w trybie 24/7.
4. **Niższe koszty**. SOCaaS eliminuje konieczność utrzymywania własnej jednostki, w tym: personelu, szkoleń pracowników, biura, sprzętu czy licencji. Szacuje się, że przy optymalnej kalibracji, SOCaaS może kosztować nawet 90% mniej niż tradycyjna wewnętrzna jednostka SOC.

Skuteczna detekcja i obsługa incydentów bezpieczeństwa są obszarami, dla których rozwiązania bazujące na sztucznej inteligencji stały się naturalne.

Wykorzystanie sztucznej inteligencji w procesie Zarządzania Incydentami Bezpieczeństwa

Dla organizacji kluczowe jest szybkie wykrycie i przerwanie trwającego ataku. Im wcześniej zagrożenie zostanie wykryte (MTTD – *Mean Time to Detect*) i rozwiązane (MTTR – *Mean Time to Respond*), tym mniejszy wpływ na organizację i potencjalne koszty. Wdrożenie sztucznej inteligencji w połączeniu z automatyzacją znacząco wpływa na powyższe parametry.

Naruszenia bezpieczeństwa w organizacjach z w pełni wdrożoną sztuczną inteligencją i automatyzacją w obszarze bezpieczeństwa kosztują o 3,05 mln USD mniej niż naruszenia w organizacjach bez takich rozwiązań. Ta 65,2-procentowa różnica w średnim koszcie naruszenia – od 3,15 mln USD przy pełnym wdrożeniu do 6,2 mln USD przy braku wdrożenia – stanowiły największe oszczędności kosztów w badaniu.
Firmy te miały również średnio o 74 dni krótszy czas na zidentyfikowanie i powstrzymanie naruszenia, znany jako cykl życia naruszenia, niż firmy bez takich rozwiązań — 249 dni w porównaniu z 323 dniami.

Źródła: https://www.ibm.com/reports/data-breach

Detekcja incydentów

Aby skutecznie zablokować atak na organizację, musimy najpierw taki atak lub próbę ataku wykryć. Klasycznym rozwiązaniem jest wdrożenie różnych rozwiązań do wykrywania poszczególnych zagrożeń, takich jak antywirus, firewall itp. Same takie narzędzia nie są jednak wystarczające.

Do skutecznej obrony przed atakami potrzebne jest dokładne zrozumienie, jak wygląda atak. Rzadko jest to pojedyncze zdarzenie – najczęściej składa się z serii powiązanych ze sobą działań, któ- →

Cyber Kill Chain

Sekwencyjny łańcuch zdarzeń prowadzących do uzyskania oczekiwanego rezultatu

Źródło: Lockheed Martin Computer Incident Response Team

re mają umożliwić atakującemu osiągnięcie celu. Bardzo dobrze opisuje to model *Cyber Kill Chain*.

Podstawowym sposobem wykrywania tak złożonych ataków jest zbieranie logów i korelowanie ich pod kątem znanych typów (sygnatur) ataków. Obecnie najpopularniejszym sposobem jest tworzenie reguł korelacyjnych na podstawie matrycy MITRE ATT&CK. Jest to publicznie dostępna baza wiedzy o taktykach i technikach powszechnie stosowanych przez atakujących, tworzona i utrzymywana dzięki obserwacjom w świecie rzeczywistym.

Jak skutecznie wdrożenie rozwiązań opartych na chmurze i wspieranych przez AI zmniejsza problemy obecne w klasycznym rozwiązaniu?

Problem 1: Obsługa ataków o nieznanej sygnaturze

Jeśli polegasz tylko na znanych sygnaturach i prostych wzorcach zachowań, istnieje duże ryzyko, że niestandardowy atak, lub atak typu *zero-day*, nie zostanie zauważony.

