Bezpieczeństwo usług finansowych w procesie cyfrowej transformacji

Podmioty oferujące usługi finansowe poszukują możliwości wykorzystywania nowych technologii do definiowania, różnicowania i wdrażania swoich strategii biznesowych. Z ich perspektywy transformacja cyfrowa to sposób na osiąganie korzyści rynkowych, wyróżnienie się i wyprzedzenie konkurencji. Możliwości cyfrowe łączą się jednak również z nowymi wyzwaniami. Rozwój narzędzi cyfrowych zwiększa prawdopodobieństwo wystąpienia wewnątrz organizacji konfliktu strategii dotyczących bezpieczeństwa i ochrony przed cyberzagrożeniami.

Aby skutecznie zarządzać tym procesem, organizacje z sektora usług finansowych muszą na nowo określić swoją strategię bezpieczeństwa i dostosować ją do tempa zmian na tym bardzo dynamicznie rozwijającym się rynku:

- Ponieważ bezpieczeństwo często ma w przedsiębiorstwach niższy priorytet niż inicjatywy związane z rozwojem czy innowacjami, kontrola nad działami IT coraz częściej przypada w udziale menadżerom różnych obszarów działalności firmy. Ich niezależne projekty tworzą „równoległe systemy informatyczne" (tzw. Shadow IT), które są przyczyną problemów związanych z bezpieczeństwem.
- Aby stawić czoło wyzwaniom związanym z zarządzaniem złożonymi procesami cyfrowymi, organizacje świadczące usługi finansowe coraz częściej współpracują z zewnętrznymi ekspertami ds. bezpieczeństwa. To sygnał, że specjaliści ds. bezpieczeństwa w branży usług finansowych decydują się na pomoc ekspertów, aby rozwiązać swoje problemy.

Najważniejsze wnioski

W niniejszym artykule eksperci firmy Cisco analizują możliwości zapewnienia bezpieczeństwa informatycznego w branży usług finansowych na podstawie danych porównawczych pochodzących z badania „Cisco Security Capabilities Benchmark Study”[1]. Przeprowadzona analiza doprowadziła nas do następujących wniosków:

- Menadżerowie poszczególnych działów firmy przejmują coraz większą odpowiedzialność za jej bezpieczeństwo. W 2014 r. 46% ankietowanych osób potwierdziło, że szefowie pionów mają wpływ na politykę i procedury dotyczące bezpieczeństwa; w 2015 r. liczba ta wzrosła do 59%.
- Branża docenia wkład niezależnych ekspertów w procesy doskonalenia mechanizmów kontroli bezpieczeństwa. Firmy zwiększyły outsourcing zespołów reagowania i analizy zagrożeń. W 2014 r. 33% firm korzystało ze wsparcia takich zespołów, natomiast w 2015 r. liczba ta wzrosła do 43%.
- Organizacje oferujące usługi finansowe ograniczają wykorzystanie narzędzi służących do wykrywania i blokowania zagrożeń. W 2014 r. 57% ankietowanych odpowiedziało, że korzysta z narzędzi kontroli dostępu i uwierzytelniania. Odsetek ten spadł do 48% w 2015 r. W 2014 r. 43% osób potwierdziło, że korzysta z narzędzi śledzenia aktywności w sieci, jednak w 2015 r. było to już tylko 32%.
- Wzrasta świadomość faktu, że poprawa bezpieczeństwa w takim samym stopniu zależy od ludzi jak od technologii. W związku z tym sektor usług finansowych coraz bardziej docenia znaczenie szkoleń. 44% dyrektorów ds. bezpieczeństwa informacji przyznało, że zwiększyli liczbę szkoleń pracowniczych z wiedzy na temat bezpieczeństwa oraz zwielokrotnili inwestycje w szkolenia dla specjalistów ds. bezpieczeństwa.

Bezpieczeństwo jako istotny element cyfrowej strategii

Zaawansowane wykorzystanie technologii cyfrowych jest obecnie postrzegane jako niezbędny element sukcesu firm z branży usług finansowych. Posiadając odpowiednie możliwości cyfrowe, firmy mogą szybko wykrywać zagrożenia, zanim staną one na drodze do osiągnięcia rynkowych celów. Kadra kierownicza w branży usług finansowych docenia wartość cyfryzacji: Ostatnie badanie„Cybersecurity as a Growth Advantage” przeprowadzone przez Cisco, ujawniło, że 69% kadry zarządzającej z różnych branż uznaje cyfryzację za bardzo ważny czynnik kształtujący ich aktualną strategię rozwoju.[2]

Rozumieją oni jednak także, że niewystarczające zabezpieczenia mogą zniweczyć te ambitne plany. W tym samym badaniu 71% przedstawicieli kadry zarządzającej przyznało, że obawy związane z bezpieczeństwem cyfrowym hamują innowacje w ich firmach. 39% z nich potwierdziło wstrzymanie inicjatyw o krytycznym znaczeniu ze względu na kwestie cyberbezpieczeństwa.

