Przedmowa
Jack Jones,
Przewodniczący
FAIR Institute

DOUGLAS W. HUBBARD
RICHARD SEIERSEN

METODY MODELOWANIA, POMIARU I SZACOWANIA RYZYKA

RYZYKO W CYBERBEZPIECZEŃSTWIE

Wydanie II

Helion
WILEY

Tytuł oryginału: How to Measure Anything in Cybersecurity Risk, 2nd Edition

Tłumaczenie: Piotr Ptaszek

ISBN: 978-83-289-0594-8

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/rywcy2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

ROZDZIAŁ 1

Ta jedna najbardziej potrzebna łatka w cyberbezpieczeństwie

Dziś wszystko jest w porządku, to jest nasze złudzenie.

— Wolter, 1759[1]

W ciągu jednego roku cyberataki poskutkowały naruszeniem miliarda rekordów danych i stratami finansowymi w wysokości 400 miliardów dolarów[2]. To spowodowało, że „Forbes Magazine" ogłosił ten rok „rokiem wielkiego wycieku danych"[3, 4]. Wkrótce potem szef największego ubezpieczyciela, Lloyd's of London — giełdy zrzeszającej towarzystwa ubezpieczeniowe, firmy reasekuracyjne i innego rodzaju instytucje finansowe — powiedział, że cyberzagrożenia to „największe i najbardziej systemowe ryzyko", jakie widział w ciągu 42 lat pracy w ubezpieczeniach[5]. Ten artykuł opublikowano w 2014 r. Od tego czasu wiele się wydarzyło.

Zgodnie z licznymi wskaźnikami, od 2014 r. ryzyko dla cyberbezpieczeństwa wzrasta z roku na rok. Na przykład według jednego ze źródeł liczba rekordów danych naruszonych w 2021 r. była 22 razy większa niż w 2014 r.[6] i od tego czasu bynajmniej nie spada. Staniemy się tylko bardziej zależni — i bardziej podatni — od technologii, które napędzają nasz dobrobyt. Możemy spróbować zmniejszyć to ryzyko, ale zasoby są ograniczone. Dla kierownictwa ryzyko to może wydawać się abstrakcyjne, zwłaszcza jeśli nie doświadczyło ono bezpośrednio strat. A jednak musimy przekonać kierownictwo, w jego języku, że kwestie cyberbezpieczeństwa wymagają jego uwagi i znacznego budżetu. Kiedy już to mamy, możemy najpierw spróbować zidentyfikować zagrożenia o wysokim priorytecie i się nimi zająć.

Tytuł tej książki mówi sam za siebie. Porozmawiamy o tym, jak możemy mierzyć ryzyko w cyberbezpieczeństwie i dlaczego ważna jest zmiana sposobu, w jaki

obecnie to robimy. Na razie przedstawimy tylko argumenty za tym, że są powody do niepokoju — zarówno przed zagrożeniami dla cyberbezpieczeństwa, jak też o adekwatność metod ich oceny.

Ubezpieczenie: kanarek w kopalni

Jeden z autorów tej książki Richard Seiersen był dyrektorem ds. bezpieczeństwa informacji (ang. *Chief Information Security Officer*, CISO), a obecnie pracuje jako dyrektor ds. ryzyka (ang. *Chief Risk Officer*, CRO) w firmie ubezpieczeniowej Resilience, zajmującej się cyberbezpieczeństwem. Te dwa punkty widzenia dają dobrą perspektywę ryzyka związanego z cyberbezpieczeństwem. Jeśli ubezpieczyciel źle skalkuluje ryzyko, poniesie konsekwencje. Jednak aby być konkurencyjnym, nie może po prostu pobierać opłat za wszystko, za co chce. Ma silną motywację do zbierania wielu danych, kalkulowania i ustalania, na co warto postawić w kontekście ryzyka, które ubezpieczenie obejmuje. To nie znaczy, że zawsze ma rację — w końcu to zakład. Ale jego analizy są zwykle lepsze niż to, co większość firm może zrobić we własnym zakresie.

Richard zwróciłby uwagę, że firmy ubezpieczeniowe ujawniają swoje obawy dotyczące ryzyka, gdy podnoszą składki, zaostrzają wymogi co do ubezpieczenia lub całkowicie rezygnują ze sprzedaży danego rodzaju ubezpieczenia. Są rodzajem kanarka w kopalni zagrożeń. To, co dzieje się w obszarze cyberubezpieczeń, jest swego rodzaju głównym wskaźnikiem, na który CISO powinni zwrócić uwagę.

Według National Association of Insurance Commissioners (NAIC) w latach 2017 – 2021 suma zebranych składek wzrosła o 45%, a udział odszkodowań wypłaconych z tytułu roszczeń i szkód wzrósł ponaddwukrotnie[7]. Oznacza to, że łączna liczba wypłaconych odszkodowań z tytułu ubezpieczenia cybernetycznego wzrosła w tym samym okresie ponadtrzykrotnie. Należy pamiętać, że odszkodowania pokrywają tylko *niektóre* straty. Wykluczają one retencję (co ubezpieczyciel konsumentów detalicznych nazwałby odliczeniem), wszystko powyżej limitu objętego ubezpieczeniem oraz wyłączenia, takie jak działania wojenne.

