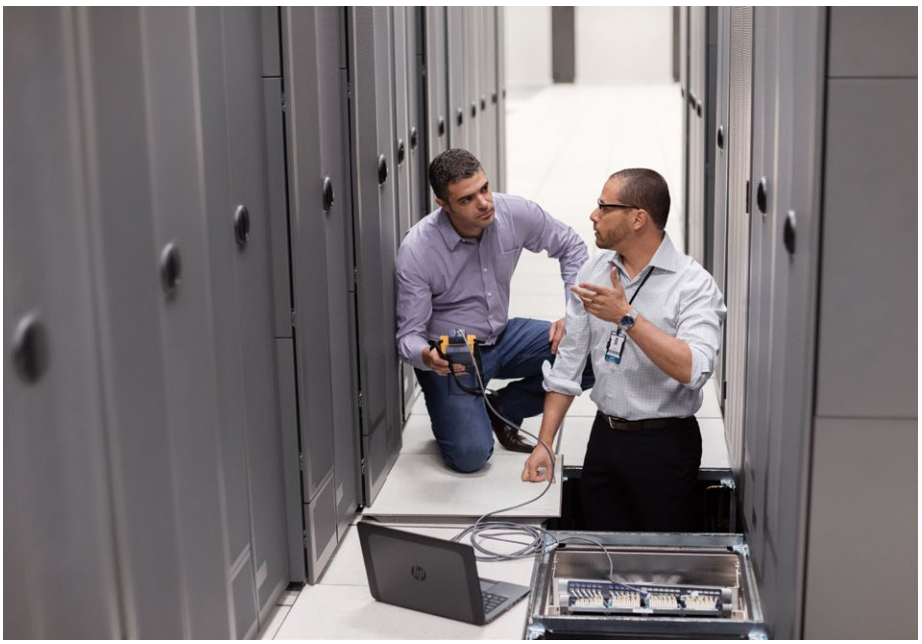
HP Polska dla Biznesu

Bezpieczeństwo. Ryzyko. Dostępność.

Raport specjalny

Wspierane przez Intel

Spis treści



Wstęp

Małe i średnie przedsiębiorstwa działajace w Polsce traktują kwestie bezpieczeństwa informacji priorytetowo. Są przygotowane na wypadek utraty danych i nie zamierzają zmniejszać budżetów na bezpieczeństwo. Większość firm nie powierza całościowego zarządzania obszarem bezpieczeństwa zewnętrznym podmiotom.

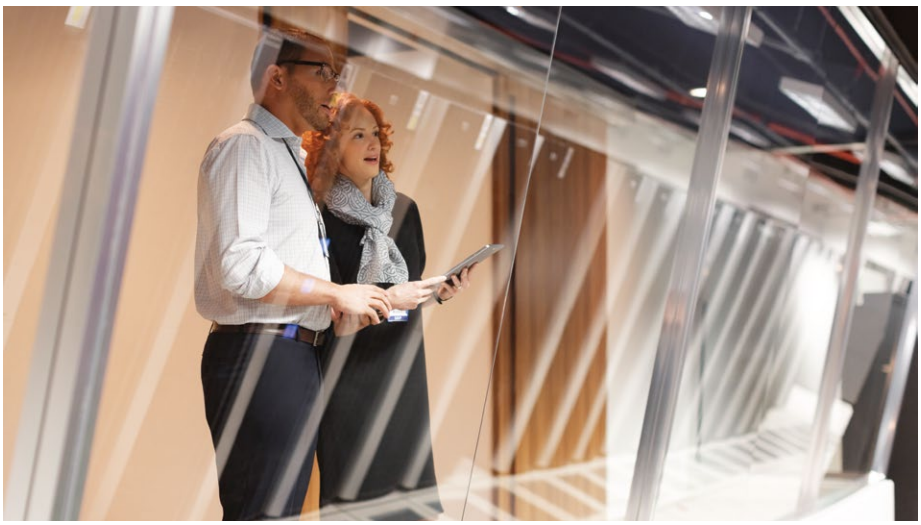
Bezpieczeństwo jest bardzo istotne we wszystkich aspektach zarządzania IT i transformacji cyfrowej, która staje się udziałem także małych i średnich przedsiębiorstw. Firmy zdają sobie sprawę, że nie jest możliwe stworzenie idealnie bezpiecznego środowiska, choćby ze względu na dynamicznie zmieniające się typy zagrożeń oraz coraz szybszy rozwój IT. Istotne jest podejście do bezpieczeństwa, uświadamianie wszystkim interesariuszom, a głównie pracownikom, konieczności przestrzegania odpowiednich procedur – zewnętrzne cyberataki to w MŚP zaledwie 5% przyczyn wszystkich przypadków utarty danych. Około połowy najcenniejszych dla firmy informacji przechowywana jest w postaci cyfrowej.

Zabezpieczenia nie mogą spowalniać pracy firmy, czy wprowadzania innowacji. Dlatego przed menedżerami odpowiedzialnymi za obszar security stoi coraz trudniejsze zadanie równoważenia priorytetu zabezpieczania danych i przyspieszania procesów czy wprowadzania nowych rozwiązań. Dla strategii bezpieczeństwa w firmie bardzo istotne jest odpowiednie rozplanowanie nacisku na zapobieganie, wykrywanie zagrożeń, reagowanie.

Zarządzanie bezpieczeństwem to obszar ważny nie tylko dla IT, ale także dla wszystkich działów biznesowych. Skutki utraty czy wycieków danych to problemy dla całej firmy: utrata reputacji, straty finansowe, przerwa w działaniu, utrata klientów, kary od regulatorów, wyciek tajemnicy handlowej. To tematy, które powinny być stale kontrolowane nie tylko przez CSO czy dział IT, ale przez cały zarząd. Rozwiązania technologiczne, procesy i ludzie muszą harmonijnie współpracować, aby bezpieczeństwo w firmie sprawnie działało.

