CTRL + SAFE

TEMAT WYDANIA:

**ZERO TRUST & IDENTITY:
NOWY FUNDAMENT BEZPIECZEŃSTWA**

- DANE
- WIEDZA
- BEZPIECZEŃSTWO

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

W tym wydaniu:

Aleksandra Polit

Zero trust 2.0 - kontekst, dane, behawioryzm

Jak dynamiczna weryfikacja użytkownika zmienia systemy bezpieczeństwa

Jeszcze kilka lat temu bezpieczeństwo cyfrowe przypominało ochronę biurowca. Wystarczyło przejść przez główne wejście, pokazać identyfikator i można było poruszać się po organizacji niemal bez ograniczeń. Dziś ten model przestaje istnieć. Firmowe zasoby znajdują się w chmurze, pracownicy logują się z domów, hoteli i telefonów, a granice sieci praktycznie zniknęły. W takim środowisku pojedyncze logowanie przestało być wystarczającym dowodem zaufania. Właśnie dlatego organizacje coraz częściej przechodzą od klasycznego Zero Trust do modelu określanego jako **Zero Trust 2.0**, który nie opiera się już na jednorazowej autoryzacji. Opiera się na ciągłej ocenie ryzyka, kontekstu i zachowania użytkownika.

Zaufanie przestaje być stałe

Klasyczny model bezpieczeństwa opierał się na prostym założeniu: jeśli użytkownik poprawnie podał hasło i przeszedł uwierzytelnienie, system uznawał go za wiarygodnego. Problem pojawia się wtedy, gdy konto zostaje przejęte. Cyberprzestępcy coraz rzadziej próbują włamywać się do infrastruktury siłowo. Znacznie częściej wykorzystują skradzione dane logowania, przejęte sesje albo zmęczenie użytkowników powiadomieniami MFA (tzw. MFA fatigue). Ataki typu session hijacking oraz Adversary-in-the-Middle (AiTM) potrafią przejmować nawet poprawnie uwierzytelnione sesje MFA. Bez łamania hasła. Bez wzbudzania podejrzeń. Dlatego Zero Trust 2.0 nie kończy analizy na etapie logowania. System ocenia użytkownika również po uzyskaniu dostępu. Nowoczesne środowiska bezpieczeństwa wychodzą z innego założenia: użytkownik może być wiarygodny o 9:00 rano, a podejrzany piętnaście minut później. Zmiana lokalizacji, nietypowe urządzenie, niecodzienny sposób pracy albo próba wykonania niestandardowej operacji mogą całkowicie zmienić ocenę ryzyka. **Dostęp przestaje być jednorazową decyzją. Staje się procesem.** System nie pyta już wyłącznie: „Kim jesteś?”, ale również: „Czy nadal zachowujesz się zgodnie z profilem, któremu można ufać?”

Kontekst staje się nową walutą bezpieczeństwa

W modelu Zero Trust 2.0 znaczenie ma cały kontekst działania użytkownika: urządzenie, lokalizacja, pora aktywności, używane aplikacje, wzorce pracy, sposób poruszania się między systemami. Kluczowa staje się zgodność tych sygnałów z dotychczasowym profilem aktywności. Nawet subtelne odchylenia mogą uruchomić dodatkową weryfikację albo ograniczyć dostęp jeszcze przed wystąpieniem incydentu.

Bezpieczeństwo zaczyna działać adaptacyjnie, a nie schematycznie

Polityki dostępu przestają być wyłącznie sztywnym zestawem reguł zapisanych w systemie. Coraz bardziej przypominają dynamiczny model oceny sytuacji, który zmienia się wraz z poziomem ryzyka. Zero Trust 2.0 odchodzi również od klasycznego pojęcia „sesji". Dostęp nie jest już czymś przyznanym na określony czas. Jest stale negocjowany między użytkownikiem a systemem.

Dane stają się nowym fundamentem ochrony

Ten model nie działa bez danych. Bez dużej ilości danych. Współczesne systemy bezpieczeństwa analizują: logowania, aktywność aplikacyjną, telemetrię urządzeń, ruch sieciowy, historię sesji, wzorce korzystania z zasobów, poziom ryzyka urządzenia, historię uprawnień i incydentów.

Problemem współczesnych organizacji przestaje być brak danych. Problemem staje się brak kontekstu. Systemy generują tysiące alertów, ale bez korelacji pozostają jedynie szumem sygnałów. Organizacje widzą pojedyncze zdarzenia, ale często nie widzą historii, którą te zdarzenia próbują opowiedzieć. Dopiero połączenie tych informacji pozwala budować rzeczywisty obraz użytkownika i jego aktywności.

Sam poprawny login i hasło nie oznaczają już bezpieczeństwa. Znacznie ważniejsze staje się to, czy wszystkie sygnały tworzą logiczną i przewidywalną całość. W wielu organizacjach problemem nie jest już brak narzędzi bezpieczeństwa, lecz nadmiar rozproszonych danych i brak wspólnego kontekstu między systemami. Jeśli IAM, EDR, SIEM i system zarządzania urządzeniami nie „rozmawiają" ze sobą, organizacja widzi jedynie fragmenty incydentu zamiast pełnego obrazu ryzyka. Nowoczesne bezpieczeństwo zaczyna przypominać analizę zależności, a nie analizę pojedynczych alertów. To właśnie dlatego rośnie znaczenie platform łączących analizę tożsamości, telemetrię urządzeń oraz silniki oceny ryzyka w czasie rzeczywistym.

