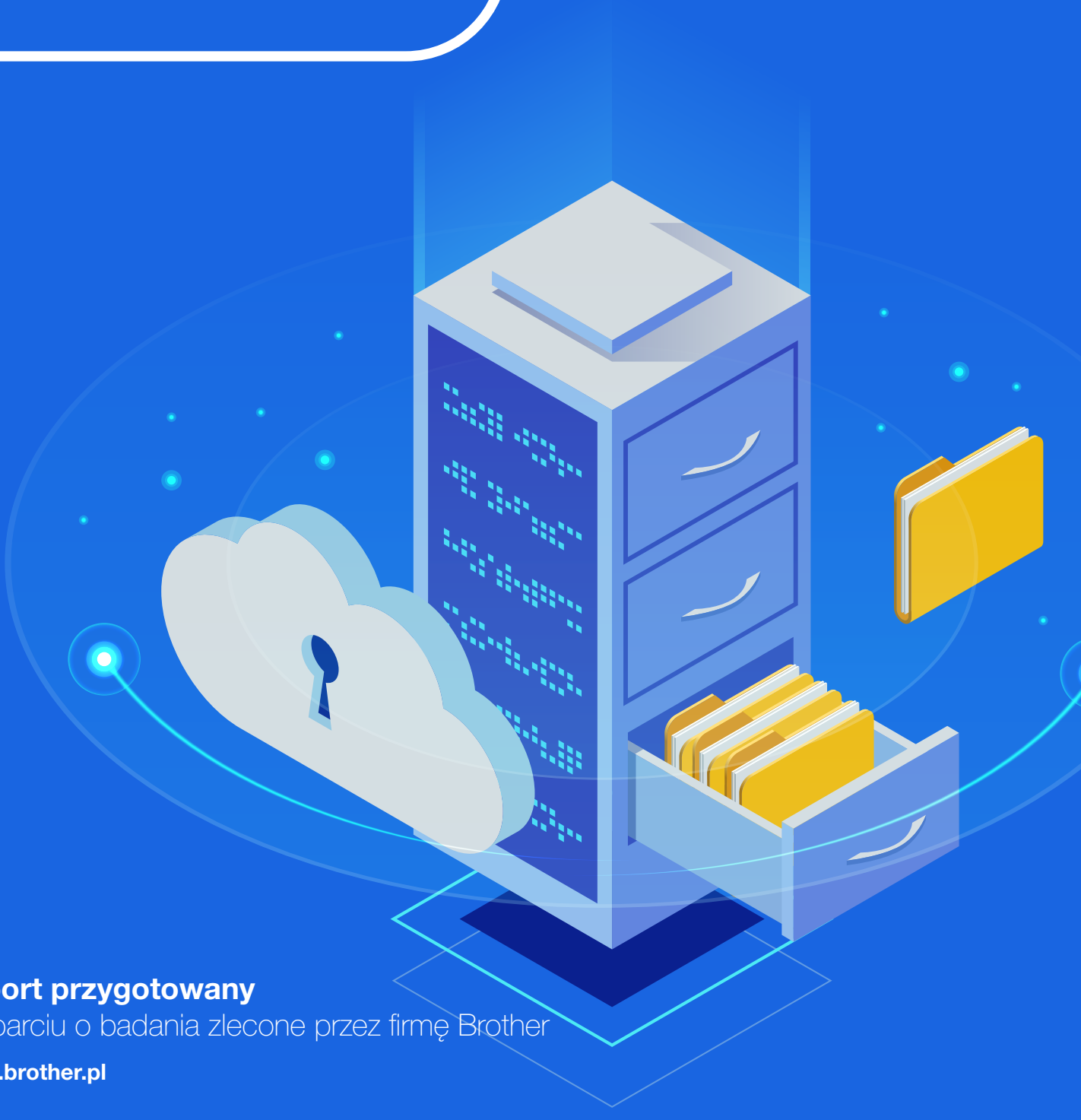
Utrzymanie bezpiecznego środowiska druku

Trzecia część serii
o cyfrowej transformacji



Raport przygotowany
w oparciu o badania zlecone przez firmę Brother

www.brother.pl

Bariery inwestycji w bezpieczeństwo druku

Rosnące ryzyko naruszeń cyberbezpieczeństwa oraz ataków hakerskich na organizacje zobowiązuje przedsiębiorców do zadbania o odpowiedni poziom ochrony zarówno gromadzonych oraz przetwarzanych danych wrażliwych, jak i systemów informatycznych.