Rozdział 1

Zarządzanie bezpieczeństwem



Bezdyskusyjny priorytet

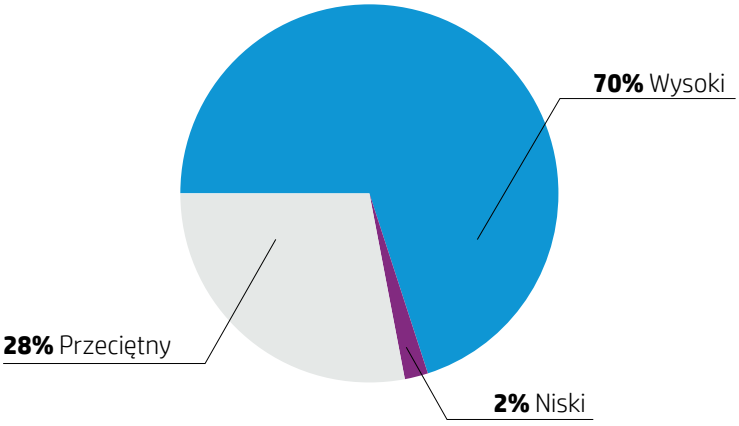
Niezależnie od wielkości i typu działalności firmy, bezpieczeństwo informacji należy do najważniejszych kwestii. Ten wniosek potwierdzają także wyniki poprzedniej edycji raportu z cyklu HP dla Biznesu: *Małe, średnie, innowacyjne* – zwiększenie bezpieczeństwa było najważniejszym wyzwaniem dla połowy uczestników wspomnianego badania.

Stale rośnie liczba i intensywność zagrożeń, w związku z czym systemy zabezpieczeń informacji wymagają nieustannego ulepszania. Przedsiębiorstwa zdają sobie z tego sprawę, jednak ich podejście w praktyce jest bardzo różne.

Kwestie bezpieczeństwa to przede wszystkim coraz bardziej zaawansowane zagrożenia, skomplikowane przepisy i rosnące potrzeby, w miarę rozwoju samego IT w firmie. Osoby odpowiedzialne za bezpieczeństwo w firmie muszą znać potencjalne zagrożenia zewnętrzne i wewnętrzne, umiejętnie zarządzać ryzykiem związanym z utratą informacji i wciąż zwiększać szczelność systemu zabezpieczeń.

W tym roku budżety na bezpieczeństwo w większości firm pozostają bez zmian. Menedżerowie muszą więc stawiać czoła rosnącym wyzwaniom i licznym zagrożeniom, decydując o proporcjach środków przydzielanych na szkolenia dla pracowników, nowe oprogramowanie zabezpieczające, albo przeniesienie części zabezpieczeń do chmury.

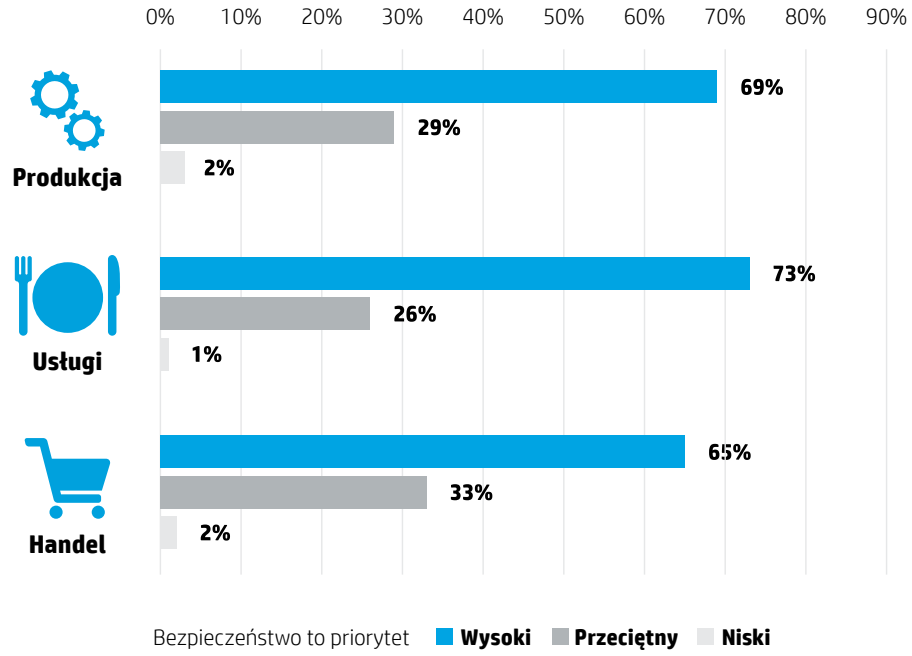
Bezpieczeństwo to priorytet



Wspierane przez Intel

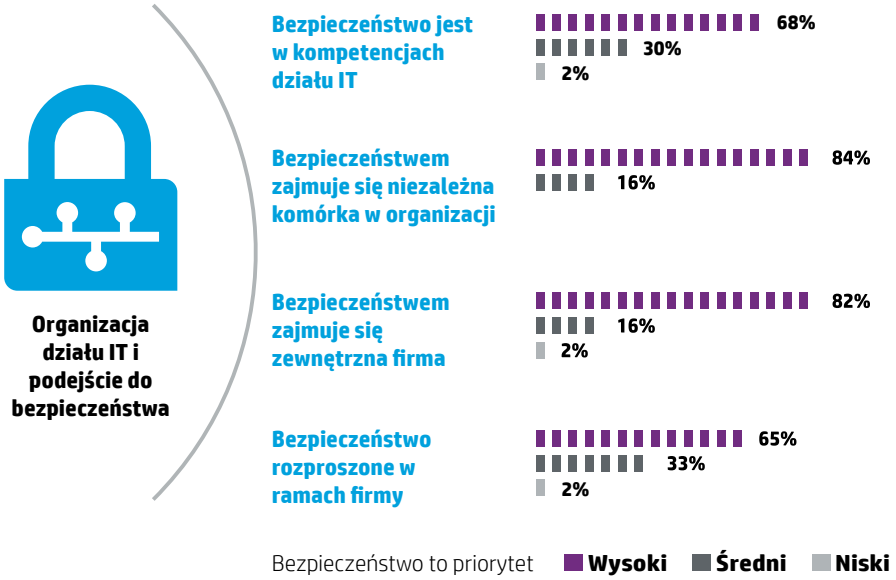
Aż dla 70% przedsiębiorstw bezpieczeństwo to wysoki priorytet, dla niemal co trzeciej – przeciętny, a tylko dla 2% – niski. Podejście do bezpieczeństwa nieco różni się w zależności od branży – w handlowej traktowane jest nieco mniej priorytetowo niż w pozostałych. W firmach o zasięgu międzynarodowym oraz w organizacjach działających wyłącznie w obszarze B2B, bezpieczeństwo rzadziej traktowane jest z najwyższym priorytetem (66% i 63% wskazań), podczas gdy w firmach o zasięgu lokalnym – w 72% przypadków.

