Zarządzanie oprogramowaniem: imperatyw bezpieczeństwa, możliwości biznesowe

BSA GLOBAL SOFTWARE SURVEY

CZERWCA 2018

SPIS TREŚCI

Wstęp

Na całym świecie oprogramowanie stało się jednym z najpowszechniejszych i niezbędnych narzędzi stosowanych przez firmy w najbardziej podstawowych, codziennych zadaniach – od zarządzania procesami sprzedaży, prowadzenia ksiąg, planowania strategii rynkowej, komunikacji z klientami i współpracy z partnerami po zwiększanie wydajności. Wraz z przełomowymi postępami zwiększającymi możliwości oprogramowania, organizacje coraz częściej używają go jako katalizatora usprawnień prowadzonej działalności, wzrostu obrotów i zysków, zdobywania nowych rynków i uzyskiwania przewagi konkurencyjnej.

Zbyt często jednak starania użytkowników w kierunku opanowania nowatorskich technologii są hamowane przez niszczące zagrożenia bezpieczeństwa, takie jak narażenie na działanie złośliwego oprogramowania (malware). Coraz bardziej oczywiste jest, że infekcje złośliwym oprogramowaniem są ściśle związane z korzystaniem z oprogramowania nielicencjonowanego. W efekcie wielu CIO zaczyna rozumieć, jakie są rzeczywiste koszty korzystania z nielicencjonowanego oprogramowania i podejmuje pragmatyczne kroki w celu usprawnienia procesów zarządzania posiadanymi zasobami.

Aby lepiej poznać te wpływy i możliwości, organizacja BSA, we współpracy z IDC, przeprowadziła ogólnoświatowe badanie Global Software Survey mające na celu ocenę ilości i wartości nielicencjonowanego oprogramowania zainstalowanego na komputerach osobistych w ponad 110 krajowych i regionalnych gospodarkach. Wyniki wskazują, że – mimo że CIO są świadomi zagrożeń bezpieczeństwa stwarzanych przez nielicencjonowane oprogramowanie – 37 procent oprogramowania zainstalowanego na komputerach osobistych to oprogramowanie nielicencjonowane.

NAJWAŻNIEJSZE TRENDY I WNIOSKI

- Stosowanie nielicencjonowanego oprogramowania, choć na nieco mniejszą skalę, jest nadal powszechne.
- CIO uważają nielicencjonowane oprogramowanie za coraz bardziej ryzykowne i coraz kosztowniejsze.
- Zwiększanie ilości legalnego oprogramowania pobudza gospodarkę i jest warunkiem koniecznym bezpieczeństwa.
- Organizacje mogą obecnie podejmować znaczące kroki w kierunku usprawnienia zarządzania oprogramowaniem i osiągnięcia istotnych zysków.

Z raportu jasno wynika zatem, że w erze podwyższonego zagrożenia cyberbezpieczeństwa organizacje muszą wykonać najważniejszy pierwszy krok, czyli ocenić zasoby wykorzystywane w swoich sieciach i wyeliminować nielicencjonowane oprogramowanie. W ten sposób mogą zmniejszyć zagrożenie szkodliwymi cyberatakami i poprawić wyniki finansowe.

Ta pogłębiona analiza korzystania z nielicencjonowanego oprogramowania pokazuje, że firmy, które wdrażają zdecydowane działania mające na celu usprawnienie sposobu zarządzania oprogramowaniem, mają teraz potężne nowe narzędzie ograniczania zagrożeń bezpieczeństwa, poprawiania wyników finansowych, skracania przestojów oraz zapewniające możliwości wzrostu.

NAJWAŻNIEJSZE WNIOSKI

Korzystanie z nielicencjonowanego oprogramowania, choć na nieco mniejszą skalę, jest nadal powszechne. Mimo spadku światowego wskaźnika instalacji nielicencjonowanego oprogramowania o dwa punkty w ostatnich dwóch latach, jest ono nadal używane na całym świecie w alarmujących ilościach, stanowiąc 37 procent oprogramowania zainstalowanego na komputerach osobistych. Choć ogólna wartość rynkowa nielicencjonowanego oprogramowania również zmalała, to wskaźniki jego wykorzystywania w większości krajów objętych badaniem nadal wynoszą 50 procent lub więcej. Tak wysokie wskaźniki nie tylko ograniczają lokalne korzyści gospodarcze związane z korzystaniem z możliwości rozwijającej się technologii, ale też hamują wzrost wyników finansowych firm i wywołują bezprecedensowe zagrożenie bezpieczeństwa.

CIO uważają nielicencjonowane oprogramowanie za coraz bardziej ryzykowne i coraz kosztowniejsze. Organizacjom grozi obecnie prawdopodobieństwo jak jeden do trzech napotkania złośliwego oprogramowania, gdy nabywają lub instalują pakiet oprogramowania nielicencjonowanego lub kupują komputer z preinstalowanym nielicencjonowanym oprogramowaniem. Każdy atak złośliwego oprogramowania może kosztować firmę przeciętnie 2,4 miliona USD, a wyeliminowanie skutków ataku może zająć nawet 50 dni. W zakresie, w którym infekcja prowadzi do przestoju firmy lub utraty danych biznesowych, może również poważnie wpłynąć na jej markę i reputację. Koszt postępowania ze złośliwym oprogramowaniem, które jest w związku z oprogramowaniem nielicencjonowanym, również rośnie. Aktualnie może to kosztować firmę ponad 10 000 USD za każdy zainfekowany komputer, a roczny koszt ponoszony przez firmy na całym świecie to niemal 359 miliardów USD. Unikanie zagrożeń bezpieczeństwa związanych ze złośliwym oprogramowaniem jest aktualnie najważniejszym powodem, dla którego CIO decydują się na instalowanie w swoich sieciach jedynie licencjonowanego oprogramowania.

Większa ilość legalnego oprogramowania pobudza gospodarkę i jest warunkiem koniecznym bezpieczeństwa. Wraz z rosnącym kosztem eliminacji skutków działania złośliwego oprogramowania szefowie firm coraz częściej decydują się na korzystanie wyłącznie z licencjonowanego oprogramowania, do którego można w ramach aktualizacji instalować poprawki stanowiące główną linię obrony przed niszczącymi atakami złośliwego oprogramowania, naruszeniami integralności danych i innymi zagrożeniami bezpieczeństwa. Coraz więcej szefów firm zaczyna także rozumieć, że zwiększenie zdolności zarządzania zasobami oprogramowania w całej organizacji może być potężnym, nowym narzędziem, umożliwiającym skrócenie przestojów i znaczne poprawienie wyników finansowych. IDC szacuje, że dzięki podjęciu pragmatycznych kroków w kierunku usprawnienia zarządzania zasobami oprogramowania, firmy mogą poprawić wyniki finansowe aż o 11 procent.

Organizacje mogą obecnie podejmować znaczące kroki w kierunku usprawnienia procesów zarządzania zasobami oprogramowania i w efekcie osiągnąć istotne zyski. Aby uzyskać dostęp do tych korzyści, organizacje mogą wdrożyć najlepsze praktyki i sprawdzone rozwiązania do zarządzania zasobami oprogramowania SAM (Software Asset Management) w celu usprawnienia tego procesu i zwiększenia stopy zwrotu z wykorzystywanych technologii. SAM umożliwia CIO nie tylko zapewnienie pełnej legalności i zgodności licencyjnej oprogramowania wykorzystywanego w ich sieciach, ale może też ograniczyć niszczący wpływ cyberzagrożeń, zwiększyć wydajność, ograniczyć przestoje, scentralizować zarządzanie licencjami i zmniejszyć koszty. Badania wykazują, że wdrażając niezawodne rozwiązania SAM wraz z programem optymalizacji polityki licencyjnej, organizacje mogą osiągnąć aż 30-procentowe oszczędności w ramach rocznych kosztów ponoszonych na oprogramowanie.[1]

Złośliwe oprogramowanie jest coraz bardziej powszechne, kosztowne i niszczące w skutkach

Konsumenci, firmy i kraje na całym świecie coraz częściej przekonują się, że ich starania mające na celu wykorzystanie aktualnych możliwości i potencjału nowych technologii skutecznie hamują poważne zagrożenia stwarzane przez złośliwe oprogramowanie. Poziom zagrożenia złośliwym oprogramowaniem pozostaje wysoki – w każdej sekundzie każdego dnia pojawia się osiem nowych zagrożeń.[2] Wzrostowi częstotliwości towarzyszy wzrost oddziaływania – zagrożenia są coraz bardziej kosztowne i niszczące.

Liczba ataków złośliwego oprogramowania rośnie nieustannie w postępie wykładniczym, zarówno pod względem liczby jak i wyrafinowania.[3] Na przykład, w 2016 roku doszło do 15 naruszeń integralności danych, obejmujących 10 milionów danych personalnych. To niemal dwa razy więcej niż w 2013 roku.[4] Ataki są wymierzone nie tylko w wielkie przedsiębiorstwa, dotykają również konsumentów i przedsiębiorstwa każdej wielkości. W 2015 roku aż 43 procent cyberataków było wymierzonych w małe firmy zatrudniające mniej niż 250 pracowników.[5] Aktualnie cyberprzestępcy wzięli także na cel sieci komórkowe. Liczba odmian złośliwego oprogramowania na urządzeniach mobilnych wzrosła w zeszłym roku o 54 procent – do 24 000 złośliwych aplikacji mobilnych blokowanych każdego dnia.[6]

Ataki te stają się także coraz bardziej kosztowne. Atak złośliwego oprogramowania kosztuje firmę przeciętnie 2,4 miliona USD.[7] Każda infekcja może prowadzić do kosztownego przestoju, utraty zdolności produkcyjnych, utraty możliwości prowadzenia działalności oraz dodatkowych kosztów pracy specjalistów IT niezbędnej do wyeliminowania skutków ataku. W zakresie, w którym infekcja prowadzi do przestoju lub utraty danych biznesowych firmy, może także poważnie wpłynąć na jej markę i reputację. Co gorsza, koszt ekonomiczny takich infekcji stale rośnie – o 20 procent od 2014 roku. Działania związane ze złośliwym oprogramowaniem kosztują obecnie gospodarkę światową zaskakującą kwotę 600 miliardów USD rocznie czyli 0,8 procent światowego PKB.[8]

Sprawę dodatkowo komplikuje fakt, że ataki te są często trudne do wykrycia i wyeliminowania. Organizacja wykrywa atak złośliwego oprogramowania przeciętnie po 243 dniach,[9] a wyeliminowanie jego skutków może zająć nawet 50 dni.[10]

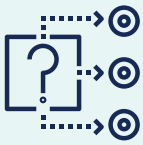
(ciąg dalszy na stronie 5)

Poziom zagrożenia złośliwym oprogramowaniem utrzymuje się nieustannie na wysokim poziomie. W każdej sekundzie każdego dnia pojawia się osiem nowych zagrożeń.

