

RAPORT Z BADANIA ILOŚCIOWEGO

MAŁE I ŚREDNIE PRZEDSIĘBIORSTWA A CYBERBEZPIECZEŃSTWO

Zrealizowano dla:

Defence **24**



Wrzesień 2026

METODOLOGIA



Czas realizacji: 21.09.2026 r. - 28.09.2026 r.



Jednostka badania: przedstawiciele MŚP



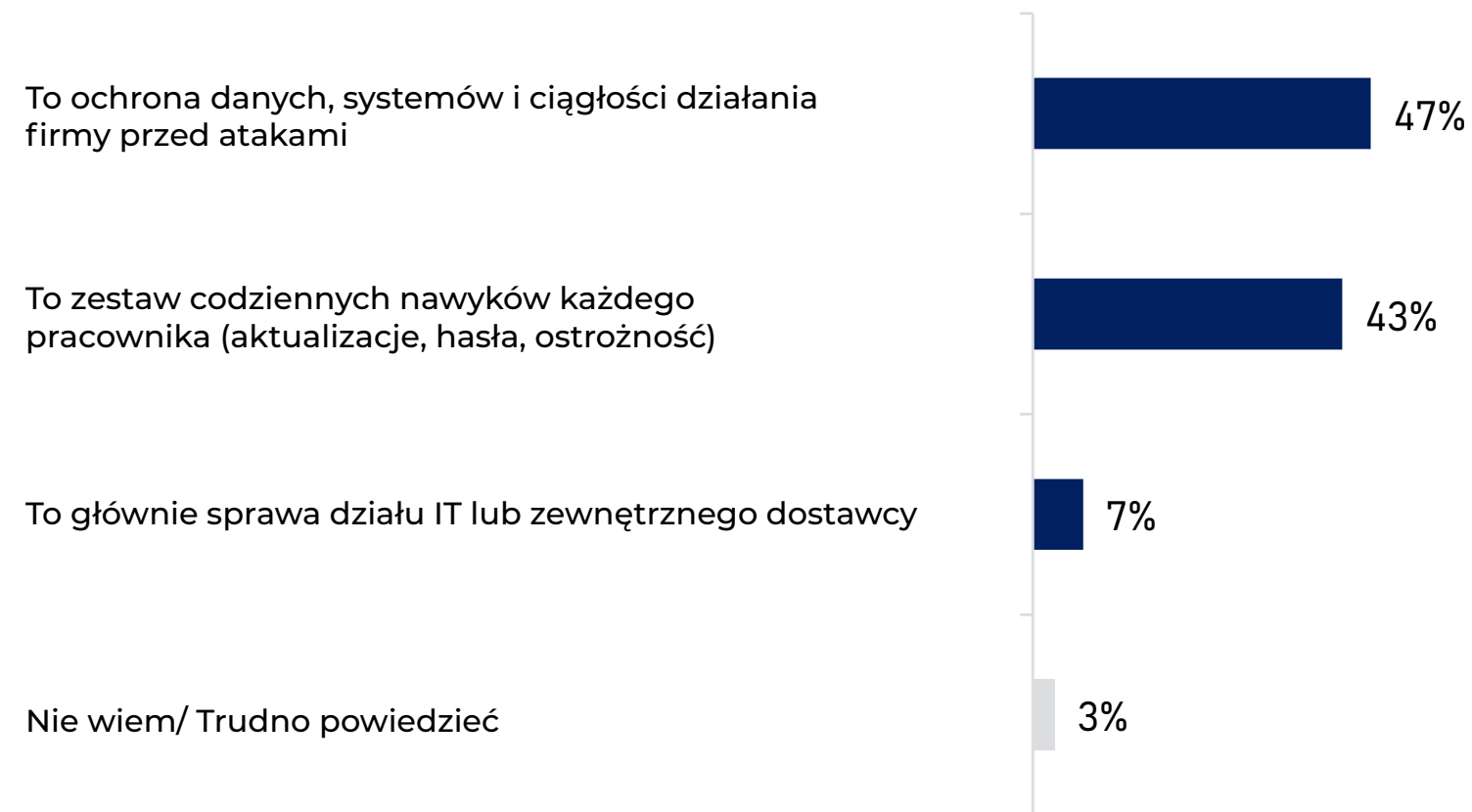
Wielkość próby: N=300



Technika badawcza: mix mode CATI/CAWI

ROZUMIENIE CYBERBEZPIECZEŃSTWA W FIRMIE

Q: Jak najlepiej opisał(a)by Pan/i, czym jest cyberbezpieczeństwo w firmie?



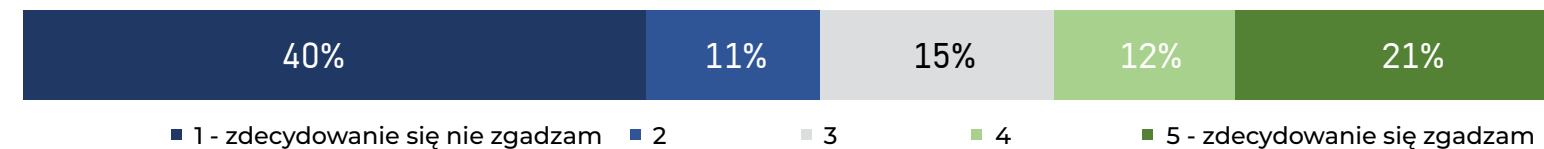
Cyberbezpieczeństwo jest najczęściej kojarzone z ochroną danych, systemów i ciągłości działania firmy przed atakami – wskazuje tak 47 proc. badanych. Niewiele mniej, 43 proc., postrzega je jako zestaw codziennych nawyków pracowników. Nieznaczny odsetek twierdzi, że jest to właściwie sprawa zewnętrzna.

