Wartość wywiadowcza danych podróżnych i architektura cyberbezpieczeństwa Booking.com w świetle książki The Machine



AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje dane rezerwacyjne nie jako narzędzie marketingowe, lecz jako strategiczny zasób wywiadowczy. Na przykładach programu Royal Concierge oraz incydentów związanych z Booking.com autor pokazuje, jak metadane o podróżach pozwalają rekonstruować rytmy życia i sieci kontaktów osób wpływowych. Tekst podkreśla, że wartość informacji kontekstowej (czas, miejsce, relacje) często przewyższa zysk finansowy z kradzieży danych kart płatniczych. Wskazuje na niebezpieczeństwa wynikające z koncentracji ogromnych zbiorów danych w rękach jednej platformy, co czyni ją atrakcyjnym celem dla służb wywiadowczych i cyberprzestępców, oraz zwraca uwagę na problem wnioskowania o prywatności na podstawie pozornie niewinnych rekordów.

The article analyzes reservation data not as a marketing tool, but as a strategic intelligence asset. Using examples from the Royal Concierge program and incidents related to Booking.com, the author shows how travel metadata allows for the reconstruction of the life rhythms and contact networks of influential people. The text emphasizes that the value of contextual information (time, place, relationships) often outweighs the financial gain from stealing payment card data. It points to the dangers resulting from the concentration of vast datasets in the hands of a single platform, making it an attractive target for intelligence services and cybercriminals, and draws attention to the problem of inferring privacy based on seemingly innocent records.

Artykuł analizuje ewolucję danych podróżnych z narzędzia marketingowego w strategiczny zasób wywiadowczy, na przykładzie platformy Booking.com. Główna teza zakłada, że informacje o mobilności ludzi posiadają wartość polityczną i szpiegowską niezależną od ich wartości finansowej, co czyni globalne systemy rezerwacyjne atrakcyjnymi celami dla służb państwowych oraz cyberprzestępców. Autor dowodzi, że w obliczu zagrożeń typu 'assume breach', firmy technologiczne muszą odejść od modelu nastawionego wyłącznie na maksymalizację konwersji i usuwanie tarć użytkownika na rzecz kompleksowej architektury odporności. Tekst rzuca światło na fundamentalny konflikt między ekonomią skali (koncentracją danych), a bezpieczeństwem ekosystemu, wskazując, że w świecie Big Tech cyberbezpieczeństwo przestało być domeną administratorów IT, a stało się strategiczną kategorią ryzyka korporacyjnego. Analiza incydentów z lat 2016 i 2019 służy jako punkt wyjścia do rozważań nad integralnością kontekstową prywatności oraz władzą epistemiczną wynikającą z posiadania wiedzy o ruchach milionów ludzi.

SŁOWA KLUCZOWE

wartość wywiadowcza danych | architektura cyberbezpieczeństwa | Booking.com | The Machine | Royal Concierge | PIN leak | attribution problem | paradoks koncentracji danych | contextual integrity | honeypot effect | data minimization | konwersja a bezpieczeństwo | ekosystem platformowy | governance cyberbezpieczeństwa

Dane podróżne jako strategiczny zasób wywiadowczy

Kto wie, dokąd jedziesz? Dane podróżne, "PIN leak", wywiad i cyberbezpieczeństwo Maszyny

Historia Booking.com nabiera innego znaczenia, gdy na dane rezerwacyjne spojrzymy nie jak na paliwo marketingu, lecz jak na informację o człowieku. Wcześniej traktowaliśmy je przede wszystkim jako fundament eksperymentów A/B, personalizacji, rankingów czy pomiaru konwersji. Ta sama infrastruktura informacyjna ma jednak drugie dno.

Rekord rezerwacji ujawnia, gdzie dana osoba zamierza przebywać, w jakim czasie, z kim podróżuje, jak długo pozostanie poza domem i z jakim podmiotem zawarła transakcję. Zestawienie wielu takich rekordów pozwala rekonstruować rytmy życia, sieci kontaktów, interesy zawodowe,

zamożność czy przebieg spotkań służbowych. Dla przedsiębiorstwa są to dane operacyjne; dla przestępcy – podstawa oszustwa, a dla wywiadu – kluczowa informacja o ruchach celu. W ten sposób gospodarcza wartość platformy i jej atrakcyjność jako celu cybernetycznego wyrastają z tego samego źródła: Maszyna wie dużo, ponieważ musi wiedzieć dużo, aby skutecznie koordynować transakcję.

Ten problem bywa przedstawiany w dramatycznym tonie, z połączeniem trzech elementów: program brytyjskiego wywiadu "Royal Concierge", incydent określany jako "PIN Leak Affair" oraz decyzję Booking.com o zatajeniu przed klientami i holenderskim organem ochrony danych zdarzenia z 2016 roku. W kilku miejscach źródło wykracza jednak poza to, co można niezależnie potwierdzić. Twierdzi m.in., że GCHQ i NSA monitorowały rezerwacje dyplomatów "dokonywane przez serwis", a w latach 2015–2016 napastnik przejął od jednego do dwóch milionów kodów PIN oraz dane kart kredytowych. Te dwa twierdzenia wymagają rozdzielenia, gdyż dotyczą różnych operacji i źródeł dowodowych, a różnią się stopniem pewności.

Program Royal Concierge ujawniono w 2013 roku na podstawie dokumentów Edwarda Snowdena. Według dostępnych relacji był to program brytyjskiego GCHQ, działający od 2010 roku i służący identyfikacji zagranicznych podróży dyplomatów oraz urzędników. Mechanizm analizował potwierdzenia rezerwacji z około 350 luksusowych hoteli, wyszukując m.in. wiadomości kierowane na rządowe domeny pocztowe. Wiedza o planowanym miejscu pobytu pozwalała przygotować dalsze operacje wywiadowcze, w tym uderzenia w urządzenia lub komunikację celu. Opisy programu nie pozwalają jednak stwierdzić, że Booking.com był kanałem pozyskiwania tych danych. Mówią one o monitorowaniu potwierdzeń hotelowych i rządowej poczty, a nie o włamaniu do systemów Booking.com. Łączenie Royal Concierge bezpośrednio z tą platformą jest zatem źródłowym skrótem, którego nie należy powtarzać jako ustalonego faktu.