SKUTKI ZŁOŚLIWEGO OPROGRA-MOWANIA

Organizacjom grozi obecnie prawdopodobieństwo jak jeden do trzech napotkania złośliwego oprogramowania, gdy nabywają lub instalują oprogramowanie nielicencjonowane.

Opanowanie skutków złośliwego oprogramowania związanego z oprogramowaniem nielicencjonowanym może kosztować więcej niż 10 000 USD za każdy zainfekowany komputer, dając łączną światową kwotę przekraczającą 359 miliardów USD.



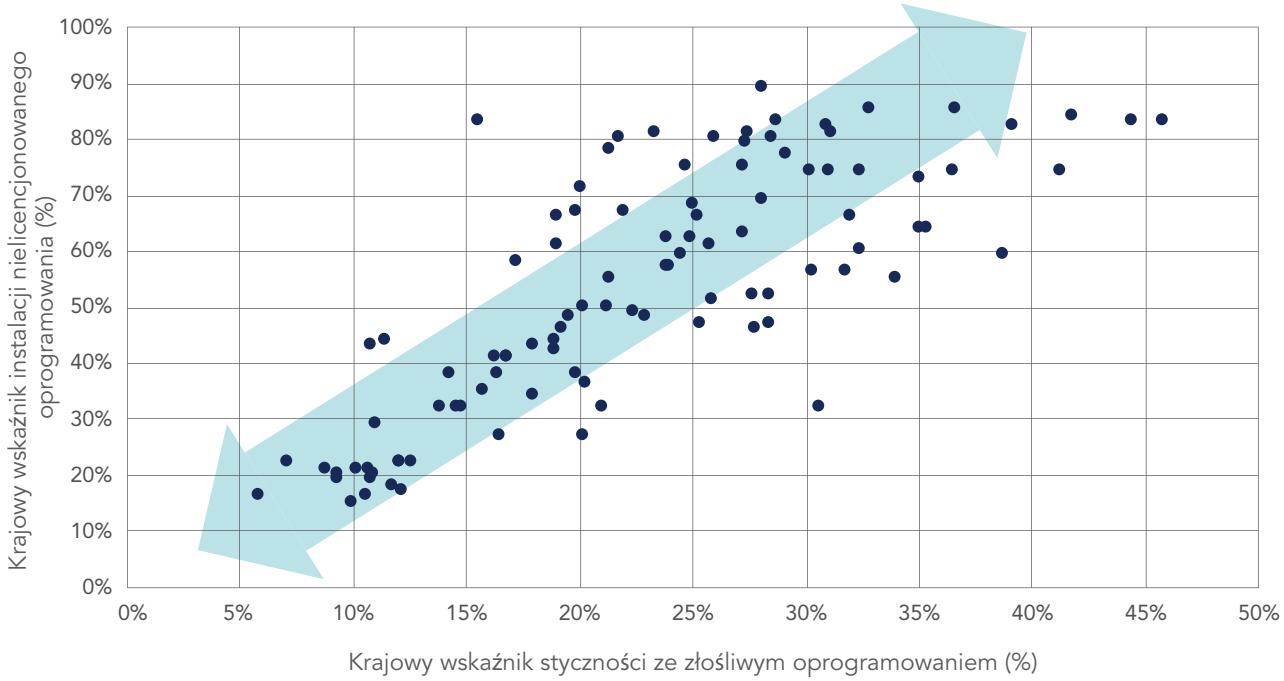
Użytkownicy to widzą: 68 procent użytkowników komputerów i 48 procent CIO uznało złośliwe oprogramowanie za jeden z trzech najważniejszych powodów niekorzystania z nielicencjonowanego oprogramowania.

Najważniejsze obawy CIO dotyczące zagrożeń związanych ze złośliwym oprogramowaniem będącym w silnej korelacji z oprogramowaniem nielicencjonowanym, to obawa o utratę danych firmowych lub osobowych, przestoje systemów, awarie sieci oraz koszt usuwania skutków infekcji systemów.

Liczba CIO wykorzystujących formalne, pisemne zasady dotyczące stosowania licencjonowanego oprogramowania w celu łagodzenia skutków takich ataków znacznie wzrosła (z 41 procent w 2015 do 54 procent w tym roku. Mimo to, tylko 35 procent pracowników ma świadomość tych formalnych, pisemnych zasad, co sugeruje występowanie krytycznej luki w edukacji.

Organizacje podejmujące aktywne działania w tym zakresie przekonują się, że 20-procentowy wzrost legalności oprogramowania potrafi zwiększyć zyski firmy o 11 procent, czyli o ponad pół miliona USD w przypadku przeciętnej wielkości firm objętych badaniem.

Nielicencjonowane oprogramowanie i ataki złośliwego oprogramowania są ze sobą ściśle związane



Źródło: IDC

INFEKCJE ZŁOŚLIWYM OPROGRAMOWANIEM SĄ ZWIĄZANE Z OPROGRAMOWANIEM NIELICENCJONOWANYM

Coraz bardziej oczywistym jest, że infekcje złośliwym oprogramowaniem są ściśle związane z korzystaniem z oprogramowania nielicencjonowanego. Im większy wskaźnik nielicencjonowanego oprogramowania w użyciu, tym większe prawdopodobieństwo niszczycielskiej infekcji złośliwym oprogramowaniem.

Bez względu na to powiązanie, nielicencjonowane oprogramowanie nadal rozprzestrzenia się w alarmującym tempie. Znaczna część oprogramowania używanego na całym świecie jest nielicencjonowana. W czterech z sześciu regionów – w Europie Środkowej i Wschodniej, na Bliskim Wschodzie i w Afryce, a także w Ameryce Łacińskiej oraz w regionie Azja-Pacyfik – większość oprogramowania zainstalowanego na komputerach osobistych to oprogramowanie nielicencjonowane. (Patrz strony 12–13).

Powiązanie między nielicencjonowanym a złośliwym oprogramowaniem, które powoduje infekcje, stwarza ogromne cyberzagrożenie. IDC szacuje, że organizacjom grozi obecnie prawdopodobieństwo jak jeden do trzech (29 procent) napotkania złośliwego oprogramowania, gdy nabywają lub instalują pakiet nielicencjonowanego oprogramowania lub kupują komputer z preinstalowanym nielicencjonowanym oprogramowaniem.

Analiza statystyczna potwierdza to powiązanie. W krajach na całym świecie konsekwentnie występuje silna korelacja (r-0,78) pomiędzy korzystaniem z nielicencjonowanego oprogramowania a napotykaniem oprogramowania złośliwego. Wskaźnik nielicencjonowanego oprogramowania w danym kraju to w istocie niezawodny predyktor wskaźnika infekcji oprogramowaniem złośliwym.

CIO rozumieją to powiązanie. Na prośbę o uszeregowanie najważniejszych korzyści ze skutecznego zarządzania licencjami do oprogramowania i poprawy wskaźnika jego legalności, 54 procent CIO wskazuje na mniejsze zagrożenie bezpieczeństwa jako główny powód zapewnienia wykorzystywanemu przez nich oprogramowaniu właściwego licencjonowania.

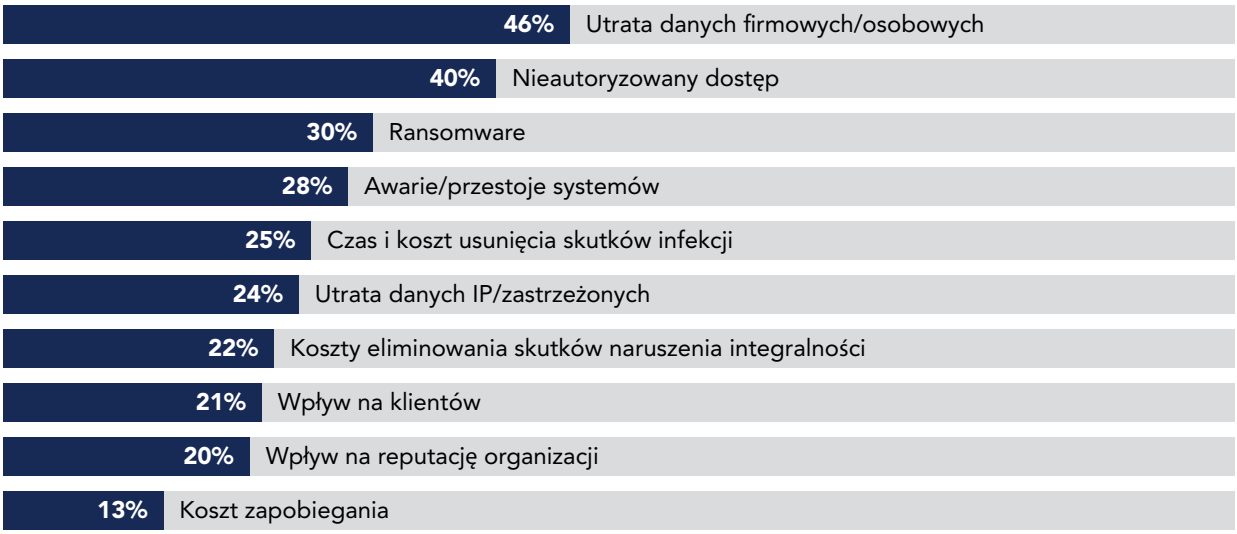
Powiązanie między złośliwym a nielicencjonowanym oprogramowaniem nie bez powodu jest dla CIO istotne. Z własnych doświadczeń znają oni niszczące skutki infekcji złośliwym oprogramowaniem. CIO biorący udział w badaniu twierdzą, że w związku ze złośliwym oprogramowaniem, które może towarzyszyć oprogramowaniu nielicencjonowanemu, ich główną obawą jest kradzież danych (46 procent). Niemal równie mocno obawiają się nieautoryzowanego dostępu do ich sieci (40 procent), konieczności zareagowania na możliwy atak przy użyciu oprogramowania ransomware (30 procent), awarii systemu i przestojów (28 procent) oraz czasochłonnego i kosztownego eliminowania

Najważniejsze zalety ścisłego przestrzegania polityki licencyjnej do oprogramowania zdaniem CIO

infekcji z sieci (25 procent). Zdają sobie przy tym sprawę z faktu, że nie są to pojedyncze przypadki. Jedno na pięć przedsiębiorstw (19 procent) biorących udział w badaniu zgłosiło występowanie przestojów w pracy sieci, witryn internetowych lub komputerów co kilka miesięcy lub częściej. Najczęstszą przyczyną awarii związanych z bezpieczeństwem było złośliwe oprogramowanie na komputerach użytkowników końcowych (56 procent), co czyni oprogramowanie nielicencjonowane ważnym wektorem ataku.

