Duże przedsiębiorstwa w Polsce a bezpieczeństwo IT

Wrzesień 2014

FORTINET®

SPIS TREŚCI

Opis badania ... 3

Opis badanej próby przedsiębiorstw ... 4

Wybór dostawcy rozwiązań bezpieczeństwa IT ... 6

Korzystanie z rozwiązań wielofunkcyjnych ... 9

Ocena urządzeń klasy Next Generation Firewall ... 11

Dodatkowy budżet na IT i proponowane zakupy ... 12

Trendy i bieżące wydarzenia na rynku IT ... 14

Rozwój nowych technologii a bezpieczeństwo IT ... 14

Konflikt na Ukrainie ... 15

FORTINET ... 17

Kontakt ... 17

PMR ... 17

Kontakt ... 17

OPIS BADANIA

FORTINET, producent zaawansowanych rozwiązań bezpieczeństwa sieciowego, zlecił firmie badawczej PMR przeprowadzenie badania pt. „Duże przedsiębiorstwa w Polsce a bezpieczeństwo IT", którego celem było dowiedzenie się, jak największe firmy w kraju podchodzą do kwestii związanych z bezpieczeństwem sieciowym. Badanie pozwoliło m.in. odpowiedzieć na następujące pytania:

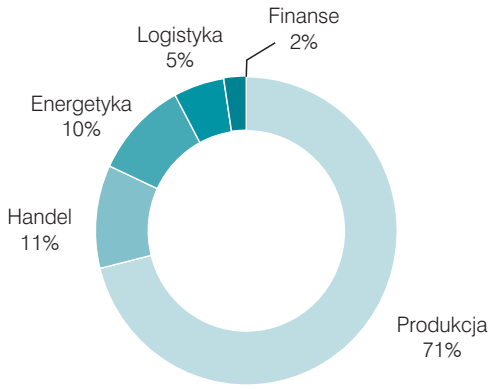
- Jakie czynniki determinują wybór producenta rozwiązań bezpieczeństwa IT w dużych firmach?;
- Czy duże przedsiębiorstwa korzystają ze wsparcia firm zewnętrznych w zakresie wyboru systemów bezpieczeństwa IT i jeśli tak, dlaczego?;
- Jak duży wpływ na wybór konkretnego rozwiązania bezpieczeństwa IT ma partner wdrożeniowy?;
- Czy przy zabezpieczaniu firmy przed atakami cyberprzestępców warto korzystać z wielofunkcyjnych rozwiązań bezpieczeństwa typu UTM, NGFW? Które z nich jest lepsze?;
- Na jakie rozwiązania IT w pierwszej kolejności firmy przeznaczyłyby dodatkowy, nadprogramowy budżet?;
- Które trendy obecnie kształtujące rynek IT (BYOD, mobilność, Big Data, chmura, wirtualizacja) niosą ze sobą największe wyzwania pod kątem bezpieczeństwa danych w dużej firmie?;
- Które z istniejących zagrożeń są najbardziej wymagające dla dużych firm i traktowane przez nie jako najbardziej niebezpieczne?;
- Czy sytuacja geopolityczna na wschodzie Europy w jakikolwiek sposób wpływa na poziom bezpieczeństwa polskich przedsiębiorstw?

W badaniu wzięło udział 166 respondentów odpowiedzialnych za zarządzanie budżetami na informatykę w polskich przedsiębiorstwach zatrudniających co najmniej 250 pracowników, działających w pięciu głównych obszarach gospodarki (produkcja, handel, energetyka, finanse i logistyka). Badanie zrealizowano w II kwartale 2014 roku.

OPIS BADANEJ PRÓBY PRZEDSIĘBIORSTW

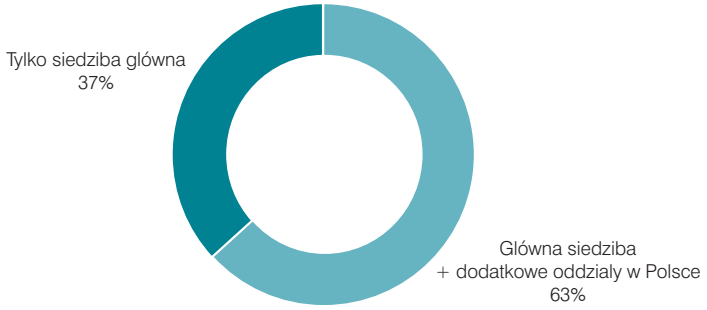
Większość badanych przedsiębiorstw stanowiły firmy produkcyjne. Znaczną grupę stanowiły także firmy handlowe oraz działające w branży energetycznej.

Struktura próby ze względu na branżę



Źródło: PMR, 2014

Czy Państwa firma posiada, oprócz głównej siedziby, także inne oddziały w Polsce



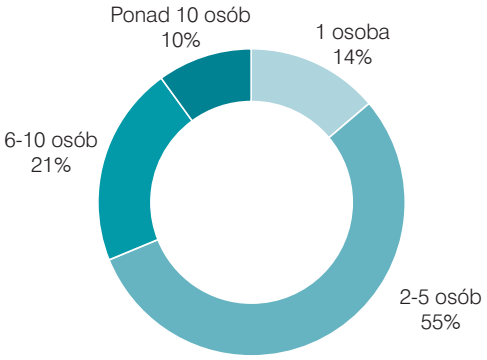
Źródło: PMR, 2014

Większość badanych przedsiębiorstw to podmioty, które oprócz głównej siedziby posiadają także dodatkowe oddziały w Polsce (63%), co jest istotną informacją w kontekście gwarantowania bezpieczeństwa wewnętrznej sieci firmowej.