Rozwiązanie

Uczenie maszynowe (*Machine Learning*, ML) najlepiej nadaje się do rozwiązywania złożonych problemów poprzez obserwację przychodzących danych i identyfikację trendów, które nie są od razu oczywiste. Korzystanie z rozwiązań chmurowych, takich jak Microsoft Sentinel, wspiera również efekt skali. Skanowanie milionów incydentów i zdarzeń, oznaczanie ich oraz rozpoznanie wzorców we wszystkich z nich jest praktycznie niemożliwe do osiągnięcia ręcznie. W uproszczeniu: AI uczy się na podstawie tysięcy ataków przeprowadzanych na różne organizacje.

Problem 2: Obsługa ataków skierowanych na użytkownika

Klasyczne rozwiązanie tylko w ograniczonym zakresie jest w stanie rozpoznać ataki skierowane na użytkownika.

Rozwiązanie

Wykorzystanie algorytmów ML pomaga nam ustalać standardowe zachowania poszczególnych użytkowników i wykrywać anomalie. Chociaż stosunkowo łatwo jest ukraść czyjąś nazwę użytkownika i hasło, chociażby używając socjotechniki, to podszy-

wanie się pod tę osobę poprzez naśladowanie jej zachowania jest znacznie trudniejsze. Kiedy więc ta osoba loguje się do systemu, a jej zachowanie odbiega od tego, co jest uważane za normalne, system wykrywa anomalie i alarmuje zespół SOC.

Problem 3: Zmęczenie alarmami

Tradycyjne rozwiązania mogą prowadzić do generowania dużej liczby fałszywych alarmów. Można oczywiście wyłączyć poszczególne reguły, ale wtedy istnieje ryzyko przeoczenia rzeczywistych ataków. Duża liczba nieistotnych lub fałszywych alarmów prowadzi do zmęczenia analityków, które jest najczęstszą przyczyną błędów w obsłudze incydentów i lekceważenia rzeczywistych zagrożeń.

Rozwiązanie

Platforma SIEM z wbudowanymi modelami uczenia maszynowego umożliwia dokładne wykrywanie i wstępną weryfikację prawdziwych zagrożeń wśród milionów generowanych zdarzeń. Poniżej przedstawiono liczbowy przykład analizy incydentów z wykorzystaniem Microsoft Sentinel.

Problem 4: Wykrywanie zagrożeń typu *low-volume* i *low-fidelity*

Ataki te charakteryzują się niską aktywnością atakującego. Mała ilość przesyłanych danych oraz aktywność występująca w dużych →

Redukcja zmęczenia alarmami

Analiza działań w usługach w chmurze w celu stworzenia przypadków bezpieczeństwa typu high-fidelity

Źródło: Microsoft Sentinel

odstępach czasu powoduje, że sygnał może zostać uznany przez analityków za fałszywy.

Rozwiązanie

Zagrożenia *low-fidelity* są szczególnie trudne do zidentyfikowania, zwłaszcza gdy występują sporadycznie. Silnik ML połączony z AI nie tylko na bieżąco analizuje nowe zdarzenia, ale także historyczne logi, szukając nietypowych trendów lub możliwości poprawy. Widok danych historycznych pozwala skorelować dane odległe w czasie, dając analitykowi pełniejszy obraz analizowanego incydentu.

> ***Organizacja może posiadać wewnętrzny zespół SOC lub skorzystać ze wsparcia strony trzeciej, korzystając z usługi SOC-as-a-Service (SOCaaS). Taka usługa zewnętrzna ma sens, gdy firma ma duże potrzeby w zakresie bezpieczeństwa, a jednocześnie ma ograniczony budżet na ten cel. Wówczas SOCaaS realizowany przez zewnętrznego dostawcę umożliwia dostęp do wiedzy eksperckiej i narzędzi branżowych bez konieczności ich zakupu na wyłączność.***