Behawioryzm wchodzi do cyberbezpieczeństwa

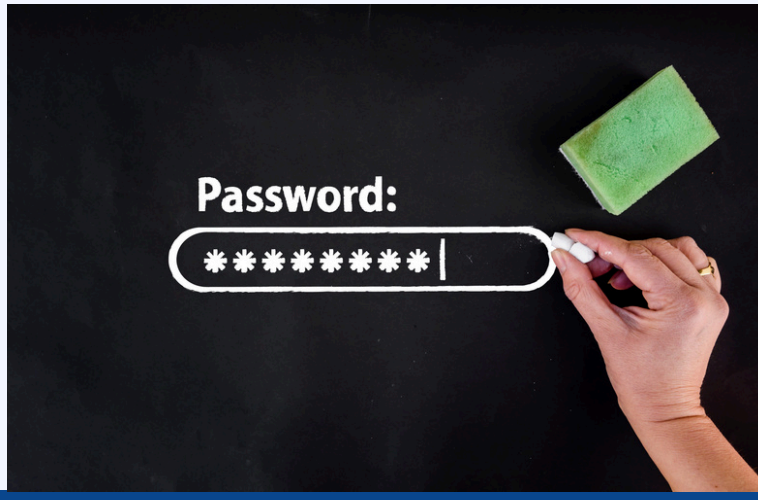
Jednym z najciekawszych kierunków rozwoju Zero Trust jest analiza behawioralna użytkownika – (UEBA – User and Entity Behavior Analytics). Systemy bezpieczeństwa uczą się, jak użytkownik korzysta z aplikacji, jak porusza się po środowisku, jakie działania wykonuje najczęściej i jak wygląda jego typowy rytm pracy. Zmiana wzorca może być równie ważnym sygnałem jak błędne hasło. Nietypowa sekwencja działań, nagła próba uzyskania dostępu do wrażliwych danych czy aktywność odbiegająca od codziennych schematów mogą wskazywać na przejęcie konta znacznie wcześniej, niż zauważy to człowiek. Analiza behawioralna ma jeszcze jedną przewagę: jest znacznie trudniejsza do podrobienia niż samo hasło lub kod MFA. Atakujący może przejąć dane logowania. Znacznie trudniej odtworzyć sposób pracy konkretnego użytkownika, jego rytm działania czy charakterystyczne wzorce aktywności. Nowoczesne systemy bezpieczeństwa nie analizują już wyłącznie tego, czy użytkownik zna hasło. Analizują również, czy zachowuje się tak, jak osoba, za którą się podaje. Takie podejście zaczyna przypomina system odpornościowy organizacji. Nie skupia się wyłącznie na znanych zagrożeniach. Obserwuje środowisko i reaguje wtedy, gdy zachowanie zaczyna odbiegać od normy.

Systemy zaczynają podejmować decyzje dynamicznie

Współczesne platformy bezpieczeństwa nie ograniczają się już do prostego „pozwól” albo „zablokuj”. Coraz częściej podejmują decyzje warunkowe. Pracownik loguje się z firmowego laptopa w standardowych godzinach pracy. Dostęp przebiega płynnie i praktycznie niewidocznie. Kilka godzin później to samo konto próbuje pobrać dużą ilość danych z nowego urządzenia w innej lokalizacji. System reaguje automatycznie. Może uruchomić dodatkową autoryzację, ograniczyć zakres dostępu, czasowo zatrzymać sesję lub podnieść poziom monitoringu. Tak działa adaptacyjne bezpieczeństwo. Ryzyko nie jest oceniane raz. Jest przeliczane cały czas. System stale obserwuje użytkownika i reaguje proporcjonalnie do poziomu zagrożenia. Dużą rolę odgrywa tutaj step-up authentication, czyli dodatkowa weryfikacja uruchamiana wyłącznie wtedy, gdy poziom ryzyka zaczyna rosnąć. Dzięki temu bezpieczeństwo staje się bardziej inteligentne i mniej uciążliwe dla użytkownika. Rośnie również poziom automatyzacji. Coraz więcej decyzji bezpieczeństwa podejmowanych jest bez udziału człowieka, w czasie rzeczywistym, na podstawie analizy tysięcy sygnałów jednocześnie.

Hasło przestaje być centrum bezpieczeństwa

Zero Trust 2.0 zmienia również podejście do samej tożsamości. Rosnące znaczenie zyskują: MFA odporne na phishing, passkeys, biometria, analiza urządzenia, ocena ryzyka sesji. W efekcie pojedyncze hasło przestaje być głównym filarem ochrony. System ocenia użytkownika szerzej: analizuje jego zachowanie, środowisko pracy, zgodność z profilem ryzyka, stan urządzenia oraz kontekst logowania. Dla organizacji oznacza to większą odporność na phishing, przejęcia kont i nadużycia uprawnień. Dla użytkowników – mniej sztywnych procedur i bardziej płynny dostęp do zasobów. Bezpieczeństwo coraz częściej działa w tle. Użytkownik zauważa je dopiero wtedy, gdy poziom ryzyka zaczyna rosnąć.



AI zaczyna oceniać zaufanie w czasie rzeczywistym

Coraz większą rolę w architekturach Zero Trust odgrywają modele AI analizujące ryzyko sesji i zachowanie użytkownika w czasie rzeczywistym. Systemy uczą się wzorców aktywności organizacji, przewidują anomalie i automatycznie dostosowują poziom dostępu. Bezpieczeństwo przestaje przypominać statyczny zbiór reguł. Zaczyna działać jak autonomiczny system nerwowy organizacji.