Badane polskie przedsiębiorstwa na dużą skalę wykorzystują rozwiązania teleinformatyczne, posiadają więc rozbudowane działy IT. Do wyjątków należą przedsiębiorstwa zatrudniające tylko jednego pracownika (14%). Regułą jest zespół 2-5 osobowy, natomiast co dziesiąte badane przedsiębiorstwo zatrudnia na etat co najmniej 10 informatyków.

Jednocześnie połowa dużych firm (46%) regularnie korzysta z usług zewnętrznych firm oferujących specjalistyczną pomoc w zakresie bezpieczeństwa IT.

Liczba pracowników działu IT w przeliczeniu na etaty.



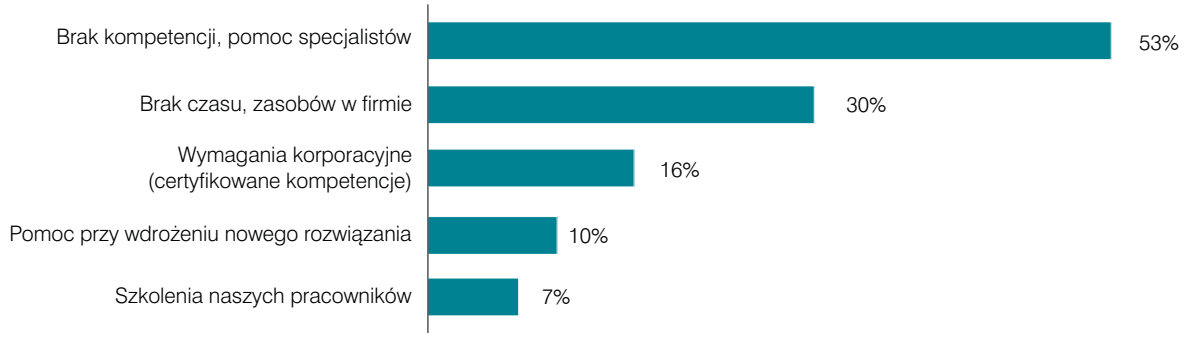
Źródło: PMR, 2014

Czy korzystacie państwo z usług zewnętrznych specjalistów bezpieczeństwa IT?

Źródło: PMR, 2014

Do listy głównych powodów korzystania z zewnętrznej pomocy respondenci wymieniali przede wszystkim brak kompetencji pracowników firmy w wąskich obszarach związanych z zabezpieczeniem sieci. Chodzi głównie o wiedzę w zakresie konfiguracji nowych urządzeń i rozwiązywania niestandardowych problemów. Firmy decydują się także na pomoc zewnętrznych usługodawców w przypadku braku zasobów ludzkich lub braku czasu pracowników na zajmowanie się danym zadaniem. W przypadku największych przedsiębiorstw częstym powodem są także wymagania korporacyjne, które wymuszają posiadanie odpowiednich certyfikacji.

Dlaczego zdecydowaliście się Państwo na oddanie prac związanych z systemami bezpieczeństwa do zewnętrznej firmy?



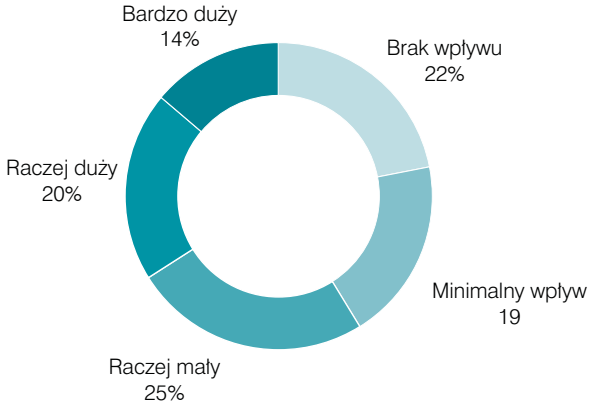
Źródło: PMR, 2014

Wiedza specjalistów w zakresie bezpieczeństwa sieciowego doceniana jest również na etapie wdrożenia. Tylko w jednej piątej przedsiębiorstw (22%) przy wdrażaniu rozwiązań bezpieczeństwa sieciowego nie sugerowano się uwagami partnera wdrożeniowego, natomiast w co trzeciej firmie partner wdrożeniowy miał duży wpływ na wybór konkretnego rozwiązania (urządzenia). Respondenci, z którymi realizowano badanie przyznawali, że korzystają z pomocy wdrożeniowców przede wszystkim dlatego, że ich wiedza jest aktualna, są zaznajomieni z obecnymi na rynku najlepszymi urządzeniami. Informatycy na co dzień zajmujący się bezpieczeństwem sieci wewnętrznej w firmie nie mają czasu ani możliwości, aby na bieżąco śledzić nowości rynkowe.

WYBÓR DOSTAWCY ROZWIĄZAŃ BEZPIECZEŃSTWA IT

Badani wskazywali, że rozeznanie produktów dostępnych na rynku robione jest dopiero w momencie podjęcia decyzji o zakupie nowego urządzenia. Nie istnieje praktyka stałego monitoringu oferty dostawców. Między innymi z tego względu pomoc partnera wdrożeniowego jest tak istotna dla wielu spośród badanych respondentów. Partner wdrożeniowy pozostaje na bieżąco z nowościami rynkowymi i może, na podstawie własnych doświadczeń, sugerować firmom konkretne rozwiązania. Najważniejszy jest jednak zakres usług oferowanych przez producentów.

Proszę ocenić jak duży wpływ na wybór konkretnego rozwiązania z zakresu sieciowego bezpieczeństwa IT w Państwa firmie miał partner wdrożeniowy?