POCZUCIE PODATNOŚCI MAŁYCH FIRM NA CYBERATAK

Q:

Czy zgadza się Pan/i ze stwierdzeniem: „**Nasza firma jest zbyt mała, by ktokolwiek chciał ją uczynić obiektem cyberataku**”?

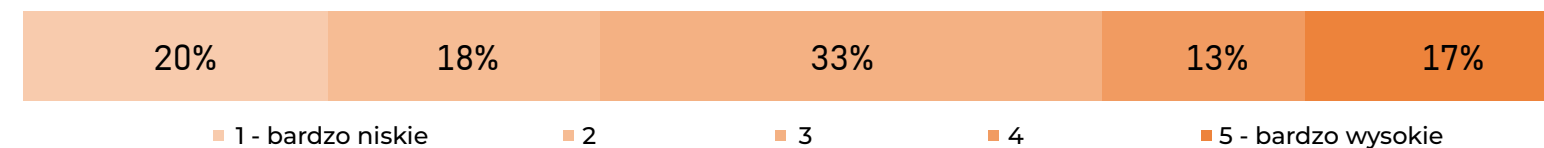
Proszę o ocenę na skali od 1 do 5, gdzie 1 oznacza zdecydowanie się nie zgadzam, a 5 zdecydowanie się zgadzam.



Q:

Jak ocenia Pan/i prawdopodobieństwo, że Pana/i firma doświadczy próby ataku (phishing, ransomware, przejęcie konta) w ciągu najbliższych 12 miesięcy?

Proszę o ocenę na skali od 1 do 5, gdzie 1-oznacza bardzo niskie, a 5- bardzo wysokie prawdopodobieństwo.

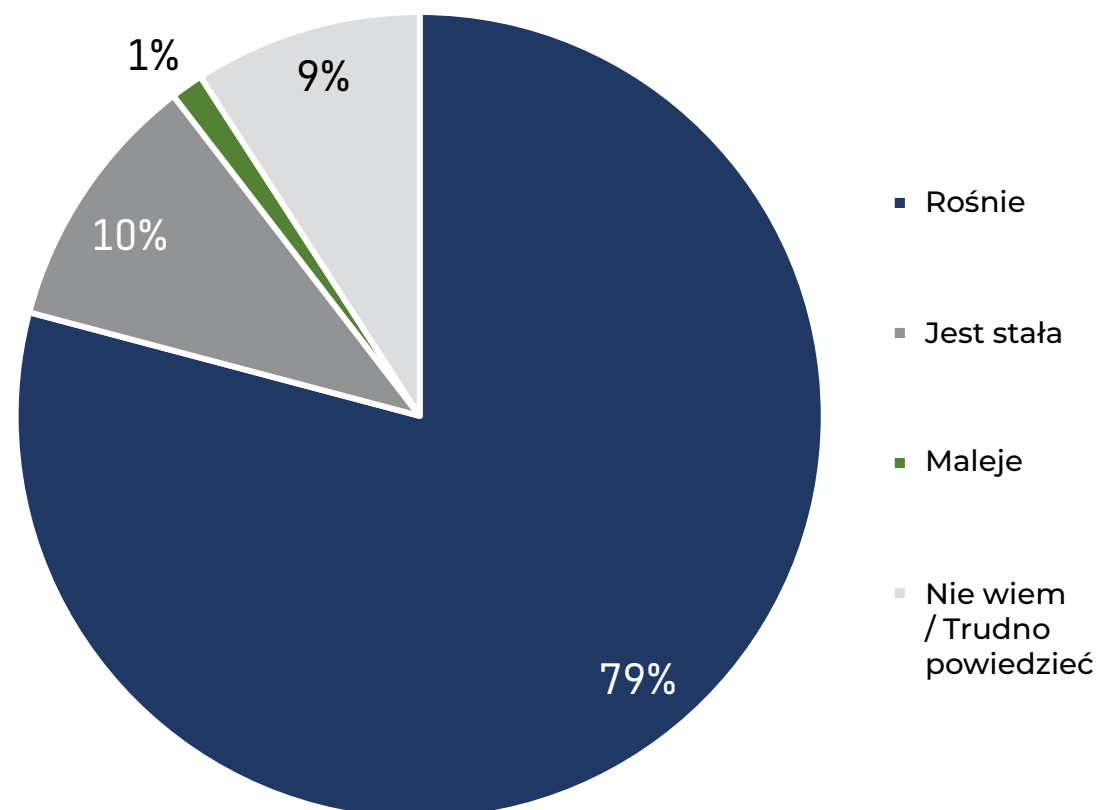


Przekonanie, że mała firma nie stanowi atrakcyjnego celu dla cyberprzestępców, nie dominuje wśród badanych – 51 proc. nie zgadza się z takim stwierdzeniem, 15 proc. wybiera środkową odpowiedź skali, a 33 proc. się z nim zgadza. Ocena ryzyka ataku w ciągu najbliższych 12 miesięcy jest bardziej wyrównana: 38 proc. ocenia je jako niskie, 33 proc. wybiera środek skali, a 30 proc. jako wysokie.