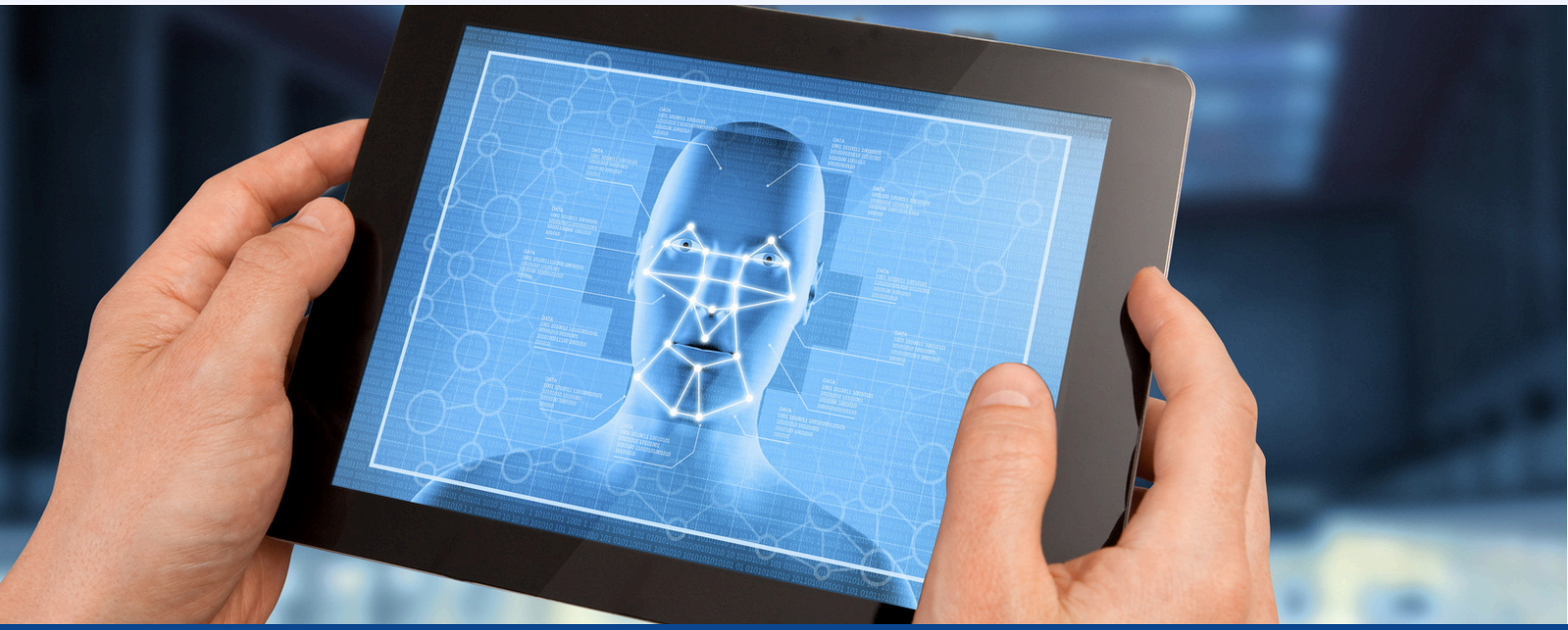
Ryzyka, ograniczenia i nowe pytania

Choć Zero Trust 2.0 znacząco zwiększa odporność organizacji, nie jest modelem pozbawionym wyzwań. Źle skalibrowane systemy mogą generować nadmierną liczbę alertów i fałszywych alarmów, utrudniając codzienną pracę użytkowników. Im bardziej system analizuje zachowanie użytkownika, tym mocniej rosną pytania o: prywatności, transparentności, granicy monitorowania pracowników i nadzoru nad automatyzacją. Organizacje wdrażające Zero Trust 2.0 coraz częściej muszą balansować między bezpieczeństwem a ryzykiem stworzenia środowiska przypominającego permanentny nadzór cyfrowy. W skrajnych przypadkach może to prowadzić do efektu „cyfrowego panoptykonu", w którym pracownik jest stale obserwowany, a granica prywatności zaczyna się rozmywać. Dlatego rośnie znaczenie:

- audytów modeli ryzyka,
- explainable AI (XAI),
- nadzoru człowieka nad automatyzacją,
- zgodności z regulacjami dotyczącymi danych i prywatności.

Przyszłość bezpieczeństwa będzie kontekstowa

Zero Trust 2.0 bardzo wyraźnie pokazuje kierunek rozwoju cyberbezpieczeństwa. Systemy odchodzą od statycznych zasad i coraz mocniej opierają się na analizie: zachowania, kontekstu, ryzyka i relacji między sygnałami. Organizacja nie chroni już wyłącznie infrastruktury. Chroni przede wszystkim ciągłość zaufania. W świecie pracy hybrydowej, rozproszonych środowisk i rosnącej liczby ataków na tożsamość, bezpieczeństwo musi być dynamiczne. Organizacje, które nauczą się łączyć dane, analizę behawioralną i ciągłą weryfikację użytkownika, zyskają przewagę nie tylko technologiczną, ale przede wszystkim operacyjną. Bo w świecie, w którym hasło można ukraść, token przejąć, a tożsamość podrobić, **najważniejszą zdolnością systemu staje się umiejętność ciągłego zadawania jednego pytania: „Czy nadal mogę Ci ufać?"**



Aleksandra Polit

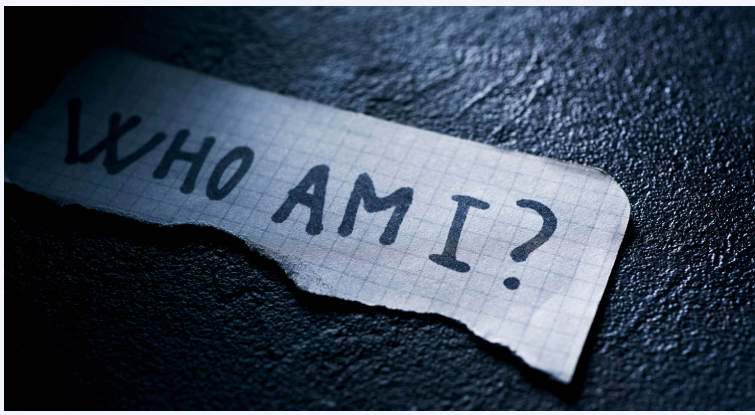
Tożsamość: największe aktywo i największe ryzyko

Nowa ekonomia dostępu

Jeszcze dekadę temu najcenniejszym zasobem organizacji były dane. Dziś większą wartość ma sam dostęp do nich. Współczesne cyberataki coraz rzadziej polegają na brutalnym łamaniu zabezpieczeń. Znacznie skuteczniejsze okazuje się wykorzystanie legalnych tożsamości, poprawnych sesji i prawidłowych uprawnień. Haker nie musi już włamywać się do organizacji. Wystarczy, że zaloguje się jak pracownik. To właśnie dlatego tożsamość staje się nowym centrum bezpieczeństwa. Nie jako login czy konto w usłudze katalogowej, ale jako cyfrowa reprezentacja zaufania, dostępu i możliwości działania w systemie.

Tożsamość przestała być statyczna

Jeszcze niedawno konto użytkownika było czymś prostym. Administrator zakładał login, nadawał hasło i przypisywał rolę. Dziś taka definicja przestała wystarczać. Tożsamość nie jest już zestawem danych przypisanych do użytkownika. Stała się strukturą opisującą możliwości działania w środowisku cyfrowym. Obejmuje nie tylko uprawnienia, ale też sposób ich wykorzystywania i relację z technologią. Nie chodzi już tylko o to, co użytkownik „ma". Chodzi o to, co realnie może zrobić. Nowoczesna tożsamość obejmuje: uprawnienia, historię dostępu, kontekst działania, urządzenie, sposób korzystania z systemów, relacje z innymi zasobami. Tożsamości nie da się już opisać jednym wpisem w katalogu użytkowników. Przestaje być czymś przechowywanym. Zaczyna być czymś obserwowanym. Nie istnieje jako statyczna informacja. Ujawnia się dopiero w interakcji z systemem. Można ją zrozumieć dopiero w działaniu.



Tożsamość staje się nową architekturą organizacji

Przez lata bezpieczeństwo budowano wokół infrastruktury: sieci, serwerów, segmentacji, ochrony perymetrycznej. Dziś ten model przestaje wystarczać. W nowoczesnym środowisku organizacja nie kontroluje już wyłącznie przestrzeni. Kontroluje przede wszystkim dostęp zapisany w tożsamości. System nie pyta: „czy jesteś w sieci?" Pyta: „do czego masz prawo i czy powinieneś korzystać z tego właśnie teraz?" Bezpieczeństwo zaczyna przypominać zarządzanie dostępem w czasie rzeczywistym. Tożsamość przestaje być elementem infrastruktury. Staje się warstwą sterującą całego środowiska.

Największe ryzyko wygląda dziś jak normalny użytkownik

Najgroźniejsze współczesne ataki rzadko zaczynają się od spektakularnego włamania. Znacznie częściej zaczynają się od:

- phishingu,
- przejęcia sesji,
- wycieku poświadczeń,
- zmęczenia użytkownika powiadomieniami MFA,
- nadmiarowych uprawnień.