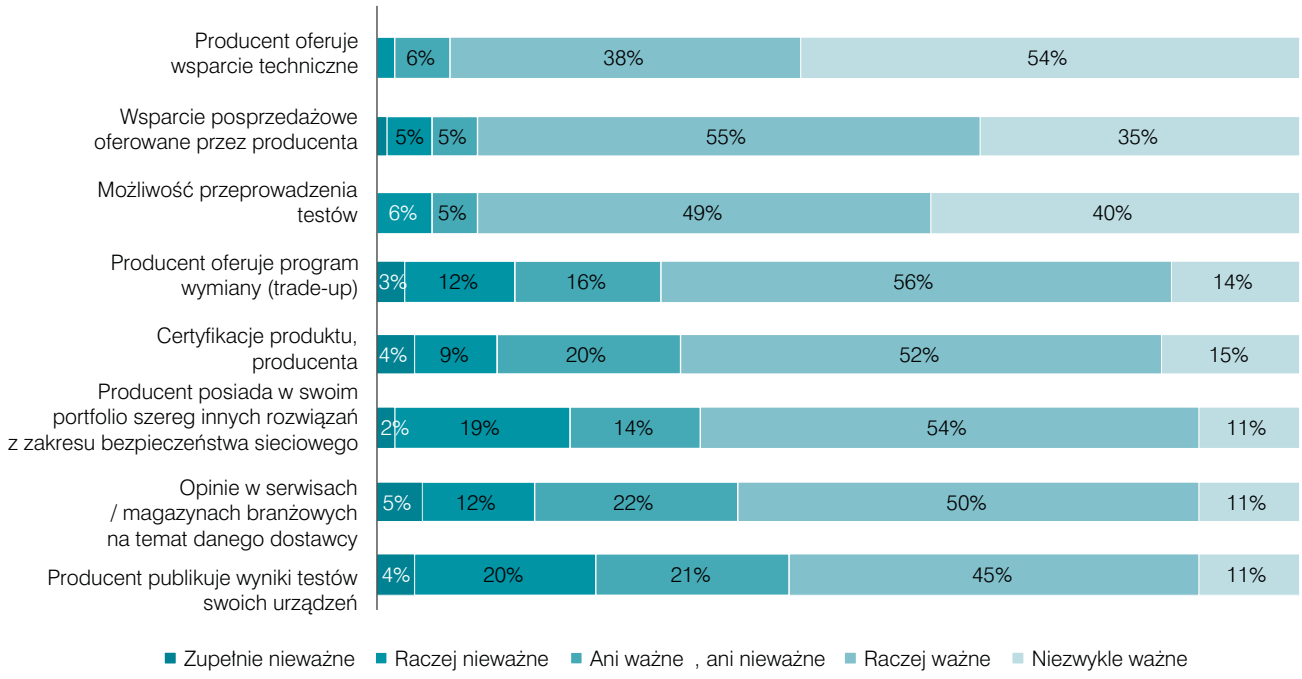
Źródło: PMR, 2014

Duże przedsiębiorstwa oczekują od dostawców rozwiązań bezpieczeństwa IT przede wszystkim szeroko rozumianego wsparcia technicznego i posprzedażowego oraz np. możliwości przeprowadzenia testów urządzeń we własnym środowisku pracy. Ponieważ rozwiązania bezpieczeństwa IT należą do produktów wysoce specjalistycznych, kosztownych i wymagających dużej wiedzy oraz doświadczenia, badani podkreślali jak bardzo kluczowymi dla nich są dobre relacje z producentami. Klienci z sektora

dużych przedsiębiorstw oczekują zindywidualizowanego podejścia do klienta, szybkiego i sprawnego wsparcia oraz błyskawicznej pomocy w rozwiązaniu zgłoszonego problemu.

Dla badanych przedstawicieli dużych firm istotne są również inne czynniki, takie jak możliwość skorzystania z modelu trade-up, posiadanie przez producenta odpowiednich certyfikacji, szerokie portfolio rozwiązań, opinie o firmie dostępne w specjalistycznych serwisach, magazynach branżowych oraz publikowane przez producenta wyniki testów oferowanych rozwiązań.