Jak wskazano powyżej, oddziaływania te mogą mieć niszczące skutki. Opanowanie cyberataku i jego następstw może kosztować firmę ponad 10 000 USD za każdy zainfekowany komputer, czyli o rząd wielkości więcej niż koszt uzyskania licencjonowanych wersji oprogramowania i o wiele więcej niż koszt samego komputera. IDC szacuje, że złośliwe oprogramowanie związane z oprogramowaniem nielicencjonowanym kosztuje firmy 360 miliardów USD rocznie.

Najważniejsze obawy przedsiębiorstw dotyczące skutków działania złośliwego oprogramowania pochodzącego z oprogramowania nielicencjonowanego



ZAGROŻENIA STWARZANE PRZEZ ZŁOŚLIWE OPROGRAMOWANIE MOGĄ SIĘ PRZEKŁADAĆ NA POWAŻNE PROBLEMY W ŚWIECIE RZECZYWISTYM

Brak profesjonalnego zarządzania zasobami oprogramowania SAM i używanie oprogramowania nielicencjonowanego ma ogromny, niekorzystny wpływ na bezpieczeństwo na całym świecie, zwłaszcza w krajach o wysokim wskaźniku korzystania z nielicencjonowanego oprogramowania. Na przykład:

- **Chiny**, w których aż 66 procent oprogramowania jest wykorzystywana bez właściwych licencji, przeżyły nieproporcjonalnie niszczące ataki złośliwego oprogramowania, które dotknęły około 40 000 instytucji w tym kraju. Zaledwie jeden atak złośliwego oprogramowania przeszedł przez pozbawione uaktualnień, nielicencjonowane oprogramowanie tak gwałtownie, że osłabił prestiżowe instytucje naukowe, takie jak Uniwersytet Tsinghua. Ponadto, zatrzymał działanie elektronicznych systemów płatniczych na stacjach benzynowych PetroChina w całym kraju, wyłączył bankomaty Bank of China i zakłócił działanie tak wielkich firm jak China Telecom i Hainan Airlines. Fińska firma F-Secure specjalizująca się w cyberzabezpieczeniach informuje, że do skali i głębokości skutków niszczycielskiego ataku w Chinach przyczyniła się ogromna liczba komputerów z nielicencjonowanym oprogramowaniem.[11] Jak wskazuje starszy inżynier sieci jednego z dostawców rozwiązań technologicznych z siedzibą w Pekinie – „większość ofiar w Chinach to użytkownicy nielicencjonowanego oprogramowania".[12]

- **Rosja**, w której 62-procentowy wskaźnik nielicencjonowanego oprogramowania odpowiada gigantycznej wartości handlowej w wysokości 1,2 miliarda USD, także niedawno przeszła niszczące w skutkach ataki złośliwego oprogramowania. W 2017 roku ataki złośliwego oprogramowania obezwładniły rosyjskie Ministerstwo Zdrowia, rosyjskie Koleje Państwowe, Ministerstwo Spraw Wewnętrznych zarządzające siłami Policji oraz firmę telekomunikacyjną Megafon. Starszy badacz w Instytucie Stosunków Międzynarodowych w Pradze wskazuje, że szeroki zasięg infekcji złośliwym oprogramowaniem w Rosji wynikł „nie z używania nieaktualizowanego oprogramowania, tylko z faktu korzystania z nieaktualizowanego pirackiego oprogramowania".[13]

Zasięg i skala oddziaływania tych zagrożeń powinna stanowić sygnał alarmowy dla wszystkich, którzy krytyczne funkcje biznesowe opierają na nielicencjonowanym oprogramowaniu, nie mają narzędzi do profesjonalnego zarządzania zasobami oprogramowania SAM lub korzystają z usług innych osób lub firm zagrożonych złośliwym oprogramowaniem związanym z oprogramowaniem nielicencjonowanym.

Zwiększanie udziału legalnego oprogramowania pobudza gospodarkę i stało się warunkiem koniecznym bezpieczeństwa.

Zarządzanie zasobami oprogramowania SAM może ograniczyć te cyberzagrożenia i poprawić wyniki finansowe

Możliwość ograniczenia cyberzagrożeń poprzez stosowanie jedynie licencjonowanego oprogramowania jest oczywista. Istnieje także odpowiednia norma międzynarodowa w tym zakresie. Niedawne aktualizacje standardu SAM Międzynarodowej Organizacji Normalizacyjnej (ISO) zapewniają podstawę ogólnego zarządzania zasobami IT (ITAM) z oprogramowaniem włącznie.[14]

Jak pokazuje niedawny przykład, wdrożenie rozwiązań SAM zgodnych z normą ISO stanowi potężne narzędzie do poprawy poziomu zabezpieczeń. W Stanach Zjednoczonych firma Equifax doprowadziła do jednego z największych w historii naruszeń integralności danych, ponieważ nie zainstalowała na jednym z serwerów aktualizacji eliminującej znaną od miesięcy lukę w zabezpieczeniach. Kosztowało to firmę około 439 milionów USD, a także zmusiło CEO i CIO do rezygnacji ze swoich stanowisk.[15] Specjaliści informują, że gdyby firma zastosowała rozwiązania SAM do śledzenia wszystkich przypadków wystąpień zagrożonego oprogramowania Apache, naruszenia integralności danych można było uniknąć.[16] Minimalizacja zagrożeń związanych ze złośliwym oprogramowaniem poprzez korzystanie jedynie z oprogramowania licencjonowanego jest niezbędna. Jednak jak dowodzi powyższy przypadek, rozwiązania SAM są konieczne nawet w firmie używającej w pełni licencjonowanego oprogramowania.

Zapewniając stosowanie jedynie licencjonowanego oprogramowania zoptymalizowanego odpowiednio do potrzeb firmy, SAM przynosi dodatkowe korzyści w postaci skróconych przestojów i oszczędności, mających swoje odbicie w wynikach finansowych. SAM umożliwia także firmom optymalne wykorzystanie posiadanych zasobów poprzez zapewnienie stosowania oprogramowania najlepiej spełniającego potrzeby firmy, a także wykorzystanie nowych technologii, takich jak usługi oferowane w chmurze. Wszystko to zwiększa efektywność organizacji i zmniejsza koszty. Badania wykazują, że wdrażając niezawodne rozwiązania SAM organizacje mogą osiągnąć aż 30-procentowe oszczędności w ramach rocznych kosztów ponoszonych na oprogramowanie.[17]

To badanie dowodzi także, że SAM jest korzystną inwestycją. Na podstawie informacji podanych przez respondentów firma IDC wyliczyła, że wystarczy zwiększyć wskaźnik legalności o zaledwie 20 procent (zmniejszając na przykład wskaźnik nielicencjonowanego oprogramowania z 24 do 19 procent), aby przedsiębiorstwo o rocznych przychodach w wysokości 83 milionów USD (jest to średnia w tym badaniu) mogło zwiększyć zyski aż o 11 procent. Te wymierne korzyści finansowe są szacowane jako 29 razy większe niż koszt wymiany nielicencjonowanego oprogramowania, niezbędnej do zwiększenia wskaźnika legalności o 20 procent.[18]

PRZYKŁADY ZE ŚWIATA RZECZYWISTEGO

W Niemczech:

OSI International Foods, firma zatrudniająca ponad 12 000 pracowników, zmniejszyła koszty policencyjne o ponad 30 procent dzięki wdrożeniu sprawniejszego modelu polityki licencyjnej do oprogramowania.[19]

W Rosji:

Baltika Breweries to czołowy rosyjski producent piwa, posiadający osiem browarów i korzystający zarówno z usług fizycznych, jak i opartych na chmurze. Firma wdrożyła SAM w celu zoptymalizowania infrastruktury IT. Dzięki przeniesieniu aplikacji biznesowych do chmury oszczędza 100 000 USD rocznie.[20]

W Wielkiej Brytanii:

University of Roehampton w Londynie wdrożył SAM w celu stworzenia planu identyfikacji zarówno starszego, nieużywanego już oprogramowania, jak i oprogramowania ze zbyt dużą ilością licencji. Dzięki temu możliwe było zrealizowanie planu inwestycji oszczędności w nowsze, bezpieczniejsze technologie o większych możliwościach. W czasie trwania projektu przewidywane jest zaoszczędzenie aż 5 milionów USD.[21]

W USA:

Na SAM skorzystać mogą także agencje rządowe i instytucje. Na przykład, agencja NASA zaoszczędziła przez sześć lat ponad 100 milionów USD dzięki wdrożeniu w swoich oddziałach sprawdzonych rozwiązań SAM.[22] Niewielkim nakładem pracy NASA była w stanie osiągnąć olbrzymie korzyści z cyfrowej transformacji swoich działań, oszczędzając przy tym pieniądze podatników.