POSTRZEGANA SKALA CYBERZAGROŻEŃ

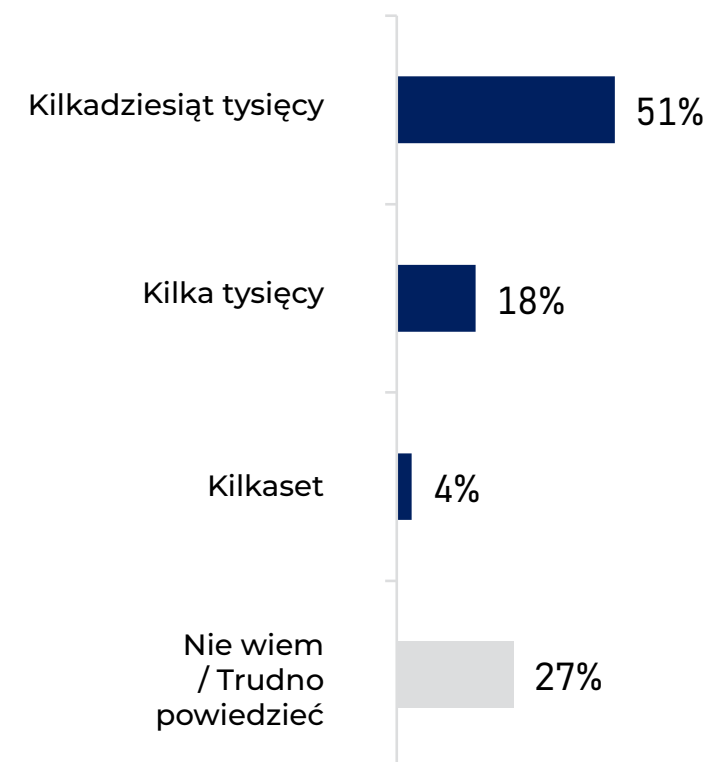
Q:

Czy sądzi Pan/i, że **liczba ataków** na polskie firmy w ostatnich latach...



Q:

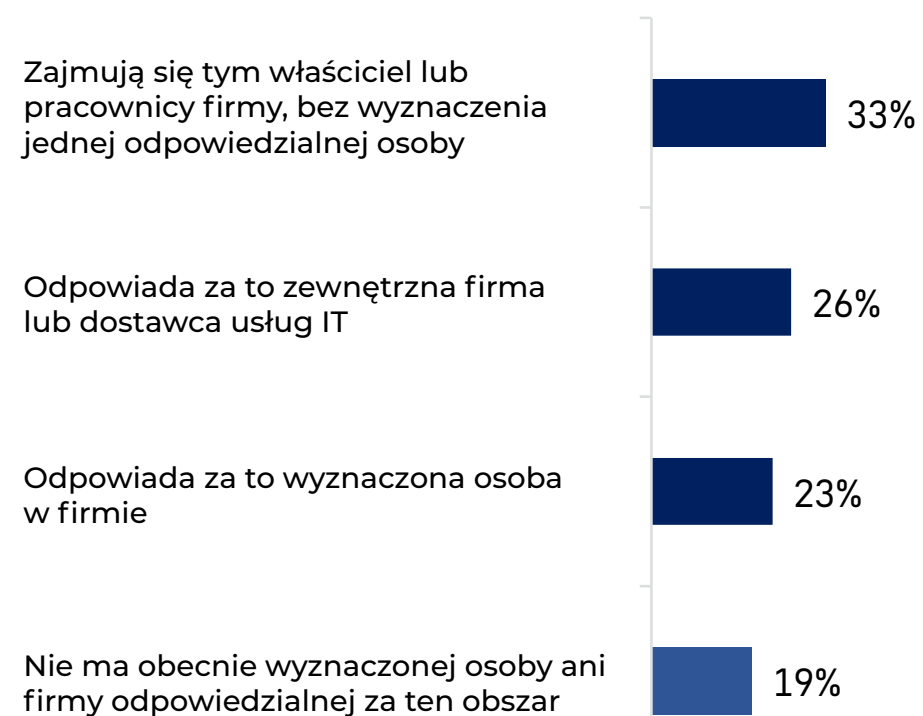
Jak Pan/i myśli, ile **incydentów cyberbezpieczeństwa** rocznie obsługuje w Polsce zespół CERT Polska?



Wzrost liczby cyberataków na polskie firmy dostrzega zdecydowana większość badanych – 79 proc. Skalę problemu odzwierciedla również fakt, że 51 proc. szacuje liczbę incydentów obsługiwanych rocznie przez CERT Polska na kilkadziesiąt tysięcy.