Jeśli roszczenia są całkowicie niezależne od siebie, to spodziewana jest pewna zmienność z roku na rok, tak jak suma uzyskana w wyniku 100 rzutów kostką do gry będzie nieco inna niż po 100 dalszych rzutach. Jednak liczba zmian zaobserwowanych przez NAIC znacznie wykracza poza to, co można by wyjaśnić jako losowy przypadek. Da się zauważyć trendy, zgodnie z którymi szkody są coraz częstsze i coraz bardziej kosztowne. Jest to „ryzyko systemowe", o którym wspomniał wcześniej szef Lloyd's. Oprócz tego, że szkody są większe i częstsze, istnieje ryzyko, że wiele szkód wystąpi w tym samym czasie, co utrudni lub uniemożliwi

ubezpieczycielowi ich pokrycie. Ponadto niektóre ostatnie wydarzenia sprawiły, że ryzyko systemowe stało się dla ubezpieczycieli jeszcze większym problemem.

Pewna batalia prawna stworzyła nowe ryzyko systemowe dla ubezpieczycieli, co zmusiło ich do zmiany polis lub, w niektórych przypadkach, wycofania się z ubezpieczeń cybernetycznych. W styczniu 2022 r. Chubb, największy dostawca cyberubezpieczeń, przegrał sprawę dotyczącą tego, czy powinien pokryć 1,4 miliarda dolarów strat zgłoszonych przez giganta farmaceutycznego Merck[8]. Firma Merck została zaatakowana złośliwym kodem znanym jako „NotPetya", który zaszyfrował dane na tysiącach jej komputerów.

Ponieważ źródłem ataku było sześciu Rosjan powiązanych z rosyjskimi agencjami wywiadowczymi, Chubb argumentował, że był to akt wojny, który zwykle jest wykluczony w ubezpieczeniach majątkowych. Ale sąd orzekł, że polityka firmy wyklucza tylko wojnę fizyczną, a nie wojnę cybernetyczną. Inni ubezpieczyciele zwrócili na to uwagę i ustanowili znacznie bardziej rygorystyczne wymagania ubezpieczeniowe. W sierpniu 2022 r. Lloyd's of London poradziła wszystkim ubezpieczycielom zajmującym się cyberubezpieczeniami, którzy prowadzą sprzedaż za pośrednictwem jej platformy, aby zaprzestali sprzedaży ubezpieczeń od cyberataków sponsorowanych przez agencje rządowe[9].

Złośliwe oprogramowanie NotPetya, które zaatakowało firmę Merck, było oparte na wcześniejszym kodzie znanym jako Petya. Chociaż Petya był używany w oprogramowaniu ransomware, atak na firmę Merck nie wiązał się z żądaniem okupu. Ten kod, stworzony przez Rosję z myślą o ataku na ukraińskie systemy, służył po prostu do niszczenia. Atak był zarówno destrukcyjny, jak i szkodliwy finansowo, ale mógł być znacznie gorszy.

Inne włamanie, do firmy SolarWinds, pokazuje, jak szeroko może rozprzestrzeniać się jeden złośliwy kod. SolarWinds opracowuje oprogramowanie do monitorowania wydajności systemu. Jeden z jej pakietów, system zarządzania siecią Orion, jest używany przez ponad 30 tysięcy instytucji publicznych i prywatnych. W 2020 r. ujawniono, że aktualizacja Oriona, którą SolarWinds wysłała swoim klientom, zawierała szkodliwy kod. Chociaż potencjalnych ofiar było wiele, wydaje się, że firmy (zwłaszcza ubezpieczeniowe) uniknęły ataku. Włamanie do SolarWinds było według wszelkich standardów poważnym atakiem, ale motywem był bardziej dostęp do tajnych danych rządowych niż do danych pojedynczych osób.

Z drugiej strony pierwotnym celem NotPetyi była pojedyncza ukraińska firma produkująca oprogramowanie, ale szkodliwy kod wyciekł do wielu ukraińskich podmiotów, takich jak Narodowy Bank Ukrainy — i rozprzestrzenił się na cały świat. Doprowadziło to do strat w wysokości miliardów dolarów — z których większość stanowiły szkody poboczne. A mimo to kod nie rozpowszechnił się tak bardzo jak złośliwe oprogramowanie udostępnione przez SolarWinds. Gdyby

jakiś atak był tak rozległy jak w przypadku SolarWinds i tak destrukcyjny jak NotPetya, sprawy potoczyłyby się zupełnie inaczej.

Dodanie wyłączeń związanych z działaniami wojennymi wraz z widocznym wzrostem częstotliwości właśnie tego rodzaju zdarzeń powiększa listę zagrożeń systemowych. Potencjalne słabości w szeroko stosowanym oprogramowaniu i współzależny dostęp do sieci między firmami, dostawcami i klientami sprawiają, że duże, skoordynowane ataki mogą dotknąć znacznie więcej niż jedną dużą firmę. Powiedzieliśmy to w pierwszym wydaniu tej książki w 2016 r. i teraz jest to równie prawdziwe, o ile nie bardziej. Jeśli skutkuje to wieloma poważnymi szkodami w krótkim okresie, może to stanowić większe obciążenie, niż ubezpieczyciele będą w stanie pokryć. To, co niepokoi firmy ubezpieczeniowe, to fakt, że nawet największe dotychczas zaobserwowane ataki nie były tak duże, jak mogłyby być.

Globalna powierzchnia ataku

Jak wspomnieliśmy powyżej, firmy ubezpieczeniowe mają możliwość ograniczenia ryzyka przez zmianę zapisów polisy lub po prostu odmowę sprzedaży ubezpieczenia, jeśli uznają, że ryzyko jest zbyt duże. Mogą po prostu zdecydować, że nie będą uczestniczyć w tym ryzyku. Ty nie masz takiej opcji. Każde ryzyko, którego ubezpieczyciele nie pokryją, nadal ponosisz. Państwa, przestępczość zorganizowana, organizacje haktywistyczne i gracze wewnątrz organizacji chcą naszych tajemnic, naszych pieniędzy i naszej własności intelektualnej, a niektórzy chcą naszego całkowitego upadku. To nie tani dramatyzm. Jeśli czytasz tę książkę, prawdopodobnie już doceniasz powagę sytuacji.