Podobnej precyzji wymaga kwestia roli NSA. Snowden był kontraktorem amerykańskiej National Security Agency, a ujawnione przez niego dokumenty obejmowały szeroko działalność anglosaskiego systemu wywiadowczego. Nie oznacza to jednak, że Royal Concierge był wspólną operacją NSA i GCHQ. Publicznie wskazanym operatorem programu było brytyjskie GCHQ. Choć można mówić o kontekście współpracy państw Five Eyes, w przypadku konkretnej operacji należy odróżnić pochodzenie dokumentów od podmiotu prowadzącego program. To istotna reguła metodologiczna: w badaniu cyberwywiadu podobieństwo aktorów i narzędzi nie uprawnia do automatycznego przypisywania jednej operacji wszystkim służbom występującym w materiale dowodowym.

Wartość wywiadowcza danych podróżnych przekracza zysk finansowy

Samo istnienie Royal Concierge potwierdza głębszą intuicję materiału: dane hotelowe posiadają wartość wywiadowczą niezależną od wartości finansowej. Podczas gdy numer karty płatniczej umożliwia kradzież pieniędzy, informacja o tym, że minister, dyplomata, menedżer korporacji lub negocjator przyleci w określonym dniu do konkretnego miasta, może być dla innego rodzaju przeciwnika znacznie cenniejsza. W teorii bezpieczeństwa informacji dane należy więc oceniać nie tylko przez pryzmat możliwości wykonania bezpośredniej transakcji finansowej. Kluczowe znaczenie ma również informacja kontekstowa – czas, miejsce, tożsamość, relacje między osobami oraz sekwencja zdarzeń. Współczesna nauka o prywatności wielokrotnie dowiodła, że pozornie niewinne metadane mogą ujawnić krytyczne szczegóły. Pojedynczy nocleg może wydawać się informacją banalną, jednak dysponując tysiącami zdarzeń dotyczących wielu osób, można budować grafy mobilności i relacji. Spotkania dwóch osób w tym samym hotelu, powtarzalne podróże do konkretnego miasta, obecność przed istotnym wydarzeniem gospodarczym czy politycznym oraz zmiana zwyczajowego wzorca przemieszczania się stają się potencjalnymi sygnałami.

Dlatego bezpieczeństwa danych nie można sprowadzać do pytania o to, czy wyciekł numer karty. Prywatność dotyczy również możliwości wnioskowania. Ta właściwość danych podróżnych tłumaczy wagę rzeczywistego incydentu w Booking.com z początku 2016 roku, który przestał być wyłącznie twierdzeniem autorów „The Machine”. Po publikacji książki serwis potwierdził, że wykrył wówczas nietypową aktywność i przeprowadził dochodzenie kryminalistyczne z udziałem zewnętrznych ekspertów. Niezależne relacje oparte na ustaleniach NRC wskazują, że napastnik poprzez niewystarczająco zabezpieczony serwer uzyskał dostęp do systemów wewnętrznych i przeglądał tysiące rezerwacji dotyczących państw Bliskiego Wschodu, m.in. Arabii Saudyjskiej, Kataru i Zjednoczonych Emiratów Arabskich. Dostępne były nazwiska podróżnych oraz ich plany wyjazdowe. W tym miejscu pojawia się pierwsza poważna korekta źródła: niezależne relacje nie potwierdzają tezy o przejęciu „1-2 milionów kodów PIN i danych kart kredytowych”, lecz opisują tysiące rezerwacji.

Sam Booking.com oświadczył później, że według dochodzenia w zdarzeniu nie uzyskano dostępu do danych wrażliwych ani finansowych. Choć stanowiska podmiotu będącego stroną incydentu nie można traktować jako ostatecznego dowodu pełnego zakresu naruszenia, to przy braku publicznego materiału potwierdzającego kradzież milionów rekordów i kart, rzetelna rekonstrukcja nie powinna jej zachowywać jako faktu. Mylący dla polskiego czytelnika może być także termin „PIN leak”. W potocznym języku PIN kojarzy się z tajnym kodem karty płatniczej, podczas gdy w relacjach o

incydencie Booking.com odnosił się on do kodów rezerwacyjnych. Ars Technica oraz inne źródła rekonstruujące książkowe ustalenia opisują właśnie kradzież identyfikatorów lub kodów rezerwacji, od których nazwano incydent. Rozróżnienie to jest istotne, gdyż „wyciek PIN-ów" sugeruje kradzież danych uwierzytelniających do środków płatniczych, czego dostępne materiały z 2016 roku nie potwierdzają. Najbardziej sensacyjny element historii dotyczy jednak tożsamości napastnika.

Według relacji opartych na ustaleniach NRC dział bezpieczeństwa Booking.com, przy wsparciu dwóch prywatnych śledczych ze Stanów Zjednoczonych, zidentyfikował Amerykanina, który miał pracować dla przedsiębiorstwa wykonującego zadania na rzecz amerykańskich służb wywiadowczych. Booking.com zwrócił się w tej sprawie również o pomoc do holenderskiej służby AIVD.

Konflikt między konwersją a bezpieczeństwem danych

Publiczne ustalenia nie pozwoliły jednak określić, która agencja amerykańska stała za operacją, ani przesądzić w sensie procesowym, że atak został formalnie zlecony przez konkretny organ państwowy. Najbezpieczniejsza formuła brzmi zatem: istnieją podstawy źródłowe do wiązania sprawcy z wykonawcą pracującym dla amerykańskich służb oraz hipoteza operacji wywiadowczej, lecz brakuje publicznego dowodu pozwalającego przypisać włamanie NSA lub innej konkretnej agencji. To zastrzeżenie nie osłabia znaczenia zdarzenia; wręcz przeciwnie – obnaża istotę attribution problem w cyberbezpieczeństwie. Ustalenie technicznego źródła połączenia nie jest tożsame z identyfikacją osoby przy komputerze, a ustalenie tej osoby nie oznacza automatycznie poznania jej zleceniodawcy. Związek zawodowy z kontraktorem służb nie stanowi jeszcze dowodu państwowego rozkazu.

Państwa wykorzystują tę warstwowość do budowania plausible deniability. Cyberoperacja może przechodzić przez serwery w wielu jurysdykcjach, korzystać z przejętej infrastruktury i zewnętrznych wykonawców, a artefakty techniczne mogą być celowo pozostawiane tak, by utrudnić lub sfałszować atrybucję. Incydent pokazuje zarazem, że model zagrożeń platformy musi obejmować przeciwników o skrajnie różnej motywacji. Zwykły cyberprzestępca szuka numerów kart i haseł, grupa ransomware chce wymusić okup, konkurent poluje na tajemnice przedsiębiorstwa, a aktywista dąży do ujawnienia konkretnych praktyk.