POSTRZEGANA SKALA CYBERZAGROŻEŃ

Q: Czy w Pana/i firmie jest konkretna **osoba lub firma odpowiedzialna za aktualizacje systemów i bezpieczeństwo komputerów?**



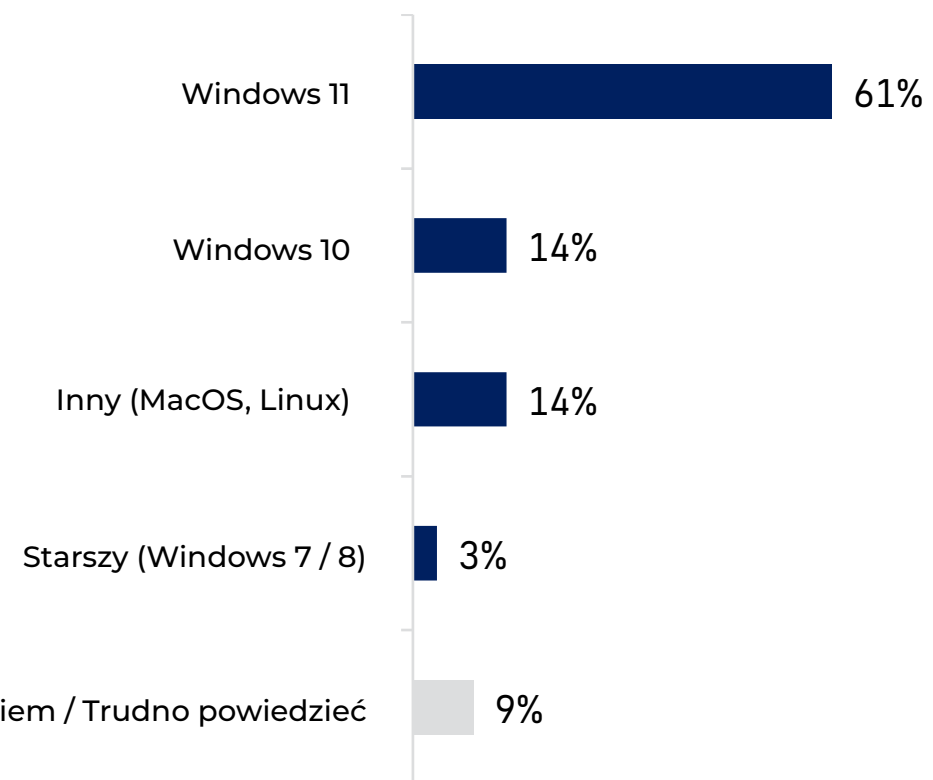
Q: Jak często aktualizowane są komputery i oprogramowanie w Pana/i firmie?



Odpowiedzialność za cyberbezpieczeństwo ma formalnie przypisaną osobę lub zewnętrznego dostawcę w 49 proc. firm.
Aktualizacje komputerów i oprogramowania najczęściej odbywają się automatycznie i na bieżąco – taką praktykę deklaruje 75 proc. badanych.

SYSTEMY OPERACYJNE WYKORZYSTYWANE W FIRMACH

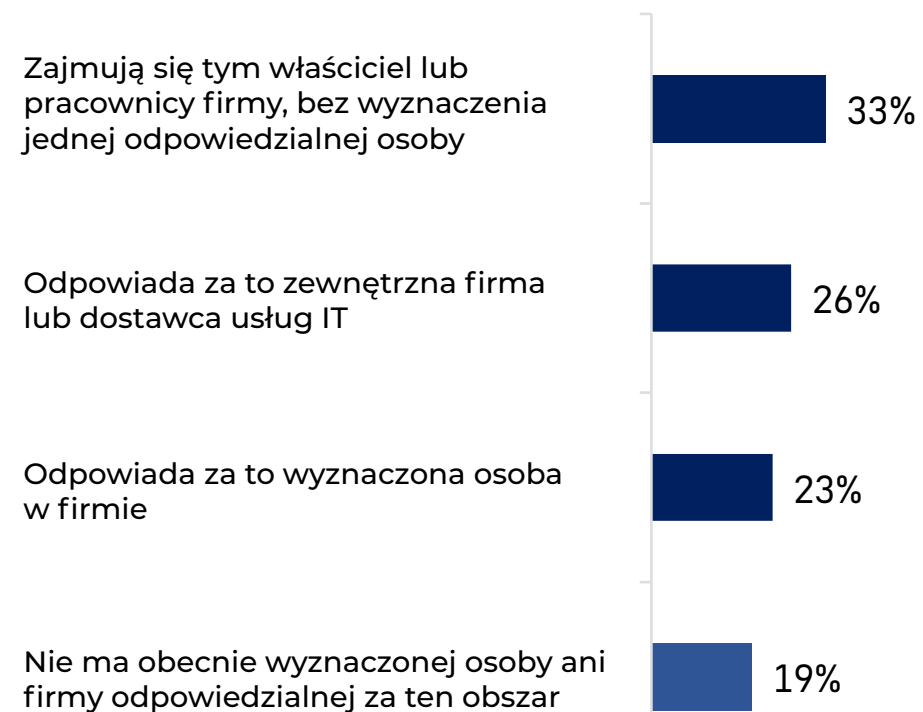
Q: Na jakim systemie operacyjnym pracuje większość komputerów w Pana/i firmie?