RZĄDY MOGĄ PODJĄĆ PRAGMATYCZNE KROKI W CELU ZWIĘKSZENIA KORZYŚCI PŁYNĄCYCH Z OPROGRAMOWANIA

Oprócz kroków, które mogą i powinny podejmować organizacje, także w zasięgu rządów znajduje się zestaw zgodnych z rozsądkiem, konkretnych działań, które można podjąć, aby zmniejszyć wskaźnik nielicencjonowanego oprogramowania i zapewnić większą energię krajowej gospodarce. Proaktywne wysiłki podejmowane przez rząd (opisane bardziej szczegółowo na stronie 15) obejmują dawanie dobrego przykładu, usprawnianie państwowego systemu zarządzania zasobami oprogramowania i upewnianie się, że wykonawcy zleceń rządowych także korzystają jedynie z autoryzowanego oprogramowania.

Aby ułatwić rządom podjęcie takich działań, BSA przygotowała praktyczny poradnik, z którego mogą skorzystać w celu usprawnienia procesów zarządzania zasobami oprogramowania.[23] Dając jasny sygnał, że rząd będzie korzystać jedynie z legalnego oprogramowania i robić interesy tylko z wykonawcami postępującymi w ten sam sposób, państwo wysyła wyraźny przekaz, który może katalizować działania zarówno w sektorze publicznym, jak i prywatnym.

WSKAŹNIKI I WARTOŚĆ RYNKOWA INSTALACJI NIELICENCJONOWANEGO OPROGRAMOWANIA NA KOMPUTERACH OSOBISTYCH

	WSKAŹNIKI INSTALACJI NIELICENCJONOWANEGO OPROGRAMOWANIA				WARTOŚĆ RYNKOWA NIELICENCJONOWANEGO OPROGRAMOWANIA (W MLN USD)			
	2017	2015	2013	2011	2017	2015	2013	2011
AZJA-PACYFIK								
Australia	18%	20%	21%	23%	540	579	743	763
Bangladesz	84%	86%	87%	90%	226	236	197	147
Brunei	64%	66%	66%	67%	18	19	13	25
Chiny	66%	70%	74%	77%	6842	8657	8767	8902
Hongkong	38%	41%	43%	43%	277	320	316	232
Indie	56%	58%	60%	63%	2474	2684	2911	2930
Indonezja	83%	84%	84%	86%	1095	1145	1463	1467
Japonia	16%	18%	19%	21%	982	994	1349	1875
Malezja	51%	53%	54%	55%	395	456	616	657
Nowa Zelandia	16%	18%	20%	22%	62	66	78	99
Pakistan	83%	84%	85%	86%	267	276	344	278
Filipiny	64%	67%	69%	70%	388	431	444	338
Singapur	27%	30%	32%	33%	235	290	344	255
Korea Południowa	32%	35%	38%	40%	598	657	712	815
Sri Lanka	77%	79%	83%	84%	138	163	187	86
Tajwan	34%	36%	38%	37%	254	264	305	293
Tajlandia	66%	69%	71%	72%	714	738	869	852
Wietnam	74%	78%	81%	81%	492	598	620	395
Pozostałe A-P	87%	87%	91%	91%	442	491	763	589
ŁĄCZNIE A-P	**57%**	**61%**	**62%**	**60%**	**16 439**	**19 064**	**21 041**	**20 998**
EUROPA ŚRODKOWA I WSCHODNIA								
Albania	74%	73%	75%	75%	10	10	10	6
Armenia	85%	86%	86%	88%	17	18	26	26
Azerbejdżan	81%	84%	85%	87%	50	90	103	67
Białoruś	82%	85%	86%	87%	59	76	173	87
Bośnia	61%	63%	65%	66%	24	24	21	15
Bułgaria	57%	60%	63%	64%	72	78	101	102
Chorwacja	50%	51%	52%	53%	48	49	64	74
Czechy	32%	33%	34%	35%	149	150	182	214
Estonia	41%	42%	47%	48%	16	16	20	25
FYROM	63%	64%	65%	66%	15	15	19	22
Gruzja	81%	84%	90%	91%	22	25	40	52
Węgry	36%	38%	39%	41%	104	107	127	143
Kazachstan	74%	73%	74%	76%	62	89	136	123
Łotwa	48%	49%	53%	54%	22	23	29	32
Litwa	50%	51%	53%	54%	35	37	47	44
Mołdawia	83%	86%	90%	90%	35	36	57	45
Czarnogóra	74%	76%	78%	79%	6	6	7	7
Polska	46%	48%	51%	53%	415	447	563	618
Rumunia	59%	60%	62%	63%	151	161	208	207
Rosja	62%	64%	62%	63%	1291	1341	2658	3227
Serbia	66%	67%	69%	72%	51	54	70	104
Słowacja	35%	36%	37%	40%	51	55	67	68
Słowenia	41%	43%	45%	46%	28	30	41	51
Ukraina	80%	82%	83%	84%	108	129	444	647
Pozostałe EŚW	86%	87%	89%	90%	69	70	105	127
ŁĄCZNIE EŚW	**57%**	**58%**	**61%**	**62%**	**2910**	**3136**	**5318**	**6133**
AMERYKA ŁACIŃSKA								
Argentyna	67%	69%	69%	69%	308	554	950	657
Boliwia	79%	79%	79%	79%	94	98	95	59
Brazylia	46%	47%	50%	53%	1665	1770	2851	2848
Chile	55%	57%	59%	61%	283	296	378	382
Kolumbia	48%	50%	52%	53%	241	281	396	295
Kostaryka	58%	59%	59%	58%	80	90	98	62
Dominikana	75%	76%	75%	76%	74	84	73	93
Ekwador	68%	68%	68%	68%	132	137	130	92
Salwador	80%	81%	80%	80%	61	63	72	58
Gwatemala	78%	79%	79%	79%	165	169	167	116
Honduras	75%	75%	74%	73%	32	36	38	24
Meksyk	49%	52%	54%	57%	760	980	1211	1249
Nikaragua	81%	82%	82%	79%	20	23	23	9
Panama	71%	72%	72%	72%	112	117	120	74
Paragwaj	83%	84%	84%	83%	76	89	115	73
Peru	62%	63%	65%	67%	190	210	249	209
Urugwaj	67%	68%	68%	68%	51	57	74	85
Wenezuela	89%	88%	88%	88%	317	402	1030	668
Pozostałe AŁ	82%	83%	84%	84%	296	331	352	406
ŁĄCZNIE AŁ	**52%**	**55%**	**59%**	**61%**	**4957**	**5787**	**8422**	**7459**

	WSKAŹNIKI INSTALACJI NIELICENCJONOWANEGO OPROGRAMOWANIA				WARTOŚĆ RYNKOWA NIELICENCJONOWANEGO OPROGRAMOWANIA (W MLN USD)			
	2017	2015	2013	2011	2017	2015	2013	2011
BLISKI WSCHÓD I AFRYKA								
Algieria	82%	83%	85%	84%	70	84	102	83
Bahrajn	52%	54%	53%	54%	32	34	27	23
Botswana	80%	79%	79%	80%	22	23	20	16
Kamerun	80%	82%	82%	83%	20	21	9	9
Egipt	59%	61%	62%	61%	64	157	198	172
Irak	85%	85%	86%	86%	107	120	116	172
Izrael	27%	29%	30%	31%	165	161	177	192
Wybrzeże Kości Słoniowej	79%	80%	80%	81%	21	22	24	16
Jordania	55%	56%	57%	58%	32	34	35	31
Kenia	74%	76%	78%	78%	99	113	128	85
Kuwejt	57%	58%	58%	59%	86	94	97	72
Liban	69%	70%	71%	71%	61	65	65	52
Libia	90%	90%	89%	90%	66	65	50	60
Mauritius	52%	54%	55%	57%	6	7	7	7
Maroko	64%	65%	66%	66%	52	57	69	91
Nigeria	80%	80%	81%	82%	123	232	287	251
Oman	60%	60%	60%	61%	56	59	65	36
Katar	47%	48%	49%	50%	64	72	77	62
Reunion	38%	39%	39%	40%	2	2	1	1
Arabia Saudyjska	47%	49%	50%	51%	356	412	421	449
Senegal	74%	75%	77%	78%	12	12	9	9
Republika Południowej Afryki	32%	33%	34%	35%	241	274	385	564
Tunezja	73%	74%	75%	74%	39	49	66	51
Turcja	56%	58%	60%	62%	208	291	504	526
ZEA	32%	34%	36%	37%	210	226	230	208
Jemen	88%	87%	87%	89%	10	11	9	15
Zambia	80%	81%	81%	82%	4	4	3	3
Zimbabwe	89%	90%	91%	92%	7	7	4	4
Pozostałe Afryka	83%	84%	85%	86%	364	419	484	363
Pozostałe BW	85%	84%	85%	87%	478	569	640	536
ŁĄCZNIE BWA	**56%**	**57%**	**59%**	**58%**	**3077**	**3696**	**4309**	**4159**
AMERYKA PÓŁNOCNA								
Kanada	22%	24%	25%	27%	819	893	1089	1141
Portoryko	41%	41%	42%	42%	27	28	27	44
Stany Zjednoczone	15%	17%	18%	19%	8612	9095	9737	9773
ŁĄCZNIE AP	**16%**	**17%**	**19%**	**19%**	**9458**	**10 016**	**10 853**	**10 958**
EUROPA ZACHODNIA								
Austria	19%	21%	22%	23%	121	131	173	226
Belgia	22%	23%	24%	24%	182	190	237	252
Cypr	44%	45%	47%	48%	14	14	19	19
Dania	20%	22%	23%	24%	167	176	224	222
Finlandia	22%	24%	24%	25%	166	171	208	210
Francja	32%	34%	36%	37%	1996	2101	2685	2754
Niemcy	20%	22%	24%	26%	1566	1720	2158	2265
Grecja	61%	63%	62%	61%	173	189	220	343
Islandia	44%	46%	48%	48%	12	10	12	17
Irlandia	29%	32%	33%	34%	79	87	107	144
Włochy	43%	45%	47%	48%	1278	1341	1747	1945
Luksemburg	17%	19%	20%	20%	20	21	30	33
Malta	43%	44%	44%	43%	4	4	5	7
Holandia	22%	24%	25%	27%	448	481	584	644
Norwegia	21%	23%	25%	27%	159	178	248	289
Portugalia	38%	39%	40%	40%	137	145	180	245
Hiszpania	42%	44%	45%	44%	859	913	1044	1216
Szwecja	19%	21%	23%	24%	260	288	397	461
Szwajcaria	21%	23%	24%	25%	399	448	469	514
Wielka Brytania	21%	22%	24%	26%	1421	1935	2019	1943
ŁĄCZNIE EZ	**26%**	**28%**	**29%**	**32%**	**9461**	**10 543**	**12 766**	**13 749**
ŁĄCZNIE NA ŚWIECIE	**37%**	**39%**	**43%**	**42%**	**46 302**	**52 242**	**62 709**	**63 456**
Unia Europejska	**28%**	**29%**	**31%**	**33%**	**9982**	**11 060**	**13 486**	**14 433**
Kraje BRIC*	**60%**	**64%**	**67%**	**70%**	**12 272**	**14 452**	**17 187**	**17 907**

***Kraje BRIC: Brazylia, Rosja, Indie i Chiny.**

Trendy światowe

Lata edukacji i egzekwowania prawa oraz rosnący poziom świadomości z korzyści płynących z prawidłowego zarządzania zasobami oprogramowania doprowadziły do niewielkiego spadku skali korzystania z nielicencjonowanego oprogramowania w skali globalnej. Od 2015 do 2017 roku światowy wskaźnik nielicencjonowanego oprogramowania zmniejszył się o 2 punkty (z 39 do 37 procent), a jego wartość rynkowa na całym świecie spadła o 8 procent (według stałych kursów walut) do 46,3 miliarda USD.