Państwowa służba wywiadowcza poszukuje natomiast informacji, których wartość nie jest wyrażana bezpośrednio w pieniądzu. Dla niej pojedyncza rezerwacja właściwej osoby może być cenniejsza od miliona anonimowych rekordów. Klasyczna triada bezpieczeństwa informacji – poufność, integralność i dostępność – dobrze porządkuje ten problem. Poufność chroni przed

nieuprawnionym poznaniem miejsca i terminu pobytu; integralność zapewnia, że rezerwacja, cena i dane klienta nie zostały podmienione; dostępność gwarantuje ciągłość działania systemu dla użytkowników i hoteli.

Cele te pozostają w stałym napięciu. Rygorystyczne uwierzytelnianie zwiększa bezpieczeństwo, lecz utrudnia legalny dostęp. Dodatkowa kontrola transakcji zmniejsza ryzyko oszustwa, ale generuje tarcie. Redundancja infrastruktury poprawia dostępność, lecz mnoży kopie danych wymagających ochrony. Bezpieczeństwo nie jest więc parametrem, który można po prostu ustawić na maksimum; to problem optymalizacji wielu rodzajów ryzyka. W Booking.com napięcie to jest szczególnie widoczne, gdyż historyczna filozofia przedsiębiorstwa polegała na usuwaniu tarcia. "Book and fuck off" oznaczało możliwie najszybsze przejście od potrzeby do transakcji.

Bezpieczeństwo często działa odwrotnie: wymaga potwierdzenia, drugiego składnika uwierzytelnienia czy blokady podejrzanej operacji. Raport Booking Holdings za 2025 rok otwarcie przyznaje, że środki chroniące przed nieautoryzowanym dostępem mogą powodować odrzucanie lub opóźnianie prawidłowych rezerwacji, co prowadzi do utraty biznesu. Spółka stwierdza jednocześnie, że podatności po stronie konsumentów i partnerów już umożliwiały wycieki danych, a ryzyko rośnie wraz z poszerzaniem oferty, integracją produktów, wdrażaniem AI i wzrostem ilości przetwarzanych informacji. Jest to niemal podręcznikowe przyznanie, że bezpieczeństwo i konwersja znajdują się na tej samej krzywej kompromisu.

W języku ekonomii bezpieczeństwa Ross Anderson i inni badacze podkreślali, że cyberbezpieczeństwo jest w równym stopniu problemem bodźców, co kryptografii. Jeśli skutki błędu ponosi inny uczestnik niż podmiot wybierający poziom zabezpieczeń, dochodzi do niedoinwestowania w ochronę. Hotel może stosować słabe hasło, lecz kradzież danych uderza w klienta i reputację Booking.com. Platforma może projektować system przyjazny dla partnera, ale jego łatwość obsługi zwiększa ryzyko przejęcia konta. Konsument z kolei może ignorować wieloskładnikowe uwierzytelnianie, bo koszt kilku sekund ponosi natychmiast, podczas gdy korzyść z bezpieczeństwa pozostaje odległa i niewidzialna.

Bezpieczeństwo platformy to nie bezpieczeństwo ekosystemu

Powstaje więc klasyczny problem najsłabszego ogniwa. Bezpieczeństwo całego ekosystemu nie jest tożsame z bezpieczeństwem serwerów centrali. Booking.com może dysponować wysoce zaawansowanymi zespołami security, jednak przestępca ominie je, wysyłając przekonujący e-mail

phishingowy do pracownika niewielkiego hotelu. Nawet jeśli hotel posiada dobrą politykę IT, urządzenie pracownika może zostać zainfekowane malwarem. Z kolei użytkownik może korzystać z bezpiecznej aplikacji, lecz fałszywa wiadomość na WhatsAppie przekona go do podania danych płatniczych na zewnętrznej stronie. W złożonym systemie atakujący nie musi przełamywać najsilniejszej ściany; szuka drzwi, których ktoś zapomniał zamknąć. Pozwala to odróżnić bezpieczeństwo samej platformy od bezpieczeństwa ekosystemu platformowego. Granica tego pierwszego kończy się tam, gdzie zaczynają się systemy hoteli, dostawców płatności, urządzenia użytkowników i zewnętrzne usługi. Z perspektywy konsumenta podział ten jest jednak niemal niewidoczny.

Jeśli po dokonaniu rezerwacji przez Booking.com klient otrzymuje wiadomość zawierającą prawidłowe nazwisko, hotel, datę pobytu i cenę, ma silne podstawy psychologiczne, aby uznać komunikat za autentyczny. Atakujący żeruje na reputacji całego ekosystemu, nawet gdy techniczna kompromitacja nastąpiła wyłącznie u jednego partnera. Mechanizm ten stał się szczególnie wyraźny w innym, odrębnym od zdarzenia z 2016 roku naruszeniu, za które holenderski organ ochrony danych nałożył później na Booking.com karę 475 tysięcy euro. W grudniu 2018 roku przestępcy zastosowali socjotechnikę wobec pracowników czterdziestu hoteli w Zjednoczonych Emiratach Arabskich, podszywając się pod personel Booking.com i przejmując dane logowania do kont partnerów. W efekcie uzyskali dostęp do danych 4 109 osób; w przypadku niemal trzystu klientów wyciek objął dane kart kredytowych, a w części przypadków również kody bezpieczeństwa. Booking.com dowiedział się o naruszeniu 13 stycznia 2019 roku, lecz zgłosił je organowi dopiero 7 lutego – po 22 dniach. Uznano to za złamanie obowiązku zgłoszenia incydentu w ciągu 72 godzin, co skutkowało administracyjną karą finansową.

Incydentu z lat 2018–2019 nie wolno mylić z „PIN leak” z 2016 roku. W pierwszym przypadku publiczne dowody potwierdzają ujawnienie danych kart i późniejszą sankcję organu nadzorczego. W przypadku wcześniejszym Booking.com twierdzi, że do informacji finansowych ani innych danych wrażliwych nie uzyskano dostępu. Zestawienie obu spraw w jednej narracji łatwo tworzy mylne wrażenie jednej ciągłej afery obejmującej miliony PIN-ów i karty kredytowe. Historycznie są to jednak dwa różne incydenty o odmiennym mechanizmie, zakresie i reżimie prawnym.