Windows 11 jest zdecydowanie najczęściej wykorzystywanym systemem operacyjnym – pracuje na nim większość komputerów w 61 proc. firm. Windows 10 wskazuje 14 proc. badanych, a starsze wersje systemu Windows – 3 proc.

POSTRZEGANA SKALA CYBERZAGROŻEŃ

Q: Czy w Pana/i firmie jest konkretna **osoba lub firma odpowiedzialna za aktualizacje systemów i bezpieczeństwo komputerów?**



Q: Jak często aktualizowane są komputery i oprogramowanie w Pana/i firmie?

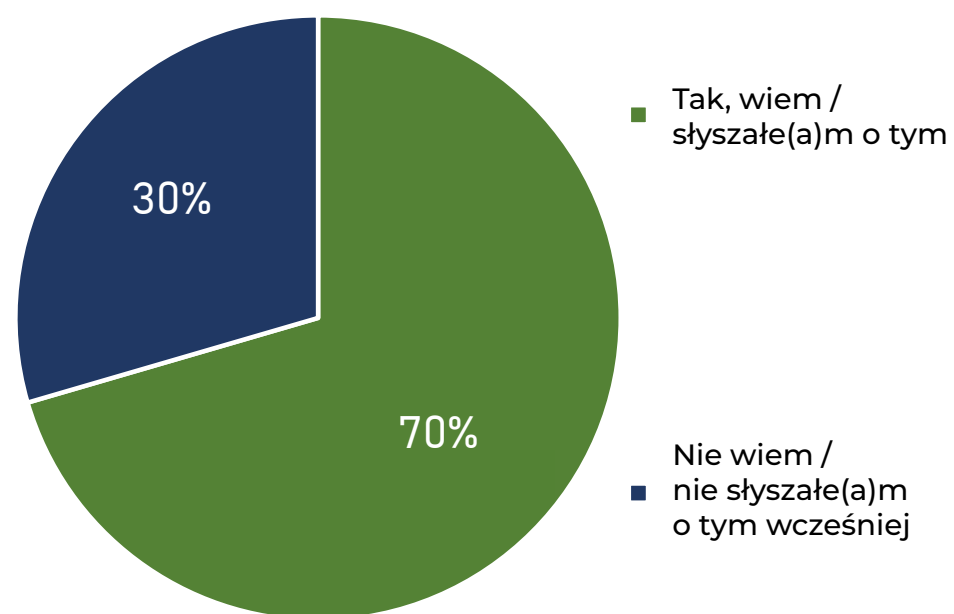


Odpowiedzialność za cyberbezpieczeństwo ma formalnie przypisaną osobę lub zewnętrznego dostawcę w 49 proc. firm.
Aktualizacje komputerów i oprogramowania najczęściej odbywają się automatycznie i na bieżąco – taką praktykę deklaruje 75 proc. badanych.

POSTRZEGANA SKALA CYBERZAGROŻEŃ

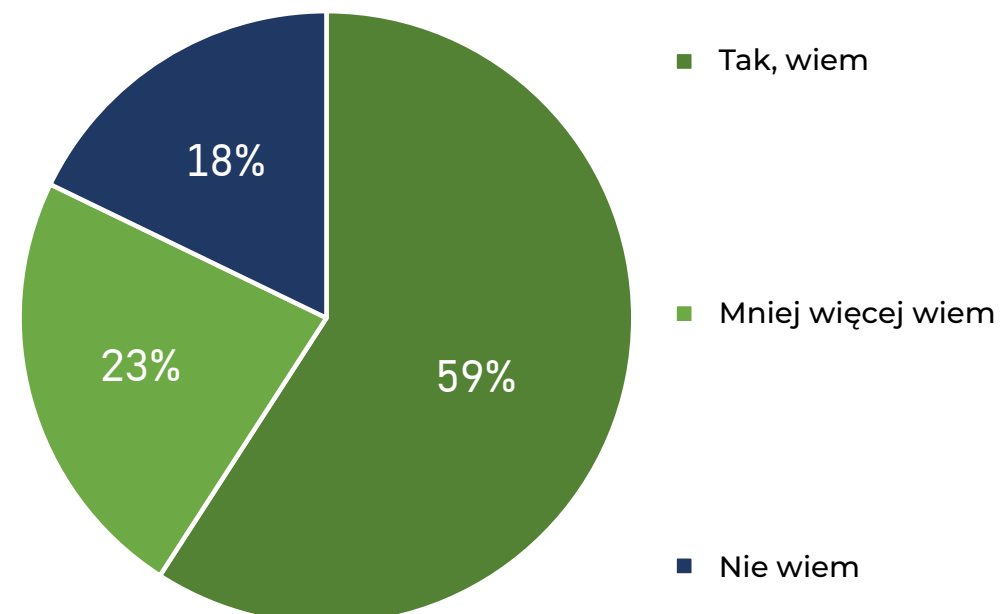
Q:

Czy słyszała Pan/i, że wsparcie dla Windows 10 zakończyło się, a ostatnie darmowe aktualizacje bezpieczeństwa wyszły w październiku 2025?