Opinie te zostały potwierdzone w niedawnym badaniu spółek giełdowych przeprowadzonym przez dział Governance Services Nowojorskiej Giełdy Papierów Wartościowych: 43% szefów firm stwierdziło, że zapewnienie bezpieczeństwa nowych produktów i usług to jedna z głównych barier w nadążaniu za tempem przemian w branży.[3] Jeśli przedsiębiorstwa z branży usług finansowych chcą z powodzeniem inwestować w rozwiązania cyfrowe, muszą inwestować także w bezpieczeństwo, aby chronić swoje procesy i dane.

[1] Więcej informacji na temat badania oraz innych opracowań z tej serii można znaleźć na ostatnich stronach niniejszego dokumentu.

[2] „Cybersecurity as a Growth Advantage”” Cisco, kwiecień 2016: http://www.connectedfuturesmag.com/CyberSecurity/

[3] *Cybersecurity in the Boardroom*, NYSE Governance Services, maj 2015: https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf

Menadżerowie działów w coraz większym stopniu odpowiadają za bezpieczeństwo

Aby sprostać wyzwaniom cyfryzacji, poszczególne działy firmy próbują czasami zarządzać elementami bezpieczeństwa samodzielnie, bez konsultacji ze specjalistami ds. bezpieczeństwa. Tego rodzaju próby prowadzą do powstawania problemu „równoległych systemów informatycznych"(tzw. Shadow IT). Na przykład, poszczególne działy chcąc zwiększyć zadowolenie klientów lub przyspieszyć procesy biznesowe, wprowadzają rozwiązania technologiczne nie konsultując ich z zespołami ds. bezpieczeństwa czy z działami IT. Takie praktyki mogą jednak mieć wpływ na widoczność w rozszerzonej sieci i wpływać na możliwości zespołu ds. bezpieczeństwa w egzekwowaniu obowiązujących procedur na każdym serwerze, aplikacji czy urządzeniu. Tego rodzaju działania mogą również skutecznie utrudniać osiągnięcie celów, jakie stawia przed firmą proces cyfryzacji, takich jak zwiększona świadomość zmian w środowisku biznesowym.

Ponieważ luka w systemie bezpieczeństwa spowodowana przez urządzenie zainstalowane przez jeden dział może wyrządzić szkody w całej firmie, ważne jest, aby poszczególne działy rozumiały wady stosowania „równoległych systemów informatycznych". Dobra wiadomość jest taka, że w branży finansowej coraz więcej menadżerów poszczególnych działów przejmuje zwiększoną odpowiedzialność za bezpieczeństwo firmy. W 2014 r. 46% ankietowanych odpowiedziało, że szefowie pionów byli zachęcani do współtworzenia polityki i procedur dotyczących bezpieczeństwa. W 2015 r. liczba ta wzrosła do 59% (Rysunek 1).

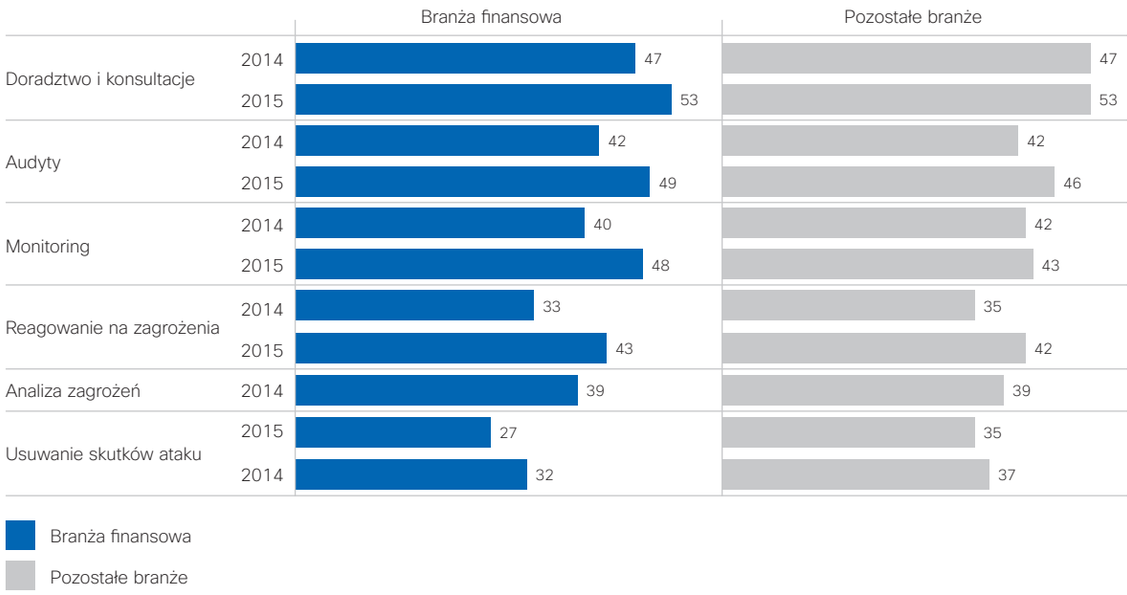
Rysunek 1. Odsetek organizacji zgadzających się z różnymi stwierdzeniami dotyczącymi bezpieczeństwa w ich organizacjach. Lata 2014 i 2015.