Choć wskaźnik nielicencjonowanego oprogramowania zmniejszył się po części wskutek spadku sprzedaży komputerów, to IDC szacuje, że mniej więcej 60 procent tego spadku to skutek zwiększonego udziału legalnego oprogramowania. To pokazuje, że wiele firm zaczyna rozumieć sens prowadzenia właściwej polityki licencyjnej w zakresie wykorzystywanego oprogramowania. Mimo tego progresu większość oprogramowania w krajach objętych badaniem jest nielicencjonowana, co dowodzi konieczności dalszych postępów na tym polu.

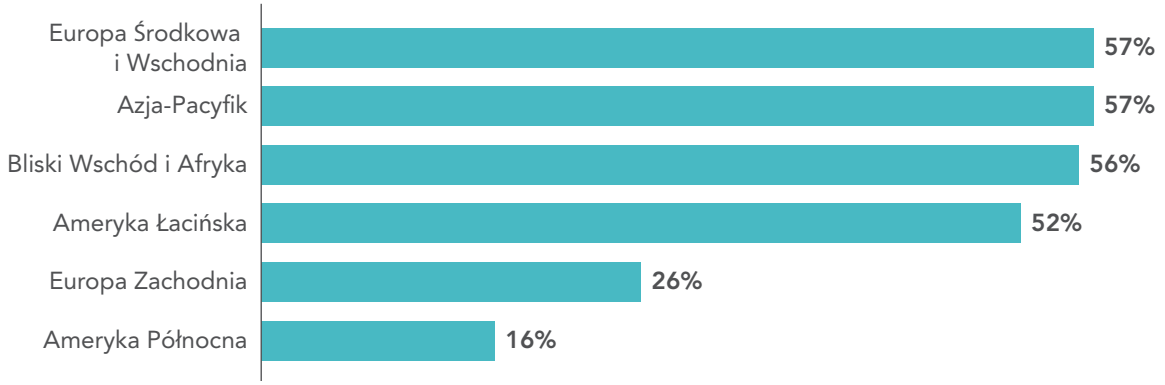
Mimo że wskaźnik nielicencjonowanego oprogramowania spadł we wszystkich regionach, to zmniejszyłby się znacznie bardziej, gdyby nie rynki wschodzące. Mają one bowiem wyższy niż statystyczny, bo aż 61-procentowy wskaźnik nielicencjonowanego oprogramowania, co stanowi wzrost w porównaniu z poprzednią edycją badania (70 procent w 2015 i 75 procent w 2017 roku).

W skali globalnej wskaźniki nielicencjonowanego oprogramowania spadły na 101 rynkach, wzrosły jedynie na sześciu. W dwunastu krajach wskaźniki te spadły w 2017 roku o 3 punkty procentowe,[24] a w Chinach i Wietnamie zanotowano spadki czteropunktowe, co jest w głównej mierze wynikiem wysokich wskaźników początkowych. Jeśli wziąć pod uwagę wartości procentowe (wskaźnik z 2017 dzielony przez wskaźnik z 2015 roku), to największe spadki nastąpiły w krajach rozwiniętych, przy czym w USA, Australii, Austrii, Japonii, Luksemburgu, Nowej Zelandii, Singapurze i Szwecji były to spadki o 10 procent lub większe, co ułatwiło tym krajom zarówno osiągnięcie korzyści gospodarczych, jak i podniesienie poziomu cyberbezpieczeństwa.

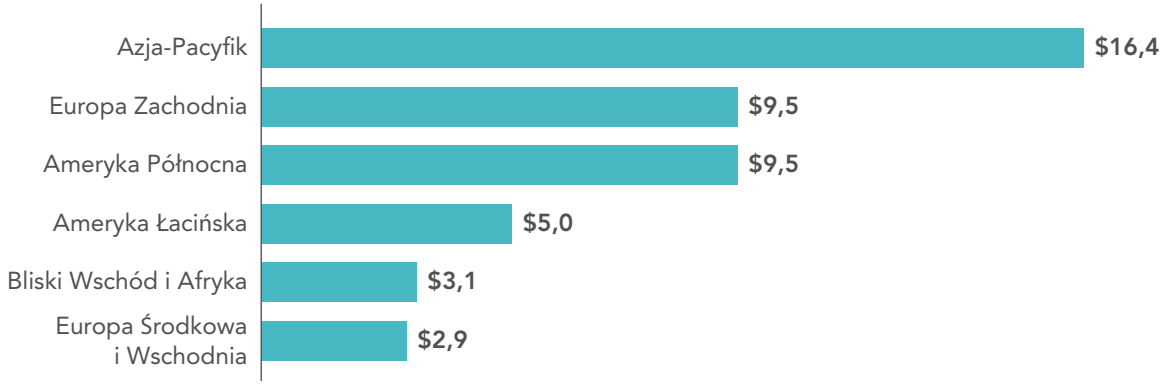
NA SPADKU WSKAŹNIKA KORZYSTANIA Z NIELICENCJONOWANEGO OPROGRAMOWANIA KORZYSTA KAŻDY REGION

- **Azja-Pacyfik:** 57-procentowa skala korzystania z nielicencjonowanego oprogramowania w tym regionie to jeden z najwyższych wskaźników na świecie, mimo czteropunktowego spadku w porównaniu do 2015 roku. W efekcie wartość rynkowa nielicencjonowanego oprogramowania sięga oszałamiającej kwoty 16,4 miliarda USD. To znacznie więcej niż we wszystkich innych regionach świata, a kwota ta stanowi ponad jedną trzecią globalnej wartości rynkowej nielicencjonowanego oprogramowania. W regionie tym tylko same Chiny korzystają z nielicencjonowanego oprogramowania o wartości rynkowej 6,8 miliarda USD.
- **Europa Środkowa i Wschodnia:** region ten wiąże z regionem Azja-Pacyfik najwyższy, 57-procentowy poziom skali korzystania z nielicencjonowanego oprogramowania (spadek zaledwie o 1 punkt w porównaniu z 2015 rokiem). W tym regionie występują ogromne różnice w zakresie użytkowania nielicencjonowanego oprogramowania. 85-procentowy wskaźnik korzystania z nielicencjonowanego oprogramowania stawia Armenię na pierwszym miejscu w regionie. Tuż za nią znalazły się Mołdawia (83 procent) i Białoruś (82 procent). Najniższy wskaźnik w regionie mają Czechy (32 procent) i Słowacja (35 procent). Największy, szacowany na 1,3 miliarda USD udział w wartości nielicencjonowanego oprogramowania w tym regionie ma Rosja.
- **Bliski Wschód i Afryka:** w tym obszarze ogólna skala spadła o jeden punkt do poziomu 56 procent, mimo że na dwóch rynkach tego obszaru wskaźnik ten wzrósł o jeden punkt, a na czterech nie uległ zmianie. Region ten nadal dzieli tylko jeden punkt procentowy od najwyższego wskaźnika na świecie. Kilka krajów w regionie znajduje się w ścisłej światowej czołówce pod względem liczby użytkowników nielicencjonowanego oprogramowania – w Libii jest ich 90 procent, w Zimbabwe 89 procent. Z kolei największe korzyści z licencjonowanego oprogramowania odnoszą Zjednoczone Emiraty Arabskie (32 procent), Republika Południowej Afryki (32 procent) i Izrael (27 procent).

Średni wskaźnik korzystania z nielicencjonowanego oprogramowania



Wartość rynkowa nielicencjonowanego oprogramowania (w miliardach USD)



- **Ameryka Łacińska:** w tym regionie 52 procent oprogramowania nie ma odpowiednich licencji, co stanowi trzypunktowy spadek od czasu ostatniego badania opublikowanego w 2015 roku. Nielicencjonowane oprogramowanie w tym regionie ma wartość rynkową niemal 5 miliardów USD. Kraje o najwyższych wskaźnikach to Wenezuela z wynikiem 89 procent (drugi z najwyższych wskaźników na świecie), Nikaragua (81 procent) i Salwador (80 procent). Z kolei Brazylia (46 procent), Kolumbia (48 procent) i Meksyk (49 procent) już teraz czerpią korzyści z niższego wskaźnika nielicencjonowanego użytkowania. Od 2015 roku Meksyk osiągnął aż trzypunktowy spadek wskaźnika nielicencjonowanego oprogramowania. Najniższy wskaźnik ma obecnie Brazylia, ale jako największy kraj w regionie używa nielicencjonowanego oprogramowania o wartości rynkowej aż 1,7 miliarda USD (największej w Ameryce Łacińskiej).
- **Europa Zachodnia:** w Europie Zachodniej ogólny wskaźnik nielicencjonowanego oprogramowania spadł o dwa punkty do poziomu 26 procent. Największy, trzypunktowy spadek zanotowała Irlandia, uzyskując 29-procentowy wskaźnik nielicencjonowanego oprogramowania. Grecja nadal odstaje od reszty regionu z nietypowym jak na tę część Europy wskaźnikiem nielicencjonowanego oprogramowania na poziomie aż 61 procent. Kilka krajów w regionie zdołało zmaksymalizować zyski ze sprzedawanego oprogramowania i ograniczyć ryzyko cyberzagrożeń, pracując nad utrzymaniem wskaźników nielicencjonowanego oprogramowania wśród najniższych na świecie. Mowa tu o Luksemburgu (17 procent), Szwecji (19 procent), Austrii (19 procent), Danii i Niemczech (20 procent) oraz Szwajcarii (21 procent). W szesnastu z 20 badanych krajów odnotowano spadek o co najmniej dwa punkty w porównaniu z 2015 rokiem.
- **Ameryka Północna:** ten region ma nadal najniższy wskaźnik (16 procent), ale ze względu na jego rozmiar wartość rynkowa nielicencjonowanego oprogramowania będącego w użyciu wynosi 9,5 miliarda USD.