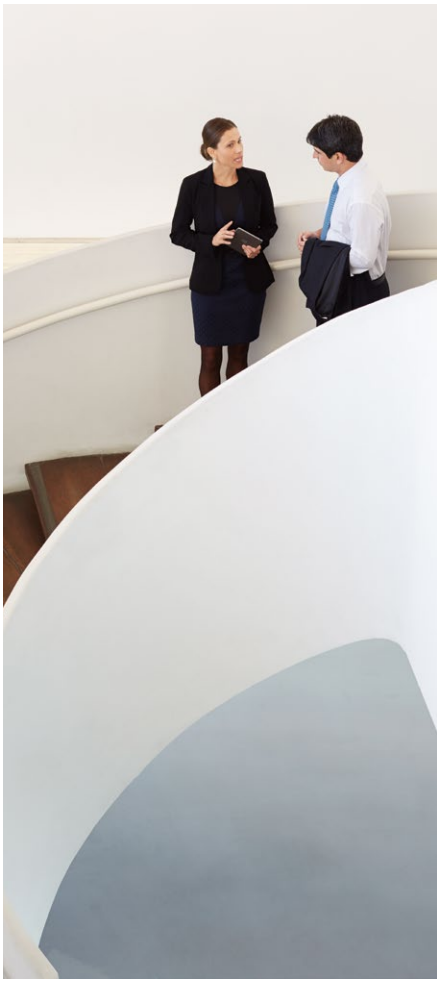
Najbezpieczniejsze branże



Wiele zależy także od organizacji zarządzania bezpieczeństwem informacji. W przedsiębiorstwach, w których zajmują się tym niezależne komórki lub zewnętrzne firmy, bezpieczeństwo jest stawiane wyżej w hierarchii ważności niż w pozostałych. Jeśli bezpieczeństwo jest częścią działu IT lub kompetencje są rozproszone w ramach całej firmy – znajduje się niżej na liście priorytetów.

Organizacja działu IT i podejście do bezpieczeństwa



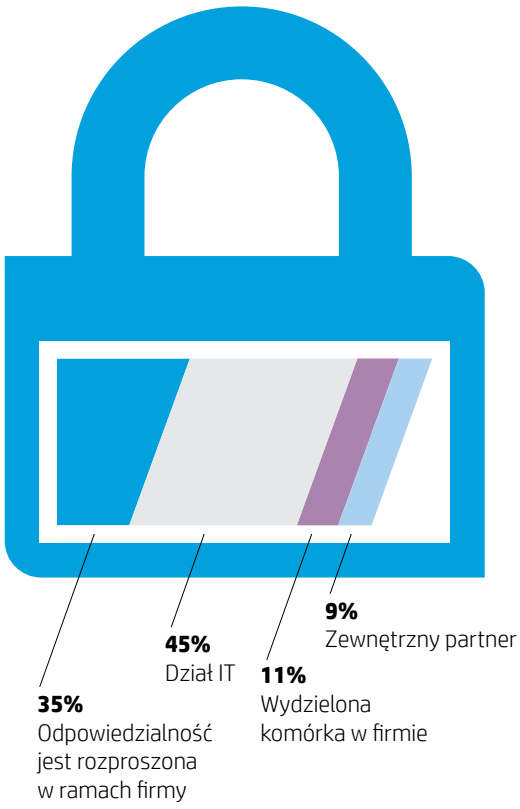


Dział wewnętrzny

W większości przypadków firmy chcą mieć kontrolę nad bezpieczeństwem i zarządza nim wewnętrzny dział. Jednak tylko co dziesiąte przedsiębiorstwo posiada wyodrębnioną komórkę zajmującą się wyłącznie tymi kwestiami. W niemal połowie przypadków bezpieczeństwo to po prostu jedna z kompetencji działu IT. Natomiast mimo ogólnych deklaracji o priorytetowym traktowaniu bezpieczeństwa, aż 36% przedsiębiorstw odpowiedzialność za tę kwestię rozprasza w różnych działach. Ta praktyka najczęściej stosowana jest w firmach działających w branży usługowej, które mają lokalny zasięg lub obsługują wyłącznie klientów B2C.

Outsourcing zarządzania bezpieczeństwem wciąż nie jest popularny w polskich MŚP – zaledwie ok. 9% podmiotów korzysta z tego modelu. Jednocześnie najpoważniej do kwestii zabezpieczania informacji podchodzą firmy, które utworzyły specjalny dział security lub właśnie korzystają z outsourcingu tego obszaru.

Kto zajmuje się bezpieczeństwem?



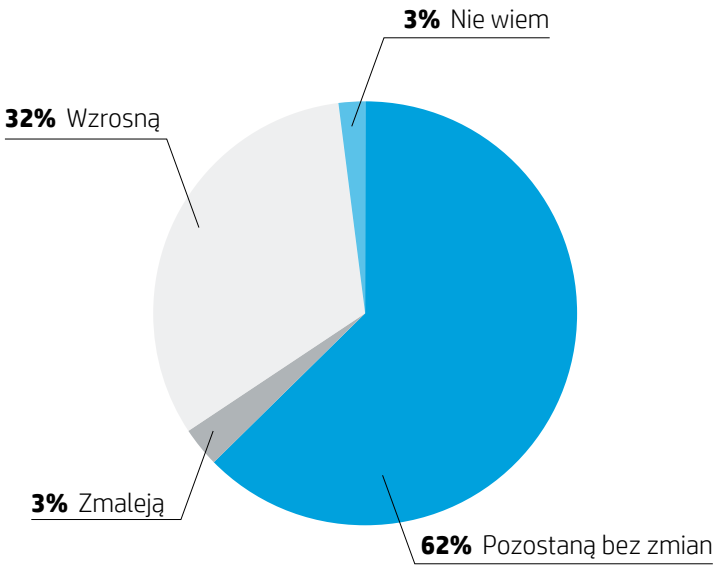
Koszt bezpieczeństwa

Choć stale zwiększa się liczba danych, które trzeba bezpiecznie przechowywać, rośnie także skala zagrożeń. Większość firm w tym roku będzie utrzymywała inwestycje w bezpieczeństwo na podobnym poziomie co w ubiegłym. Tylko co trzecia zamierza zwiększyć wydatki na ten cel.

Skłonność do inwestowania w bezpieczeństwo rośnie wraz ze skalą przedsiębiorstwa – aż 40% organizacji zatrudniających powyżej 200 osób zadeklarowało podniesienie nakładów w tym roku. Jest to też wyróżnik firm, które posiadają wyłącznie klientów B2B.