Wiedza niezależnych ekspertów pomaga wypełnić luki w zabezpieczeniach

Jeśli przedsiębiorstwa z branży usług finansowych chcą rozwijać się dzięki włączeniu technologii cyfrowych do swojej oferty, muszą zrozumieć, że bezpieczeństwo cyfrowe jest podstawą takiego rozwoju. Ci, którzy doceniają znaczenie bezpieczeństwa w procesie cyfrowego rozwoju firmy rozumieją, że cyfryzacja to droga do sukcesu, nie tylko taktyka obronna. Rozumieją oni także, że digitalizacja wymaga odpowiedzi na istotne pytania. Na przykład, w jaki sposób firma może oferować klientom więcej, chroniąc jednocześnie swoje dane? Korzystanie z pomocy zewnętrznych ekspertów i narzędzi jest coraz powszechniejszą praktyką wśród

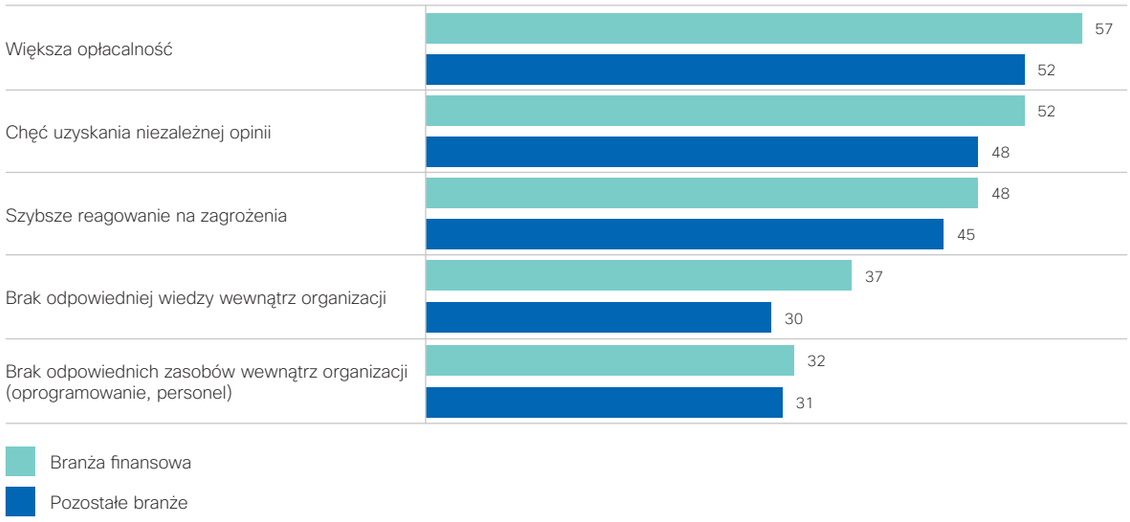
organizacji w branży finansowej.. W 2015 r. organizacje te były bardziej skłonne do zlecania usług związanych z bezpieczeństwem podmiotom zewnętrznym niż rok wcześniej. Przykładowo, częściej korzystano z usług zespołów reagujących na zagrożenia. W 2014 r. 33% firm korzystało z zewnętrznych zespołów, w 2015 r. liczba ta wzrosła do 43% (Rysunek 2).

Rysunek 2. Odsetek organizacji zlecających zadania związane z bezpieczeństwem podmiotom zewnętrznym. Lata 2014 i 2015.



Przedsiębiorstwa z branży finansowej coraz częściej uświadamiają sobie potrzebę wsparcia z zewnątrz. Respondenci z 37% organizacji korzystających z outsourcingu usług związanych z bezpieczeństwem przyznali, że nie posiadają w firmie odpowiednich ekspertów. Zaledwie 30% respondentów z innych branż odpowiedziało w ten sam sposób (Rysunek 3).