Zarządzanie zasobami oprogramowania: jak chronić organizację przed ryzykiem i zwiększać jej wartość

Firmy mają dostęp do obowiązujących globalnie najlepszych praktyk zarządzania oprogramowaniem, które mogą zastosować w celu stałego zwiększania korzyści uzyskiwanych przez nie z zasobów technologicznych oraz ograniczania zagrożeń związanych z nielicencjonowanym oprogramowaniem powodowanych przez oprogramowanie złośliwe. Badania wykazują, że wdrażając niezawodne rozwiązania SAM organizacje mogą osiągnąć aż 30-procentowe oszczędności w ramach rocznych kosztów ponoszonych na oprogramowanie.[25]

Wersja normy ISO/IEC 19770-1 z 2017 roku zapewnia holistyczne podejście do skutecznego i zgodnego z normą ISO programu wdrażania SAM. Wdrożenie normy umożliwia ciągłe doskonalenie procesu w trzech progresywnych obszarach procesowych. Takie wielopoziomowe podejście pozwala organizacjom odpowiednio rozłożyć fazy wdrożenia. Norma rozpatruje stosowanie tych poziomów w stanowiącym standard branżowy procesie, na który składa się: (1) utworzenie dedykowanego i wszechstronnego planu wdrożenia, (2) wykonanie planu w kontrolowany i zdyscyplinowany sposób, (3) ocena postępu w porównaniu do planu oraz (4) odpowiednie dostosowanie planu w celu zapewnienia jego ciągłego doskonalenia.

OBSZAR PROCESOWY 1

WIARYGODNE DANE

Pierwsze stadium obejmuje dokładne poznanie stanu posiadania umożliwiające kompleksowe zarządzanie zasobami oprogramowania. Zaczyna się od oceny oprogramowania wykorzystywanego w systemie pod względem jego zgodności z umowami licencyjnymi. Oprócz zarządzania licencjami, ten obszar procesowy pozwala organizacjom także na opracowanie procesów niezbędnych do zarządzania zmianą, danymi oraz zabezpieczeniami.

OBSZAR PROCESOWY 2

INTEGRACJA CYKLU ŻYCIA

Drugie stadium korzysta z efektów pierwszego i pozwala organizacjom osiągnąć większą sprawność oraz opłacalność poprzez udoskonalenie zarządzania całym cyklem życia zasobów IT: od specyfikacji po nabycie, opracowanie, wydanie, instalację, użytkowanie i wycofanie z eksploatacji.

OBSZAR PROCESOWY 3

OPTYMALIZACJA

Trzecie stadium pozwala organizacjom osiągnąć większą sprawność i opłacalność poprzez koncentrację na obszarach funkcjonalnych, takich jak umowy i zarządzanie finansowe.

DZIAŁANIA, KTÓRE MOGĄ PODJĄĆ RZĄDY

W celu odblokowania mnóstwa nowych miejsc pracy, zwiększenia podstawy opodatkowania i uzyskania korzyści gospodarczych pochodzących z organizacji będących w stanie w pełni wykorzystać najnowsze postępy technologii, oprócz kroków, które mogą i powinny podejmować organizacje, również w zasięgu rządów znajduje się zestaw zgodnych z rozsądkiem, konkretnych kroków, które można podjąć, aby zmniejszyć wskaźnik nielicencjonowanego oprogramowania i zapewnić większą energię krajowej gospodarce.

1 PRZYKŁAD IDZIE Z GÓRY:

Rządy są największymi na świecie użytkownikami oprogramowania. Tak jak wszystkie organizacje mogą skorzystać z możliwości ograniczenia zagrożeń, zwiększenia niezawodności technologii i wdrożenia rozwiązań SAM. Rządy mogą także promować SAM i wymagać korzystania w przedsiębiorstwach państwowych (a także wśród ich wykonawców i dostawców) jedynie z licencjonowanego oprogramowania.

2 PODNOSZENIE POZIOMU EDUKACJI PUBLICZNEJ I ZWIĘKSZANIE ŚWIADOMOŚCI:

Rządy, specjaliści w dziedzinach księgowości i audytów, konsultanci branżowi, zrzeszenia zawodowe i organizacje biznesowe powinny edukować inne organizacje w kwestiach przestrzegania licencji do oprogramowania i zagrożeń związanych z instalowaniem i użytkowaniem oprogramowania nielicencjonowanego.

3 MODERNIZACJA PRAWA W CELU UWZGLĘDNIENIA INNOWACJI:

Wraz z nadejściem technologii chmury obliczeniowej i upowszechnieniem sieciowych urządzeń przenośnych, oprogramowanie zaczęło być przechowywane, dostarczane i wykorzystywane na nowe, pomysłowe sposoby. Prawodawcy powinni zapewnić jego ochronę bez względu na format lub metody dostawy.

4 TWORZENIE ŚRODOWISKA SPRZYJAJĄCEGO EGZEKWOWANIU PRAWA:

Rządy powinny zapewnić rozwiązania prawne gwarantujące skuteczność dochodzenia odszkodowań i promujące współpracę interesariuszy nad ograniczeniem naruszania praw autorskich do oprogramowania.

WIĘKSZE MOŻLIWOŚCI DZIĘKI PRZEJŚCIU DO CHMURY

Chmura staje się jedną z najbardziej transformacyjnych technologii pokolenia, ponieważ rewolucjonizuje od podstaw metody kupowania, sprzedawania i dostarczania zasobów obliczeniowych. Umożliwia niemal wszystkim firmom, bez względu na wielkość, możliwość korzystania z technologii niegdyś dostępnych tylko wielkim organizacjom. Umożliwione przez technologię chmury równouprawnienie cyfrowe doprowadziło do ogromnego wzrostu ilości, jakości i różnorodności usług opartych na chmurze, z których korzystają dzisiaj firmy. Szacuje się, że liczba opartych na chmurze aplikacji używanych przez przeciętne przedsiębiorstwo potroiła się w ciągu trzech lat.[26] W wielu przypadkach chmura dostarcza tradycyjne i wzbogacone funkcje danego oprogramowania jako usługę, do której dostęp uzyskuje się przez Internet. IDC szacuje, że chmura dostarcza 22 procent wszystkich funkcji oprogramowania dostępnego na całym świecie.

Firmy śpieszą się korzystać z usług opartych na chmurze ze względu na ich naturalną zdolność redukcji kosztów, zwiększania sprawności, zmniejszania złożoności i wzmacniania zabezpieczeń.

- **CHMURA JEST OPŁACALNA:** organizacje IT, które z powodzeniem przeszły na technologię chmury, mają przeciętnie o 21 procent niższe koszty IT niż inne firmy z branży, które nadal zarządzają wielkimi centrami danych i serwerami aplikacji na swoim terenie.[27] Liderzy ci wiedzą już, że chmura pozwala organizacjom zmniejszyć koszty IT dzięki unikaniu kosztownych inwestycji kapitałowych niezbędnych do modernizacji i utrzymania istniejącej infrastruktury sprzętowej. Organizacje redukują swoje koszty również dlatego, że chmura zapewnia im możliwość płacenia tylko za niezbędne zasoby (efekt skali), jednocześnie dając dostęp do niemal nieskończonej mocy obliczeniowej i pamięci masowej przez Internet.
- **CHMURA JEST BEZPIECZNA I ELASTYCZNA:** unikatowa architektura chmury zapewnia również niespotykaną dotąd elastyczność, nie tylko zmieniając sposób kupowania, sprzedawania i dostarczania zasobów obliczeniowych, ale też umożliwiając dostęp do aplikacji w dowolnej chwili, z dowolnego urządzenia i z każdego miejsca na świecie. Dla niektórych największą zaletą chmury jest ogromne udoskonalenie zabezpieczeń w porównaniu do modeli tradycyjnych. Dostawcy chmury widzą zagrożenia w szerszym kontekście, co pozwala szybciej je identyfikować i wdrażać technologie zabezpieczeń o wyższym poziomie zaawansowania niż rozwiązania dostępne cenowo dla klientów indywidualnych. Są również w stanie podnosić poziom bezpieczeństwa poprzez wdrażanie zaawansowanych technologii ochrony przed zagrożeniami, szyfrowanie zapisanych i przesyłanych danych oraz automatyzację procesów aktualizacji w celu szybszego zabezpieczania systemów przed nowo odkrytymi zagrożeniami. Łącznie możliwości te mogą zwiększyć odporność danych i wzmocnić zabezpieczenia organizacji.
- **SAM ZWIĘKSZA MOŻLIWOŚCI MIGRACJI DO CHMURY:** jako że chmura oferuje firmom niezrównany potencjał wprowadzania w całym przedsiębiorstwie cyfrowych innowacji, rozwiązania SAM stały się niezbędnym elementem przyśpieszającym przejście do chmury. SAM pozwala organizacjom zwiększyć ich gotowość do przejścia do chmury na kilka sposobów. Umożliwia organizacjom optymalizację ich strategii licencyjnej, uzyskanie nowych danych dotyczących dodatkowych oszczędności osiągalnych dzięki przejściu do chmury oraz opracowanie strategii niezbędnej do przygotowania się na przejście na technologię chmury. Jedynie dysponując taką strategią przedsiębiorstwa mogą w pełni wykorzystać potencjał oferowany przez usługi oparte na chmurze. Na przykład University of Roehampton w Londynie, korzystając z rozwiązań SAM opracował wszechstronną strategię migracji do chmury. Dzięki umożliwieniu płynnej migracji większości infrastruktury informatycznej uczelni do chmury możliwe było uniknięcie poważnych, nowych inwestycji w sprzęt niezbędny w centrum danych, uzyskanie nowej elastyczności i skalowalności, zwiększenie bezpieczeństwa oraz wygenerowanie oszczędności w wysokości aż 40 procent w ciągu 10 lat (około 4,7 milionów USD).[28]

Wiele organizacji liczy obecnie na uzyskanie strategicznej przewagi rynkowej dzięki chmurze i nierzadko stara się wykonać podstawowe kroki niezbędne do płynnej migracji. Wdrożenie SAM pozwala firmom przyspieszyć uzyskanie transformacyjnych korzyści, które można osiągnąć migrując do chmury.