Cyberprzestępcy wiedzą, że najskuteczniejsze wejście do systemu nie polega na jego łamaniu. Polega na wykorzystaniu istniejącego dostępu. Jeśli konto zostaje przejęte, system sam otwiera kolejne drzwi. Bo system nie widzi ataku. Widzi użytkownika. Dlatego najniebezpieczniejszy użytkownik w organizacji to często ten, który wygląda całkowicie normalnie.

Tożsamość zaczyna mieć własny „biorytm”

Jednym z najważniejszych kierunków rozwoju bezpieczeństwa jest analiza zachowania użytkownika. Systemy analizują nie tylko to, kim jest użytkownik, ale jak działa. Każdy ma swój charakterystyczny rytm: tempo pracy, kolejność działań, sposób poruszania się po systemie, schemat korzystania z danych, rytm aktywności. Tożsamość zaczyna mieć własny rytm. To właśnie ten rytm najtrudniej podrobić. Atakujący może przejąć hasło lub sesję. Znacznie trudniej odtworzyć sposób działania konkretnej osoby. Dlatego zachowanie staje się częścią tożsamości. Często bardziej wiarygodną niż samo uwierzytelnienie.

Tożsamości nieludzkie – cicha ekspansja ryzyka

Tożsamość coraz rzadziej oznacza wyłącznie człowieka. Obejmuje również: aplikacje, integracje, API, procesy automatyczne, konta usługowe, boty i systemy AI. W wielu organizacjach liczba takich tożsamości przekracza już liczbę pracowników. Każda z nich posiada dostęp. Każda reprezentuje określone uprawnienia. Każda może stać się punktem wejścia dla atakującego. To właśnie tutaj zaczyna pojawiać się nowa powierzchnia ryzyka.

Maszyny zaczynają mieć więcej dostępów niż ludzie

W wielu organizacjach największym problemem bezpieczeństwa przestają być konta pracowników. Znacznie większym wyzwaniem stają się tożsamości maszynowe: tokeny API, konta aplikacyjne, klucze dostępowe workloadów, sekrety wykorzystywane przez automatyzację i komunikację między systemami. Większość tych tożsamości działa „w tle”. Nie zmienia haseł. Nie przechodzi szkoleń bezpieczeństwa. Często posiada bardzo szerokie uprawnienia i działa przez lata bez kontroli. Organizacje zaczynają odkrywać, że liczba aktywnych tożsamości nieludzkich wielokrotnie przewyższa liczbę pracowników. To fundamentalnie zmienia sposób myślenia o bezpieczeństwie. Bezpieczeństwo tożsamości przestaje być problemem użytkowników. Staje się problemem całego ekosystemu cyfrowego.

Uprawnienia stały się nową walutą cyberprzestępców

Współczesny atak rzadko zaczyna się od exploita. Znacznie skuteczniejsze okazuje się przejęciem legalnego dostępu: aktywnej sesji VPN, tokenu API, konta uprzywilejowanego, zapomnianego klucza dostępowego. Przejęte uprawnienia bywają cenniejsze niż najbardziej

zaawansowane malware. Dlatego bezpieczeństwo przestaje koncentrować się wyłącznie na ochronie infrastruktury. Najważniejsze staje się pytanie: kto, do czego i na jak długo otrzymuje dostęp. Współczesny cyberatak coraz rzadziej polega na łamaniu zabezpieczeń. Coraz częściej polega na cierpliwym korzystaniu z legalnego dostępu.

Tożsamość staje się centrum organizacji

Identity-centric security przestaje być wyłącznie elementem cyberbezpieczeństwa. Zaczyna wpływać na całe funkcjonowanie organizacji. Tożsamość decyduje dziś o:

- dostępie do danych,
- szybkości onboardingu,
- doświadczeniu użytkownika,
- automatyzacji procesów,
- komunikacji między systemami,
- ciągłości operacyjnej.

Bezpieczeństwo, dostęp i operacje przestają być oddzielnymi obszarami. Tworzą jeden wspólny mechanizm decyzji. Tożsamość przestaje być komponentem systemu. Staje się jego control plane.

Kto kontroluje dostęp, kontroluje wszystko

Przyszłość cyberbezpieczeństwa nie będzie polegała na budowaniu coraz wyższych murów. Będzie polegała na rozumieniu:

- kto korzysta z dostępu,
- w jaki sposób go wykorzystuje,
- jakie posiada uprawnienia,
- czy nadal powinien je posiadać.

W świecie rozproszonych środowisk i automatycznych systemów kontrola dostępu staje się kontrolą zaufania. **A kto kontroluje dostęp – kontroluje całe środowisko.**

Mateusz Widziszewski

Phishing 3.0 – czyli o oszustwie przemawiającym ludzkim głosem

Czasy, gdy phishing polegał wyłącznie na wysłaniu do przypadkowej ofiary, niespójnej, chaotycznej wiadomości, odchodzą w zapomnienie. Fałszywe maile z banku czy instytucji publicznych nikogo już nie dziwią (a przynajmniej nie powinny) i w dużej mierze są łatwo identyfikowane, a tym samym nie pozwalają cyberprzestępcy na osiągnięcie zamierzonego celu. Ze względu na zmniejszoną skuteczność swoich działań, przestępcy coraz mocniej ewoluują w swoich atakach, skupiając się na targetowanych ofiarach, wykorzystując do tego coraz to bardziej zaawansowane metody phishingu, wspomagane AI.

Witamy w erze ataków, których celem nie jest już hasło, lecz tożsamość

Wraz ze zmieniającym się światem, naszym przywiązaniem i życiem w cyberprzestrzeni, a także rozwojem narzędzi wykorzystujących sztuczną inteligencję, ewoluują również formy zagrożeń na jakie jesteśmy narażeni w cyfrowym świecie. Działania w modelu Phishing 3.0 bazują na specjalnie tworzonych rozwiązaniach AI, które są w powszechnym użytku i umożliwiają prowadzenie spersonalizowanych, interaktywnych ataków.

Mogą one przybierać formę wiadomości tekstowych, rozmów głosowych, a coraz częściej także materiałów wideo. W świecie cyfrowym coraz mocniej rozpycha się deepfake, którego działanie zasilane i wspomagane jest sztuczną inteligencją, a także zawiera w sobie metody socjotechniczne, mające na celu manipulację naszymi emocjami tu i teraz. Dotychczas ataki phishingowe nie do końca potrafiły skorelować wszystkie wykorzystywane elementy ataków, obecnie przy wykorzystaniu pomocy AI, warstwa techniczna i psychologiczna zazębia się ze sobą, tworząc jednolite narzędzie w rękach cyberprzestępców. Najgroźniejszy phishing wygląda obecnie jak normalna rozmowa.