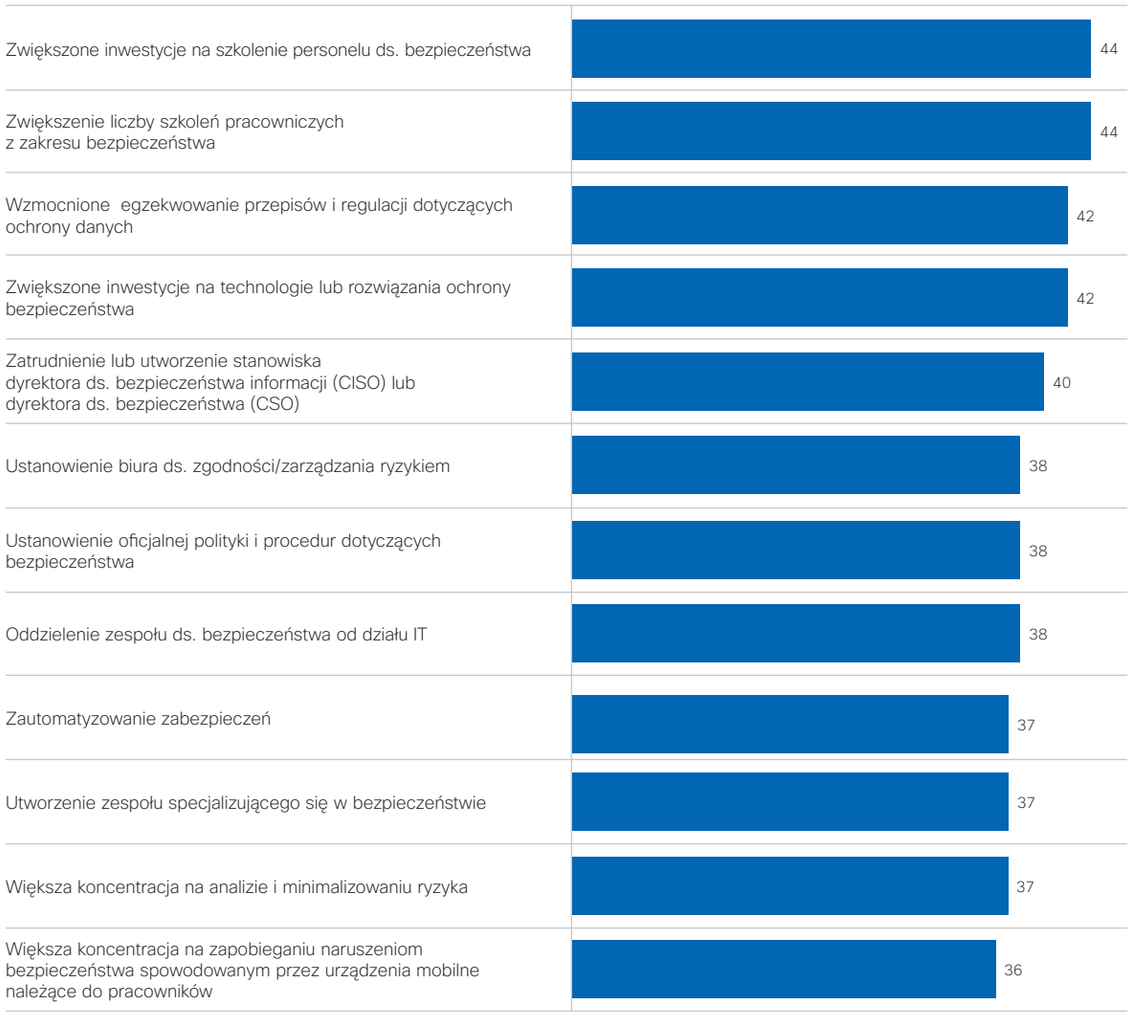
Rysunek 3. Powody, dla których organizacje z branży finansowej zlecają usługi związane bezpieczeństwa podmiotom zewnętrznym



Szkolenie podnosi kwalifikacje pracowników

Szkolenia z zakresu bezpieczeństwa, zarówno zespołu ds. bezpieczeństwa, jak i pozostałych pracowników nie tylko pozwalają na efektywniejszą walkę z zagrożeniami, ale również zwiększają świadomość kwestii bezpieczeństwa w całej firmie. Cieszy fakt, że branża finansowa dostrzega ten potencjał inwestując w poszerzanie zakresu wiedzy pracowników. To krok w dobrym kierunku, ponieważ walka z zagrożeniami wymaga zarówno zintegrowanych rozwiązań technologicznych jak i wykwalifikowanego personelu. Przykładowo, wśród organizacji, które były przedmiotem kontroli władz z powodu naruszenia bezpieczeństwa danych, 44% respondentów przyznało, że zwiększyli oni liczbę szkoleń z zakresu bezpieczeństwa dla pracowników oraz zainwestowali większe środki w szkolenie specjalistów ds. bezpieczeństwa (Rysunek 4).