Ocenia ważności czynników przy wyborze dostawcy rozwiązań z zakresu IT security



Źródło: PMR, 2014

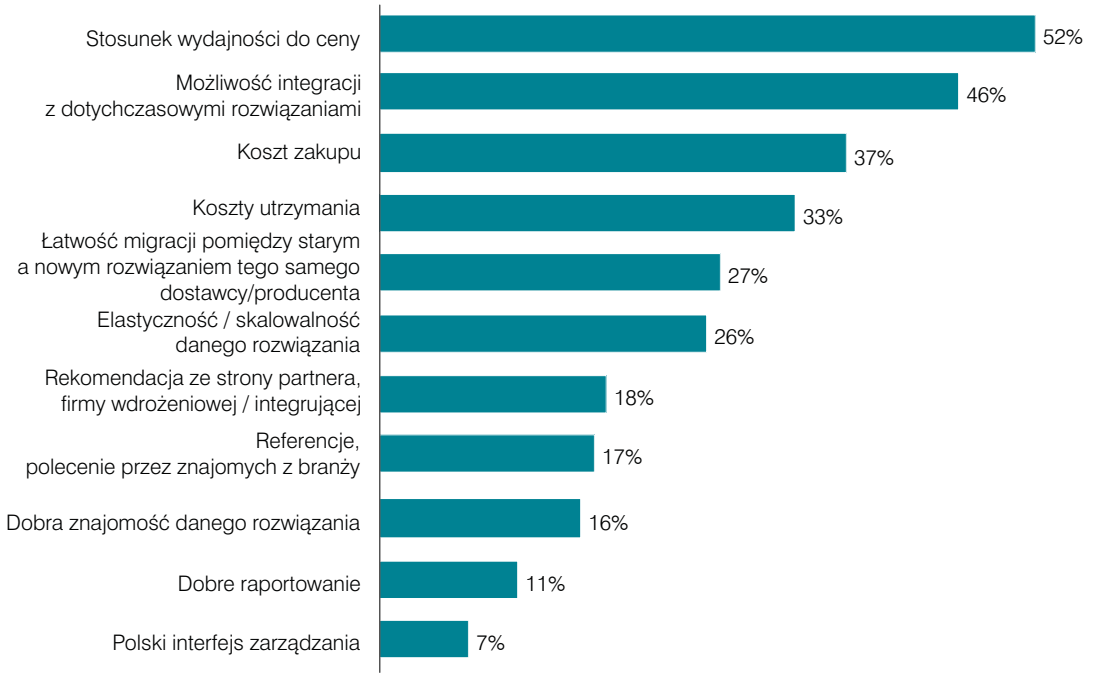
Wybierając konkretny produkt klienci ostatecznie kierują się kryterium stosunku wydajności rozwiązania do ceny – weryfikują jakie funkcjonalności oraz jakość oferuje producent przy danym typie kosztów. Z punktu widzenia użytkowników znaczenie ma nie tylko sam koszt zakupu, ale także koszt utrzymania rozwiązania – wliczając koszty serwisu urządzenia, wyszkolenia pracowników firmy, którzy będą obsługiwali maszynę oraz ewentualne koszty szkolenia i wsparcia oferowanego przez zewnętrznych ekspertów.

Niebagatelne znacznie z punktu widzenia dużych przedsiębiorstw, w których korzysta się na duża skalę z rozwiązań bezpieczeństwa IT jest także możliwość integracji sprzętu z dotychczas wykorzystywanymi rozwiązaniami, ponieważ rzadko kiedy w grę wchodzi możliwość wymiany całej infrastruktury zabezpieczającej. Warto w tym miejscu zwrócić uwagę na korporacyjne wymogi największych przedsiębiorstw, które ze względu na obowiązujące w powiązanych spółkach standardy, ograniczają listę dostawców do kilku liderów rynku. Inercja organizacji działa hamująco na tempo

wymiany sprzętu i wdrażanie najnowszych rozwiązań. Decyzje na temat zakupów zapadają w tego typu firmach najczęściej w zagranicznej centrali. Dla badanych ważna jest zatem również łatwość migracji ze starszych rozwiązań do najnowszych urządzeń danego producenta (sygnalizowany wcześniej trade-up).

Co interesujące, respondenci rzadko poza ceną wskazywali na parametry lub charakterystyki samych rozwiązań (skalowalność, raportowanie, polski interfejs), co może też sugerować, że producenci sprzętu w opinii badanych oferują rozwiązania podobnej klasy. Różnica między nimi widoczna jest przede wszystkim na poziomie jakości obsługi przed i posprzedażowej, przy czym warto tu podkreślić, że respondenci przyznawali często, że bazują na zasłyszanej opinii.

Jakie czynniki biorą P. pod uwagę wybierając konkretne rozwiązania w zakresie bezpieczeństwa sieciowego



Źródło: PMR, 2014

W większości segmentów polskiego rynku IT współczynnik ceny do jakości (wydajności) ma największe znaczenie dla nabywcy i od niego zaczyna się podejmowanie decyzji zakupowych. Zaraz za tym czynnikiem znajdują się wsparcie techniczne i serwis, jak również koszty utrzymania rozwiązania. Widać jak na dłoni, że rynek bezpieczeństwa sieciowego nie jest w tym przypadku żadnym wyjątkiem. Warto przy tym podkreślić, że im większa firma, tym większą wagę mają strategia długookresowa i planowanie, a także już posiadana infrastruktura. W rezultacie integracja z już funkcjonującym ekosystemem nabiera dużo większego znaczenia, podobnie jak perspektywa wymiany i migracji do nowej generacji urządzeń w przyszłości. W przypadku podobnej klasy rozwiązań o wyborze danego producenta będzie decydować wsparcie posprzedażowe. Nie do przecenienia jest też możliwość przetestowania danego rozwiązania, między innymi po to, by przekonać się nie tylko o jego wydajności i parametrach, ale przede wszystkim by sprawdzić, czy w praktyce jest adekwatne do wymagań i oczekiwań. Pomaga to uniknąć rozczarowań i budowania negatywnych opinii o producencie, który ma zwykle w ofercie cały wachlarz rozwiązań i często dopiero testy pozwalają ocenić, co klientowi najbardziej odpowiada.

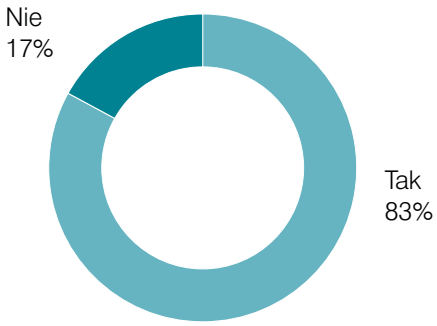
Paweł Olszynka – Główny Analityk Rynku Telekomunikacyjnego i IT w PMR

KORZYSTANIE Z ROZWIĄZAŃ WIELOFUNKCYJNYCH

Dla zdecydowanej większości ekspertów ds. bezpieczeństwa sieciowego w dużych przedsiębiorstwach, korzyści z wykorzystywania rozwiązań wielofunkcyjnych są oczywiste. Przede wszystkim chodzi o integrację wielu różnych funkcji bezpieczeństwa w jednym urządzeniu. Takie rozwiązanie ma szereg zalet:

- prostsza administracja jednego urządzenia vs. kilku urządzeń punktowych;
- mniejszy nakład pracy (liczby pracowników) do monitorowania stanu sieci;
- konieczność przeszkolenia mniejszej liczby pracowników (niższe koszty pracownicze);
- niższy koszt utrzymania (serwisowania) jednego urządzenia vs. kilku różnych, zwłaszcza gdy pochodzą od różnych dostawców;

Czy dostrzega P. korzyści płynące z budowania bezpieczeństwa firmy w oparciu o wielofunkcyjne systemy zabezpieczeń np. NGFW lub UTM?