Co powoduje tak dramatyczny wzrost naruszeń i jeszcze większą liczbę spodziewanych naruszeń? Nazywa się to „powierzchnią ataku". Powierzchnię ataku zwykle definiuje się jako sumę wszystkich rodzajów narażenia systemu informatycznego. Oznacza ona wystawienie wartości zasobów na ryzyko ze strony niezaufanych źródeł. Nie musisz być specjalistą od bezpieczeństwa, aby to rozumieć. Twój dom, Twoje konto bankowe, Twoja rodzina i Twoja tożsamość mają powierzchnię ataku. Jeśli otrzymałeś ochronę przed kradzieżą tożsamości jako pracownik federalny lub jako klient dużego sprzedawcy detalicznego, otrzymałeś to przez powierzchnię ataku. Firmy te umieszczają cyfrowego Ciebie w zasięgu przestępców. Bezpośrednio lub pośrednio, ułatwił to Internet. Ta ewolucja nastąpiła szybko i nie zawsze za wiedzą lub bezpośrednią zgodą wszystkich interesariuszy, takich jak Ty.

Różne definicje powierzchni ataku uwzględniają drogi do systemu i z systemu, mechanizmy obronne tego systemu, a czasami wartość danych w tym systemie[10,11]. Niektóre definicje odnoszą się do powierzchni ataku systemu, a inne

do powierzchni ataku sieci, ale mogą one być zbyt wąskie nawet dla danej firmy. Możemy również zdefiniować „powierzchnię ataku przedsiębiorstwa", na którą składają się nie tylko wszystkie systemy i sieci w tej organizacji, ale także osoby trzecie. Obejmuje to wszystkich w ekosystemie przedsiębiorstwa, w tym głównych klientów, dostawców i być może agencje rządowe. Jak w 2013 r. widzieliśmy w przypadku wycieku danych głównego detalisty Target, każde możliwe połączenie ma znaczenie. Tamten exploit pochodził od dostawcy mającego dostęp do systemów HVAC firmy[12].

Być może cała powierzchnia ataku, która dotyczy wszystkich obywateli, konsumentów i rządów, jest swego rodzaju „globalną powierzchnią ataku": całkowitym zestawem zagrożeń dla bezpieczeństwa cybernetycznego — obejmującym wszystkie systemy, sieci i organizacje — z którym wszyscy mamy do czynienia, robiąc zakupy kartą kredytową, przeglądając Internet, otrzymując świadczenia medyczne, a nawet po prostu przez bycie zatrudnionym. Ta globalna powierzchnia ataku jest zjawiskiem na poziomie makro, napędzanym co najmniej czterema czynnikami wzrostu na poziomie makro, którymi są: rosnąca liczba użytkowników na całym świecie, różnorodność użytkowników na całym świecie, wzrost liczby odkrytych i wykorzystywanych luk w zabezpieczeniach oraz coraz większe wzajemne powiązania organizacji, co skutkuje ryzykiem „awarii kaskadowej".

- *Rosnąca liczba osób w Internecie*. Liczba użytkowników Internetu na całym świecie wzrosła w latach 2001 – 2022 10-krotnie (z 0,5 miliarda do 5 miliardów)[13]. Może to nie być oczywiste, że liczba użytkowników jest wymiarem w części obszarów ataku, ale niektóre miary obszaru ataku obejmują również wartość celu, która jest częściowo funkcją liczby użytkowników (np. uzyskanie dostępu do większej liczby rekordów danych osobowych)[14]. Ponadto w skali globalnej działa to jako ważny mnożnik przy poniższych czynnikach.
- *Każda osoba robi coraz więcej online*. Dużo już robiliśmy online, a pandemia to przyspieszyła. W 2020 r., pierwszym roku pandemii, e-commerce wzrósł o 43%[15]. Wideokonferencja stała się w czasie pandemii nową normą spotkań. Istnieje również inny rodzaj „pandemii", w postaci rosnącej liczby podłączonych urządzeń na osobę. Internet rzeczy (ang. *Internet of Things*, IoT) to kolejny potencjalny sposób korzystania z Internetu przez jednostkę nawet bez jej aktywnego udziału — liczba ataków na urządzenia IoT wzrosła trzykrotnie w pierwszej połowie 2019 r.[16]
- *Rosnąca liczba luk w zabezpieczeniach*. Naturalną konsekwencją dwóch wcześniej omówionych czynników jest wzrost liczby sposobów złośliwego wykorzystania takich zastosowań. Według bazy danych Mitre CVE całkowita liczba znanych luk rosła od 2005 r. do 2015 r. w tempie poniżej 8% rocznie, a następnie, od 2016 r. do 2021 r., o ponad 20% rocznie. Wiele podmiotów hakerskich stale szuka sposobów na znajdowanie i wykorzystywanie kolejnych luk.

- *Możliwość poważnego naruszenia kaskadowego*. Atak NotPetya pokazał, jak destrukcyjny może być atak dla organizacji, które padły jego ofiarą, a SolarWinds pokazał, jak powszechny może być taki atak. Ale nawet w 2013 r. naruszenia pokazują — przykładem choćby wspomniana już firma Target — jak rutynowe i przyziemne połączenia między organizacjami mogą być wektorem ataku. Organizacje takie jak Target mają wielu dostawców, z których część z kolei ma wielu dużych klientów korporacyjnych i rządowych. Mapowanie tego cyberekosystemu połączeń jest prawie niemożliwe, ponieważ z pewnością wymagałoby od wszystkich tych organizacji ujawnienia informacji poufnych. Nie ma ogólnie dostępnych informacji dotyczących tego czynnika, w przeciwieństwie do trzech wcześniej omówionych. Podejrzewamy jednak, że większość dużych organizacji jest powiązana ze sobą poprzez co najmniej jednego pośrednika.