Q:

Czy wie Pan/i, z czym się wiąże „brak łatek bezpieczeństwa” (czyli brak aktualizacji)?



O zakończeniu wsparcia dla Windows 10 słyszało 70 proc. badanych.

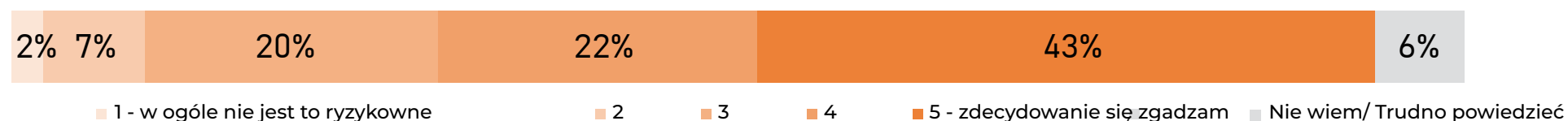
Z konsekwencji braku aktualizacji bezpieczeństwa zdaje sobie sprawę lub częściowo zdaje sobie sprawę łącznie 82 proc.

OCENA RYZYKA ZWIĄZANEGO Z NIEAKTUALNYM SYSTEMEM I GOTOWOŚĆ DO ZMIANY SYSTEMU

Q:

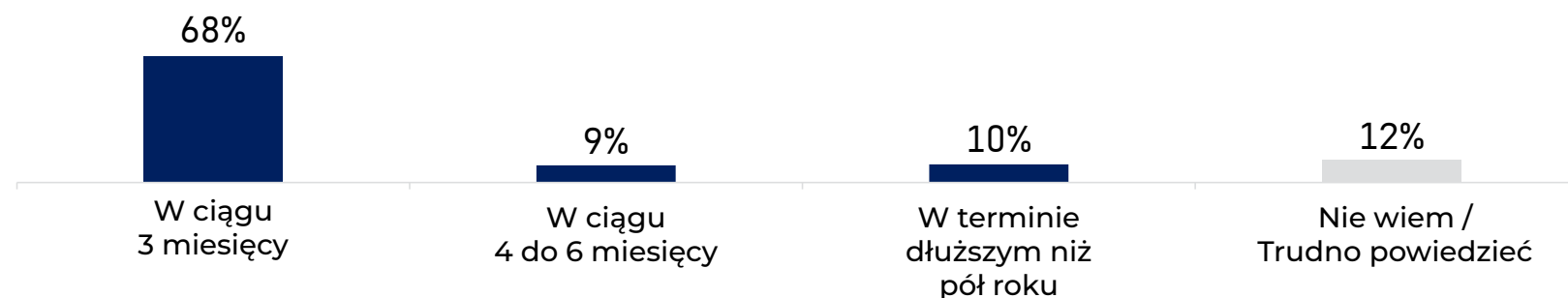
Jak ocenia Pan/i ryzyko dla bezpieczeństwa firmy związane z pracą na starym nieaktualizowanym systemie operacyjnym?

Proszę o odpowiedź na skali od 1 do 5, gdzie: 1 – w ogóle nie jest to ryzykowne, a 5 – jest to bardzo duże ryzyko.



Q:

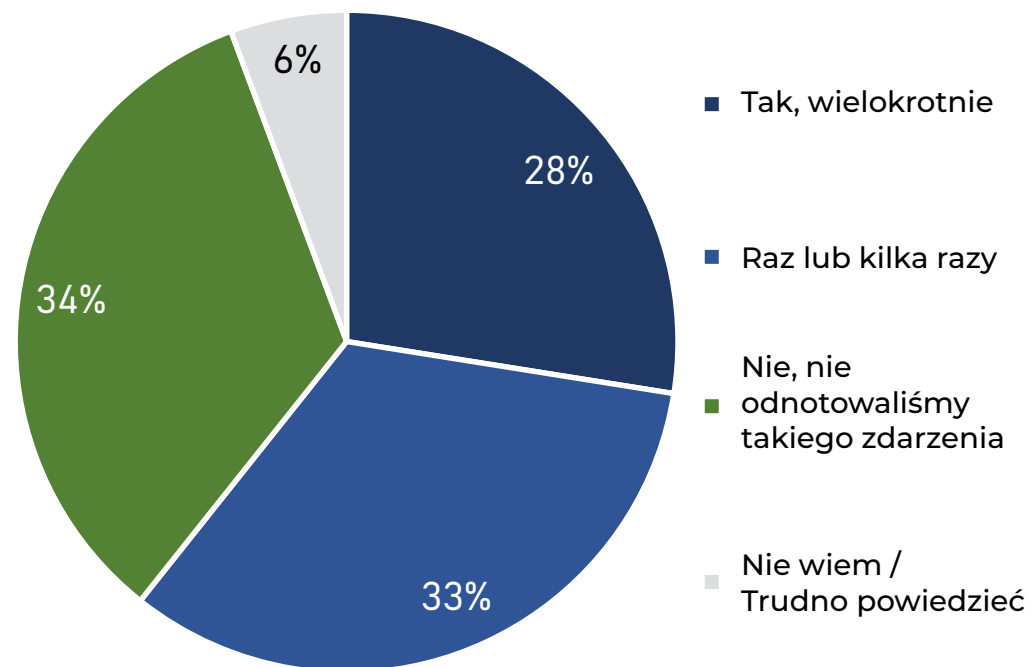
Gdyby obecny system, z którego korzysta firma przestałby być wspierany, to jak szybko firma byłaby zdolna zmienić go na nowy system?