Metodologia

Ogólnoświatowe badanie ankietowe BSA ocenia ilość i wartość nielicencjonowanego oprogramowania zainstalowanego na komputerach osobistych w ponad 110 krajowych i regionalnych gospodarkach w danym roku – w tym przypadku w roku 2017. Obejmuje ono także globalne badanie ankietowe z udziałem ponad 22 500 respondentów z 32 krajów, będących konsumentami i pracownikami używającymi komputerów osobistych w domu lub pracy. Badanie to ma zapewnić najważniejsze dane dotyczące nastawienia do właściwego licencjonowania oprogramowania oraz nowe informacje na temat bezpośredniego wpływu ograniczenia skali korzystania z nielicencjonowanego oprogramowania na gospodarkę. W celu stworzenia raportu BSA ściśle współpracowała z IDC, jedną z czołowych niezależnych firm badawczych na świecie, aby zmierzyć, zrozumieć i ocenić użytkowanie licencjonowanego i nielicencjonowanego oprogramowania w skali globalnej.

Pomiar skali i zakresu korzystania z nielicencjonowanego oprogramowania stawia oczywiście przed badaczami pewne wyzwania. Choć badanie to jest uznawane za jedną z najbardziej zaawansowanych na świecie ocen skali naruszania praw autorskich do oprogramowania, BSA i jej partnerzy nieustannie poszukują nowych metod zwiększania wiarygodności danych. W 2011 roku, we współpracy z dwoma wybitnymi uczonymi w dziedzinie ekonomii IT, BSA dokonała kilku modyfikacji mających na celu umożliwienie szczegółowej analizy danych wejściowych i zapewnienie możliwie najdokładniejszego oszacowania skali korzystania z nielicencjonowanego oprogramowania.

OGÓLNOŚWIATOWE BADANIE ANKIETOWE UŻYTKOWNIKÓW OPROGRAMOWANIA

Kluczowym elementem BSA Global Software Survey jest ogólnoświatowe badanie ankietowe z udziałem 22 500 respondentów używających komputerów osobistych w domu i w firmach, przeprowadzone przez IDC w listopadzie 2017 roku. Badanie ankietowe przeprowadzono przez Internet lub telefonicznie na 32 rynkach stanowiących próbę reprezentatywną dla świata pod względem regionów geograficznych, poziomów zaawansowania technologii informatycznych oraz różnorodności kulturowej. Ponadto w 23 krajach przeprowadzono równoległe badanie ankietowe wśród 2300 specjalistów odpowiedzialnych na środowisko IT w swoich organizacjach.

Badania ankietowe zostały użyte po części do określenia tzw. poziomu „ładunku oprogramowania" poszczególnych krajów, to jest szacunkowej liczby programów zainstalowanych na jednym komputerze, w tym programów płatnych, open source i o mieszanych źródłach. Respondentów pytano o liczbę i typy pakietów oprogramowania zainstalowanych na ich komputerach osobistych w poprzednim roku: jaki procent stanowiło oprogramowanie nowe lub uaktualnienia, czy było ono instalowane na używanych komputerach czy też preinstalowane na nowo zakupionym sprzęcie oraz czy zostało nabyte przed 2017 rokiem. Pytania te zadawano zarówno użytkownikom indywidualnym, jak i firmowym.

Badania ankietowe służą ponadto do oceny społecznego nastawienia i zachowań dotyczących własności intelektualnej, korzystania z nielicencjonowanego oprogramowania i innych kwestii związanych z nowymi technologiami. Dane te zapewniają co roku świeży punkt widzenia na dynamikę leżącą u podstaw wykorzystywania nielicencjonowanego oprogramowania na całym świecie.

Kraje biorące udział w badaniu wybierane są przy użyciu strategii rotacyjnej, zapewniającej rok do roku jak największy światowy zasięg. Jedenaście rynków priorytetowych jest badanych w każdym cyklu, a 52 kraje nie rzadziej niż co dwa lub trzy cykle. Pozostałe kraje są wybierane doraźnie. W każdym cyklu raportu badana populacja reprezentuje ponad 85 procent łącznej liczby jednostek zainstalowanego oprogramowania i około 90 procent jednostek płatnych, zapewniając zarazem przebadanie większości rynków co najmniej raz na trzy lata badań.

OBLICZANIE WSKAŹNIKÓW INSTALACJI NIELICENCJONOWANEGO OPROGRAMOWANIA

Od 2003 roku BSA współpracuje z IDC, czołowym dostawcą statystyk rynkowych i prognoz dla branży IT, nad określaniem wskaźników korzystania z nielicencjonowanego oprogramowania i wartości rynkowej tych instalacji.

Podstawowa metoda określania wskaźnika i wartości rynkowych w danym kraju jest następująca:

1. Określenie ilości oprogramowania zainstalowanego w ciągu roku przez użytkowników indywidualnych i firmowych.

2. Określenie ilości oprogramowania, za które zapłacono lub w inny sposób nabyto legalnie w ciągu roku (na przykład ilości oprogramowania open source, bezpłatnego lub z licencją uzupełniającą), ponownie z podziałem na użytkowników indywidualnych i firmowych.

3. Odjęcie drugiej liczby od pierwszej w celu uzyskania ilości nielicencjonowanego oprogramowania. Po uzyskaniu tej liczby wskaźnik nielicencjonowanego użytkowania jest obliczany jako odsetek całego zainstalowanego oprogramowania.

Wskaźnik nielicencjonowanego użytkowania
=
liczba jednostek nielicencjonowanego oprogramowania / łączna liczba zainstalowanych jednostek oprogramowania

Łączna liczba zainstalowanych jednostek oprogramowania
=
liczba komputerów, na których zainstalowane jest oprogramowanie X / liczba jednostek oprogramowania na jednym komputerze osobistym

W celu określenia łącznej liczby zainstalowanych jednostek oprogramowania (mianownika ułamka) IDC określa liczbę komputerów w danym kraju oraz liczbę komputerów, na których zainstalowano oprogramowanie w ciągu danego roku. IDC rejestruje te informacje w kwartalnych sprawozdaniach z badań „PC Trackers" obejmujących 92 kraje. Na potrzeby tego raportu w pozostałych krajach prowadzone są coroczne badania.

Po określeniu przez IDC liczby komputerów, zarówno należących do użytkowników indywidualnych jak i firm oraz zastosowaniu danych o ładunku oprogramowania zebranych w badaniu ankietowym, można określić łączną liczbę zainstalowanych jednostek licencjonowanego i nielicencjonowanego oprogramowania w poszczególnych krajach.

W celu oszacowania ładunku oprogramowania w krajach nieobjętych badaniem ankietowym IDC stosuje technikę analizy skupień, aby znaleźć podobne cechy w krajach o różnych ładunkach oprogramowania i stosuje te cechy w celu przypisania ładunków krajom nieobjętym badaniem. IDC weryfikuje to sprawdzając wskaźniki korelacji między znanymi ładunkami oprogramowania z krajów objętych badaniem, a ich wynikami w pomiarze rezultatów rynków wschodzących, publikowane przez Międzynarodowy Związek Telekomunikacyjny (International Telecommunications Union) w zestawieniu „ICT Development Index" (wskaźnik rozwoju ICT), a następnie dzieląc je na kohorty w celu porównania z krajami nieobjętymi badaniem ankietowym.

Aby uzyskać liczbę jednostek nielicencjonowanego oprogramowania (licznik ułamka w równaniu) IDC musi określić wartość rynku legalnie nabytego oprogramowania. IDC rutynowo publikuje dane rynku oprogramowania z około 80 krajów, a ponadto niesystematycznie bada jeszcze około 20 kolejnych. W nielicznych, pozostałych krajach IDC prowadzi coroczne badania naukowe na potrzeby tego raportu. Te badania naukowe podają wartość rynku legalnie nabytego oprogramowania. Wartość jest dzielona przez liczbę użytkowników indywidualnych i firmowych.

Aby przeliczyć wartość rynku oprogramowania na liczbę jednostek, IDC oblicza średnią cenę jednostki oprogramowania dla całego oprogramowania na komputerach osobistych użytkowników indywidualnych i firmowych w kraju. W tym celu opracowywana jest macierz cen oprogramowania w danym kraju (w sprzedaży detalicznej, licencji zbiorczych, OEM, bezpłatnych i open source) w ramach macierzy produktów, takich jak zabezpieczenia, automatyzacja biura, systemy operacyjne i inne.

Informacje IDC o cenach pochodzą z jej rejestrów oraz z badań lokalnych analityków. Dane dotyczące współczynników korygujących (OEM i sprzedaży detalicznej, użytkowników indywidualnych i firmowych) pochodzą z badań ankietowych IDC. IDC mnoży dwie macierze, aby uzyskać końcową, uśrednioną cenę jednostki oprogramowania.

W celu obliczenia łącznej liczby legalnych jednostek oprogramowania IDC stosuje następujący wzór:

Liczba jednostek legalnego oprogramowania
=
wartość rynku oprogramowania / średnia cena jednostki oprogramowania

W 2011 roku IDC zastosowała kilka miar w celu sprawdzenia poprawności obliczeń średniej ceny jednostki oprogramowania. Zespoły analityków w 25 krajach dostarczyły dodatkowych informacji o cenach oprogramowania według kategorii i użytkowników (indywidualnych lub firmowych) i oszacowań typu nabycia (to jest w sprzedaży detalicznej, w ramach

licencji zbiorczej, bezpłatnie/open source), które posłużyły do kontroli krzyżowej wartości obliczonych przez IDC. Coroczna rotacja krajów, dla których zbierane są informacje, pozwala IDC co pewien czas ponownie kalibrować ceny oprogramowania i zapewnia dokładniejsze oszacowanie liczby jednostek legalnego oprogramowania na podstawie przychodów branży.