Wydaje się, że trzy pierwsze trendy potęgują ten ostatni. Jeśli tak, ryzyko poważnego naruszenia kaskadowego może rosnąć najszybciej.

Nasza naiwna i oczywista hipoteza? Powierzchnia ataku i naruszenia są skorelowane. Zbliżamy się do historycznego wzrostu powierzchni ataku, a co za tym idzie — skali naruszeń, które przyćmią to, co obserwowano do tej pory. Biorąc to wszystko pod uwagę, twierdzenia takie jak w komentarzu Lloyd's of London są aktualne i nie można ich odrzucić jako zbyt alarmistycznych. Nawet po gigantycznych naruszeniach w Target, Anthem i Sony wierzymy, że nie widzieliśmy jeszcze naprawdę dużego ataku.

Odpowiedź na zagrożenie cybernetyczne

Aby odpowiedzieć na zakusy konkurencji i pandemię, organizacje musiały jeszcze bardziej agresywnie podejść do wdrażania rozwiązań online. Społeczeństwo chce robić zakupy online, zamawiać posiłki online, śledzić dostawy online i nie tylko. Firmy i szkoły musiały pozwolić na więcej pracy zdalnej i przeprowadzać więcej spotkań za pośrednictwem usług takich jak Zoom, Webex i Teams.

To jest trochę sytuacja bez wyjścia, ponieważ sukces w biznesie jest silnie skorelowany z narażeniem. Bankowość, kupowanie, uzyskiwanie pomocy medycznej, a nawet zatrudnienie są uzależnione od narażenia. Musisz udostępnić dane biznesowi transakcyjnemu, a jeśli chcesz robić więcej interesów, oznacza to większą powierzchnię ataku. Kiedy jesteś narażony, cyberprzestępcy mogą Cię zauważyć i możesz stać się podatny na nieoczekiwane złośliwe techniki. W celu obrony specjaliści ds. cyberbezpieczeństwa próbują „utwardzić" (ang. *hardening*) systemy — to znaczy usunąć wszystkie nieistotne elementy, w tym programy, użytkowników, dane, uprawnienia i luki w zabezpieczeniach. Hardening kurczy

powierzchnię ataku, chociaż jej nie eliminuje. Jednak nawet to częściowe zmniejszenie powierzchni ataku wymaga znacznych zasobów, a trendy pokazują, że zapotrzebowanie na zasoby będzie rosło.

Czy organizacje przynajmniej zwracają uwagę na te zagrożenia i nadają im priorytety? Istnieje kilka ankiet, które mogą odpowiedzieć na to pytanie. Niemal każda duża firma konsultingowa sporządza roczne raporty na temat ryzyka na podstawie ankiet przeprowadzonych wśród ich klientów na szczeblu kierowniczym. Raporty te mają obejmować wszystkie zagrożenia, nie tylko dla cyberbezpieczeństwa, ale jest ono coraz częściej obecne w tych raportach. Metody selekcji kadry kierowniczej, pytania zadawane w ankietach i analiza wyników różnią się, ale wnioski są zbliżone: cyberbezpieczeństwu poświęca się coraz większą uwagę. W niektórych przypadkach wskaźniki cyberbezpieczeństwa budzą wśród kierownictwa większe obawy niż jakiekolwiek inne ryzyko.

McKinsey, największa i najstarsza z czołowych firm konsultingowych, sporządza roczne raporty dotyczące wszystkich rodzajów ryzyka, na jakie narażona jest organizacja. W raporcie dotyczącym zagrożeń korporacyjnych z 2010 r. o cyberbezpieczeństwie nie wspomniano ani razu. W 2016 r. wspomniano o bezpieczeństwie cybernetycznym, ale poświęcono mu mniej wzmianek niż jakiemukolwiek innemu ryzyku. W raporcie *McKinsey on Risk* z 2021 r. o ryzyku związanym z cyberbezpieczeństwem wspominano częściej niż o pozostałych zagrożeniach razem wziętych, w tym finansach, regulacjach, geopolityce, konkurencji, a nawet COVID.

W opublikowanym w 2022 r. *25th Annual Global CEO Survey* firmy PWC zapytano prezesów, jakie rodzaje zagrożeń dla wzrostu najbardziej ich dotyczą. Jako zagrożenie numer jeden najczęściej (49%) wymieniali cyberbezpieczeństwo. Wyprzedziło ono konflikt geopolityczny, niestabilność makroekonomiczną i zagrożenia dla zdrowia — w roku inwazji Rosji na Ukrainę i po dwóch latach COVID.

Ogólnie rzecz biorąc, wzrosło zainteresowanie kadry zarządzającej zagrożeniami cybernetycznymi, a za zainteresowaniem podążają zasoby. Zarząd zaczyna zadawać pytania, takie jak „Czy się do nas włamią?", „Czy jesteśmy lepsi niż ta inna firma z naszej branży, do której się włamano?" lub „Czy wydaliśmy wystarczająco dużo na właściwe ryzyko?".