Konflikt interesów w raportowaniu incydentów danych

Incydent z początku 2016 roku miał miejsce jeszcze przed wejściem w życie RODO. Booking.com argumentował później, że zgodnie z obowiązującą wówczas holenderską ustawą o ochronie danych oraz po konsultacjach z ekspertami, nie powstał obowiązek powiadomienia organu ani

użytkowników. Uzasadniano to brakiem dowodów na dostęp do informacji wrażliwych lub finansowych, a tym bardziej brakiem negatywnych skutków dla prywatności osób poszkodowanych. Część ekspertów cytowanych przez holenderskie media kwestionowała jednak tę ocenę, wskazując, że same dane o podróżach również mogą prowadzić do niekorzystnych konsekwencji.

Nie można zatem po prostu stwierdzić, że firma "zataiła bezprawnie" zdarzenie, skoro w tej konkretnej sprawie brakuje publicznego rozstrzygnięcia organu, które potwierdzałoby naruszenie obowiązku zgłoszenia. Tu zarysowuje się istotna różnica między tajemnicą a naruszeniem transparentności. Organizacja nie ma bowiem ogólnego obowiązku publikowania każdego incydentu bezpieczeństwa; wręcz przeciwnie – przed usunięciem podatności ujawnienie informacji może pomóc napastnikom i pogorszyć sytuację. Prawo definiuje jednak momenty, w których interes osób, których dane dotyczą, lub interes organu nadzoru przeważa nad korporacyjną poufnością. RODO wprowadziło znacznie bardziej rygorystyczny reżim proceduralny: administrator musi zgłosić naruszenie ochrony danych bez zbędnej zwłoki i, jeśli to możliwe, nie później niż w ciągu 72 godzin od uzyskania o nim wiedzy, chyba że jest mało prawdopodobne, by incydent powodował ryzyko dla praw i wolności osób fizycznych. Kara nałożona w późniejszej sprawie Booking.com dotyczyła właśnie przekroczenia tego obowiązku.

Z punktu widzenia teorii organizacji obowiązek szybkiego raportowania ma skorygować naturalny konflikt interesów. Firma, która odkryła wyciek, dąży najpierw do zrozumienia jego pełnego zakresu, ograniczenia strat wizerunkowych i uniknięcia pochopnej komunikacji. Tymczasem osoba poszkodowana może potrzebować informacji natychmiast, by zastrzec kartę, zmienić hasło, ustrzec się przed phishingiem lub ocenić ryzyko fizyczne. Z kolei organ nadzorczy chce mieć możliwość interwencji, zanim przedsiębiorstwo samodzielnie rozstrzygnie wszystkie sporne kwestie. Rygor czasowy ingeruje więc w sekwencję zarządzania kryzysem: uniemożliwia sytuację, w której firma najpierw wszystko ustala we własnym zakresie, a dopiero potem decyduje, czy regulator powinien zostać poinformowany.

Właśnie ten aspekt zaakcentował holenderski organ w sprawie Booking.com z 2019 roku. W publicznym uzasadnieniu podkreślono, że platforma ponosi szczególną odpowiedzialność ze względu na wartość i zakres gromadzonych informacji. Krytyka dotyczyła m.in. faktu, że przedsiębiorstwo najpierw prowadziło własne dochodzenie, a dopiero później dokonało formalnego zgłoszenia. Governance cyberbezpieczeństwa nie może więc być całkowicie zamkniętą funkcją korporacyjną. W systemie ochrony danych pewne informacje o incydencie muszą w odpowiednim momencie opuścić organizację, aby możliwy był niezależny nadzór. Odmienny problem stanowi data minimization. Najbezpieczniejsza baza danych to w skrajnym sensie baza, która nie istnieje.

Informacji, której przedsiębiorstwo nie gromadzi lub którą skutecznie usuwa, nie można później wykraść z systemu. Platformowy model gospodarczy działa jednak w przeciwnym kierunku.

Paradoks koncentracji danych i instytucjonalizacja cyberbezpieczeństwa

Historia rezerwacji ułatwia obsługę klienta, a dane behawioralne pozwalają na lepszą personalizację. Wieloletnie rekordy z kolei umożliwiają wykrywanie oszustw, analizę eksperymentów, budowę programów lojalnościowych czy trenowanie modeli machine learning. Większa ilość danych podnosi zatem jakość usługi, ale jednocześnie zwiększa skalę potencjalnej szkody. Można to określić jako paradoks koncentracji danych. Centralizacja informacji przynosi ekonomię skali poznawczej: im więcej przypadków analizuje platforma, tym skuteczniej modeluje popyt, wykrywa anomalie i personalizuje ofertę. Ten sam efekt skali zwiększa jednak potencjalną nagrodę dla napastnika.

Włamanie do niewielkiej recepcji może ujawnić kilkaset rezerwacji; dostęp do centralnego systemu globalnego pośrednika otwiera zasób o rzędy wielkości większy. W efekcie sukces sieciowy wytwarza honeypot effect: system staje się coraz atrakcyjniejszym celem właśnie dlatego, że coraz lepiej spełnia swoją funkcję gospodarczą. Ekonomiczna wartość danych i koszt ich zabezpieczenia rosną więc równolegle – dane są jednocześnie aktywem i zobowiązaniem, czego tradycyjny bilans rachunkowy nie oddaje w pełni.

Wartość modeli, rekomendacji i relacji z klientem opartych na danych bywa ogromna, podczas gdy potencjalne zobowiązanie wynikające z incydentu ma charakter probabilistyczny. Dopóki do zdarzenia nie dochodzi, bezpieczeństwo często postrzegane jest jedynie jako centrum kosztów. Po naruszeniu okazuje się jednak, że wydatki na ochronę były formą kapitału odpornościowego. Tutaj powraca problem inwestycji prewencyjnej, analizowany wcześniej przy długu technicznym. Sprawny system bezpieczeństwa produkuje rezultat kontrfaktyczny: atak nie powiódł się, więc zarząd nigdy nie doświadczył katastrofy, której uniknięto. Powoduje to asymetrię w budżetowaniu.