Źródło: PMR, 2014

Powyższe czynniki mają w opinii respondentów proste przełożenie na zwiększenie poziomu bezpieczeństwa danych wewnątrz sieci firmowej, poprzez ułatwienie w administrowaniu urządzeniami i obniżenie kosztów ich obsługi.

Proszę powiedzieć jakie korzyści dostrzega P. z budowania bezpieczeństwa firmy w oparciu o wielofunkcyjne systemy zabezpieczeń np. NGFW/ UTM?

Źródło: PMR, 2014

Jeden z podstawowych wniosków płynących z badania zakłada, że firmy, bez względu na ich wielkość i branżę, doceniają wygodę, jaką daje wykorzystanie urządzeń wielofunkcyjnych. Oczywiście szczególnie dla większych przedsiębiorstw urządzenie wyspecjalizowane w ochronie konkretnego obszaru może okazać się koniecznością z uwagi na chęć podniesienia poziomu zabezpieczeń, lecz nie zmienia to ogólnego przeświadczenia, że urządzenia wielofunkcyjne są opcją, którą zawsze warto rozważyć, a już szczególnie w przypadku ograniczonego budżetu. Wyniki badania potwierdzają też tezę, że termin NGFW (ang. Next Generation Firewall, czyli firewall nowej generacji) nie jest rozpowszechniony wśród polskich firm. Dość powiedzieć, że gros specjalistów przyznaje, iż nie zapadł on im jeszcze na tyle w pamięć, by byli w stanie sensownie się na ten temat wypowiedzieć. Dla części badanych NGFW to nie tyle grupa produktów, ile element nazwy własnej. Co ciekawe, mimo przekazu zawartego w nazwie nie widać też przewagi „nowoczesności" NGFW nad znanym dobrze UTM-em.

Paweł Olszynka – Główny Analityk Rynku Telekomunikacyjnego i IT w PMR

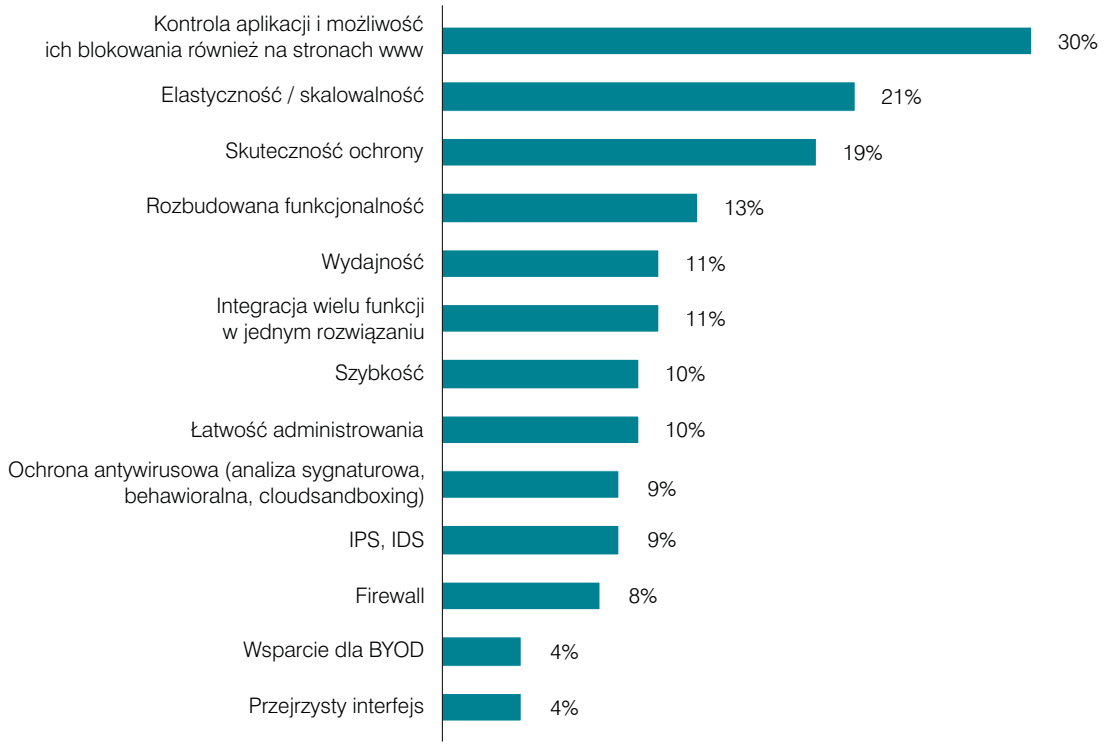
OCENA URZĄDZEŃ KLASY NEXT GENERATION FIREWALL

Wprowadzone w 2009 r. przez firmę Gartner pojęcie NGFW nie przyjęło się dotychczas na polskim rynku bezpieczeństwa sieciowego. Zaledwie 43% badanych było w stanie wypowiedzieć się na temat tego rozwiązania.

Wśród najciekawszych funkcji jakie wnosi ta klasa rozwiązań największy odsetek badanych wymienia możliwość kontroli konkretnych aplikacji i możliwość blokowania ich działania, także tych, które uruchamiane są za pośrednictwem stron WWW (np. na portalach społecznościowych).