Rysunek 4. Odsetek organizacji podejmujących kroki mające na celu zwiększenia ich bezpieczeństwa

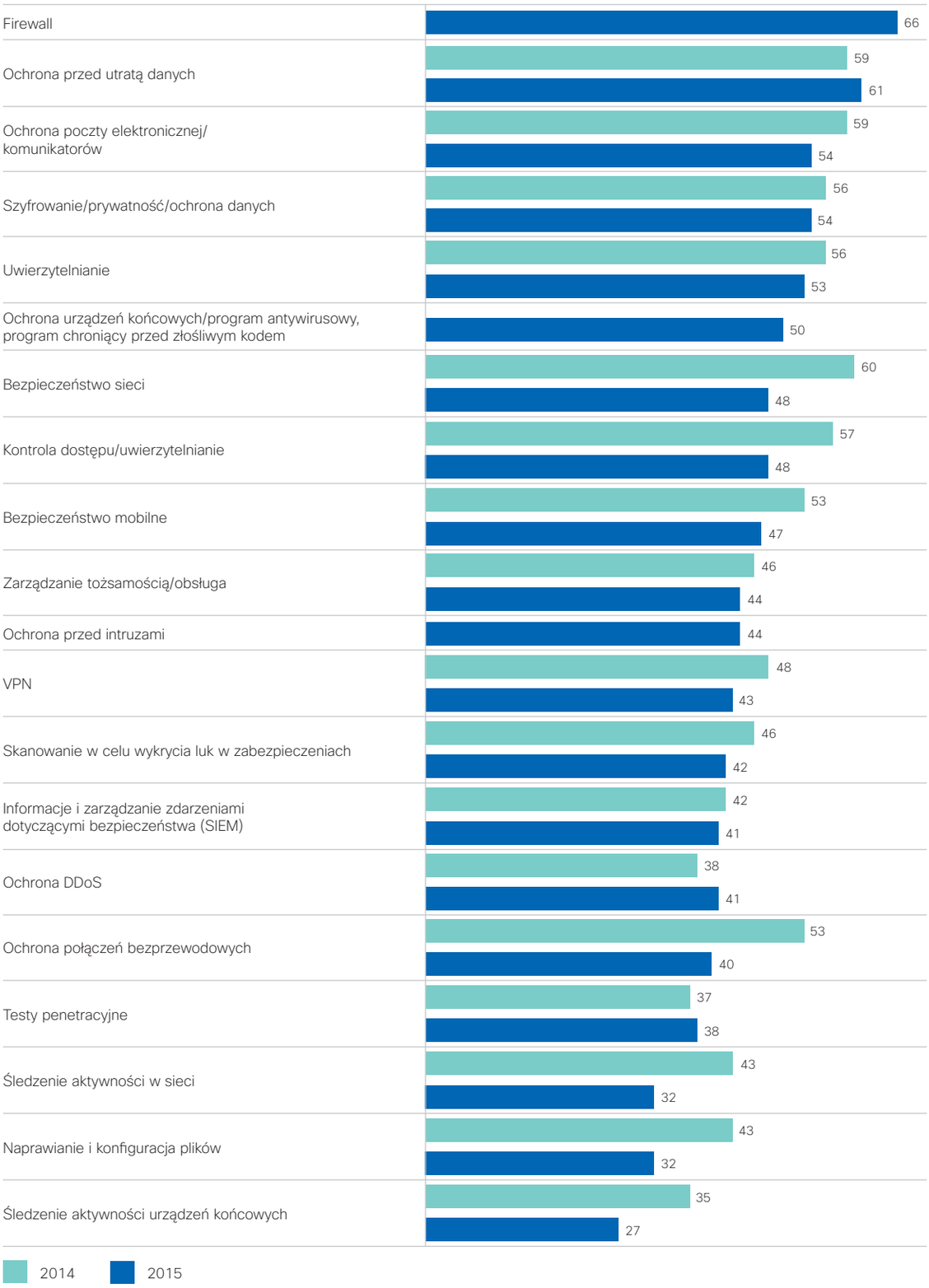


Równoczesne wykorzystanie różnych narzędzi ochrony przed zagrożeniami

Ponieważ organizacje z sektora usług finansowych postrzegają bezpieczeństwo cyfrowe jako element przewagi konkurencyjnej i korzystają z usług ekspertów w celu budowania swojej architektury bezpieczeństwa, mogą one w mniejszym stopniu korzystać z dodatkowych narzędzi ochrony. Z drugiej strony, konsolidacja narzędzi ochrony przed zagrożeniami mogłaby oznaczać, że organizacje finansowe nie odpowiadają w pełni na złożone potrzeby w zakresie bezpieczeństwa.

W 2014 r. 57% ankietowanych odpowiedziało, że korzysta z narzędzi kontroli dostępu i uwierzytelniania, jednak liczba ta spadła w 2015 r do 48%. W 2014 r. 43% osób potwierdziło, że korzysta z narzędzi śledzenia aktywności w sieci, jednak w 2015 r. było to już tylko 32% (Rysunek 5).