Nowa funkcja sprzedażowa generuje wzrost przychodu, a segmentacja marketingowa zwiększa konwersję. Zespół bezpieczeństwa prosi natomiast o środki na rozwiązanie, którego najlepszym wynikiem będzie brak jakichkolwiek wiadomości. Właśnie dlatego cyberbezpieczeństwo wymaga poziomu governance wyższego niż zwykła kolejka projektów produktowych. Współczesna struktura Booking Holdings wskazuje, że problem ten przeniesiono na poziom zarządczy grupy. W raporcie zrównoważonego rozwoju za 2025 rok spółka podkreśla globalną odpowiedzialność Chief Security

Officer i Chief Privacy Officer, współpracę poszczególnych marek z centralnymi funkcjami bezpieczeństwa oraz nadzór rady dyrektorów i Audit Committee. W ramach komitetu audytu funkcjonuje Cybersecurity Subcommittee, który spotyka się co najmniej cztery razy w roku, raportując o istotnych ryzykach cybernetycznych i prywatności. Cyberbezpieczeństwo przestaje w takiej strukturze być wyłącznie zadaniem administratora systemu; staje się kategorią ryzyka przedsiębiorstwa porównywalną z finansami, prawem czy ciągłością działalności. Ta instytucjonalizacja jest typowa dla dojrzewania systemów technologicznych.

W młodym start-upie bezpieczeństwo bywa domeną tych samych osób, które utrzymują serwer i rozwijają produkt. W globalnej platformie powstają już ścisłe specjalizacje: security operations, application security, fraud prevention, privacy engineering, incident response, threat intelligence, red teaming, zarządzanie podatnościami oraz compliance. Sama liczba specjalistów nie gwarantuje ochrony, ale obrazuje zmianę natury problemu. W pewnym momencie zabezpieczanie platformy zaczyna przypominać utrzymywanie infrastruktury krytycznej bardziej niż administrowanie zwykłą witryną internetową. Przy tym bezpieczeństwo Booking.com nie może być rozpatrywane w oderwaniu od bezpieczeństwa hoteli.

Bezpieczeństwo jako wyścig zbrojeń między technologią a psychologią

Dzisiejsze materiały platformy skierowane do partnerów wprost wymieniają przejęcia kont w wyniku phishingu, infekcje urządzeń, nieautoryzowany dostęp do danych gości oraz oszustwa oparte na socjotechnice. Platforma zaleca, a w określonych obszarach wręcz wymusza uwierzytelnianie dwuskładnikowe; z kolei podróżni są ostrzegani przed wiadomościami, które wykorzystują autentyczne szczegóły pobytu oraz presję czasu, by wymusić ponowne podanie danych płatniczych. Zagrożenie ma zatem charakter nie tylko techniczny, lecz poznawczy: przestępca atakuje sposób, w jaki człowiek rozpoznaje wiarygodność. Kevin Mitnick i literatura dotycząca social engineering od dawna wskazywały, że człowiek nie jest „błędem" umieszczonym obok systemu informatycznego, lecz jego integralnym elementem.

Uwierzytelnienie rozmówcy, rozpoznanie fałszywego maila, decyzja o kliknięciu w link czy reakcja na presję czasu są częścią procesu bezpieczeństwa równie realnie jak szyfrowanie. Paradoksalnie techniki stosowane przez przestępców często opierają się na tych samych heurystykach psychologicznych, które analizowaliśmy wcześniej w kontekście perswazji sprzedażowej: autorytecie, rzadkości i presji czasu. Komunikat „Musisz natychmiast potwierdzić płatność, inaczej

stracisz rezerwację” to niemal podręcznikowe połączenie awersji do straty z poczuciem pilności. Tutaj historia zatacza niepokojące koło.

Booking.com nauczył się, że informacja o ograniczonej dostępności skłania użytkownika do szybszej decyzji. Cyberprzestępca wykorzystuje analogiczną wiedzę behawioralną przeciwko klientowi platformy, komunikując ryzyko utraty istniejącej rezerwacji. Sama platforma oczywiście nie odpowiada za zamiary oszusta, musi jednak mieć świadomość, że jej marka, język komunikacji i przyzwyczajenia użytkowników tworzą środowisko podatne na imitację. Im silniejsza marka, tym bardziej wiarygodne staje się podszywanie pod nią. To jedna z przyczyn, dla których uwierzytelnianie wieloskładnikowe jest czymś więcej niż techniczną funkcją. Zmienia ekonomię ataku. Skradzione hasło przestaje wystarczać, gdy niezbędny jest drugi, niezależny składnik. Należy jednak pamiętać, że ten drugi element również może zostać wyłudzony, przechwycony lub zatwierdzony przez zmanipulowanego użytkownika.

Bezpieczeństwo ewoluuje więc jak wyścig zbrojeń. Każdy skuteczny mechanizm obronny wymusza zmianę strategii napastnika, który przenosi wysiłek tam, gdzie koszt przełamania zabezpieczeń pozostaje najniższy. W tym miejscu kluczowa staje się koncepcja attack surface. Im więcej funkcjonalności, integracji, API, kont partnerów, aplikacji mobilnych, dostawców technologicznych, systemów płatności i produktów podróżnych, tym więcej potencjalnych punktów wejścia. Connected Trip zwiększa wartość ekonomiczną systemu poprzez integrację, ale jednocześnie podnosi złożoność jego bezpieczeństwa. Booking Holdings w raporcie za 2025 rok przyznaje, że rozszerzanie zakresu usług, integrowanie produktów i rosnące wykorzystanie AI zwiększają ekspozycję na ryzyka cybernetyczne oraz zagrożenia dla prywatności. Strategia integracji generuje więc koszt bezpieczeństwa podobny do długu technologicznego: więcej połączeń oznacza więcej zależności wymagających ochrony.

Szczególnie wymagające okazują się systemy uczenia maszynowego. Choć mogą one usprawnić detekcję fraudów poprzez rozpoznawanie anomalii nieuchwytnych dla ręcznych reguł, jednocześnie wprowadzają nowe kategorie podatności: zatruwanie danych, nadużycia automatyzacji, wycieki z modeli, ataki na mechanizmy klasyfikacji oraz generowanie coraz bardziej przekonującego phishingu przy użyciu generatywnej AI. W 2026 roku bezpieczeństwo platformy turystycznej nie jest już kwestią samych firewalli i haseł w rozumieniu początku wieku; obejmuje ono cały ekosystem przepływu danych, modeli i ludzkich decyzji.

Istotne jest w tym kontekście, że historia bezpieczeństwa Booking.com nie zamknęła się na incydentach z 2016 czy 2019 roku. W kwietniu 2026 roku platforma potwierdziła nowe zdarzenie, w którym osoby trzecie uzyskały dostęp do części informacji o rezerwacjach niektórych gości. Booking.com poinformował, że po wykryciu aktywności podjął działania ograniczające incydent,

zmienił numery PIN powiązane z dotkniętymi rezerwacjami i powiadomił użytkowników. Według przekazów medialnych ujawnione mogły zostać dane kontaktowe oraz szczegóły rezerwacji, natomiast dane finansowe pozostały bezpieczne. Polski CERT potwierdził, że wśród poszkodowanych byli również użytkownicy z Polski.