Praktyczna strona Phishingu 3.0

Jeśli wyobrażamy sobie cyberprzestępcę stereotypowo, jako osobę siedzącą w czeluściach budynku, w bluzie z kapturem (*nic nie mam osobiście do takiego ubioru, ba sam też noszę* 😊), to w pewnym sensie wciąż jest to prawda, ale tylko częściowo. Działania powodujące zagrożenia, na które jesteśmy narażeni, realizowane są obecnie przez zorganizowane grupy osób, działających na zasadzie organizacji nastawionych na zysk.

Struktury odpowiednio dobranych osób tworzą odpowiednie modele ataku, wykorzystując przy tym sztuczna inteligencję i dobierając właściwe metody socjotechniczne, a same ataki, aby były skuteczne i prowadziły do zamierzonego celu, poprzedzone są godzinami analiz, zbierania danych i profilowania ofiary. Grupy cyberprzestępców przygotowując się do ataku, skrupulatnie wybierają sobie cele, gromadząc przy tym dane i informacje, które nierzadko uzyskują od samych ofiar. Cyberprzestępcy manipulują pozyskanymi z ogólnodostępnych źródeł danymi, wizerunkami, głosem w celu przygotowania skutecznych ataków. Przygotowane ataki (tekstowe, głosowe, wideo) nakierowane są na określone wcześniej grup użytkowników i często pozbawione są *(naprawdę, wielkie dzięki AI!)* błędów, które wcześniej mogły powodować u użytkowników „red light".

Wytworzone odpowiednio materiały, wyglądają autentyczne, a w swoim przesłaniu bazują na ludzkich emocjach, powodując po stornie użytkownika zamierzone przez cyberprzestępców działanie. Atakujący nie musi już zdobywać zaufania. Potrafi je wygenerować. Wraz z ewolucją, sztuczna inteligencja stara się (nieświadomie – nie miejmy pretensji do AI), tworzyć najlepsze rozwiązania dla swoich właścicieli – cyberprzestępców. Działania te powodują, że Phishing 3.0 charakteryzuje się trudnością jego wykrycia.

Atak nie musi być techniczny, żeby był skuteczny. Wystarczy, że będzie przekonujący.

Czy jesteśmy gotowi na nowe „wyzwania"?

Jak zwykle odpowiedź nie jest jednoznaczna, a wiele zależy od nas samych. Phishing 3.0 opiera się na połączeniu socjotechniki i AI, a celuje w naturalne słabości nas wszystkich, my jako „najsłabsze ogniwo" w systemie bezpieczeństwa jesteśmy celem takich ataków. Paradoksalnie jednak, **każdy z nas może być najlepszym strażnikiem bezpieczeństwa.** Stosowane środki bezpieczeństwa pomimo zaawansowanych metod, nie zawsze odpowiadaj zagrożeniom. Ciężko jest przewidzieć następujące zmiany, metody i środki jakie będą chcieli wykorzystać cyberprzestępcy. Zatem zasadnym jest użycie stwierdzenia, że środki są zawsze krok za zagrożeniem. Jak to mówią, potrzeba jest matką wynalazków, zatem i w tym przypadku (niestety), wraz ze wzrostem świadomości użytkowników, co do standardowych ataków phishingowych, cyberprzestępcy wykorzystują coraz bardziej zaawansowane narzędzia i metody. Dlatego też, tak istotna jest rola samych użytkowników w procesie, nasza wiedza i umiejętność właściwego podejścia do stawianych nam wyzwań. Phishing 3.0 nie próbuje wyglądać wiarygodnie. On tworzy wiarygodność.

Bez końca, bez przerwy...

Phishing 3.0 to dla wielu spora ewolucja w świecie cyberataków, która bazując na zaawansowanych metodach socjotechnicznych i sztucznej inteligencji, ma za zadanie omijać dotychczas rozpoznawalne elementy sugerujące zagrożenie i wzbudzać w użytkownikach poczucie, że wszystko jest ok, aż do momentu, w którym pojawią się realne konsekwencje. Nie będzie lekko i trzeba się przyzwyczaić, że Phishing 3.0 będzie obecny z nami przez cały czas, czekając na okazję do działania. Nie odejdzie w zapomnienie, dopóki przynosi korzyści dla cyberprzestępców, a ewolucja zapewne będzie pchała świat cyfrowy w coraz to nowsze zagrożenia. Phishing 3.0 nie próbuje już oszukać systemów. Próbuje oszukać człowieka. Człowiek nadal pozostaje najcenniejszą tożsamością w cyfrowym świecie. **Hasło można zmienić. Numer telefonu można zablokować. Najtrudniej odzyskać utracone zaufanie.**

Czy wiesz, że cyberprzestępcy mogą stosować różnego rodzaju formy phishing?

- Spear Phishing,
- Smishing,
- Vishing,
- Whaling,
- Pharming,
- Quishing,
- Clone phishing,
- Angler phishing.

Phishing ma dziś wiele twarzy: od sprecyzowanych ataków, przez wiadomości SMS, po rozmowy głosowe, deepfake i inne. Pytanie nie brzmi, czy je znasz. **Pytanie brzmi, czy potrafisz je rozpoznać w odpowiednim momencie?**

AI Agents dostają własne paszporty

Agent AI, który zamawia usługi, analizuje dane, wysyła wiadomości i negocjuje z innymi systemami, nie może działać jako „konto techniczne nr 457". Coraz częściej mówi się o Agent Identity – cyfrowej tożsamości stworzonej specjalnie dla autonomicznych agentów. W praktyce oznacza to, że agent będzie miał własny profil, historię działań, uprawnienia, a nawet możliwość udowodnienia, kim jest. W najbliższych latach firmy będą zarządzać nie tylko pracownikami i klientami, ale również flotami cyfrowych współpracowników. Krótko mówiąc: onboarding dla AI właśnie wchodzi do korporacji.

Deepfake Helpdesk

Przez lata bezpieczeństwo skupiało się na ochronie logowania. Tymczasem coraz więcej ataków omija ten etap całkowicie. Atakujący dzwonią na helpdesk, używając głosu wygenerowanego przez AI, podszywają się pod pracowników podczas wideokonferencji albo wykorzystują wygenerowane dokumenty do resetowania dostępu. Efekt? Najbardziej ryzykownym momentem przestaje być logowanie. Staje się nim odzyskiwanie konta. Paradoks współczesnego IAM: łatwiej chronić login niż człowieka po drugiej stronie telefonu.

Zero Trust dla maszyn

Przez lata hasło Zero Trust oznaczało: „nie ufaj użytkownikowi". W 2026 roku coraz częściej oznacza: „nie ufaj również maszynie". Systemy zaczynają weryfikować nie tylko człowieka, ale także każde API, kontener, model AI czy automatyczny proces. Sam fakt, że coś działa wewnątrz organizacji, przestaje być wystarczającym dowodem zaufania. To moment, w którym serwer musi udowodnić swoją tożsamość równie często jak pracownik.