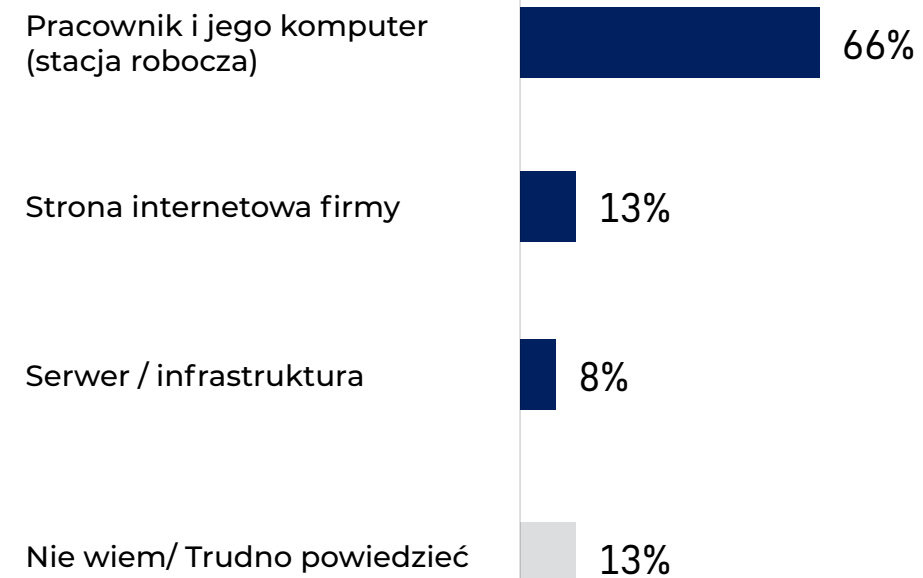
Praca na starym, nieaktualizowanym systemie jest najczęściej postrzegana jako poważne zagrożenie – 65 proc. badanych ocenia związane z nią ryzyko jako duże lub bardzo duże. W razie zakończenia wsparcia 68 proc. deklaruje możliwość zmiany systemu w ciągu trzech miesięcy.

DOŚWIADCZENIA Z CYBERZAGROŻENIAMI I ICH ŹRÓDŁA

Q: Czy w ciągu ostatniego roku **ktoś w Pana/Pani firmie otrzymał podejrzaną wiadomość (e-mail lub SMS) próbującą wyłudzić hasło, dane lub kliknięcie w link?**



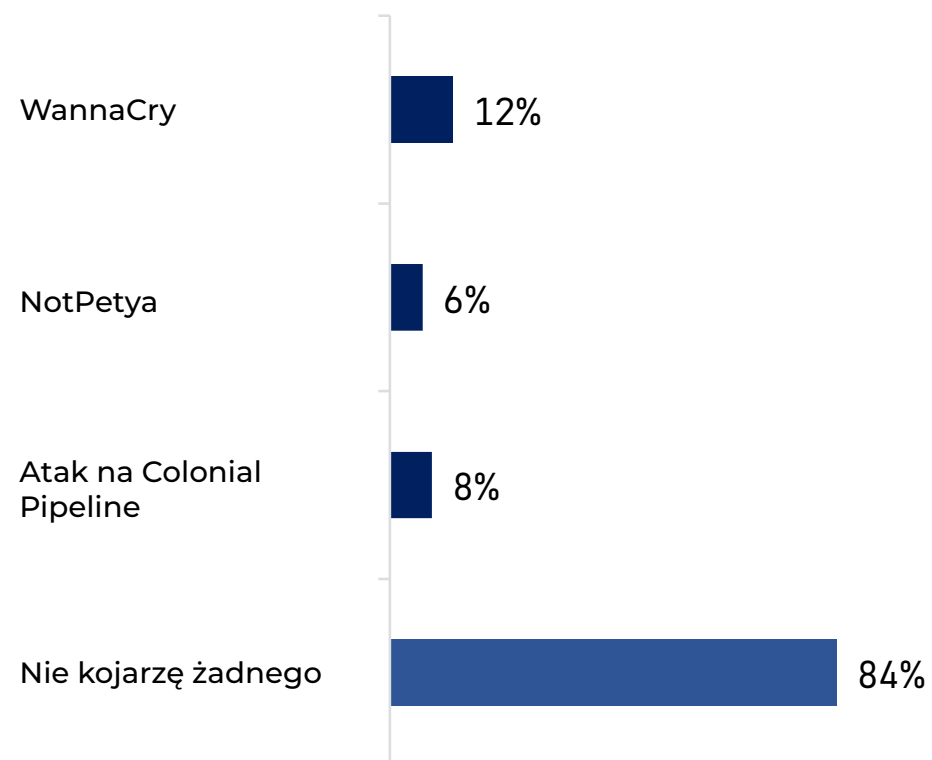
Q: Jak Pan/i sądzi, **co jest najsłabszym ogniwem bezpieczeństwa w firmach i najczęstszym punktem, przez który zaczyna się cyberatak?**