Badani doceniają również skalowalność tych rozwiązań (21%) i gwarantowaną skuteczność ochrony, jaka wiąże się z korzystaniem z NGFW (19%).

Proszę powiedzieć jakie funkcje rozwiązania NGFW osobiście uważa P. za najbardziej wartościowe?



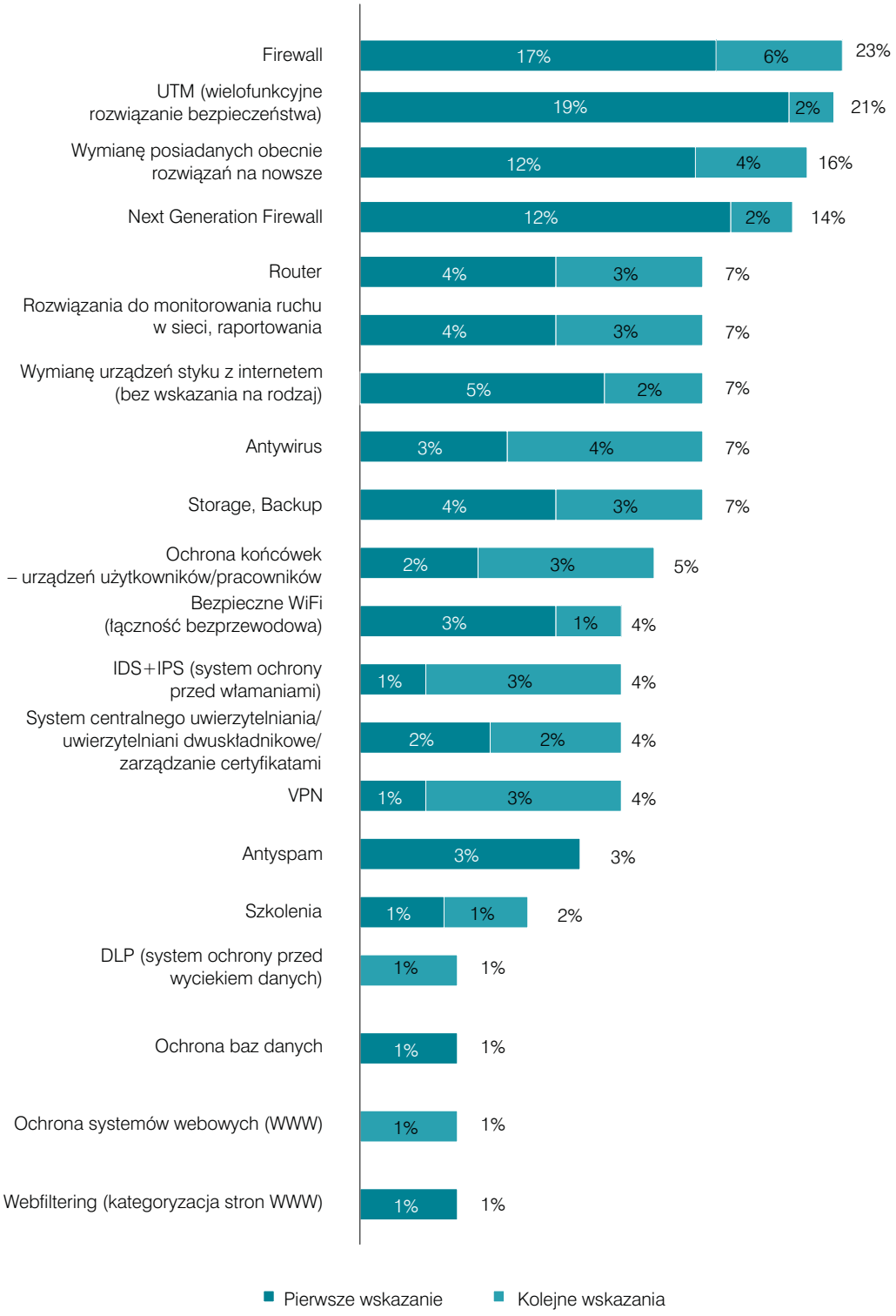
Źródło: PMR, 2014

DODATKOWY BUDŻET NA IT I PROPONOWANE ZAKUPY

Nie zaskakuje fakt, że w przypadku posiadania dodatkowego budżetu polskie firmy decydują się na przeznaczenie środków na rozwiązania doskonale im znane i sprawdzone. Respondenci znają zarówno ich mocne strony, jak i ograniczenia, i dlatego czują się pewnie z takim wyborem. Chęć inwestycji dodatkowych środków w rozwiązania, zdawałoby się, podstawowe, również nasuwa dwa wnioski. Z jednej strony – rynek jest daleki od nasycenia. Warto przy tym zwrócić uwagę, że na polskim rynku widać wyraźnie, że chęć rozwoju bezpieczeństwa IT i podkreślanie konieczności inwestycji w rozwiązania z zakresu bezpieczeństwa IT nadal spotyka się z ograniczeniami finansowymi. w Polsce budżet na te działania wciąż pozostaje na relatywnie niskim poziomie – według różnych szacunków waha się w granicach 1-3% środków przeznaczanych na IT, podczas gdy w Europie Zachodniej jest to przeciętnie dwukrotnie wyższy udział. Inna konkluzja jest taka, że polskie firmy, zgodnie z trendami globalnymi – zresztą nie tylko na rynku bezpieczeństwa IT – przede wszystkim stawiają na prostotę w miejsce mnogości funkcji, modułów i nowinek. Widać tu analogię na przykład do rynku systemów klasy ERP, gdzie po okresie promowania coraz bardziej rozbudowanych aplikacji naszpikowanych mnóstwem opcji, przyszedł odwrót w stronę ograniczenia całości do najbardziej przydatnych funkcji, by zyskać na przejrzystości, szybkości działania i wygodzie.