Machine Identity Explosion

Jeszcze kilka lat temu organizacje zarządzały głównie użytkownikami. Dziś największym wyzwaniem stają się maszyny. API, kontenery, workloady chmurowe, mikrousługi, agenci AI i automatyzacje generują miliony certyfikatów, tokenów i kluczy dostępowych. W wielu organizacjach liczba tożsamości nieludzkich jest już setki razy większa niż liczba pracowników. Problem polega na tym, że większość tych „użytkowników" nigdy nie bierze urlopu, nie zmienia hasła i często nikt nie pamięta, po co właściwie powstały. Identity sprawl staje się nowym shadow IT.

Passwords Are the New Fax Machine

Hasła coraz bardziej przypominają faks: wszyscy wiedzą, że istnieją, ale nikt nie chce już z nich korzystać. Passkeys, biometria i uwierzytelnianie oparte na urządzeniu eliminują konieczność pamiętania skomplikowanych ciągów znaków. Jednocześnie są znacznie bardziej odporne na phishing i przejmowanie sesji. Najciekawsze jest jednak to, że po raz pierwszy w historii bezpieczeństwo staje się jednocześnie wygodniejsze. Rzadko zdarza się technologia, którą użytkownicy lubią bardziej niż cyberprzestępcy.

ANALIZA RZECZYWISTOŚCI

MFA to tarcza nie do przebicia

Rzeczywistość: Przez lata branża bezpieczeństwa traktowała MFA jak superbohatera uwierzytelniania. Włącz drugi składnik i problem przejęcia kont znika. Niestety, cyberprzestępcy przeczytali tę samą instrukcję. Dziś coraz częściej nie próbują łamać MFA. Próbują sprawić, żeby użytkownik sam je zatwierdził. Fałszywe strony logowania, przejęcie sesji, MFA fatigue czy socjotechnika pozwalają ominąć dodatkową warstwę ochrony bez potrzeby jej „hakowania". MFA nadal pozostaje jednym z najskuteczniejszych zabezpieczeń kont. Problem w tym, że przestało być zabezpieczeniem wystarczającym. MFA znacząco podnosi bezpieczeństwo, ale nie gwarantuje bezpieczeństwa. Atakujący coraz rzadziej łamią MFA. Coraz częściej przekonują użytkownika, żeby zrobił to za nich.

Hasło jest dowodem tożsamości

Rzeczywistość: Hasło jest dowodem znajomości sekretu. To nie to samo. Jeżeli ktoś zna Twoje hasło, system nie wie, czy jesteś pracownikiem, cyberprzestępcą czy kotem spacerującym po klawiaturze. Dlatego nowoczesne systemy coraz częściej analizują również urządzenie, lokalizację, zachowanie i poziom ryzyka. Hasło odpowiada na pytanie: „Czy znasz sekret?" Tożsamość odpowiada na pytanie: „Czy naprawdę jesteś tym, za kogo się podajesz?"

Zero Trust oznacza brak zaufania do pracowników

Rzeczywistość: To najczęstsze nieporozumienie. Zero Trust nie zakłada, że pracownik jest podejrzany. Zakłada, że każde konto może zostać przejęte. Model nie pyta: „Czy ufamy Annie z finansów?". Pyta: „Czy mamy pewność, że to nadal Anna z finansów?". To subtelna różnica, która zmienia całe podejście do bezpieczeństwa.

ANALIZA RZECZYWISTOŚCI

Największym problemem są hakerzy z zewnątrz

Rzeczywistość: Coraz więcej incydentów zaczyna się od czegoś znacznie mniej spektakularnego: starego konta, niepotrzebnego dostępu albo zapomnianego tokena. Atakujący często nie szukają dziury. Szukają bałaganu. A bałagan bywa znacznie łatwiejszy do znalezienia niż podatność zero-day.

Zero Trust to technologia

Rzeczywistość: To bardziej sposób myślenia niż produkt. Nie można kupić "Zero Trust w pudełku". Można kupić narzędzia, które pomagają go wdrożyć. Zero Trust to decyzja o tym, że zaufanie nie jest przyznawane raz na zawsze, ale musi być stale potwierdzane. To nie kolejna ikonka w centrum danych. To filozofia bezpieczeństwa.

Boty nie są użytkownikami

Rzeczywistość: W wielu organizacjach największe uprawnienia posiadają nie ludzie, lecz systemy. Boty, integracje, API, workloady chmurowe i automatyzacje wykonują miliony operacji każdego dnia. Każda z tych rzeczy posiada własną tożsamość. Każda może zostać przejęta. I żadna nie zadzwoni na helpdesk, żeby zgłosić problem.

Biometria jest nie do podrobienia

Rzeczywistość: Przez lata twarz i głos były traktowane jak cyfrowy odcisk palca. Potem pojawiły się generatywne modele AI. Dziś można wygenerować głos prezesa, stworzyć realistyczny deepfake wideo i podszyć się pod konkretną osobę znacznie łatwiej niż jeszcze kilka lat temu. Najbardziej wiarygodne oszustwa przyszłości mogą wyglądać dokładnie tak jak prawda.

Możesz mieć więcej cyfrowych tożsamości niż pamiętasz?

To nie jest kolejny tekst o logowaniu. To tekst o czymś, o czym prawie nikt nie myśli. Przeciętny użytkownik pamięta kilka kont: służbowy e-mail, Teams, LinkedIn, Instagram, bank. Tymczasem przez lata tworzymy dziesiątki, a czasem setki, cyfrowych tożsamości:

- stare konta w serwisach,
- zapomniane aplikacje,
- platformy szkoleniowe,
- sklepy internetowe,
- systemy partnerów,
- środowiska testowe,
- konta po zakończonych projektach.

Wiele z nich nadal istnieje długo po tym, gdy przestajemy z nich korzystać.

Problem nie leży tam, gdzie go szukasz

Paradoks polega na tym, że cyberprzestępcy coraz rzadziej zaczynają od aktywnych kont. Znacznie częściej szukają tych, które zostały porzucone. Nieaktualny dostęp, stary login albo konto, którego nikt nie wyłączył po projekcie, mogą być dla atakującego cenniejsze niż najnowsza podatność. To właśnie tam najczęściej nie patrzy już nikt.

Najciekawsza ironia

W cyberbezpieczeństwie problemem coraz częściej nie jest to, kim jesteś. Problemem jest to, **iloma osobami byłeś w przeszłości i które z nich nadal istnieją.**

Wniosek dla managera

Jednym z najważniejszych pytań bezpieczeństwa nie jest dziś: „Kto ma dostęp?" Coraz częściej brzmi ono: **„Które dostępy nadal istnieją, choć nikt już o nich nie pamięta?"**

Paradoks przyszłości

W erze Zero Trust organizacje będą musiały zarządzać nie tylko aktywnymi tożsamościami. Coraz większym wyzwaniem staje się coś innego: **odnajdywanie dostępu, który powinien już dawno zniknąć.**

GŁOS SPOŁECZNOŚCI

Czy Zero Trust 2.0 oznacza, że już nigdy nie „logujemy się” naprawdę?