Wspierane przez Intel

Wydatki na bezpieczeństwo w tym roku

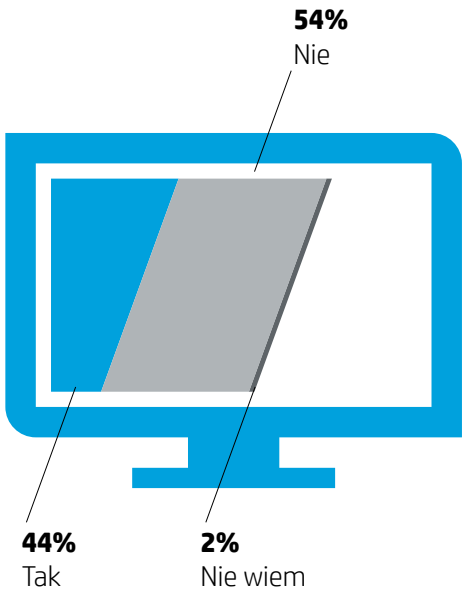


Kontrola i zaufanie

W obliczu rosnącej skali zagrożeń, zabezpieczenia muszą być stale uaktualniane. Jednak audyt bezpieczeństwa systemów IT nie jest jeszcze stałą praktyką dla większości firm. Tylko mniej niż połowa regularnie prowadzi kontrole zabezpieczeń.

Najczęściej audyty bezpieczeństwa przeprowadzane są w firmach, które oddały te kompetencje na zewnątrz lub wydzieliły w swoich strukturach komórkę zajmującą się bezpieczeństwem.

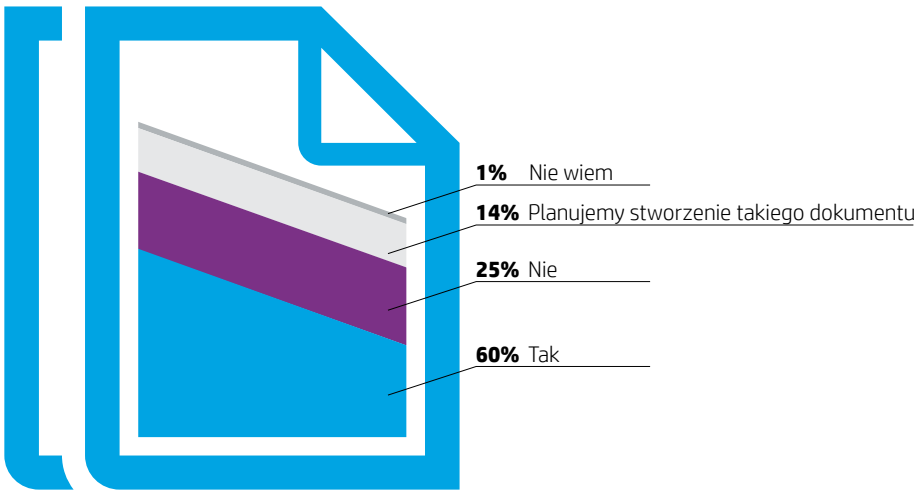
Regularnie przeprowadzamy audyt bezpieczeństwa systemów IT



Plan awaryjny

Mimo wysokiej świadomości tego, jak ważne jest bezpieczeństwo i zachowanie ciągłości działania, ten obszar wciąż jest słabo sformalizowany w wielu firmach. W jaki sposób MŚP są przygotowane na ewentualne awarie bezpieczeństwa? Nieco ponad połowa (60%) przedsiębiorstw ma udokumentowany plan zachowania ciągłości działania na wypadek awarii systemów IT. Około 14% planuje stworzenie takiego dokumentu, zaś co czwarta przyznaje, że po prostu go nie posiada. Jeśli bezpieczeństwem zajmuje się niezależna komórka lub zewnętrzna firma, jego standardy są wyższe – aż 73% takich firm ma plany działania na nieprzewidziane okoliczności.

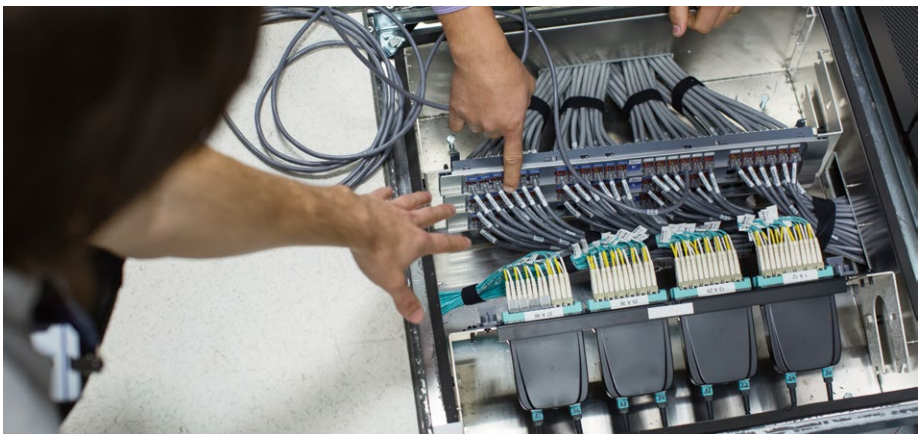
Czy firma posiada plan zachowania ciągłości działania na wypadek awarii systemów IT?



W przypadku sytuacji kryzysowej, spowodowanej np. atakiem na systemy IT czy wyciekiem danych liczy się każda minuta. Dlatego istotne jest posiadanie przez firmę przygotowanych planów i procedur działania, wyznaczenie odpowiednich osób z różnych działów.
Dotyczy to nie tylko zasobów zajmujących się IT i bezpieczeństwem, ale także kwestiami prawnymi czy wizerunku. Brak z góry opracowanych procedur naraża firmę na podjęcie nietrafnych decyzji i wyższe straty materialne. Badanie pokazuje, że świadomość tego ryzyka jest wciąż zbyt niska w MŚP.