Zarządzanie cyberbezpieczeństwem to wyzwanie, któremu należy stawić czoła całościowo – dbając przy tym o wszystkie ogniwa tworzące sieć organizacji. Drukarki, skanery i kopiarki muszą być tak samo bezpieczne, jak inne urządzenia IT. Jeśli zostaną przeoczone, istnieje duże ryzyko, że to właśnie one będą dla hakerów „łatwą furtką" dostępu do firmowych danych. Przedsiębiorstwa z sektora MŚP są świadome wagi tego problemu – **72%** organizacji twierdzi, że bezpieczeństwo ich urządzeń drukujących ma kluczowe znaczenie. Zapewnienie odpowiedniego poziomu cyberbezpieczeństwa to jeszcze większe wyzwanie dla firm przetwarzających dane wrażliwe w takich branżach jak usługi profesjonalne **(82%)** czy opieka zdrowotna **(81%)**.

Jednak nadal prawie jedna trzecia organizacji nie dostrzega tego problemu. A jednocześnie prawie połowa z nich zauważa, że ich firma w niewystarczającym stopniu zadbała o bezpieczeństwo sprzętu drukującego.

Dlaczego przedsiębiorstwa, które rozumieją potrzebę inwestowania w bezpieczeństwo druku, nadal tego nie robią?

Nasze badania wskazują na dwa wyraźne powody:

Brak osoby odpowiedzialnej za bezpieczeństwo druku

Brak wiedzy na temat zagrożeń i standardów bezpieczeństwa

Głównym celem tego raportu jest pomoc kadrze menadżerskiej z sektora MŚP w zrozumieniu istoty bezpieczeństwa druku. Sprawozdanie jest częścią większej serii, która powstała, aby wesprzeć wdrożenie technologii cyfrowych. Raporty oparte są na badaniach przeprowadzonych wśród menadżerów wyższego szczebla z MŚP w regionie EMEA. Seria została podzielona na cztery sprawozdania, z których każde dotyczy jednego z poniższych tematów:

- Tworzenie cyfrowego przepływu pracy
- Wybór i wdrożenie właściwych rozwiązań dla firmy
- Bezpieczne środowisko druku
- Zrównoważony rozwój

Kto jest odpowiedzialny za bezpieczeństwo druku?

Prawie połowa firm z sektora MŚP w Europie Zachodniej **(44%)** informuje, że w ich organizacji nie jest jasne, kto odpowiada za bezpieczeństwo druku. W przedsiębiorstwach, w których ta odpowiedzialność jest „rozmyta", istnieje duże prawdopodobieństwo, że ucierpi na tym proces wdrażania dedykowanych rozwiązań z zakresu ochrony procesu druku – co z kolei zwiększy podatność firm na ataki ze strony hakerów.

Odpowiedzialność za bezpieczeństwo urządzeń drukujących nie jest zazwyczaj przypisana do konkretnej osoby, ponieważ te sprzęty z reguły nie są postrzegane jako „słabe ogniwa" sieci. Nasze badania obrazują, że kadra menadżerska większych organizacji zaczyna zdawać sobie sprawę z wagi bezpieczeństwa druku w firmie. Niestety małe i średnie przedsiębiorstwa bardzo często nie dostrzegają tego problemu.

To właśnie firmy z sektora MŚP są szczególnie narażone na negatywne konsekwencje nieodpowiednich zabezpieczeń druku. W małych przedsiębiorstwach zazwyczaj kilku pracowników zajmuje się wszystkimi zagadnieniami związanymi z wątkami technologicznymi i informatycznymi w całej organizacji. Niestety, jeżeli specjaliści zatrudnieni w firmie nie są świadomi ryzyka związanego z brakiem odpowiedniego poziomu bezpieczeństwa druku, może zostać ono zaniedbane.