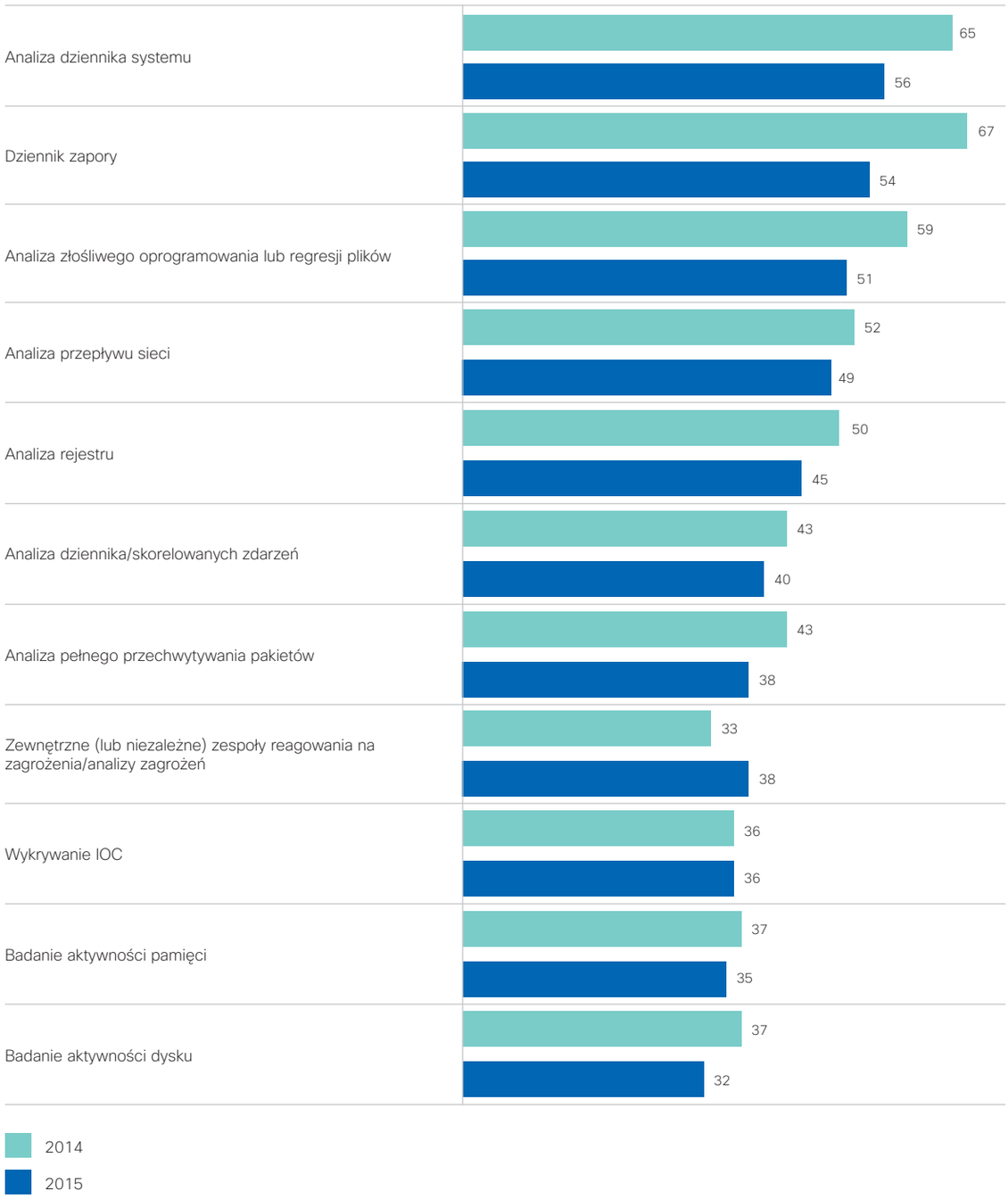
Rysunek 5. Odsetek organizacji korzystających z podstawowych narzędzi ochrony przed zagrożeniami. Lata 2014 i 2015.



Uwaga: Firewall, ochrona przed intruzami oraz ochrona urządzeń końcowych/program antywirusowy, program chroniący przed złośliwym kodem zostały dodane jako niezależne elementy w 2015 r. Z tego względu ich wartości dla 2014 r. nie są dostępne.

Organizacje z sektora usług finansowych wykazują również malejące zainteresowanie wykorzystaniem procesów analizujących naruszenia i eliminujących przyczyny incydentów związanych z bezpieczeństwem. W 2014 r. 65% organizacji z sektora usług finansowych korzystało z analiz dziennika systemu, w 2015 r. liczba ta wynosiła zaledwie 56% (Rysunek 6). Podobnie w 2014 r. 49% takich organizacji korzystało z innych narzędzi w celu przywrócenia systemów do ich wcześniejszego stanu; w 2015 r. wartość ta spadła do zaledwie 39%.