Paweł Olszynka – Główny Analityk Rynku Telekomunikacyjnego i IT w PMR

Proszę sobie wyobrazić, że dostają P. dodatkowy budżet równy rocznym nakładom na bezpieczeństwo IT w P. firmie. Proszę powiedzieć, w jakie rozwiązania z zakresu bezpieczeństwa sieciowego zainwestowaliby P. te środki?



Źródło: PMR, 2014

TRENDY I BIEŻĄCE WYDARZENIA NA RYNKU IT

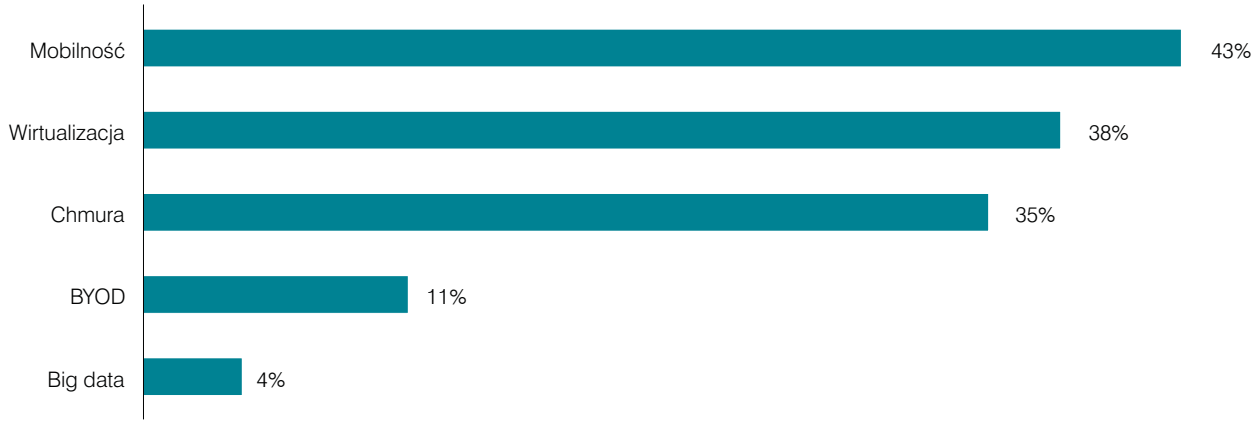
Rozwój nowych technologii a bezpieczeństwo IT

Specjaliści ds. bezpieczeństwa sieciowego pracujący w dużych przedsiębiorstwach w Polsce są jednogłośni w kwestii trendów i wyzwań, z jakimi w najbliższej przyszłości zmierzyć się będą musieli specjaliści w zakresie bezpieczeństwa sieciowego.

Największy odsetek badanych zwrócił uwagę na trend w kierunku rosnącej mobilności. W przypadku dużych przedsiębiorstw jest to niebagatelne wyzwanie, ponieważ mowa jest o co najmniej setkach urządzeń zewnętrznych, które codziennie zdalnie łączą się z siecią wewnętrzną i zasobami firmy. Respondenci przyznają, że powszechne łączenie się z firmową siecią Wi-Fi za pośrednictwem prywatnych urządzeń pracowników firmy (w modelu BYOD, jak i do celów prywatnych) stanowi dla nich prawdziwe wyzwanie i mocno utrudnia zabezpieczanie sieci wewnętrznej.

Specjaliści ds. bezpieczeństwa zwracają także uwagę na problemy, jakie wynikają z coraz powszechniejszej wirtualizacji i korzystania z danych lub usług w chmurze. Oprócz zagadnień czystko technicznych, dodatkowym problemem są kwestie prawne i brak „fizycznej" lokalizacji danych w jednym miejscu.

Jakie trendy w zakresie korzystania z technologii IT stanowią obecnie największe wyzwanie pod względem zagwarantowania bezpieczeństwa wewnętrznej sieci w P. firmie?



Źródło: PMR, 2014

Konflikt na Ukrainie

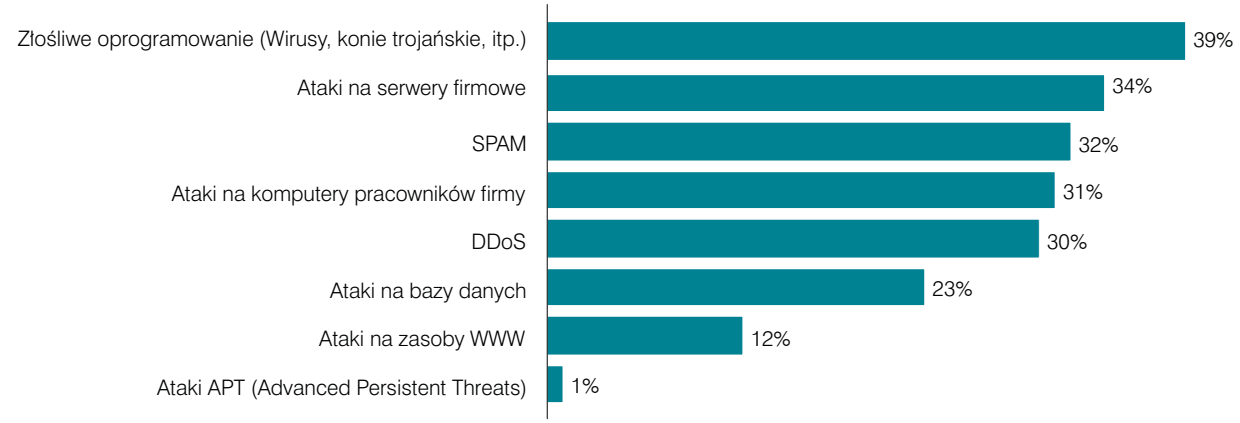
W II kwartale 2014 roku, gdy realizowane było badanie, konflikt pomiędzy Ukrainą a Rosją dopiero nabierał na sile. Wówczas tylko co dziesiąty spośród badanych przyznał, że spodziewa się wzrostu ryzyka ataku na sieć firmową w kontekście bieżących wydarzeń geopolitycznych.