Należy zwrócić szczególną uwagę na fakt, że w zasadzie wszyscy pracownicy w organizacji są w pewnym stopniu odpowiedzialni za zapewnienie bezpieczeństwa wrażliwym danym.

W kompetencji specjalistów IT leży zapewnienie odpowiedniej ochrony urządzeniom, jednak wszyscy pracownicy odpowiadają za kontrolę przepływających danych – jest to najbardziej newralgiczny obszar pod kątem troski o ochronę poufnych informacji handlowych.

Bezpieczeństwo danych obejmuje szeroki zakres zagrożeń, w tym:

- nieautoryzowany dostęp do wydruków
- niewylogowanie się po wydrukowaniu poufnych dokumentów
- brak możliwości prześledzenia, kto miał dostęp do drukarki i do jakich dokumentów

Prawie 9 na 10 firm doświadczyło incydentu cyberbezpieczeństwa związanego z drukarką...

… a siedem na dziesięć przedsiębiorstw **(72%)** twierdzi, że bardziej zagrożone jest bezpieczeństwo danych niż samych urządzeń. Jednak mniej niż jedna na trzy firmy jest przekonana, że jej infrastruktura druku jest w pełni bezpieczna. W tym zestawieniu **53%** organizacji uważa, że dysponuje odpowiednimi zabezpieczeniami sprzętowymi.

Większość przedsiębiorców z sektora MŚP **(64%)** deklaruje, że zapewnienie bezpieczeństwa danym jest dla nich najwyższym priorytetem – postrzegają to jako kluczowe wyzwanie, które może stanowić rzeczywistą przeszkodę w skutecznym działaniu.

Obecnie prawie połowa małych i średnich przedsiębiorstw **(48%)** twierdzi, że posiada zaledwie kilka procedur umożliwiających im monitorowanie tego, kto drukuje lub zleca inne zadania urządzeniu drukującemu. Nie jest więc zaskoczeniem, że prawie dziewięć na dziesięć firm **(86%)** zgłosiło incydent bezpieczeństwa związany z drukiem.

Takie sytuacje są najczęściej związane z zostawieniem poufnych dokumentów bez nadzoru przy drukarce, nieodebraniem wydruków lub przechwyceniem wydrukowanych materiałów innych pracowników.

W rezultacie większość małych i średnich przedsiębiorstw **(64%)** zaczyna wprowadzać działania, których celem jest rozwiązanie problemów bezpieczeństwa druku – ograniczając dostęp do niektórych urządzeń drukujących, wprowadzając karty identyfikacyjne lub kody PIN przypisane konkretnym pracownikom. Dzięki wdrożeniu odpowiednich zabezpieczeń pracodawca może nie tylko monitorować wykorzystanie urządzeń przez pracowników, ale również nadawać dostęp do określonych funkcjonalności konkretnym osobom.

To krok w bardzo dobrym kierunku, ponieważ w nadchodzących latach istotne będzie, aby wszystkie przedsiębiorstwa wprowadziły bezpieczniejsze procesy w obrębie całej organizacji. Dlatego to ważne, aby firmy, które już są na tej drodze, utrzymały i ulepszyły swoje działania w zakresie odpowiedzialności oraz audytu.

Istnieją trzy główne atrybuty bezpieczeństwa, obejmujące zarówno urządzenia, jak i same dane:

Poufność

Ochrona wrażliwych danych biznesowych polega na udostępnianiu ich tylko docelowemu odbiorcy. Przy takim założeniu kluczowe są środki uwierzytelniania i autoryzacji, które wymagają od użytkowników zweryfikowania ich tożsamości przed uzyskaniem dostępu do jakiegokolwiek dokumentu.

Nienaruszalność

Pewność, że oprogramowanie urządzenia jest odpowiednio zabezpieczone i odporne na włamania oraz inne zagrożenia zewnętrzne.

Dostępność

Gwarancja gotowości do pracy oraz dostępności urządzenia tylko i wyłącznie dla autoryzowanych użytkowników, którzy wykonują na nich operacje związane z obowiązkami służbowymi.