Obsługa incydentów bezpieczeństwa

Kolejnym kluczowym elementem procesu jest odpowiedź na incydenty bezpieczeństwa, z którą wiąże się zdecydowana większość zadań wykonywanych przez analityków SOC. Pierwszą myślą, jaka pojawia się, kiedy myślimy o AI w kontekście odpowiedzi na incydent jest kompletna automatyzacja procesu. Oczami wyobraźni widzimy system, w którym analitycy SOC nie są już potrzebni. Rzeczywistość wygląda trochę inaczej – wprawdzie AI jest wykorzystywana do automatycznej obsługi bardziej typowych zadań, ale jej głównym zadaniem jest wsparcie analityka SOC w podejmowaniu decyzji. Mówimy wtedy o inteligencji rozszerzonej (*Intelligence Amplification*, IA). Jej definicja skupia się wokół partnerstwa między ludźmi a AI. Jest to forma uczenia maszynowego, która ma na celu usprawnienie ludzkiego procesu decyzyjnego i związanych z nim działań.

Poniżej przedstawiono przykładowe aktywności wspierane przez sztuczną inteligencję w obszarze cyberbezpieczeństwa.

▸ Podpowiadanie danych

Reagując na incydent, analityk SOC korzysta z logów z różnych systemów. Jest to bardzo czasochłonny proces. AI już podczas tworzenia incydentu przeszukuje i pobiera niezbędne dane.

▸ Identyfikacja ryzyka i priorytetyzacja incydentów

Jednym z pierwszych zadań analityka jest tzw. *triage*. Analityk określa ryzyko, weryfikuje dotknięte systemy oraz określa rodzaj zagrożenia. Algorytmy ML bazujące na dostępnych danych i poprzednich incydentach umożliwiają automatyzację tego kroku. W praktyce pozwala to analitykom skupić się na incydentach priorytetowych, bez konieczności przeprowadzania pełnego, czasochłonnego *triage'u*.

▸ Automatyzacja działań powstrzymujących

Celem działań powstrzymujących (*containment*) jest ograniczenie szkód spowodowanych przez aktualny incydent bezpieczeństwa i zapobieganie dalszym szkodom. Jest to jedna z pierwszych czynności, które wykonuje analityk SOC. Dla przykładu: incydent został spowodowany wykryciem podejrzanych logowań z konta jednego użytkownika. Działaniem powstrzymującym byłoby zablokowanie konta danego użytkownika. Z drugiej strony istnieje ryzyko, że incydent zostanie podjęty zbyt późno, aby mógł zostać rozwiązany przez analityka. W tym miejscu na ratunek przychodzi AI. Po stwierdzeniu wysokiego prawdopodobieństwa włamania, blokada konta zostanie wykonana automatycznie. Analityk będzie mógł natychmiast przejść do kolejnych kroków w obsłudze incydentu.

▸ Rekomendacje

Algorytmy uczenia maszynowego mogą tworzyć podpowiedzi dotyczące wymaganych czynności w obsłudze określonych typów incydentów. Jest to szczególnie przydatna funkcja umożliwiająca skrócenie czasu reakcji i poprawę jej jakości – proponowane są kroki zoptymalizowane na podstawie wcześniejszych reakcji na podobne incydenty. Rekomendacje są szczególnie przydatne w przypadku incydentów, które występują bardzo rzadko, ponieważ w takich przypadkach analitycy mogą nie pamiętać, jak skutecznie rozwiązać incydent.

Opisane powyżej cechy i zalety *SOC-as-a-Service*, a także sposoby, w jakie sztuczna inteligencja usprawnia i automatyzuje pracę analityków bezpieczeństwa, pozwalają stwierdzić, że ten sposób monitorowania i obsługi incydentów bezpieczeństwa jest optymalnym rozwiązaniem dla wszystkich instytucji, dla których obszar bezpieczeństwa jest istotny, ale nie stanowi głównego obszaru działalności. Wówczas korzyści z outsourcingu tych zadań znacznie przewyższają koszty.