Największym zagrożeniem w opinii badanych jest wszelkiego rodzaju złośliwe oprogramowanie: programy szpiegujące, konie trojańskie i wirusy, które dostają się do sieci firmowej najczęściej poprzez komputery szeregowych pracowników. W większości przypadków są to drobne incydenty, które chociaż chwilowo obciążają sieć firmową, szybko są usuwane.

Respondenci deklarują, że administrowana przez nich sieć jest dobrze zabezpieczona przed atakami z zewnątrz. Słabym ogniwem z ich punktu widzenia są pracownicy firmy, zwłaszcza korzystający z rozwiązań mobilnych. Jest to kolejny dowód na to, że mobilność oraz BYOD stanowią wyzwanie dla zabezpieczania sieci firmowej.

Naturalnie najpoważniejszym zagrożeniem są ataki na serwery firmowe, bazy danych oraz ataki typu DDoS, z uwagi na poufny charakter zgromadzonych na nich danych. Tylko jeden badany przyznał, że miał do czynienia z atakiem (DDoS) na administrowaną przez siebie sieć, pozostali respondenci deklarowali, że posiadane systemy zabezpieczeń skutecznie blokowały sieć przed zewnętrznymi zagrożeniami.

Abstrahując od wydarzeń politycznych, jakiego typu ataki w P. opinii są obecnie największym zagrożeniem?



Źródło: PMR, 2014

Zgodnie z naszymi przewidywaniami, a także adekwatnie do trendów światowych, to mobilność jest dzisiaj największym wyzwaniem dla zapewnienia bezpieczeństwa sieciowego w firmach. Z dostępem zdalnym do zasobów firmy ściśle wiąże się również ekspansja rozwiązań w chmurze. W przypadku tych ostatnich bezpieczeństwo jest postrzegane jako czynnik skłaniający firmy do migracji w kierunku rozwiązań chmurowych oferowanych przez zewnętrznego dostawcę, który gwarantuje odpowiedni poziom bezpieczeństwa. Szczególnie w przypadku małych i średnich

firm, o ograniczonym budżecie, taka opcja może być najlepszym rozwiązaniem. Z drugiej strony, dla części firm kwestia bezpieczeństwa danych to jeden z głównych argumentów, by w cloud computing nie wchodzić. Badanie potwierdza również, że BYOD, a już tym bardziej Big Data to trendy relatywnie nowe na polskim rynku i rodzime firmy jeszcze nie zderzyły się z nimi w takim stopniu jak przedsiębiorstwa w Europie Zachodniej.

Paweł Olszynka – Główny Analityk Rynku Telekomunikacyjnego i IT w PMR

FORTINET

Fortinet (NASDAQ: FTNT) zabezpiecza sieci, użytkowników i dane przed dynamicznie powstającymi i zmieniającymi się zagrożeniami. Jako światowy lider w dostarczaniu najwyższej jakości rozwiązań z zakresu bezpieczeństwa sieciowego, Fortinet umożliwia zarówno prywatnym przedsiębiorstwom, jak i jednostkom administracji publicznej konsolidację i integrację autonomicznych technologii bez uszczerbku na ich wydajności. W przeciwieństwie do kosztownych, nieelastycznych i mało wydajnych rozwiązań alternatywnych, narzędzia Fortinet umożliwiają klientom czerpanie korzyści z wykorzystywania nowych technologii i możliwości biznesowych przy jednoczesnej ochronie kluczowych danych i treści.

KONTAKT

Kontakt z przedstawicielami FORTINET przez:

Jacek Dąbrowski
Public Relations Specialist
mobile: +48 662 858 219
jacek.dabrowski@sarota.pl

SAROTA PR
Al. Beliny-Prażmowskiego 69/7
31-514 Kraków, Polska

tel.: +48 12 349 03 52
www.sarota.pl

PMR

PMR to firma badawczo-konsultingowa działająca w ponad 25 krajach Europy Środkowo-Wschodniej. Od 1995 roku przy naszym wsparciu ponad 500 globalnych korporacji oraz wiele lokalnych firm zwiększyło swoje udziały rynkowe, z sukcesem weszło na nowe rynki oraz zoptymalizowało koszty działalności. Specjalizujemy się w sektorach: budowlanym, handlu detalicznego, farmaceutycznym, ochrony zdrowia, IT i telekomunikacji, ale nasze doświadczenie obejmuje również wiele innych branż. Zatrudniamy 100 profesjonalistów płynnie posługujących się w sumie ponad 15 językami. Usługi badawcze i konsultingowe realizowane na indywidualne zamówienie uzupełniamy pakietem prawie 100 gotowych raportów rynkowych i serwisów informacyjnych rocznie.

KONTAKT

Zapraszamy do kontaktu z autorami raportu:

Maciej Kasperczyk
Badacz Rynku
mobile: +48 609 021 798
maciej.kasperczyk@pmrcorporate.com

PMR Ltd. Sp. z o.o.
ul. Dekerta 24
30-703 Kraków, Polska

tel.: +48 12 618 90 00,
www.pmrcorporate.com