Brak wiedzy to wątpliwe bezpieczeństwo firmy

Mniej niż jedna trzecia **(32%)** kadry menadżerskiej IT pracującej w sektorze MŚP twierdzi, że posiada zaawansowaną wiedzę na temat bezpieczeństwa i potencjalnych zagrożeń.

Warto zauważyć, że jeżeli decydenci IT nie będą posiadać wystarczającej wiedzy na temat zagrożeń, firmy nadal będą miały trudności z wdrożeniem odpowiednich środków ochrony. W małych i średnich przedsiębiorstwach osoby zarządzające IT zazwyczaj odpowiadają za wiele różnych rozwiązań technologicznych w firmie. To zrozumiałe, że mogą nie być ekspertami w dziedzinie bezpieczeństwa środowiska druku.

Często współwinny jest również żargon, czyli język branżowy. Ponad połowa organizacji z sektora MŚP **(51%)** zwraca uwagę, że specyficzne słownictwo, którego używa się mówiąc o bezpieczeństwie drukarek, jest często trudne do zrozumienia. To zjawisko jest szczególnie widoczne we Francji i Włoszech.

Nie jest też zaskoczeniem, że firmy przede wszystkim wybierają znane marki, przy czym wciąż w pełni nie rozumieją, jakie środki bezpieczeństwa są przez tych podwykonawców stosowane.

Po stronie partnerów technologicznych leży nie lada wyzwanie, ponieważ muszą pomóc przedsiębiorstwom rozszyfrować żargon dotyczący standardów bezpieczeństwa i zapewnić wybór najlepszego rozwiązania dla danej firmy.

Wskazówki od Brother

Wyciek informacji może prowadzić do znaczących strat finansowych, prawnych lub też wizerunkowych. Uwzględniając złożoność problemu zapewnienia odpowiedniego poziomu bezpieczeństwa druku, Brother opracował 7 wskazówek, które pomogą firmom uchronić biznes przed utratą danych.

Zarządzaj bezpieczeństwem strategicznie

Zapewnienie kompleksowego bezpieczeństwa druku firmie, w tym ochrona przed cyberatakami i nakładanie na pracowników obowiązku dbania o ochronę danych wrażliwych w połączeniu z wymogami ustawy o RODO, wychodzi poza kompetencje działu IT. Problem ten powinien być rozpatrywany strategicznie na poziomie zarządu z udziałem Dyrektora lub Szefa departamentu IT.

Przeprowadź dokładny audyt wewnętrzny

Z punktu widzenia biznesu kluczowe jest zweryfikowanie wszelkich potencjalnych luk w zabezpieczeniach druku poprzez objęcie tego zagadnienia regularnymi audytami bezpieczeństwa. Jest to szczególnie ważne, gdy w firmie znajdują się zarówno nowe, jak i starsze urządzenia. Jeśli chodzi o Usługę Zarządzania Drukiem (MPS), większość dostawców oferuje pełną ocenę i analizę procesów drukowania, w tym optymalizację, zabezpieczenie oraz bieżące monitorowanie urządzeń.

Zmień hasła administratora

Domyślne lub wstępnie ustawione hasła administratora są słabym punktem urządzeń drukujących. Można to w szybki i łatwy sposób naprawić. Chcąc zapewnić drukarkom wyższy poziom ochrony, wystarczy zmienić hasło zaraz po zainstalowaniu urządzenia.

Zaktualizuj oprogramowanie

Potencjalne luki w zabezpieczeniach urządzeń drukujących można zminimalizować dzięki dbaniu o bieżącą aktualizację oprogramowania i konfigurację sprzętu. W razie jakichkolwiek pytań lub problemów dotyczących wgrania nowego oprogramowania, należy skontaktować się z producentem drukarki.

Chroń dane

Nie tylko drukarki wymagają ochrony, ale także dokumenty, które wysyłasz do druku. Kompleksowe szyfrowanie ruchu sieciowego zapewnia bezpieczne przesyłanie plików do urządzeń drukujących. Należy jednak pamiętać, że większość z nich przez jakiś czas przechowuje pliki do wydrukowania, dlatego równie istotne jest zadbanie o kompleksowe szyfrowanie danych.