Zadawanie tych pytań ostatecznie skłania niektórych do zatrudnienia dyrektora ds. bezpieczeństwa informacji (CISO). Pierwsza rola CISO w firmie z listy Fortune 100 pojawiła się w latach 90., ale potem przez większość czasu wzrost liczby CISO był powolny. „Magazyn CFO" przyznał, że zatrudnianie CISO jeszcze w 2008 r. uważano za „zbędne"[17]. Od tego czasu do opublikowania pierwszego wydania tej książki (2016 r.) rola CISO stawała się coraz bardziej powszechna. Obecnie prawie wszystkie firmy z listy Fortune 500 mają CISO lub podobną

osobę na stanowisku wiceprezesa lub starszego wiceprezesa albo kogoś na poziomie „C", kto zajmuje się cyberbezpieczeństwem[18].

Firmy wykazują również gotowość — być może wolniej, niż chcieliby tego specjaliści od cyberbezpieczeństwa — do przeznaczenia dużych zasobów na rozwiązanie tego problemu. Wydatki na cyberbezpieczeństwo na pracownika wzrosły w latach 2012 – 2020 ponadczterokrotnie (nawet po uwzględnieniu inflacji), do 2691 dolarów[19]. Według cyberseek.org w sierpniu 2022 r. rynek pracy w USA osiągnął kamień milowy w postaci *miliona pracowników zajmujących się cyberbezpieczeństwem*.

Co więc robią organizacje z tym napływem pieniędzy do cyberbezpieczeństwa? Przede wszystkim wyszukują luki w zabezpieczeniach, wykrywają ataki i eliminują wycieki danych. Oczywiście rozmiar powierzchni ataku oraz sama liczba luk w zabezpieczeniach, ataków i wycieków danych oznaczają, że organizacje muszą dokonywać trudnych wyborów; nie wszystko zostaje naprawione, zatrzymane, odzyskane i tak dalej. Musi istnieć jakiś poziom akceptowalnych strat. To, jakie rodzaje ryzyka są do przyjęcia, często nie jest udokumentowane, a jeśli jest, to określa się je miękkimi, niewymiernymi terminami, których nie można jasno wykorzystać w kalkulacjach w celu ustalenia, czy dany wydatek jest uzasadniony, czy nie.

Doprowadziło to do tak zwanego „zarządzania podatnościami". Po stronie ataku jest „zarządzanie zdarzeniami bezpieczeństwa", które można uogólnić na „zarządzanie informacjami o bezpieczeństwie i zdarzeniami". Ostatnio doszły „threat intelligence" oraz „threat management". Wszystko to mieści się w przestrzeni taktycznych rozwiązań bezpieczeństwa, ale zarządzający próbują ustalić, co robić dalej. Jak więc organizacje zarządzają bezpieczeństwem? W jaki sposób ustalają priorytety alokacji znacznych, ale ograniczonych zasobów w przypadku rosnącej listy luk w zabezpieczeniach? Innymi słowy, w jaki sposób podejmują decyzje dotyczące cyberbezpieczeństwa, aby przydzielić ograniczone zasoby w walce z tak niepewnymi i rosnącymi zagrożeniami?

Z pewnością, jak zawsze w zarządzaniu, duży jest w tym udział eksperckiej intuicji. Ale są też bardziej systematyczne podejścia: ankiety przeprowadzone w 2016 r. przez Hubbard Decision Research wykazały, że około 80% organizacji zajmujących się cyberbezpieczeństwem stosuje jakąś metodę „punktacji". Na przykład mając aplikację z wieloma podatnościami, możemy je wszystkie zagregować i nadać im punktację. Korzystając z podobnych metod w innej skali, grupy aplikacji można następnie agregować w „zestaw" i połączyć z innymi zestawami. Proces agregacji jest zazwyczaj jakąś formą matematyki, nieznaną aktuariuszom, statystykom i matematykom.

Nieco ponad 50% respondentów przedstawia zagrożenia na dwuwymiarowej macierzy. W tym podejściu „prawdopodobieństwo" i „wpływ" będą oceniane subiektywnie, być może w skali od 1 do 5, i te dwie wartości zostaną użyte do

nakreślenia konkretnego ryzyka na macierzy (zwanej różnie: „macierzą ryzyka", „mapą ciepła", „mapą ryzyka" itp.). Macierz — podobna do tej pokazanej w tabeli 1.1 — jest następnie często dalej dzielona na sekcje niskiego, średniego i wysokiego ryzyka. Zdarzenia o wysokim prawdopodobieństwie i dużym wpływie znajdują się w prawym górnym rogu „wysokiego ryzyka", podczas gdy zdarzenia o niskim prawdopodobieństwie i niskim wpływie byłyby w przeciwległym rogu, „niskiego ryzyka". Chodzi o to, że im wyższy wynik, tym coś jest ważniejsze i tym szybciej należy się tym zająć. Intuicyjnie sądzimy, że takie podejście jest rozsądne, i jeśli tak pomyślałeś, jesteś w dobrym towarzystwie.

TABELA 1.1. Znana macierz ryzyka (inaczej mapa ciepła lub mapa ryzyka)

			Wpływ				
			Nieistotny	Drobny	Umiarkowany	Krytyczny	Katastrofalny
			1	2	3	4	5
Prawdopodobieństwo	Częste	5	Średnie	Średnie	**Wysokie**	**Wysokie**	**Wysokie**
	Prawdopodobne	4	Średnie	Średnie	Średnie	**Wysokie**	**Wysokie**
	Okazjonalne	3	Niskie	Średnie	Średnie	Średnie	**Wysokie**
	Rzadkie	2	Niskie	Niskie	Średnie	Średnie	Średnie
	Nieprawdopodobne	1	Niskie	Niskie	Niskie	Średnie	Średnie