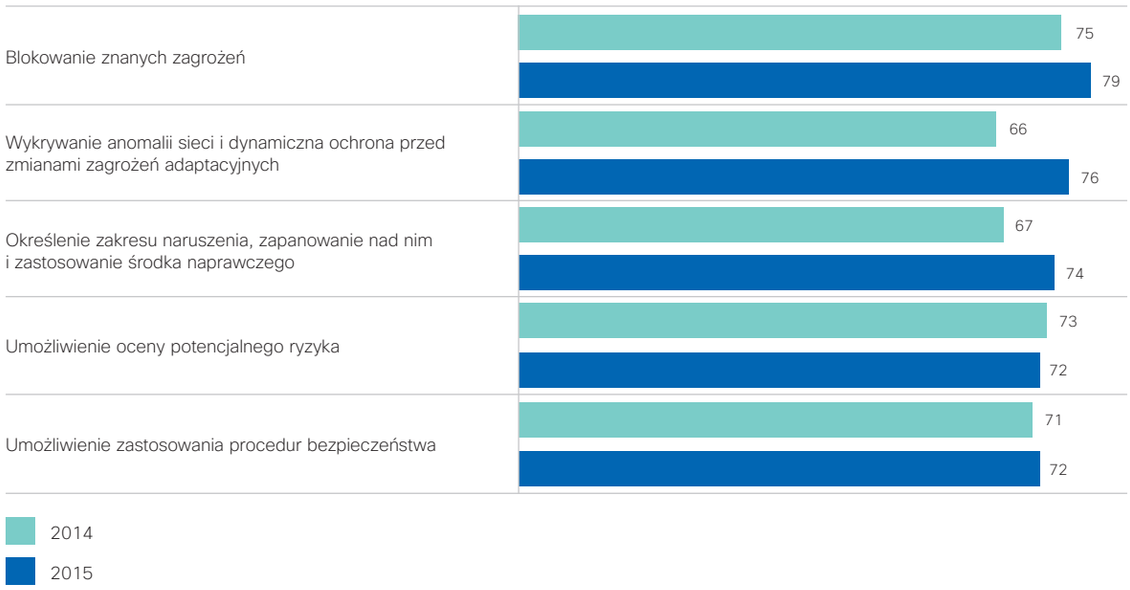
Rysunek 6. Odsetek organizacji korzystających z procesów mających na celu analizę naruszeń i wyeliminowanie przyczyn incydentów związanych z bezpieczeństwem.



Wzrost przekonania o skuteczności zabezpieczeń

Organizacje z sektora usług finansowych muszą stale usprawniać integrację i zarządzanie złożonymi procesami swojego systemu bezpieczeństwa. Przykładanie coraz większej wagi do szkoleń i poleganie na zewnętrznych ekspertach może przyczynić się do wzmocnienia przekonania co do możliwości systemu zabezpieczeń firmy. W 2014 r. 66% badanych stwierdziło, że ich systemy bardzo skutecznie wykrywają anomalie w sieci i chronią ją przed zagrożeniami. W 2015 r. liczba ta wzrosła do 76%. Podobnie w 2014 r. 67% stwierdziło, że ich narzędzia zabezpieczeń są w stanie skutecznie określić zakres naruszenia. Odsetek ten wzrósł do 74% w 2015 r. (Rysunek 7).

Rysunek 7. Odsetek respondentów przekonanych o skuteczności swoich narzędzi zabezpieczeń.



Wnioski: Strategia bezpieczeństwa podstawą cyfrowego rozwoju

Organizacje z branży finansowej coraz częściej budują swój sukces bazując na cyfrowych modelach biznesowych, a kwestie bezpieczeństwa są integralną częścią planu ich rozwoju. Warto jednak zwrócić uwagę na wyzwania jakie stoją przed firmami z branży finansowej – problem tzw. równoległych systemów informatycznych (Shadow IT), czy coraz rzadsze korzystanie z powszechnych narzędzi ochrony przed zagrożeniami.

Innowacyjność i efektywność to kluczowe czynniki decydujące o konkurencyjności w świecie usług finansowych. Odpowiednie administrowanie kwestiami bezpieczeństwa czyni je równie istotnym czynnikiem decydującym o rozwoju firmy, jak jakość obsługi klienta czy sposób zarządzania. Bezpieczeństwo stało się kluczowym elementem zapewniającym płynność i efektywność działań firmy. Aby bezpieczeństwo stało się również istotnym czynnikiem umożliwiającym osiągnięcie sukcesu w branży finansowej, firmy powinny wykorzystywać potencjał zaawansowanych technologii, procesów oraz wykwalifikowanych pracowników. Te trzy elementy muszą ze sobą współdziałać. Sukces jest możliwy do osiągnięcia, jeśli bezpieczeństwo jest integralną częścią ogólnego planu digitalizacji firmy i jej funkcjonowania w erze cyfrowej transformacji.

Integrując kwestie bezpieczeństwa od podstaw z działalnością firmy, przedsiębiorstwa z branży finansowej mają szansę uniknąć efektu fragmentarycznej ochrony czy potencjalnych luk w systemie zabezpieczeń. Zalecenia dla specjalistów ds. bezpieczeństwa w branży usług finansowych:

- Wiedza na temat zagrożeń jako centralna część strategii bezpieczeństwa pozwala zyskać wysoką świadomość procesów potrzebną do osiągnięcia sukcesu i umożliwia szybką i świadomą reakcję na zagrożenia.
- Weryfikacja zakresu wykorzystania usług ekspertów zewnętrznych umożliwi uporanie się ze złożonością procesów, które musi przejść organizacja na drodze cyfryzacji.
- Ścisła współpraca z menadżerami poszczególnych działów w celu wypracowania spójnej strategii bezpieczeństwa i uświadamianiu znaczenia bezpieczeństwa jako kluczowego czynnika rozwoju.