Stale monitoruj

Wgląd w całe środowisko druku gwarantuje znajomość aktualnego stanu urządzeń drukujących. Firmy powinny rozważyć wykorzystanie oprogramowania do monitorowania urządzeń, aby móc natychmiast reagować na pojawiające się problemy. Tego typu rozwiązania generują dużą ilość danych, które często mogą być wykorzystywane do identyfikacji niebezpiecznych zdarzeń i pozwalają na szybką reakcję na potencjalne ataki. Użytkownicy Usługi Zarządzania Drukiem (MPS) mogą również otrzymywać regularne raporty zgodności, w których powinno się znaleźć monitorowanie i raportowanie ewentualnych naruszeń danych.

Edukuj pracowników

Wiele przypadków utraty danych zostało spowodowanych nieumyślnie. To ważne, aby firmy edukowały swoich pracowników na temat znaczenia ochrony poufnych informacji i podnoszenia świadomości na temat złośliwych ataków. Często dostawcy Usług Zarządzania Drukiem (MPS) oferują pomoc w zakresie szkoleń.

Podsumowanie

W przeszłości systemy drukujące były pomijane w aspekcie bezpieczeństwa organizacji – na szczęście firmy coraz częściej zdają sobie sprawę z ich znaczenia. Niemniej jednak nadal stoją przed nami istotne wyzwania związane z wdrażaniem bezpieczeństwa druku.

Firmy z sektora MŚP muszą sprecyzować, kto odpowiada za bezpieczeństwo druku w ich organizacji. Osoba odpowiedzialna będzie dbała o właściwą ochronę urządzeń tak, aby były one przygotowane na potencjalne ataki. Oprócz troski o bezpieczeństwo sprzętów istotna jest również odpowiednia kontrola nad danymi wrażliwymi klientów i partnerów handlowych. Do tego koniecznie jest ścisła współpraca pomiędzy pracownikami.

Nawet jeśli przedsiębiorstwa z sektora MŚP wystarczająco jasno zdefiniują obowiązki w ramach swojej struktury, to brak odpowiedniej wiedzy, która umożliwiłaby skuteczne zarządzanie bezpieczeństwem druku wciąż stanowi duże wyzwanie. Technologia druku jest coraz bardziej złożona i przepełniona specjalistycznym żargonem. Firmy powinny korzystać z usług zaufanych dostawców w celu podejmowania rozsądnych decyzji.

Skuteczna konfiguracja druku to nie tylko bezpieczeństwo. Pozostałe raporty z serii Cyfrowa transformacja zawierają więcej informacji na temat wdrażania cyfrowych przepływów pracy, maksymalizacji wydajności i zrównoważonego rozwoju organizacji.