Odpowiedź: W pewnym sensie tak, ale nie w sposób znany z filmów science-fiction. W Zero Trust logowanie przestaje być momentem wejścia do systemu. Staje się jednym z wielu sygnałów analizowanych w czasie rzeczywistym. Tożsamość nie jest już bramką. Jest strumieniem danych: urządzenie, lokalizacja, zachowanie, historia aktywności. Możesz być zalogowany i jednocześnie częściowo niezaufany.

Czy w Zero Trust 2.0 to system decyduje, kim jestem?

Odpowiedź: Nie. Ale system coraz częściej decyduje, czy zachowujesz się jak Ty. Tożsamość przestaje być deklaracją („login i hasło”). Staje się modelem zachowań, który system nieustannie aktualizuje. Paradoks? Im bardziej cyfrowe środowisko, tym mniej „stała” jest tożsamość.

Czy w przyszłości tożsamość może zmienić się bez mojej wiedzy?

Odpowiedź: W praktyce już tak się dzieje. Każda zmiana urządzenia, sieci, sposobu pracy czy nawet tempa wykonywania zadań wpływa na profil ryzyka. System nie czeka, aż użytkownik coś „zadeklaruje”. On obserwuje i aktualizuje obraz tożsamości na bieżąco. W Zero Trust 2.0 tożsamość nie jest edytowana ręcznie. Ona ewoluuje.

Czy największym problemem nadal jest przejęcie hasła?

Odpowiedź: Coraz rzadziej. Znacznie większym wyzwaniem staje się przejęcie kontekstu: sesji, tokenu, zachowania użytkownika. W takim świecie hasło jest tylko jednym z wielu elementów układanki, często najmniej istotnym.

GŁOS SPOŁECZNOŚCI

Czy można jeszcze mówić o „jednej tożsamości” użytkownika?

Odpowiedź: W nowoczesnych organizacjach jedna osoba ma wiele równoległych tożsamości: w systemach, aplikacjach, chmurze, narzędziach AI, automatyzacjach. Do tego dochodzą tożsamości nieludzkie – boty, API, workloady. W efekcie „ktoś” w systemie nie jest już pojedynczym bytem, ale siecią powiązanych ról i dostępów.

Czy Zero Trust 2.0 ufa mniej ludziom niż poprzedni model?

Odpowiedź: Nie. On nie zmienia poziomu zaufania do ludzi – tylko sposób jego mierzenia. Zamiast pytać „czy ten użytkownik jest zaufany?”, system pyta „czy w tej sekundzie jego zachowanie jest zgodne z profilem, który znamy?”. Zaufanie przestaje być etykietą. Staje się zmienną.

Czy tożsamość w przyszłości będzie bardziej jak profil, czy jak proces?

Odpowiedź: Jak proces. To właśnie jest jedna z najważniejszych zmian w całym podejściu do bezpieczeństwa. Tożsamość nie jest już „stanem posiadania”. Jest ciągłym odtwarzaniem odpowiedzi na pytanie: kim jesteś teraz, w tym konkretnym kontekście, z tego konkretnego miejsca i w tym konkretnym czasie.

CASE STUDY

Sytuacja: Użytkownik loguje się z poprawnymi danymi i MFA. System zauważa Nietypowe tempo pracy, inne wzorce nawigacji, zmienione konteksty użycia.

Decyzja: Ograniczenie dostępu do części zasobów – mimo poprawnego logowania.

Wniosek: To nie logowanie jest dziś najważniejsze. Najważniejsze jest to, co dzieje się po nim.

QUIZ CHALLENGE

W poprzednim numerze zapytaliśmy, czy Twoja wiedza o AI to „state-of-the-art.” czy raczej „outdated model”. Czas sprawdzić wyniki.

1. System AI blokuje konto pracownika o 3:00 nad ranem. Co robisz jako szef bezpieczeństwa?

a) Śpię spokojnie – AI wie, co robi.
b) Dzwonię do HR, żeby szykowali wypowiedzenie.
c) Sprawdzam uzasadnienie (XAI) – może to tylko pracoholik przed urlopem?
d) Odłączam prąd w całym biurowcu (na wszelki wypadek).

2. Twoja firma wdraża AI do monitoringu sieci. Co model będzie „zjadał” na śniadanie najczęściej?

a) Treść prywatnych plotek na Slacku.
b) Logi systemowe i biometrię behawioralną (czyli to, jak specyficznie piszesz na klawiaturze).
c) Zdjęcia z Twoich ostatnich wakacji.
d) Kanapki z kuchni socjalnej.

3. Co jest „piętą achillesową” nowoczesnych systemów AI (tzw. Black Box)?

a) Zbyt wysoki rachunek za prąd.
b) Brak wyjaśnialności – AI mówi „źle”, ale nie powie „dlaczego”.
c) To, że AI nie pije kawy i za szybko pracuje.
d) Zbyt ładny interfejs graficzny.

4. Kiedy RODO zaczyna groźnie patrzeć na Twoje AI?

a) Gdy AI pracuje w nadgodzinach.
b) Gdy automat podejmuje decyzje o człowieku (np. blokada) bez żadnej furtki dla interwencji ludzkiej.
c) Gdy AI ma serwery w chmurze, która nazywa się „Cumulus”.
d) Tylko wtedy, gdy AI zaczyna mówić po niemiecku.

5. Czy hakerzy używają AI?

a) Nie, oni wolą tradycyjne rzemiosło i wirusy „domowej roboty”.
b) Tak, ale tylko do poprawiania błędów ortograficznych w mailach.
c) Tak – tworzą „złe bliźniaki” Twojego szefa (deepfake) i piszą phishing, który brzmi jak od Twojej mamy.
d) Tak, ale tylko w filmach na Netflixie.

6. Idealna rola AI w Twoim zespole to:

a) Samodzielny sędzia i kat, który zwalnia ludzi mailem.
b) Genialny analityk, który przesiewa miliony danych, by podać Ci gotowe wnioski na tacy.
c) Robot, który zastępuje dział IT, żeby zaoszczędzić na owocowych czwartkach.
d) Tajny agent, o którym nikt w firmie nie wie.