Różne wersje wyników i map ryzyka są zatwierdzane i promowane przez kilka głównych organizacji, standardów i frameworków, takich jak National Institute of Standards and Technology (NIST), International Standards Organization (ISO), MITRE.org i Open Web Application Security Project (OWASP). Większość organizacji w obszarze cyberbezpieczeństwa twierdzi, że co najmniej jedna z nich jest częścią ich schematu oceny ryzyka. W rzeczywistości większość głównych organizacji zajmujących się oprogramowaniem, takich jak Oracle, Microsoft i Adobe, ocenia swoje luki za pomocą rozwijanego przez NIST systemu oceniania zwanego „Common Vulnerability Scoring System" (CVSS). Wiele rozwiązań bezpieczeństwa obejmuje również oceny CVSS, czy to pod kątem luk w zabezpieczeniach, czy ataków. Chociaż zalecenia dotyczące kontroli zawarte w wielu z tych ram są dobre, to kierujemy się tutaj zasadą ustalania priorytetów w zarządzaniu ryzykiem w skali przedsiębiorstwa, co zwiększa ryzyko.

Dosłownie setki dostawców zabezpieczeń, a nawet organizacje standaryzujące przyjęły jakąś formę systemu oceniania, w tym macierz ryzyka. Rzeczywiście, metody punktacji i macierze ryzyka są podstawą podejścia do zarządzania ryzykiem w branży bezpieczeństwa.

We wszystkich przypadkach opierają się one na założeniu, że takie metody są do pewnego stopnia korzystne. Oznacza to, że zakłada się, że są one co najmniej ulepszeniem w stosunku do nieużywania takiej metody. Jak ujęła to jedna z organizacji standaryzujących, ocena ryzyka w ten sposób jest odpowiednia:

> *Gdy tester zidentyfikuje potencjalne ryzyko i chce się dowiedzieć, jak poważne ono jest, to pierwszym krokiem jest oszacowanie* prawdopodobieństwa. *Na najwyższym poziomie jest to przybliżona miara prawdopodobieństwa wykrycia i wykorzystania tej konkretnej luki przez atakującego. W tym oszacowaniu nie trzeba być bardzo precyzyjnym.* Generalnie wystarczy określić, czy prawdopodobieństwo jest niskie, średnie czy wysokie.
>
> — OWASP[20]

Czy to ostatnie zdanie, stwierdzające, że „wystarczy określić, czy prawdopodobieństwo jest niskie, średnie czy wysokie", należy przyjąć na wiarę? Biorąc pod uwagę krytyczny charakter decyzji, które będą następować po zastosowaniu metody, twierdzimy, że nie. Jest to testowalna hipoteza i faktycznie *została* przetestowana na wiele różnych sposobów. Rosnące trendy samych ataków cybernetycznych wskazują, że być może nadszedł czas, aby spróbować czegoś innego.

Wyjaśnijmy więc nasze stanowisko w sprawie obecnych metod: *Są one porażką. Nie działają.* Dokładna analiza badań nad tymi metodami i ogólnie metodami podejmowania decyzji wskazuje na to, co następuje (wszystko to zostanie szczegółowo omówione w dalszych rozdziałach):

- Nie ma dowodów na to, że punktacje i macierze ryzyka powszechnie stosowane w cyberbezpieczeństwie poprawiają osąd.
- Z drugiej strony istnieją dowody na to, że metody te dodają do procesu oceny szum i błędy. Jeden z badaczy, Tony Cox, o którym będziemy mówić dalej, posuwa się nawet do stwierdzenia, że mogą być „gorsze niż losowe".
- Wszelkie „działania" są prawdopodobnie rodzajem „analitycznego placebo". Oznacza to, że w wyniku użycia metody możesz poczuć, że jest lepiej, nawet jeśli działanie nie zapewnia wymiernej poprawy w szacowaniu ryzyka (lub nawet dodaje błąd).
- W opublikowanych badaniach istnieje przytłaczająca liczba dowodów na to, że ilościowe metody probabilistyczne są ulepszeniem w stosunku do niewspomaganej intuicji eksperta.
- Poprawa w stosunku do niewspomaganej intuicji eksperta jest mierzalna nawet wtedy, gdy dane wejściowe są częściowo lub całkowicie subiektywne — dopóki dane wejściowe są *jednoznacznymi* wielkościami pochodzącymi od *skalibrowanych* ekspertów.

- Na szczęście większość ekspertów ds. cyberbezpieczeństwa wydaje się chętna i zdolna do przyjęcia lepszych rozwiązań ilościowych. Jednak powszechne niezrozumienie, jakie niektórzy wykazują — w tym błędne przekonania na temat podstawowych statystyk — stwarzają pewne przeszkody w przyjmowaniu lepszych metod.

Sposób, w jaki oceniamy ryzyko, i sposób ustalania, o ile je zmniejszamy, jest podstawą do określenia, gdzie należy nadać priorytet wykorzystania zasobów. A jeśli ta metoda jest niedoskonała — lub nawet pozostawia miejsce na znaczną poprawę — to jest to problem o najwyższym priorytecie, z którym cyberbezpieczeństwo musi się uporać.

To nie koniec złych wieści. W dalszej części tej książki pokażemy, że kwantyfikacja ryzyka cybernetycznego (ang. *Cyber Risk Quantification*, CRQ) zyskuje na popularności i jest stosowana w coraz większej liczbie narzędzi. Jak pokażemy w dalszych rozdziałach, nawet proste metody kwantyfikacji będą lepsze niż wciąż szeroko stosowana macierz ryzyka.