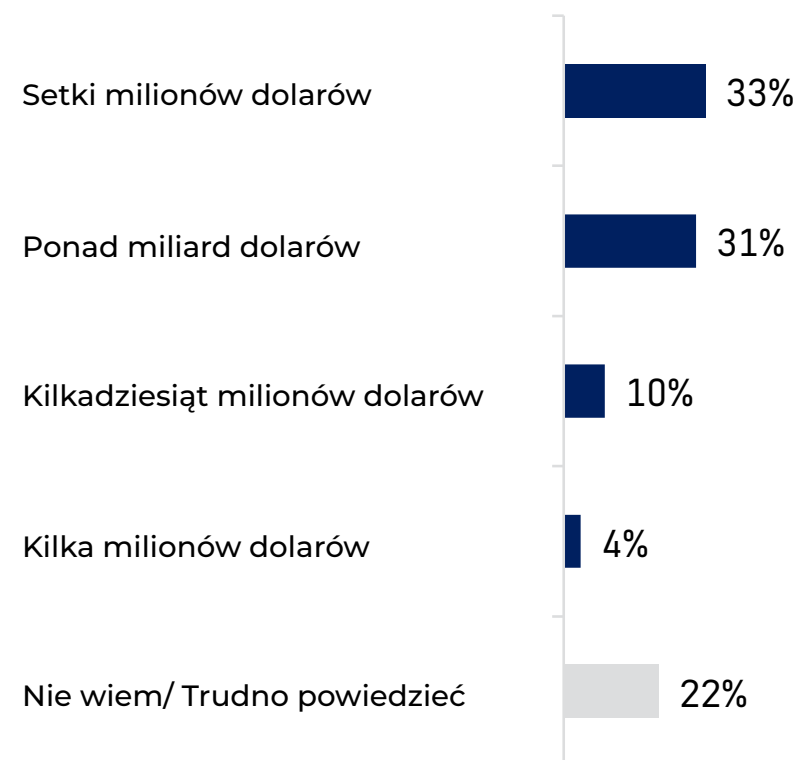
Próby wyłudzenia danych są stosunkowo częstym doświadczeniem firm – 61 proc. badanych deklaruje, że w ciągu ostatniego roku pojawiła się u nich co najmniej jedna podejrzana wiadomość. Za najsłabsze ogniwo bezpieczeństwa najczęściej uznawany jest pracownik i jego komputer – wskazuje tak 66 proc.

WIEDZA O CYBERATAKACH I ICH KONSEKWENCJACH

Q: Czy słyszał/a Pan/i o którymś z poniższych cyberataków ransomware?



Q: Jak Pan/i uważa, ile rocznie na świecie cyberprzestępcy wyłudniają z samych okupów za zaszyfrowane wskutek ataku dane?



Znajomość konkretnych przykładów ataków ransomware pozostaje ograniczona – 84 proc. badanych nie kojarzy żadnego z wymienionych przypadków. Skalę finansową cyberprzestępczości większość ocenia jako wysoką – 64 proc. wskazuje na setki milionów lub ponad miliard dolarów rocznie.

PODSUMOWANIE

- Cyberbezpieczeństwo jest najczęściej rozumiane jako **ochrona danych, systemów i ciągłości działania firmy (47 proc.)** oraz jako **zestaw codziennych nawyków pracowników (43 proc.)**.
- Większość badanych dostrzega rosnącą skalę zagrożeń – **79 proc. uważa, że liczba ataków na polskie firmy rośnie**. Ponad połowa (**51 proc.**) **nie zgadza się też z opinią, że ich firma jest zbyt mała, by stać się celem cyberataku**.
- Organizacja cyberbezpieczeństwa przyjmuje różne formy – w **49 proc. firm odpowiada za nie wyznaczona osoba lub zewnętrzny dostawca**, a w **33 proc. zajmują się nim właściciel lub pracownicy bez wskazania jednej odpowiedzialnej osoby**. Aktualizacje systemów w 75 proc. firm odbywają się automatycznie.
- **Najczęściej wykorzystywanym systemem jest Windows 11 (61 proc.)**. O zakończeniu wsparcia dla Windows 10 wie 70 proc. badanych, a 82 proc. deklaruje przynajmniej częściową znajomość konsekwencji braku aktualizacji bezpieczeństwa.
- Ryzyko pracy na starym, nieaktualizowanym systemie jako **duże ocenia 65 proc. badanych**. W razie zakończenia wsparcia **68 proc. deklaruje możliwość zmiany systemu w ciągu trzech miesięcy**.
- **Próby wyłudzenia danych są częstym doświadczeniem firm** – 61 proc. badanych deklaruje, że w ostatnim roku zetknęło się z nimi co najmniej raz. **Za najsłabsze ogniwo cyberbezpieczeństwa 66 proc. uznaje pracownika i jego komputer**.

DZIĘKUJEMY ZA UWAGĘ

ZOSTAŃMY W KONTAKCIE

Tel.: +48 22 266 00 15

E-mail: biuro@ibris.pl

www.ibris.pl

AL. Jerozolimskie 96,
00-807 Warszawa