Rozdział 2

W przypadku awarii

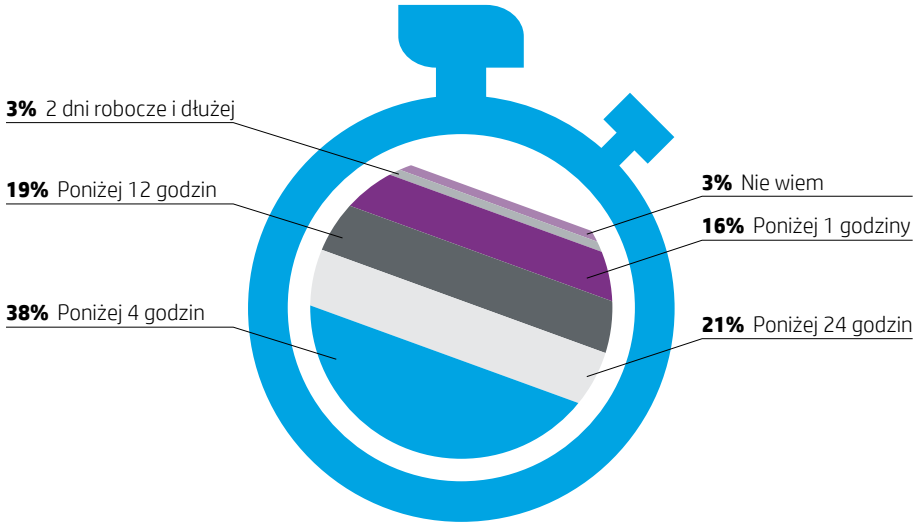


Gra na czas

W jaki sposób polskie MŚP podchodzą do kwestii zachowania ciągłości działania?

Cztery godziny to najczęściej wymieniany czas na usunięcie awarii akceptowany przez kierownictwo przedsiębiorstw.

Maksymalny akceptowany czas usunięcia awarii systemu IT



Tylko 16% firm z segmentu MŚP deklaruje konieczność usunięcia ewentualnej awarii systemu IT w ciągu najwyżej 60 minut. Zwłaszcza w branży handlowej szybki powrót systemu do pełnej sprawności jest krytyczny. Największa grupa daje sobie na to do 4 godzin. Natomiast niemal jedna piąta stosuje wymóg usunięcia awarii w czasie krótszym niż 12 godzin lub doba. Jednocześnie, utrata danych pochodzących z ostatniej godziny to problem pomijalny dla dwóch trzecich firm.

Dobrze przygotowani na najgorsze

Większość firm deklaruje, że ich systemy informatyczne są dobrze przygotowane na utratę danych na skutek awarii oprogramowania lub sprzętu.

Najgroźniejsze wydają się klęski żywiołowe, które mogą zakłócić ciągłość funkcjonowania systemów. Ok. 19% osób odpowiedzialnych za bezpieczeństwo uważa, że ich przygotowanie do takich zdarzeń jest niskie, a tylko 35% – że dobre.

Trudnym zagrożeniem są także wewnętrzne, nieuprawnione działania pracowników i wyciek danych. Okazuje się, że jedynie 42% firm uważa swoje przygotowanie do takich sytuacji za dobre, a 45% – za wystarczające, natomiast co dziesiąta firma zdaje sobie sprawę, że jest to jej słaba strona.

W jakim stopniu firma jest przygotowana na awarię?
Dane w %

	Dobre	Wystarczające	Niskie	Nie wiem
Utrata danych na skutek awarii oprogramowania	62	34	3	1
Utrata danych na skutek awarii sprzętu	60	33	6	1
Atak z zewnątrz	46	45	7	2
Wyciek danych	45	42	11	2
Nieuprawnione działania pracowników	42	45	11	2
Klęski żywiołowe	35	42	19	4

Podnoszenie bezpieczeństwa informacji – najpierw edukacja, później narzędzia

Firmy starają się podnosić bezpieczeństwo IT stosując całą paletę działań. Ludzie to często najsłabsze ogniwo łańcucha mającego zapewnić bezpieczeństwo informacji. Ponieważ nieuprawnione działania pracowników są jednym z najpoważniejszych zagrożeń, przedsiębiorstwa przykładają dużą wagę do edukacji. Bardzo istotne jest szkolenie użytkowników końcowych i pracowników IT. Ponad połowa przedsiębiorstw uważa także, że powinna wprowadzić bardziej restrykcyjną politykę określającą zasady bezpieczeństwa.

Większość przedstawicieli MŚP twierdzi, że na poprawę bezpieczeństwa informacji w istotny sposób wpłynęłaby modernizacja infrastruktury IT, inwestycje w rozwiązania do archiwizacji i backupu, wprowadzenie narzędzi monitorujących ochronę danych. Natomiast niewielu zdecydowałoby się na przeniesienie kluczowych danych do chmury (15% wskazań) czy przekazanie zarządzania infrastrukturą zewnętrznemu dostawcy (13%).

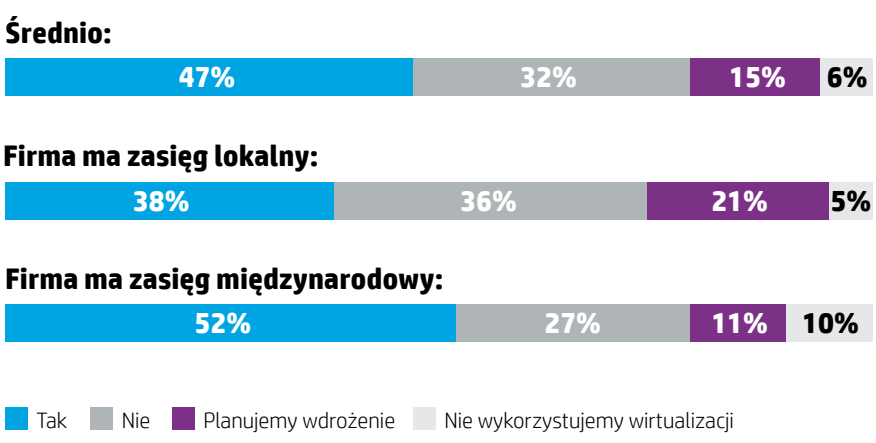
Jakie działania mogłyby podnieść bezpieczeństwo informacji w firmie?

Wirtualizacja i bezpieczeństwo

MŚP coraz częściej wybierają wirtualizację – ok. 36% firm wykorzystuje wirtualizację systemów, a 13% – pamięci masowych, zaś ok. 9% planuje takie wdrożenie. Serwery wirtualne są narażone na ataki w podobnym stopniu, co ich fizyczni „koledzy", cyberprzestępcy stale tworzą specjalne oprogramowanie, które namierza i atakuje wirtualne środowiska. Jednak, czy MŚP uświadamiają sobie specyficzne potrzeby związane z bezpieczeństwem zwirtualizowanych środowisk? Ochrona danych w środowiskach wirtualnych jest jednym z najistotniejszych problemów w obszarze składowania danych dla 13% ankietowanych przez nas menedżerów. Specjalne narzędzia ochrony stosuje tylko połowa firm korzystających z wirtualizacji. Częściej robią to przedsiębiorstwa działające w skali międzynarodowej niż lokalnej.