Od iluzji ochrony do architektury odporności i integralności kontekstowej

Nie należy łączyć tego zdarzenia przyczynowo z incydentami historycznymi. Mechanizmy mogą być odmienne, infrastruktura przez dekadę została wielokrotnie przebudowana, a samo występowanie kilku naruszeń w długim czasie nie dowodzi istnienia jednej, ciągłej podatności. Aktualne zdarzenie jest jednak wartościowe analitycznie, gdyż pokazuje trwałość problemu: ryzyko wycieku danych rezerwacyjnych nie jest zamkniętym rozdziałem historii internetu sprzed RODO. Im większy ekosystem, tym bardziej bezpieczeństwo staje się permanentnym procesem zarządzania zmieniającym się przeciwnikiem.

Dlatego najtrafniejszym sposobem oceny cyberbezpieczeństwa nie jest pytanie o to, czy firmę „zhakowano". Niemal każda globalna organizacja działająca przez dostatecznie długi czas doświadcza prób włamań, phishingu, malware, błędów konfiguracji czy naruszeń u dostawców. Kluczowe jest pytanie o odporność: jak szybko organizacja wykrywa incydent, ogranicza jego zakres, zabezpiecza dowody, komunikuje się z poszkodowanymi, powiadamia regulatorów, usuwa podatność i wykorzystuje zdarzenie do zmiany architektury. Współczesna inżynieria bezpieczeństwa odchodzi zatem od fantazji absolutnej ochrony ku pojęciu assume breach. Założenie to brzmi: należy projektować system tak, jak gdyby pewna warstwa ochrony została kiedyś przełamana. Segmentacja sieci ogranicza wówczas możliwość przemieszczania się napastnika, a zasada least privilege sprawia, że przejęte konto daje jedynie minimalny, niezbędny zakres uprawnień. Szyfrowanie zmniejsza wartość przejętych danych, natomiast monitoring pozwala zauważyć nietypowe zachowania.

Rotacja credentiali ogranicza czas użyteczności skradzionego sekretu, a kopie bezpieczeństwa umożliwiają odtworzenie działania systemu. Bezpieczeństwo przestaje być murem; staje się architekturą ograniczania skutków nieuniknionych błędów. Cyberbezpieczeństwo jest tu bliskie teorii odporności organizacyjnej omawianej w kontekście pandemii. System odporny nie zakłada, że szok się nie wydarzy, lecz przyjmuje, że po jego wystąpieniu nie utraci całkowitej zdolności działania. Podobnie system bezpieczny nie może opierać się wyłącznie na przekonaniu, że nikt nie pozna hasła; musi przewidzieć, co stanie się w momencie, gdy do tego dojdzie.

Redundancja, segmentacja, monitoring i procedury incydentowe są cyfrowym odpowiednikiem rezerw płynności, zapasowych dostawców i planów ciągłości działania. Jednocześnie każde zabezpieczenie generuje koszt. Booking Holdings wprost ostrzega inwestorów, że środki bezpieczeństwa mogą opóźniać lub odrzucać legalne transakcje. Jest to kwestia krytyczna dla firmy wyrosłej z kultury konwersji: security engineer może dążyć do dodatkowej weryfikacji, podczas gdy product manager dostrzeże w tym spadek BPD.

Dla pierwszego odrzucona podejrzana transakcja jest sukcesem; dla drugiego odrzucona legalna transakcja jest stratą. Nie istnieje jedna metryka, która automatycznie rozstrzygnęłaby ten konflikt. Znów dochodzimy do granicy eksperymentalizmu. Test A/B może wykazać, ile rezerwacji tracimy po wprowadzeniu dodatkowego uwierzytelniania, ale nie pokaże bezpośrednio wartości włamania, do którego dzięki temu zabezpieczeniu nigdy nie doszło.

Rzadkie katastrofy są metodologicznie trudne, gdyż nie pozostawiają wystarczającej liczby obserwacji dla zwykłej optymalizacji statystycznej. Jeśli bezpieczeństwo zostanie podporządkowane wyłącznie krótkookresowym miernikom, niemal zawsze będzie wydawać się zbyt drogie – aż do chwili, gdy okaże się niewystarczające. Charles Perrow w teorii normal accidents analizował systemy, w których duża złożoność i silne sprzężenie sprawiają, że pewnych awarii nie da się całkowicie wyeliminować. Booking.com nie jest elektrownią jądrową i mechaniczne przenoszenie tej teorii byłoby przesadą, jednak jej intuicja pozostaje użyteczna. Im więcej współzależnych elementów, tym więcej istnieje kombinacji zdarzeń, których projektanci nie przewidzieli. Globalna platforma, miliony partnerów, urządzenia klientów, dostawcy chmurowi, API, płatności i systemy AI tworzą środowisko, w którym bezpieczeństwo nie może polegać wyłącznie na katalogu znanych scenariuszy.

W tym miejscu ekonomia danych spotyka się z etyką prywatności. Platforma może posiadać formalną podstawę prawną do przetwarzania informacji i nadal powinna pytać, czy potrzebuje każdej z nich, jak długo musi je przechowywać i kto rzeczywiście powinien mieć do nich dostęp. Helen Nissenbaum rozwija koncepcję contextual integrity: prywatność nie oznacza prostego ukrywania informacji, lecz zgodność przepływu danych z normami konkretnego kontekstu społecznego. Podróżny podaje hotelowi lub platformie dane po to, aby zarezerwować pobyt.

To, że informacja istnieje cyfrowo, nie oznacza, że jej przepływ do dowolnego innego aktora jest społecznie równoważny. Royal Concierge dobrze obrazuje radykalne naruszenie takiej integralności kontekstowej: informacja tworzona w kontekście gościnności i logistyki podróży zyskała zupełnie nową funkcję w ramach operacji wywiadowczej. Incydent Booking.com z 2016 roku prowadzi do analogicznego problemu – nawet bez danych finansowych sama wiedza o podróżach określonych osób może mieć konsekwencje wykraczające daleko poza oczekiwania użytkownika. Wartość

danych nie jest więc właściwością samego rekordu; zależy od tego, kto go posiada, z czym łączy i w jakim celu wykorzystuje.