Propozycja zarządzania ryzykiem cybernetycznym

W tej książce zaproponujemy inny kierunek dla cyberbezpieczeństwa. Każde proponowane rozwiązanie będzie ostatecznie zgodne z tytułem tej książki. Oznacza to, że rozwiązujemy problemy, opisując, jak mierzyć ryzyko związane z cyberbezpieczeństwem — *wszystko*, co dotyczy ryzyka związanego z cyberbezpieczeństwem. Pomiary te będą narzędziem w proponowanych rozwiązaniach, ale także ujawnią, dlaczego te rozwiązania zostały wybrane w pierwszej kolejności. Zaproponujmy zatem przyjęcie nowego ilościowego podejścia do cyberbezpieczeństwa, zbudowanego na następujących zasadach:

- *Możliwe jest znaczne udoskonalenie istniejących metod*. Jak już wspomnieliśmy, wiemy, że niektóre metody wymiernie przewyższają inne, nawet jeśli porównujemy dwie czysto subiektywne metody. Podejścia, które są obecnie najpopularniejsze, wykorzystują metody, które należą do najsłabszych. Jest to nie do zaakceptowania przy skali problemów, z jakimi boryka się cyberbezpieczeństwo.
- *Cyberbezpieczeństwo może wykorzystywać ten sam język ilościowej analizy ryzyka, co inne obszary*. Jak zobaczysz, istnieje wiele pól o ogromnym ryzyku, minimalnych danych i głęboko chaotycznych podmiotach, które są regularnie modelowane przy użyciu tradycyjnych metod matematycznych. Nie musimy na nowo wymyślać terminologii ani metod, możemy zapożyczyć je z innych dziedzin, które również mają trudne problemy z analizą ryzyka.

- *Te udoskonalone metody są całkowicie wykonalne*. Wiemy o tym, ponieważ już to zrobiono. Obaj autorzy mają bezpośrednie doświadczenie w stosowaniu każdej metody opisanej w tej książce w rzeczywistych środowiskach korporacyjnych. Metody te są obecnie stosowane przez analityków cyberbezpieczeństwa z różnych środowisk w wielu różnych branżach. Prawie wszyscy analitycy, których przeszkoliliśmy w zakresie tych metod, nie mieli doświadczenia w ilościowej analizie ryzyka (tj. statystycy, aktuariusze itp.). To nie jest tylko teoria.
- *Nawet te udoskonalone metody można dalej ulepszać — ciągle.* Masz dostęp do większej ilości danych, niż myślisz, z różnych istniejących i nowo powstających źródeł. Nawet jeśli danych jest mało, metody matematyczne z ograniczonymi danymi mogą nadal być ulepszeniem samej subiektywnej oceny. Nawet same metody analizy ryzyka można mierzyć i śledzić w celu ciągłego doskonalenia.

Dzięki udoskonalonym metodom specjalista ds. cyberbezpieczeństwa może skutecznie określić rodzaj „zwrotu z kontroli" (ang. *return on control*). Możemy ocenić, czy dana strategia obronna lepiej wykorzystuje zasoby niż inna. Krótko mówiąc, możemy mierzyć i monetyzować ryzyko oraz je redukować. Aby to osiągnąć, potrzebujemy tylko poradnika dla profesjonalistów odpowiedzialnych za przydzielanie ograniczonych zasobów do zwalczania stale rosnących zagrożeń cybernetycznych i wykorzystywanie tych zasobów do optymalnej redukcji ryzyka.

Ta książka jest podzielona na trzy części. W części I przedstawię prostą metodę ilościową, która wymaga nieco więcej wysiłku niż obecne metody punktacji, ale wykorzystuje techniki, które wykazały wymierną poprawę oceny. Następnie omówię sposoby mierzenia samych metod pomiarowych. Innymi słowy, spróbujemy odpowiedzieć na pytanie: „Skąd wiemy, że to działa?", dotyczące różnych metod oceny cyberbezpieczeństwa. W ostatnim rozdziale części I przedstawię powszechne zastrzeżenia wobec metod ilościowych, szczegółowo omówię argumenty przeciwko metodom punktacji oraz omówię błędne przekonania i nieporozumienia, które powstrzymują niektórych przed przyjęciem lepszych metod.

W części II przejdziemy od pytania „dlaczego" o używane metody i skupimy się na tym, jak dodać dalsze ulepszenia do prostego modelu opisanego w części I. Porozmawiamy o tym, jak dodać przydatne szczegóły do prostego modelu, o tym, jak poprawić zdolności ekspertów ds. cyberbezpieczeństwa do oceny niepewności, oraz o sposobach ulepszenia modelu za pomocą danych empirycznych (nawet jeśli ilość danych wydaje się ograniczona).

W części III cofniemy się do szerszego obrazu tego, w jaki sposób metody te można wdrożyć w przedsiębiorstwie, w jaki sposób mogą pojawić się nowe zagrożenia oraz w jaki sposób rozwijające się narzędzia i metody mogą jeszcze

bardziej udoskonalić pomiar zagrożeń cyberbezpieczeństwa. Postaramy się opisać wezwanie do działania dla całej branży cyberbezpieczeństwa.

Na początek w następnym rozdziale zbudujemy podstawy tego, jak powinniśmy rozumieć termin „pomiar". Może się to wydawać proste i oczywiste, ale nieporozumienia co do tego terminu i metod wymaganych do wykonania tego, co się za nim kryje, leżą u podstaw przynajmniej części oporu przed stosowaniem pomiarów w cyberbezpieczeństwie.

Powiedzmy jasno, o czym ta książka nie jest. To nie jest książka o bezpieczeństwie technicznym — jeśli szukasz książki o „etycznym hakowaniu", to z pewnością trafiłeś w złe miejsce. Nie będzie dyskusji o tym, jak wykonać przepełnienie stosu, przełamać algorytmy szyfrowania lub wykonać SQL Injection. Jeśli rozmawiamy o takich rzeczach, to tylko w roli parametrów w modelu ryzyka.