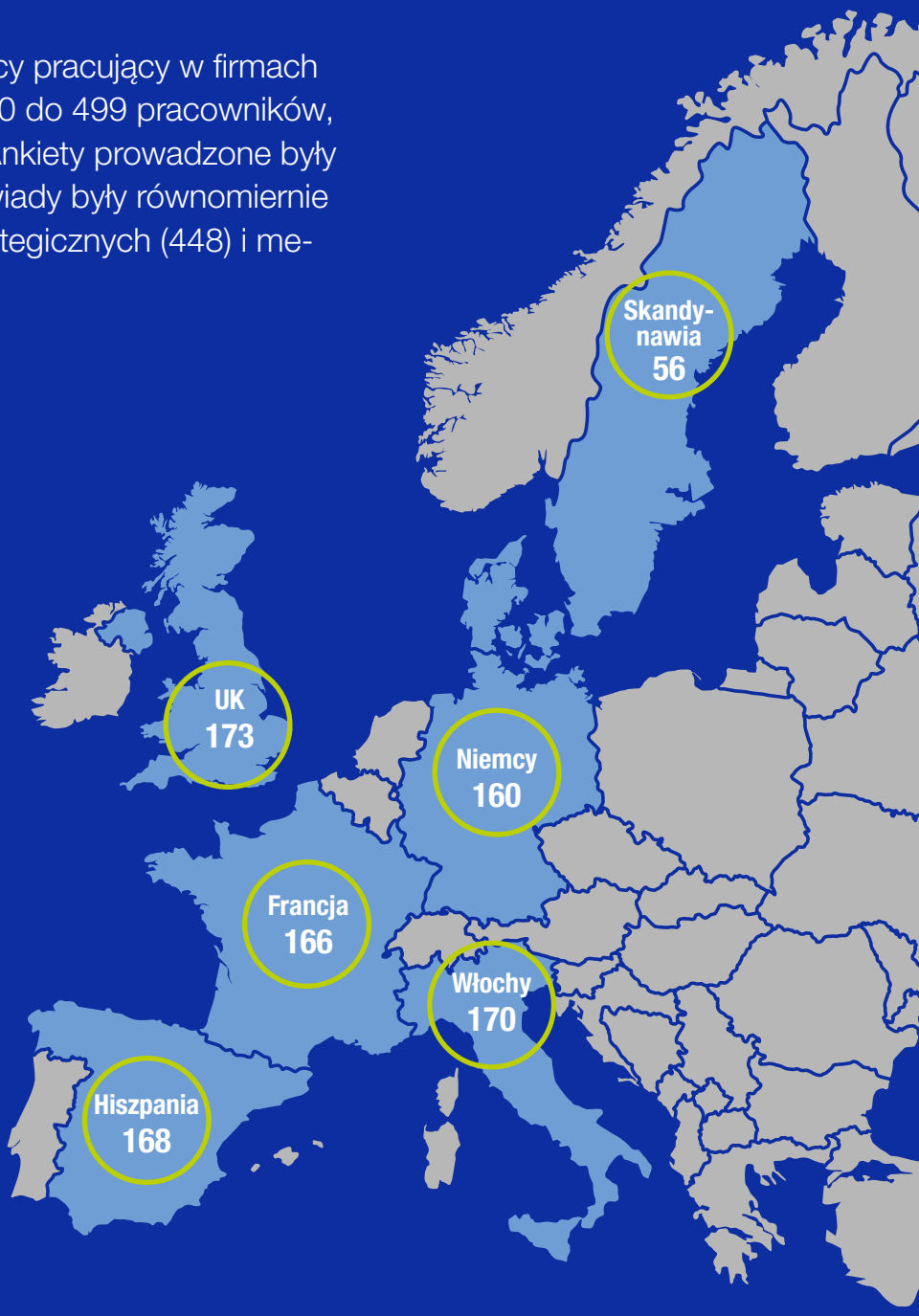
Nasza metodologia

Niniejszy raport opiera się na 893 ankietach online, przeprowadzonych wśród informatyków i menadżerów.

Respondenci: informatycy i kierownicy pracujący w firmach z sektora MŚP, zatrudniających od 10 do 499 pracowników, w kilku krajach Europy Zachodniej. Ankiety prowadzone były w 2019 r. i na początku 2020 r. Wywiady były równomiernie podzielone między menadżerów strategicznych (448) i menadżerów IT (445).

Kluczowe branże, z którymi przeprowadzono wywiady:

- Służba zdrowia – 152
- Handel – 117
- Logistyka – 113
- Usługi – 81
- Transport i składowanie – 62
- Usługi specjalistyczne – 65
- Produkcja – 54
- Finanse – 53
- Edukacja – 51
- Budownictwo – 39



Część ankiet pochodziła z innych branż i sektorów, m.in. energetycznej, farmaceutycznej, rolniczej, obronnej, nieruchomości, sportowej i rozrywkowej.

Badanie zostało przeprowadzone przez agencję badań rynkowych Savanta.

Sięgnij po informacje

Nasze kolejne raporty z serii Cyfrowa Transformacja.

brother
at your side

www.brother.pl

Brother Central and Eastern Europe GmbH
Oddział w Polsce
ul. Marynarska 15
02-674 Warszawa