Firmy korzystające z wirtualizacji serwerów lub pamięci masowych

Firma stosuje specjalistyczne narzędzia do ochrony środowisk wirtualnych



Wspierane przez Intel

Rozdział 3

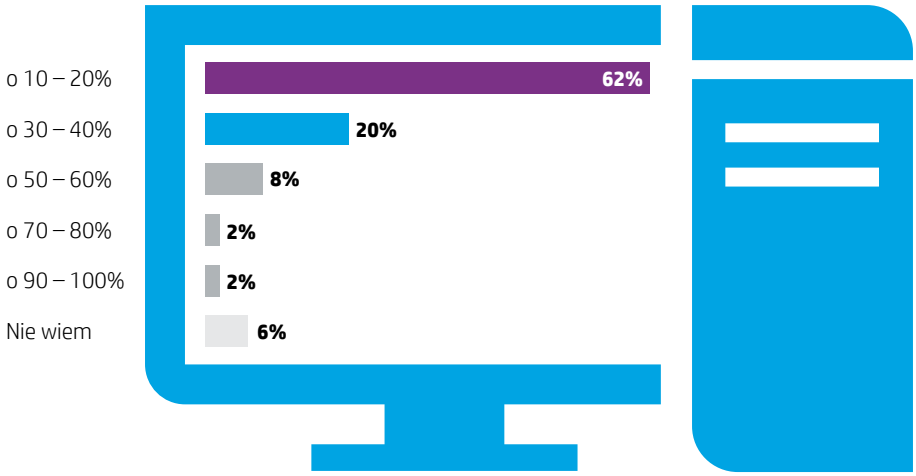
Najważniejsze aktywa

Cenne dane

Ilość danych przyrasta w ogromnym tempie, rośnie nie tylko wolumen, ale także ich różnorodność i złożoność. Statystycznie, tempo zmian przekracza możliwości tradycyjnego oprogramowania, architektury i procesów, które mają umożliwić efektywne zarządzanie i wykorzystanie. Analitycy Gartnera prognozują, że ilość danych na świecie wzrośnie o 800% w ciągu 5 lat, a 80% z tych danych będzie nieustrukturyzowane[1].

Aż 94% MŚP biorących udział w badaniu przewiduje, że w tym roku wolumen przechowywanych przez nie danych wzrośnie, z czego w co piątej nawet o 40%. Firmy potrzebują odpowiednich zabezpieczeń i wydajnych metod przechowywania informacji, ponieważ prawie połowa przechowuje większość istotnych danych w postaci cyfrowej, choć forma papierowa nadal ma się dobrze w co drugim przedsiębiorstwie.

Przewidywany wzrost ilości danych w najbliższym roku



Firma przechowuje istotne dane w postaci cyfrowej

45% firm
przechowuje
70 – 100% danych

26% firm
przechowuje
10 – 40% danych

23% firm
przechowuje
50 – 60% danych

[1] Raport „Monetize Big Data" – HP

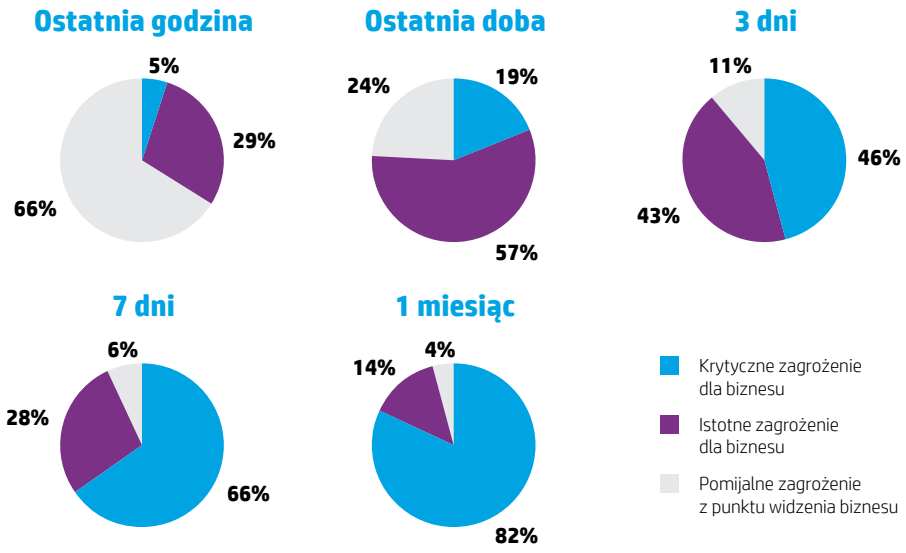
Wspierane przez Intel

Utrata danych

Dane należą do najcenniejszych aktywów każdej firmy, przedsiębiorstwa uświadamiają sobie ryzyko związane z ich utratą. Mimo szybkiego przyrostu ilości danych, o którym mówi gros firm, dopiero utrata zapisów całego miesiąca jest przerażającym scenariuszem dla większości badanych (82%).

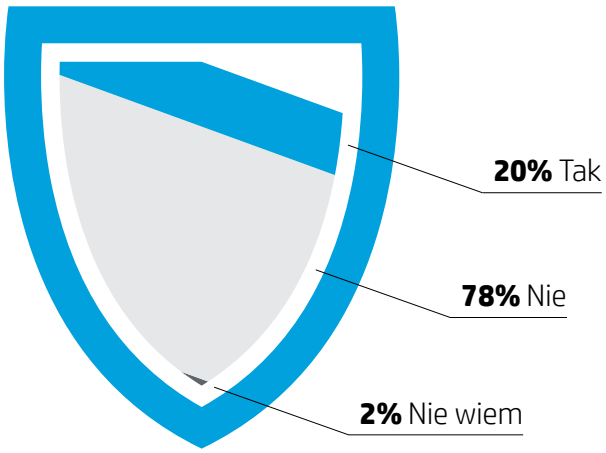
Utrata danych z ostatniej godziny stanowi pomijalne zagrożenie dla niemal dwóch trzecich MŚP, natomiast utrata danych z ostatniej doby jest istotnym zagrożeniem dla ponad połowy firm, a z tygodnia – krytycznym zagrożeniem dla 66% respondentów.