Ale nie bądź rozczarowany, jeśli jesteś osobą techniczną. Z pewnością będziemy wchodzić w analityczne szczegóły dotyczące bezpieczeństwa z perspektywy analityka lub lidera, który próbuje przyjąć lepsze założenia co do możliwych przyszłych strat.

---

[1] Wolter, *Poème sur le désastre de Lisbonne* (Wiersz o katastrofie w Lizbonie), 1759.

[2] Stephen Gandel, *Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year*, Fortune.com, 23 stycznia 2015, *http://fortune.com/2015/01/23/cyber-attack-insu*
↪*rance-lloyds/*.

[3] Sue Poremba, *2014 Cyber Security News Was Dominated by the Sony Hack Scandal and Retail Data Breaches*, „Forbes Magazine", 31 grudnia 2014.

[4] Kevin Haley, *The 2014 Internet Security Threat Report: Year of the Mega Data Breach*, „Forbes Magazine", 24 lipca 2014.

[5] Matthew Heller, *Lloyd's Insurer Says Cyber Risks Too Big to Cover*, CFO.com, 6 lutego 2015.

[6] Risk Based Security, *2021 Year End Data Breach QuickView Report*, luty 2022.

[7] National Association of Insurance Commissioners, Memorandum to Property and Casualty Insurance Committee, *Report on the Cybersecurity Insurance Market*, 20 października 2021.

[8] Andrea Vittorio, *Merck's $1.4 Billion Insurance Win Splits Cyber from „Act of War"*, „Bloomberg Law", 19 stycznia 2022.

[9] Daphne Zhang, *Lloyd's Cyber Insurance Tweaks Stir Coverage Restriction Concern*, „Bloomberg Law", 26 sierpnia 2022.

[10] Stephen Northcutt, *The Attack Surface Problem*, SANS.edu. 7 stycznia 2011, *www.sans.edu/research/security-laboratory/article/did-attack-surface, https://nprofit.net/pl/co-to-jest-i-jak-wykorzystac-wayback-machine-archive-org/*.

[11] Pratyusa K. Manadhata i Jeannette M. Wing, *An Attack Surface Metric*, „IEEE Transactions on Software Engineering 37", no. 3 (2010): 371 – 386.

[12] Matthew J. Schwartz, *Target Ignored Data Breach Alarms*, Dark Reading (blog), „InformationWeek", 14 marca 2014, *www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712*.

[13] DataReportal.com, *Digital 2022 April Global Statshot*, 21 kwietnia 2022.
[14] Jim Bird i Jim Manico, *Attack Surface Analysis Cheat Sheet*, OWASP.org, 18 lipca 2015.
[15] Mayumi Brewster, *Annual Retail Trade Survey Shows Impact of Online Shopping on Retail Sales During Covid-19 Pandemic*, United States Census Bureau, 27 kwietnia 2022.
[16] *Top Cybersecurity Statistics, Trends, and Facts*, CSO Online, październik 2021.
[17] Alissa Ponchione, *CISOs: The CFOs of IT*, CFO, 7 listopada 2013.
[18] *List of Fortune 500 Chief Information Security Officers*, „Cybercrime Magazine", 2022.
[19] Deloitte, *Reshaping the Cybersecurity Landscape*, lipiec 2020.
[20] OWASP, *OWASP Risk Rating Methodology*, ostatnia modyfikacja: 3 września 2015.

Lord Kelvin powtarzał, że jeśli nie potrafisz czegoś zmierzyć, to nie znasz tego wystarczająco dobrze. Ta zasada w pełni odnosi się do analizy ryzyka w cyberbezpieczeństwie, a słabość pomiarów prowadzi do podejmowania błędnych decyzji.

Ta książka nauczy Cię nowych sposobów myślenia o problemie. Uważam, że jest lekturą obowiązkową dla naszej dziedziny!

— **John „Four" Flynn,** CISO Amazon Stores

Oto drugie wydanie książki, którą specjaliści CISO uznali za przełomową. Dowiesz się z niej, jak kwantyfikować niepewność i jak za pomocą prostych metod i narzędzi poprawić ocenę ryzyka w nowoczesnych organizacjach. Znalazły się tu nowe techniki modelowania, pomiaru i szacowania, a także mnóstwo praktycznych wskazówek dotyczących wdrażania tych rozwiązań w formie spójnego programu. Nauczysz się też oceniać ryzyko, gdy masz dostęp do niewielu danych. Przekonasz się, że zamiast metod jakościowych dużo lepsze efekty w zarządzaniu ryzykiem cyberbezpieczeństwa osiąga się dzięki kwantyfikacji i zaplanowanym pomiarom.

Ta książka umożliwia pewne poruszanie się w złożonym krajobrazie cyberbezpieczeństwa.

— **Jason Chan,** były wiceprezes do spraw bezpieczeństwa informacji, Netflix

---

Douglas W. Hubbard jest wynalazcą metody Applied Information Economics (AIE) i założycielem firmy Hubbard Decision Research, a także uznanym ekspertem w dziedzinie nauki o decyzjach.

Richard Seiersen jest dyrektorem do spraw ryzyka w firmie Resilience. Zajmuje się modelowaniem i pomiarami ryzyka cybernetycznego. Był współzałożycielem firmy Soluble, specjalizującej się w bezpieczeństwie natywnym dla chmury.

Opisane przez Hubbarda i Seiersena metody są praktyczne. Każdy, kto zajmuje się cyberbezpieczeństwem, powinien je stosować.

— **Nick Shevelyov,** były CISO banku Silicon Valley

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0594-8
9 788328 905948
Cena: 87,00 zł
WILEY