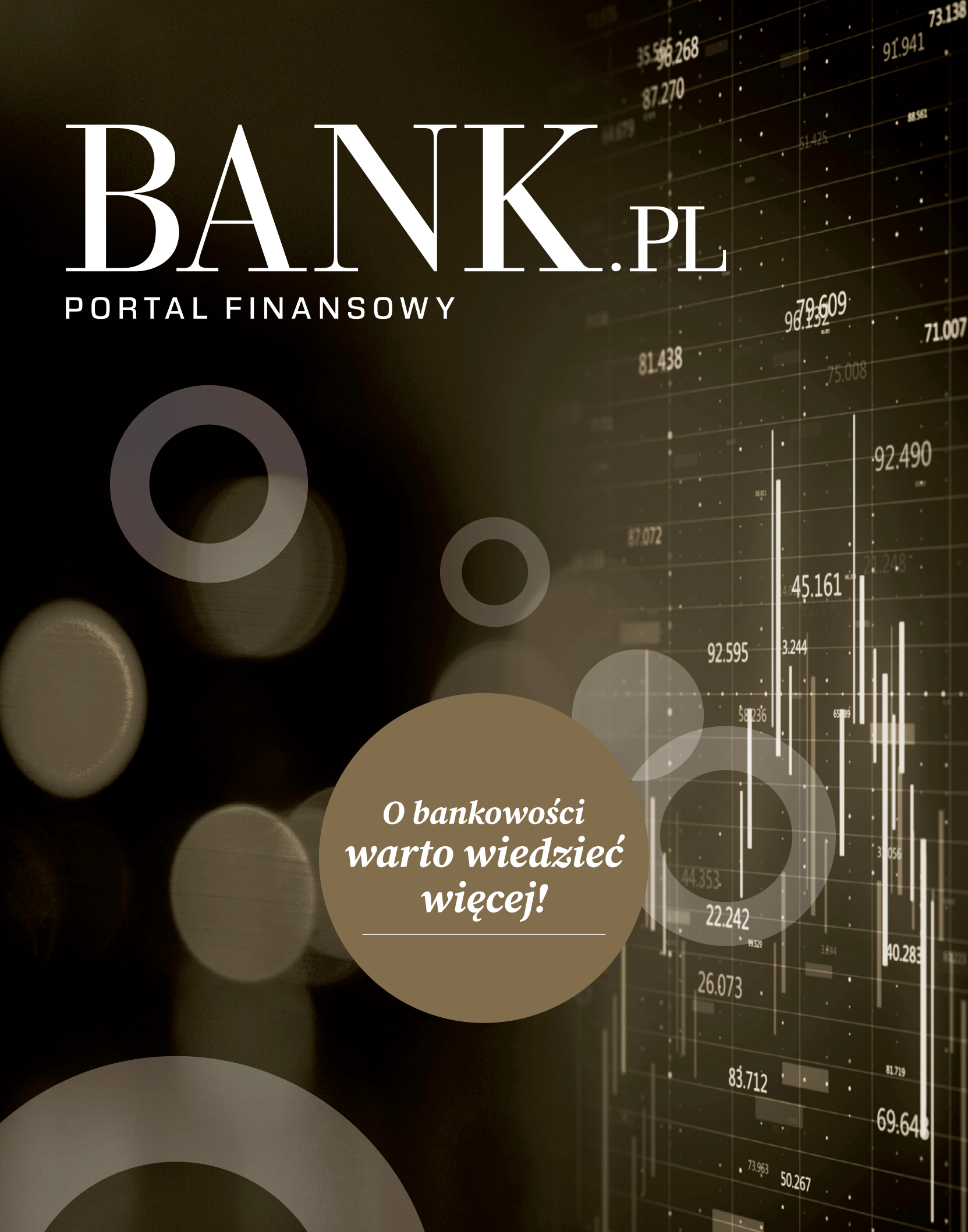
Sii Polska specjalizuje się w świadczeniu usług *SOC-as-a-Service*. Posiadamy duży zespół certyfikowanych specjalistów oraz doświadczenie w świadczeniu tego typu usług dla dużych instytucji finansowych w Polsce i na świecie. •

„Miesięcznik Finansowy BANK”
profesjonalny magazyn środowiska bankowego, istniejący już od 30 lat

Dziękujemy, że jesteście z nami!

BANK.PL

PORTAL FINANSOWY



O bankowości
warto wiedzieć
więcej!