Jeśli firma straciłaby dane z określonego okresu miało by to wpływ na ciągłość biznesu

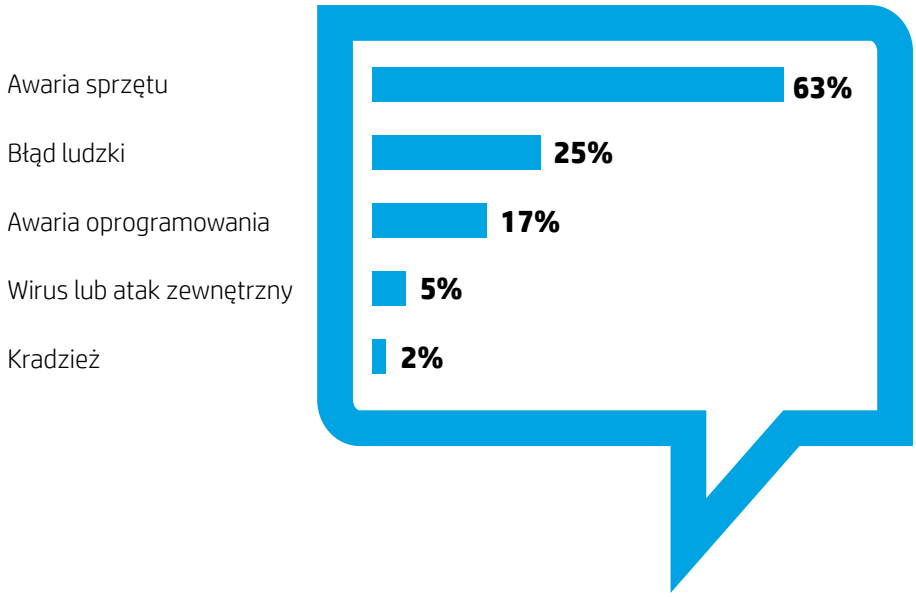


Utrata danych jest częstym zjawiskiem – co piąta firma przyznaje, że w ciągu ostatnich trzech lat miała tego typu zdarzenie. Na ogół powodem była awaria sprzętu, i aż w co czwartym przypadku był to błąd ludzki. Tylko 5% stanowiły wirusy lub ataki zewnętrzne.

Czy w ciągu ostatnich 3 lat w firmie nastąpiła utrata danych?



Z jakiego powodu nastąpiła utrata danych?



Coś poszło nie tak...

Jakie są najczęstsze problemy związane ze składowaniem danych w firmach?

Nie jest zaskoczeniem, że firmy najczęściej mają problem z niedoskonałością sprzętu – w 37% przypadków (i aż 48% w branży usługowej), zwłaszcza, że ilości danych i wymagania stale rosną (zbyt szybki przyrost danych to problem dla 23% firm, przy czym dla 27% w sektorze produkcji). Problem może także stanowić zbyt duży rozmiar backupów (28%) i zbyt długi czas odtwarzania zasobów (23%). Istotne są wysokie koszty zarządzania pamięciami masowymi, zbyt długie okno backupu i ochrona danych w środowiskach wirtualnych.

W branży handlowej bolączką jest zbyt duży rozmiar backupów (37%) i zbyt długi czas odtwarzania zasobów (28%).

Problemy ze składowaniem danych
Dane w %

	Średnia firm	Branża produkcyjna	Branża usługowa	Branża handlowa
Awarie sprzętu	37	32	48	21
Zbyt duży rozmiar backupów	28	24	26	37
Zbyt długi czas odtwarzania zasobów	23	22	22	28
Zbyt szybki przyrost danych	23	27	18	27
Wysokie koszty zarządzania pamięciami masowymi	17	16	20	12
Zbyt długie okno backupu	15	17	13	16
Ochrona danych w środowiskach wirtualnych	13	11	12	20

Bezpieczne dane

Firmy stale pracują nad poprawą bezpieczeństwa danych. W tym roku ponad połowa przedsiębiorstw chciałaby, aby usprawniony został proces backupu i odzyskiwania danych. Ważna jest także lepsza ochrona dostępu do danych i jednocześnie ułatwienie tego dostępu. Zapewnienie zgodności z regulacjami prawnymi jest priorytetowe dla 39%. Dla co piątej firmy istotne jest obniżenie kosztu składowania i zarządzania danymi, a jedynie 17% zwraca uwagę na problem zarządzania przyrostem ich ilości.

Priorytety w zarządzaniu bezpieczeństwem danych

54% Usprawnienie procesów backupu i odzyskiwania danych

47% Zwiększenie ochrony dostępu do danych

39% Zapewnienie zgodności z regulacjami prawnymi

25% Podniesienie poziomu dostępności danych

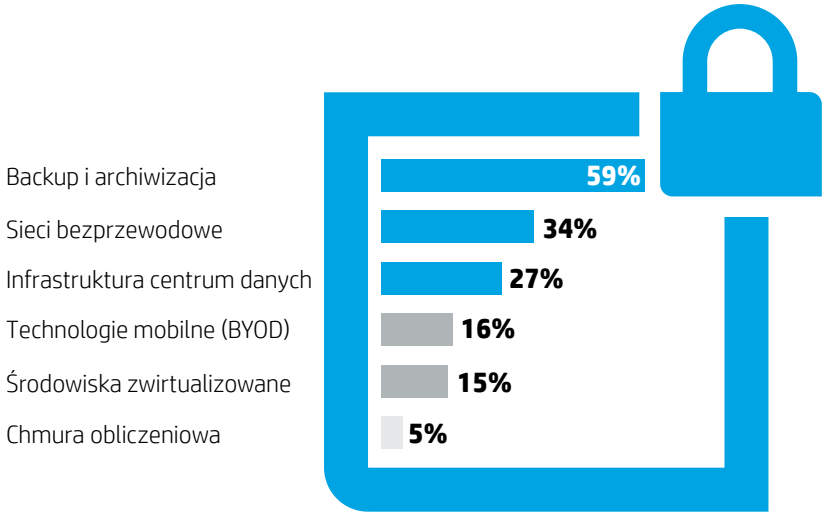
22% Obniżenie kosztu składowania i zarządzania

17% Zarządzanie przyrostem ilości danych

Lista zadań

Backup i archiwizacja danych są najważniejszymi zadaniami w ramach zapewnienia bezpieczeństwa informacji dla ponad połowy firm. Wśród priorytetów znalazły się także sieci bezprzewodowe (istotne zwłaszcza dla branży handlowej), infrastruktura centrum danych, środowiska zwirtualizowane. Jedynie 16% ankietowanych wskazuje na technologie mobilne, które wymagają specjalnej polityki bezpieczeństwa w większości firm. Najmniej istotna w tym roku jest chmura obliczeniowa.