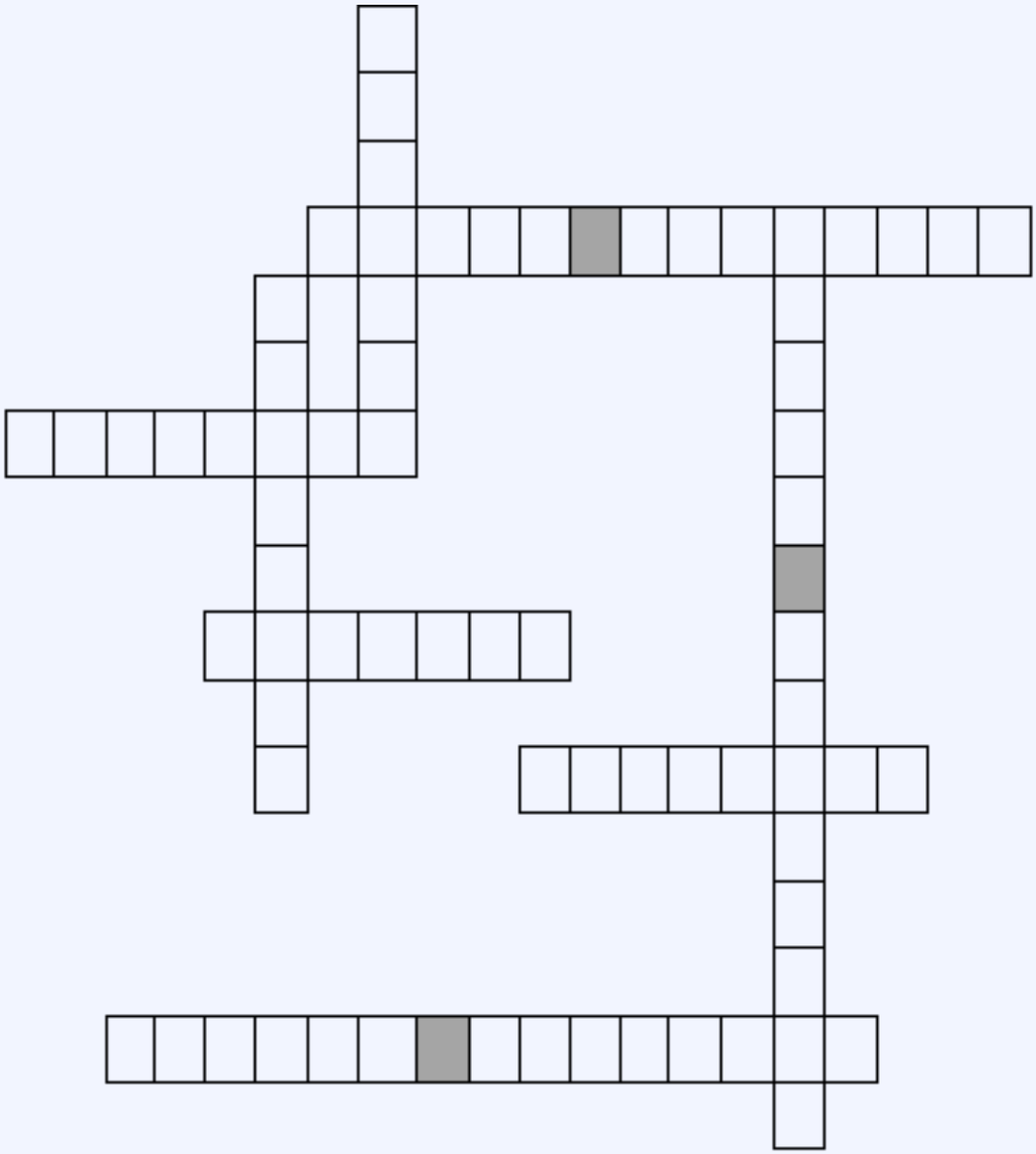
7. Chcesz wdrożyć AI w bezpieczeństwie. Od czego zaczynasz?

a) Od zakupu najdroższej licencji z napisem „Cyber-Magic”.
b) Od analizy ryzyka (DPIA), porządkowania danych i zapewnienia nadzoru człowieka.
c) Od wrzucenia wszystkich danych firmy do publicznego ChatGPT.
d) Od modlitwy o to, żeby nic nie wybuchło.

QUIZ CHALLENGE

Sprawdź, jak radzisz sobie w praktyce.
czy rozpoznasz atak zanim zrobi to system?

1. Atak dopasowany do Ciebie jak garnitur na miarę – wykorzystuje Twoje dane, stanowisko i kontekst pracy.
2. SMS, który trafia idealnie w moment („dopłata do paczki", „problem z przesyłką"). Klikasz, bo to ma sens.
3. Telefon z banku – wszystko się zgadza. Ton, język, scenariusz. Jedyny problem: to nie bank.
4. Atak na „dużą rybę" – prezesa, dyrektora, osobę z dostępem do decyzji i pieniędzy.
5. Wszystko wygląda poprawnie – adres, strona, certyfikat. A jednak zostałeś przekierowany gdzieś indziej.
6. Kod QR zamiast menu, plakatu lub biletu… i punkt wejścia dla ataku w Twoim telefonie.
7. Mail, który już kiedyś dostałeś, tylko ktoś „lekko go poprawił" i dodał coś od siebie.
8. Atak, który zaczyna się tam, gdzie masz największe zaufanie – w komentarzach, wiadomościach i social mediach.



*Poprawne odpowiedzi ujawnimy w kolejnym numerze.

Następny numer już wkrótce!

Temat wydania: Dane 2.0: co naprawdę chronimy w świecie, w którym dane nie znikają

1. OKIEM EKSPERTA

- Data Sprawl: gdy dane wymykają się organizacji
- Synthetic Data: dane, które nigdy nie istniały
- Data Ownership is Dead: gdy dane przestają mieć jednego właściciela

2. TREND ALERT

- Najciekawsze zjawiska wokół danych – co naprawdę zmienia zasady gry, a co tylko tak wygląda

3. ANALIZA RZECZYWISTOŚCI

- Dane są w systemach organizacji? Sprawdzamy, gdzie naprawdę kończy się ich granica i dlaczego często… w ogóle jej nie ma.

4. CZY WIESZ, ŻE...

- Ciekawostki o danych, które podważają to, co wydaje się oczywiste. Niektóre z nich mogą zmienić sposób, w jaki myślisz o tym, gdzie dane naprawdę są… i co się z nimi dzieje.

5. SPOŁECZNOŚĆ W AKCJI

- Prawdziwe pytania, realne dylematy i doświadczenia czytelników – bez filtrów i marketingowych sloganów.

Wydaje Ci się, że kontrolujesz swoje dane? Najpierw sprawdź, czy naprawdę rozumiesz, czym są w dzisiejszym świecie.

Dziękujemy za przeczytanie naszego biuletynu!

Masz pytania?

Skontaktuj się z nami

www.forsafe.pl

600 005 880

biuro@forsafe.pl

ul. Traktorowa 170, 91-203 Łódź