Michel Foucault wiązał wiedzę z władzą nie dlatego, że każda informacja automatycznie daje kontrolę, lecz dlatego, że systematyczna obserwacja zwiększa zdolność klasyfikowania, przewidywania i oddziaływania. Booking.com wykorzystywał tę zależność gospodarczo: lepsza obserwacja zachowań użytkownika poprawiała produkt i sprzedaż. Wywiad może korzystać z podobnej struktury dla zupełnie innego celu: obserwacja mobilności zwiększa zdolność identyfikowania miejsc i momentów podatności celu. Cyberprzestępca wykorzystuje jeszcze inną funkcję: szczegóły prawdziwej rezerwacji zwiększają wiarygodność oszustwa.

Bezpieczeństwo danych to nie to samo co prywatność

Te same dane uczestniczą zatem w kilku odmiennych reżimach władzy, co sprawia, że prywatność i bezpieczeństwo nie są tożsame. Bezpieczeństwo odpowiada na pytanie, czy dane pozostają chronione zgodnie z przyjętymi uprawnieniami; prywatność pyta natomiast, czy zakres tych uprawnień jest w ogóle właściwy. Doskonale zabezpieczona baza może być problematyczna prywatnościowo, jeśli gromadzi nadmiar informacji lub wykorzystuje je w nieoczekiwanym celu. Z kolei system respektujący zasadę minimalizacji danych może okazać się źle zabezpieczony. Dojrzały governance danych musi łączyć oba te wymiary: nie tylko chronić to, co przedsiębiorstwo posiada, lecz także ograniczać to, co powinno posiadać i w jaki sposób może z tego korzystać. Współczesny Booking Holdings realizuje takie podejście poprzez zasady transparentności, celu, kontroli, bezpieczeństwa, privacy by design oraz odpowiedzialności, które organizują politykę prywatności grupy. Deklaracja korporacyjna nie jest oczywiście dowodem perfekcyjnego wdrożenia tych zasad, ma jednak znaczenie instytucjonalne: prywatność została przesunięta z poziomu regulaminu dla klienta na poziom systemu kontroli korporacyjnej. To ta sama ewolucja, którą obserwowaliśmy przy DMA i DSA – prywatna Maszyna wytwarza własne procedury samokontroli, działając jednocześnie w ramach coraz gęstszego zewnętrznego systemu rozliczalności.

Różnicę między Booking.com z 1996 roku a Booking.com z 2026 roku można więc zdefiniować nie liczbą serwerów, lecz strukturą odpowiedzialności. Pierwotna firma musiała przede wszystkim zadbać o to, by informacja o wolnym pokoju skutecznie dotarła od hotelu do klienta. Dzisiejsza platforma musi rozstrzygać, kto może tę informację zobaczyć i jak długo może być ona przechowywana; jak udostępnić ją zgodnie z DMA, zabezpieczyć przed cyberprzestępcą, odpowiedzieć na żądanie organu państwowego, zareagować na przejęcie konta partnera czy poinformować użytkownika o naruszeniu.

Skala danych zmienia kategorię problemu z technicznej na strategiczną

To kolejny dowód na to, że skalowanie nie polega jedynie na powtarzaniu tej samej transakcji milion razy. Skala zmienia kategorię problemu. Dziesięć rezerwacji to informacja operacyjna; miliardy rezerwacji tworzą już infrastrukturę wiedzy o mobilności społecznej. Mała strona internetowa jest celem cyberprzestępczym o ograniczonej wartości, natomiast globalna platforma staje się atrakcyjna dla zorganizowanego cybercrime, operatorów phishingowych, szpiegostwa gospodarczego i potencjalnie aktorów państwowych. Wraz ze wzrostem rentowności rośnie budżet obrony, ale równocześnie rośnie motywacja przeciwnika.

Dlatego opowieść o "NSA hack" należy zastąpić bardziej precyzyjnym i intelektualnie mocniejszym wnioskiem. Nie możemy potwierdzić, że NSA włamała się do Booking.com. Możemy jednak potwierdzić, że w 2016 roku serwis doświadczył włamania obejmującego tysiące rezerwacji na Bliskim Wschodzie; późniejsze śledztwo powiązało sprawcę z przedsiębiorstwem wykonującym prace dla amerykańskich służb, lecz nie pozwoliło publicznie wskazać konkretnej agencji. Wiemy także, że wcześniej GCHQ prowadziło niezależny program Royal Concierge skierowany na dane hotelowe dyplomatów. Te zdarzenia nie dowodzą jednej spójnej operacji przeciw Booking.com, lecz czegoś bardziej ogólnego: informacja o podróży jest zasobem strategicznym. Ta konstatacja przybliża nas do odpowiedzi na pytanie "co wolno Big Tech?". Władza platformy nie sprowadza się bowiem do ustalania prowizji, rankingu czy sposobu wyświetlania ceny.

Istnieje również władza epistemiczna wynikająca z posiadania informacji o zachowaniach milionów ludzi. Prawo ochrony danych próbuje ograniczyć sposób wykorzystywania tej wiedzy, cyberbezpieczeństwo ma zapobiegać jej przejęciu przez nieuprawnionych aktorów, a prawo konkurencji reguluje możliwość monopolizowania danych. Służby państwowe działają natomiast według własnych reżimów bezpieczeństwa narodowego, często pozostających w napięciu z prywatnością. Platforma znajduje się wówczas pomiędzy sprzecznymi powinnościami: ma znać użytkownika wystarczająco dobrze, by zaoferować mu właściwy hotel, a jednocześnie nie wiedzieć o nim więcej, niż jest to potrzebne.

Musi przechowywać dane wystarczająco długo, aby obsłużyć reklamację i zwalczać fraud, lecz ograniczać retencję tam, gdzie nie jest ona uzasadniona. Ma udostępniać określone dane partnerom na podstawie DMA i chronić je przed nieautoryzowanym dostępem, mogąc jednocześnie być zobowiązaną do odpowiadania na prawomocne żądania organów publicznych. Te zobowiązania nie tworzą jednego prostego optimum; są konstytucją informacyjną platformy. W ten sposób Maszyna po raz kolejny przekracza granicę pierwotnej funkcji.