Szybsza droga do bezpiecznej cyfryzacji

Usprawnienia w zakresie bezpieczeństwa powinny być częścią rozmów na temat planów rozwoju cyfrowego. Oto przykłady najlepszych praktyk wykorzystania bezpieczeństwa jako elementu przewagi konkurencyjnej:

- Redukcja ryzyka poprzez wybór projektów o wysokim współczynniku ryzyka zamiast profilu o niskim poziomie ryzyka. Stawiający na bezpieczną cyfryzację podejmują większe ryzyko, ale płynące z niego korzyści przewyższają koszty.
- Przeprojektowanie procesów cyfrowych, w taki sposób aby cyberbezpieczeństwo stanowiło ich fundament. Zidentyfikowanie niezabezpieczonych technologii i procesów biznesowych, które się na nich opierają. Zastąpienie ich technologiami, które posiadają zintegrowane od podstaw rozwiązania cyberbezpieczeństwa.
- Zwiększenie wiedzy na temat bezpieczeństwa cyfrowego na każdym poziomie organizacji. Te same aktywne działania, które pomagają firmom osiągnąć sukces w dziedzinie bezpieczeństwa cyfrowego mogą także stymulować rozwój produktów, wspierać ochronę przed ryzykiem oraz usprawniać procesy analizy i reagowania na zagrożenia w innych obszarach działalności organizacji.

Więcej informacji na temat wpływu bezpieczeństwa na konkurencyjność organizacji można znaleźć w raporcie „Cybersecurity as a Growth Advantage” dostępnym na stronie www.connectedfuturesmag.com/cybersecurity

Więcej informacji

Więcej informacji na temat szerszej oferty firmy Cisco w zakresie ochrony przed zagrożeniami można znaleźć pod adresem www.cisco.com/go/security

Cisco Security Capabilities Benchmark Study 2015 – Informacje

Badanie Cisco 2015 Security Capabilities Benchmark Study analizuje technologie ochronne w trzech wymiarach: zasobów, możliwości i stopnia zaawansowania. Badanie obejmuje organizacje z kilku branż działające w 12 krajach. Łącznie w badaniu wzięło udział ponad 2400 specjalistów ds. bezpieczeństwa, w tym dyrektorzy ds. bezpieczeństwa informacji oraz kierownicy ds. bezpieczeństwa. Byli to ankietowani z następujących krajów: Australia, Brazylia, Chiny, Francja, Indie, Japonia, Meksyk, Niemcy, Rosja, Stany Zjednoczone, Wielka Brytania i Włochy. Kraje te zostały wybrane ze względu na ich znaczenie gospodarcze oraz zróżnicowanie geograficzne.

Analizę wyników szerszego badania Cisco Security Capabilities Benchmark Study można znaleźć w Rocznym raporcie firmy Cisco dotyczącym bezpieczeństwa 2016 („Cisco 2016 Annual Security Report") dostępnym pod adresem www.cisco.com/go/asr2016

Informacje na temat niniejszej serii

Zespół specjalistów Cisco dla określonych branż i rynków przeanalizował wyniki badania Cisco Security Capabilities Benchmark Study 2015. W swojej analizie przedstawili oni swoje dokładne opinie na temat sektora bezpieczeństwa w 10 krajach i czterech branżach (usługi finansowe, ochrona zdrowia, telekomunikacja i transport). Opracowania z tej serii opisują obszar bezpieczeństwa i wyzwania związane z bezpieczeństwem cyfrowym, jakie stoją przed organizacjami. Ten proces pozwolił ukazać wyniki badania w szerszym kontekście, a także skupić się na tematach odpowiednich dla każdego przeanalizowanego kraju i branży.

O firmie Cisco

Cisco tworzy skuteczne rozwiązania, które są zintegrowane, zautomatyzowane, otwarte i proste w użyciu. Czerpiąc z niezrównanej sieci połączeń oraz najbardziej rozbudowanych i zaawansowanych technologii i wiedzy eksperckiej, firma Cisco zapewnia najlepszą możliwą widoczność i odpowiedź na zagrożenia, umożliwiając szybsze ich zwalczanie. Korzystając z rozwiązań firmy Cisco w zakresie bezpieczeństwa, firmy są lepiej przygotowane do korzystania z nieograniczonych możliwości cyfrowych rozwiązań dla biznesu.

Americas Headquarters
Cisco Systems Inc.
San Jose CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Firma Cisco posiada ponad 200 oddziałów na całym świecie.
Adresy wraz z numerami telefonu i faksu można znaleźć na stronie internetowej Cisco pod adresem **www.cisco.com/go/offices**