Na koniec, odjęcie liczby jednostek legalnego oprogramowania od łącznej liczby jednostek oprogramowania ujawnia liczbę jednostek nielicencjonowanego oprogramowania zainstalowanych w ciągu danego roku.

Liczba jednostek nielicencjonowanego oprogramowania
=
łączna liczba zainstalowanych jednostek oprogramowania
–
liczba jednostek legalnego oprogramowania

Ten proces zapewnia dane niezbędne do podstawowego równania wskaźnika.

OBLICZANIE WARTOŚCI RYNKOWEJ NIELICENCJONOWANEGO OPROGRAMOWANIA

Wartość rynkowa nielicencjonowanego oprogramowania zapewnia inną miarę skali korzystania z niego i umożliwia dokonanie istotnych porównań zmian użytkowania oprogramowania rok do roku.

Obliczana jest na podstawie tej samej uśrednionej ceny, na bazie której IDC określa średnią cenę jednostki oprogramowania, obejmującej sprzedaż detaliczną, licencje zbiorcze, OEM, bezpłatne, open source, użytkowników indywidualnych lub firmowych itd. Średnia cena jednostki oprogramowania jest niższa niż ceny sprzedaży w sklepach detalicznych.

Dzięki obliczeniu łącznej liczby jednostek zainstalowanego oprogramowania, liczb zainstalowanych jednostek legalnego i nielicencjonowanego oprogramowania oraz średniej ceny jednostki oprogramowania, IDC jest w stanie obliczyć wartość rynkową nielicencjonowanego oprogramowania.

UWZGLĘDNIANE OPROGRAMOWANIE

W badaniu BSA Global Software Survey obliczana jest liczba instalacji nielicencjonowanego oprogramowania uruchamianego na komputerach osobistych – stacjonarnych, przenośnych i ultraprzenośnych (netbooki).

Uwzględniane są systemy operacyjne, oprogramowanie systemowe (takie jak bazy danych i pakiety zabezpieczeń), aplikacje biznesowe oraz aplikacje konsumenckie, takie jak gry, programy do obsługi finansów osobistych i oprogramowanie użytkowe. W badaniu brana jest również pod uwagę dostępność bezpłatnego legalnego oprogramowania i oprogramowania open source, które jest licencjonowane na zasadzie przynależności do domeny publicznej powszechnego użytku. Zazwyczaj jest ono bezpłatne, ale może być również stosowane w produktach płatnych.

W badaniu NIE jest uwzględniane oprogramowanie fabryczne tabletów ani smartfonów. Wyłączone jest również oprogramowanie serwerów i komputerów centralnych (mainframe) oraz standardowe sterowniki urządzeń, jak również pobierane bezpłatnie programy narzędziowe (takie jak wygaszacze ekranu), które nie zastępują oprogramowania płatnego lub zazwyczaj nie są uznawane przez użytkowników za programy.

W badaniu uwzględniane są także usługi obliczeniowe chmury, takie jak oprogramowanie jako usługa (SaaS) i platforma jako usługa (PaaS), zastępujące oprogramowanie, które mogłoby zamiast nich zostać zainstalowane na komputerach osobistych. Oprogramowanie sprzedawane w ramach programów legalizacji (takich jak sprzedaż hurtowa rządowi do dystrybucji w szkołach) również jest uwzględniane w badaniu.

WPŁYW KURSÓW WALUTOWYCH

Przed 2009 rokiem kwoty w USD w tabelach wartości podawane były według kursów z poprzedniego roku. Na przykład, wartość nielicencjonowanego oprogramowania publikowana w 2007 roku podawana była w USD według kursów z 2006 roku, aby ułatwić porównania rok do roku. W 2009 roku BSA postanowiła publikować kwoty wartości według bieżących kursów dolara z roku przeprowadzenia badania. Wartości z 2009 roku są zatem podawane według kursów USD z roku 2009, wartości z 2017 roku według kursów USD z roku 2017 itd. Poprzednie wartości nie są przeliczane według kursów bieżących.

Jest to ważne podczas oceny zmian wartości w czasie. Niektóre zmiany oparte będą na rzeczywistej dynamice rynków, a inne na wahaniach kursów wymiany rok do roku.

PRZYPISY

[1] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[2] McAfee Labs Threat Report (March 2018), available at https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf.

[3] "Cyber-Attacks Occurring More Frequently and With Greater Sophistication, NTT Security Report Finds," Security InfoWatch (August 9, 2017), available at www.securityinfowatch.com/press_release/12358487/cyber-attacks-occurring-more-frequently-and-with-greater-sophistication-ntt-security-report-finds.

[4] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[5] In 2015, 43 percent of cyber-attacks worldwide were against small businesses with less than 250 workers. Elizabeth MacDonald, "Cyber Attacks on Small Businesses on the Rise," *Fox Business* (April 26, 2016), available at www.foxbusiness.com/features/cyber-attacks-on-small-businesses-on-the-rise.

[6] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[7] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[8] "Global Cybercrime Costs Top $600 Billion," DarkReading (February 21, 2018), available at https://www.darkreading.com/attacks-breaches/global-cybercrime-costs-top-$600-billion-/d/d-id/1331106.

[9] M-Trends 2013: Attack the Security Gap, Mandiant (2013), available at https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2013-mtrends.html.

[10] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[11] Paul Mozur, "China, Addicted to Bootleg Software, Reels From Ransomware Attack," *New York Times* (May 15, 2017), available at www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html.

[12] "China's Fondness for Pirated Software Raises Risks in Attack," *Phys Org* (May 16, 2017), available at https://phys.org/news/2017-05-china-fondness-pirated-software.html.

[13] "Jakub Kroustek, a malware researcher with Avast, a security software company in the Czech Republic, said in a blog post that Russia was the most-affected country so far [from a malware attack]."Elizabeth Dwoskin and Karla Adam, "More Than 150 Countries Affected by Massive Cyberattack, Europol Says," *Washington Post* (May 14, 2017), available at https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.

[14] International Organization for Standardization, *ISO/IEC 19770-1:2017 Information Technology—IT Asset Management*, available at www.iso.org/standard/68531.html.

[15] "Equifax Breach to Cost Total of $439M," PYMNTS (March 5, 2018), available at www.pymnts.com/news/security-and-risk/2018/equifax-cost-275m/.

[16] "How Could ITAM Have Helped the Equifax CIO?" *The ITAM Review* (October 19, 2017), available at www.itassetmanagement.net/2017/10/19/equifax-itam/.

[17] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[18] These important benefits are derived from the combination of better security by reducing malware that may accompany unlicensed software, fewer disruptive audits that take precious time to respond to, reduced legal risks around license compliance violations, better IT productivity by eliminating outdated or unsupported software, more trusted brand identity by avoiding risky behavior, and better relationships with vendors.

[19] With a more effective licensing model in place, OSI reduced costs by more than 30 percent and achieved 100 percent compliance with Microsoft guidelines. See "OSI International Foods Increases Software License Visibility and Reduces Costs by 30 Percent," Microsoft Customer Solution Case Study, available at http://download.microsoft.com/download/7/F/1/7F18B556-BC4D-4B5C-BAB8-9386515BF1EB/Germany-OSI_International_Foods.doc.

[20] Baltika conducted a SAM project that now saves them $100,000 per year in the workstation, software, and servers. See "Baltika Breweries Unlocks the Power of Microsoft Technologies Through SAM," YouTube, available at www.youtube.com/watch?v=yocvl9nl8o0&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at www.microsoft.com/en-us/sam/customers.aspx.

[21] "University of Roehampton Benefits From Azure Migration Through Microsoft SAM," YouTube, available at https://www.youtube.com/watch?v=hAHHvZ_8zz4&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at https://www.microsoft.com/en-us/sam/customers.aspx.

[22] Using a specialized SAM tool and other strategies, the space agency uncovered software consolidation opportunities. For NASA, it meant eliminating duplicate software licenses and negotiating better prices for the software it already buys. "How NASA Saved $100 Million on Software Licenses," *FedTech* (February 23, 2017), available at https://fedtechmagazine.com/article/2017/02/how-nasa-saved-100-million-software-licenses.

[23] See BSA | The Software Alliance, *Government Guide for Software Asset Management*, available at www.bsa.org/~/media/Files/Tools_And_Resources/Guides/SoftwareManagementGuide/SoftwareManagementGuide_Government.pdf.

[24] Azerbaijan, Belarus, Bulgaria, Georgia, Hong Kong, Ireland, Mexico, Moldova, Philippines, Singapore, South Korea, and Thailand.

[25] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[26] Ajmal Kohgadai, "12 Must-Know Statistics on Cloud Usage in the Enterprise," SkyHigh Networks, available at https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/.

[27] "Cloud Users Enjoy Significant Savings," Computer Economics (April 2016), available at https://www.computereconomics.com/article.cfm?id=2185.

[28] Case Study: A Confident Move to the Cloud for the University of Roehampton," available at https://www.civica.com/globalassets/7.document-downloads/2.uk-docs/case-studies/roehampton-case-study.pdf.

INFORMACJE O BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance (www.bsa.org) jest czołowym rzecznikiem światowej branży oprogramowania wobec rządów i na rynku międzynarodowym. Członkowie organizacji należą do najbardziej innowacyjnych firm na świecie, tworzących rozwiązania w zakresie oprogramowania, które napędzają gospodarkę i polepszają jakość współczesnego życia.

Z siedzibą w Waszyngtonie i oddziałami w ponad 60 krajach na całym świecie, BSA jest pionierem programów zgodności licencyjnej, które promują korzystanie z legalnego oprogramowania oraz prowadzi międzynarodową politykę pobudzającą rozwój innowacji technologicznej i gospodarki cyfrowej.

www.bsa.org

Siedziba Główna BSA

20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA Azja-Pacyfik

300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072
@BSAnewsAPAC

BSA Europa, Bliski Wschód i Afryka

65 Petty France
Ground Floor
London, SW1H 9EU
Wielka Brytania

+44.207.340.6080
@BSAnewsEU