Technologie i obszary funkcjonowania IT, które wymagają największej uwagi pod kątem zapewnienia bezpieczeństwa informacji



Wspierane przez Intel

Technologie backupu

Bezpieczne przechowywanie i dostęp do danych to priorytet dla większości MŚP. Firmy najczęściej umieszczają kopie krytycznych zasobów na zewnętrznych dyskach – robi tak aż 77% uczestników badania. Kopia na dyski wewnętrzne również jest popularnym rozwiązaniem – korzysta z niego 61% respondentów. Poza tym stosują cały szereg różnorodnych metod przechowywania danych, od kopiowania na nośniki optyczne, nośniki USB po kopie na taśmę w bibliotece taśmowej. Co czwarta firma korzysta z backupu online – w tym do chmury obliczeniowej.

Z jakich technologii backupu korzysta firma
Dane w %

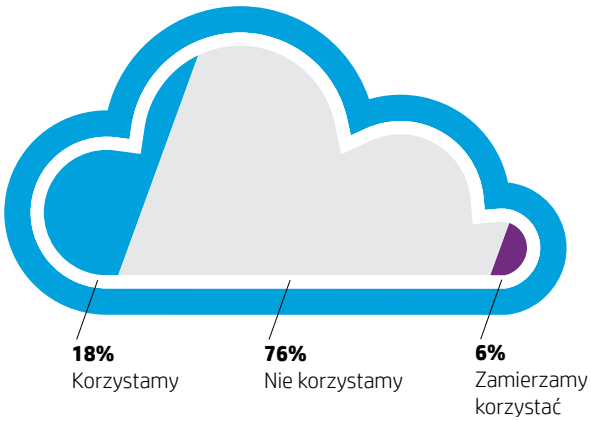
	Średnia	Branża produkcyjna	Branża usługowa	Branża handlowa	Tylko klienci B2C	Tylko klienci B2B	B2C i B2B
Kopia na dyski zewnętrzne	77	78	77	78	72	76	80
Kopia na dyski wewnętrzne	61	59	66	55	61	47	65
Kopia na nośnik optyczny	48	43	57	36	61	28	49
Kopia na nośnik USB	44	30	52	48	54	20	47
Kopia na urządzenia do backupu dyskowego	41	44	38	41	27	44	45
Replikacja danych pomiędzy macierzami	35	36	31	40	24	39	37
Kopia migawkowa (snapshot) na macierzy dyskowej	30	32	26	36	19	41	31
Kopia migawkowa (klon) na macierzy dyskowej	29	31	27	34	18	40	31
Backup online (do chmury, na urządzenia hostowane, BAAS)	26	26	27	23	21	29	27
Kopia na taśmę lokalną (DAT, LTO, LTFS)	19	26	13	23	10	28	20
Kopia na taśmę w bibliotece taśmowej (LTO)	15	16	13	17	9	28	13

Backup w chmurze

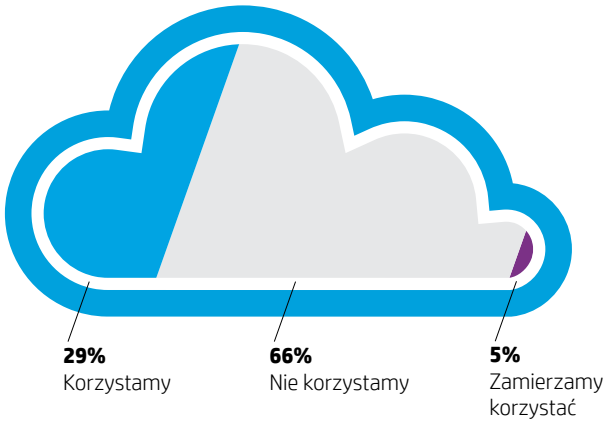
Backup danych w cloudzie wciąż nie jest popularnym rozwiązaniem w MŚP – korzysta z niego zaledwie 18% przedsiębiorstw, a 6% planuje korzystać.

Firmy, w których zarządzaniem bezpieczeństwem zajmują się niezależne komórki chętniej korzystają w z backupu danych on line (w chmurze lub hostowanych).

Backup online (hostowany lub w chmurze) – średnia firm

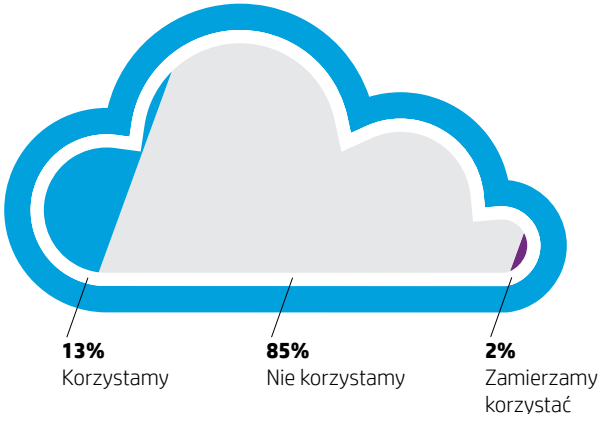


Backup online (hostowany lub w chmurze) – gdy bezpieczeństwem zajmuje się niezależna komórka



Natomiast zewnętrzne firmy odpowiadające za bezpieczeństwo danych raczej niechętnie decydują się na korzystanie z cloudu.

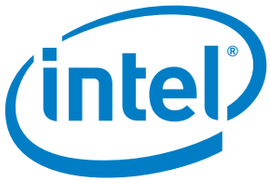
Backup online (hostowany lub w chmurze) – gdy bezpieczeństwem zajmuje się zewnętrzna firma



O badaniu

Badanie zostało przeprowadzone w 500 firmach z sektora małych i średnich przedsiębiorstw działających w Polsce, z różnych branż. Wywiady zostały przeprowadzone w grudniu 2014 r. z osobami odpowiedzialnymi w firmie za IT (dyrektor, kierownik, specjalista IT).

Wspierane przez Intel



FUNDACJA MAŁYCH I ŚREDNICH
PRZEDSIĘBIORSTW

KRAJOWA IZBA GOSPODARCZA