Miała rezerwować pokój. Zaczęła porządkować rynek. Następnie zaczęła poznawać konsumenta, kształtować jego wybór, organizować hotelarzom dostęp do popytu i przechowywać ogromny zasób informacji o mobilności ludzi. Im lepiej działała jako infrastruktura podróży, tym większa stawała się odpowiedzialność za to, kto może zajrzeć do jej pamięci. A jednak największym błędem byłoby zakończyć tę historię konkluzją o technologicznej degeneracji. Incydenty bezpieczeństwa, konflikty regulacyjne, dług techniczny, kryzys pandemiczny i spory pracownicze nie zatrzymały ekonomicznego wzrostu platformy. Maszyna nadal działa, a skala jej działania jest obecnie większa niż w okresie opisywanym przez źródłową książkę. To właśnie ten fakt stanowi konieczny kontrapunkt dla wszystkich dotychczasowych kontrowersji. Jeśli chcemy odpowiedzieć na pytanie, dlaczego Booking.com odniósł sukces i co naprawdę wolno Big Tech, nie możemy opisać firmy wyłącznie jako systemu, który z czasem się zepsuł. Trzeba wyjaśnić trudniejszy paradoks: jak przedsiębiorstwo może być równocześnie krytykowane za lokalne maksimum, dług technologiczny, władzę rynkową i manipulacyjne interfejsy – a mimo to nadal zwiększać skalę, przychody i znaczenie infrastrukturalne trzy dekady po powstaniu.

> W świecie, gdzie informacja o jednym noclegu może stać się kluczem do operacji wywiadowczej, granica między luksusowym serwisem a infrastrukturą krytyczną ulega całkowitemu zatarciu. Pozostaje pytanie: czy w pogoni za idealną konwersją i wygodą użytkownika nie zbudowaliśmy cyfrowego panoptikonu, w którym cena za 'szybką rezerwację' jest wypłacana w walucie naszej strategicznej prywatności? Paradoksalnie, im sprawniej działa Maszyna, tym bardziej staje się ona niebezpiecznym trofeum w globalnym wyścigu zbrojeń.

Inspiracje

[1] **"The Machine"** Stijn Bronzwaer

Stijn Bronzwaer (ur. 1981 w Heerlen w Holandii) jest holenderskim dziennikarzem śledczym, reporterem technologicznym i autorem. Studiował komunikację społeczną na Uniwersytecie Radboud oraz dziennikarstwo na Uniwersytecie w Utrechcie i Uniwersytecie Amsterdamskim. Od 2007 roku pracuje dla wiodącej holenderskiej gazety ogólnokrajowej NRC, gdzie pełnił różne funkcje, w tym redaktora ds. mediów, zastępcy redaktora naczelnego i reportera technologicznego, koncentrującego się na firmach technologicznych, startupach i sztucznej inteligencji. Bronzwaer jest również współzałożycielem NRC Vandaag, jednego z najchętniej słuchanych codziennych podcastów informacyjnych w Holandii. Wraz z kolegami Jorisem Kooimanem i Merijnem Rengersem zdobył szerokie uznanie za współautorstwo książki „De Machine" (opublikowanej po angielsku pod tytułem „The Machine"), śledztwa w sprawie Booking.com, które zdobyło prestiżową nagrodę dziennikarstwa śledczego De Loep. W 2026 roku zespół opublikował Ali Niknam: De eenzame strijd van een techmiljardair, nieautoryzowaną biografię założyciela bunq.

Stijn Bronzwaer *(born 1981 in Heerlen, Netherlands) is a Dutch investigative journalist, technology reporter, and author. He studied communication science at Radboud University and journalism at Utrecht University and the University of Amsterdam. Since 2007, he has worked for the leading Dutch national newspaper NRC, where he has served in several capacities, including media editor, deputy editor-in-chief, and tech reporter focusing on tech companies, startups, and artificial intelligence. Bronzwaer also co-founded NRC Vandaag, one of the Netherlands' most listened-to daily news podcasts. He achieved widespread acclaim alongside colleagues Joris Kooiman and Merijn Rengers for co-authoring De Machine (published in English as The Machine), an investigation into Booking.com that won the prestigious De Loep investigative journalism award. In 2026, the team published Ali Niknam: De eenzame strijd van een techmiljardair, an unauthorized biography of the bunq founder.*

NRC

Literatura uzupełniająca

Książki

Książki autorów przywoływanych i literatura pokrewna:



[1] "Permanent Record"

Edward Snowden

Macmillan | ISBN: 9781529035667



[2] "Security Engineering: A Guide to Building Dependable Distributed Systems"

Ross Anderson

John Wiley & Sons | ISBN: 9781118008362



[3] "Security Engineering: A Guide to Building Dependable Distributed Systems, 1st edition"

Ross Anderson

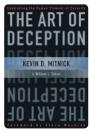
John Wiley & Sons | ISBN: 9781118008362



[4] "Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition"

Ross Anderson

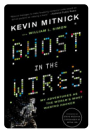
John Wiley & Sons | ISBN: 9781118008362



[5] "The Art of Deception"

Kevin Mitnick

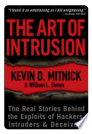
Wiley | ISBN: 9780471237129



[6] "Ghost in the Wires"

Kevin Mitnick

ISBN: 9780316201605



[7] "The Art of Intrusion"

Kevin Mitnick

John Wiley & Sons | ISBN: 9780470503829



[8] "Normal accidents : living with high-risk technologies : with a new afterword and a postscript on the Y2K problem"

Charles Perrow

Princeton University Press | ISBN: 9780691004129



[9] "Normal Accidents"

Charles Perrow

Princeton University Press | ISBN: 9781400828494



[10] **"Monitoring laws: profiling and identity in the world state"**

Helen Nissenbaum

Cambridge University Press | ISBN: 9781108426626

Artykuły naukowe

Prace autorów przywoływanych w tekście:

[1] **"Security Engineering: A Guide to Building Dependable Distributed Systems"**

Ross Anderson

2001 | DOI: 10.1002/9781119644682

Źródło

[2] **"Why information security is hard - an economic perspective"**

Ross Anderson

2005 | DOI: 10.1109/acsac.2001.991552

Źródło

[3] **"The Economics of Information Security"**

Ross Anderson, Tyler Moore

2006 | Science | DOI: 10.1126/science.1130992

Źródło

[4] **"AI models collapse when trained on recursively generated data"**

Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Nicolas Papernot, Ross Anderson

2024 | Nature | DOI: 10.1038/s41586-024-07566-y

Źródło

[5] **"The Art of Deception: Controlling the Human Element of Security"**

Kevin D. Mitnick, William L. Simon

2001

Źródło

Treść tworzy Fundacja Dobre Państwo.

Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.

APA ONE Publishing System

Fundacja Dobre Państwo © 2026

Article ID: 3f820090-9610-43b9-9b2e-6cad97af214f