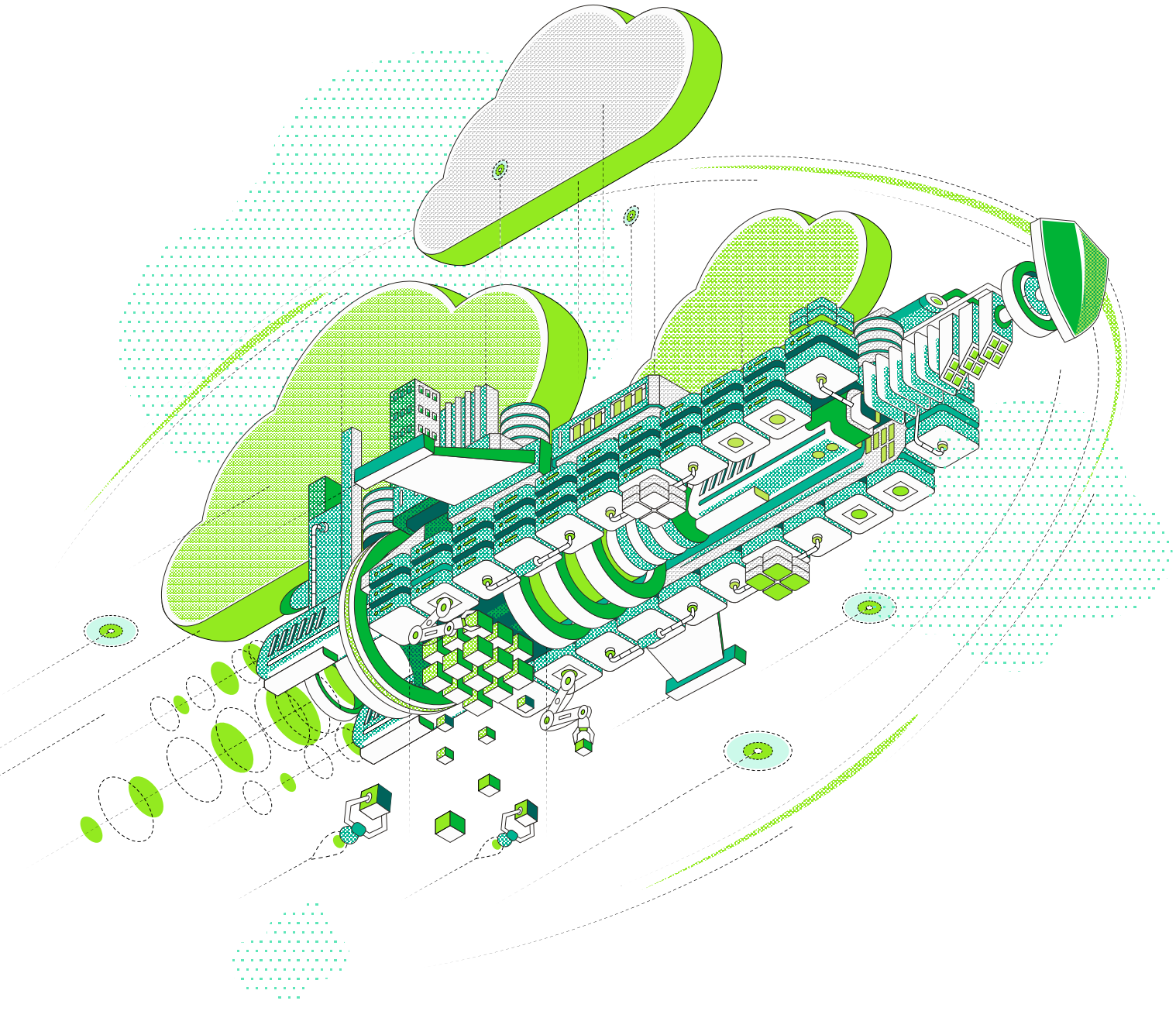
STRESZCZENIE

2022

Główne trendy w ochronie danych

Wersja dotycząca Europy Wschodniej, w tym Polski, Czech, Węgier, Rumunii itd.



W branży IT zachodzą coraz szybsze zmiany, ale jak dokładnie firmy wdrażają nowoczesną ochronę danych? W okresie od października do grudnia 2021 r. niezależna firma badawcza zapytała ponad 3000 decydentów i specjalistów z obszaru IT o czynniki wpływające na rozwój środowisk IT i ochronę danych w ich firmach oraz o strategie na 2022 r. Niemal wszyscy respondenci pochodzili z przedsiębiorstw zatrudniających ponad 1000 pracowników i ogółem reprezentowali 28 krajów. W ich gronie było 186 respondentów z Europy Wschodniej — Polski, Czech, Węgier, Rumunii itd.

Jeśli chodzi o budżet na ochronę danych, obejmujący zarówno backup, jak i ciągłość działania / odzyskiwanie po awarii, respondenci oczekiwali, że w 2002 r. wzrośnie on o **5,9%** w ujęciu globalnym oraz o **6,0%** w Europie Wschodniej, w tym w Polsce, w Czechach, na Węgrzech, w Rumunii itd. Jeśli weźmiemy pod uwagę szczególne okoliczności, takie jak stagnacja w obszarze lokalnych środowisk IT spowodowana przez kwarantanny i problemy z ciągłością dostaw w trakcie pandemii, a także powiązane z tymi czynnikami coraz szybsze wdrażanie chmury, jest czymś zrozumiałym, że w 2022 r. nasilą się inwestycje w ochronę danych, które będą musiały uwzględnić aktualne zróżnicowanie środowisk produkcyjnych.

Celem tegorocznego badania trendów w ochronie danych — już trzeciego corocznego badania z tego cyklu — było ilościowe uchwycenie przesunięć w dziedzinie ogólnych obaw, celów i strategii ochrony danych, a także poznanie obecnej sytuacji rynkowej w obszarach ochrony danych, odzyskiwania po awarii, cyberzabezpieczeń / ochrony przed atakami ransomware i rozwiązań kontenerowych.

Chmura hybrydowa i środowisko wielu chmur weszły do głównego nurtu

Ponad **8000** punktów danych zebranych w trakcie trzech kolejnych lat tego badania nie pozostawia wątpliwości: „nową normalnością" w nowoczesnych środowiskach IT jest równomierny rozkład liczby serwerów między środowiskiem lokalnym i chmurą. W centrach danych konsekwentnie stosowane są platformy zarówno fizyczne, jak i wirtualne. W obszarze chmury można zaobserwować zdrową kombinację platform hiperskalowych i infrastruktur hostowanych przez dostawców usług zarządzanych.

23%

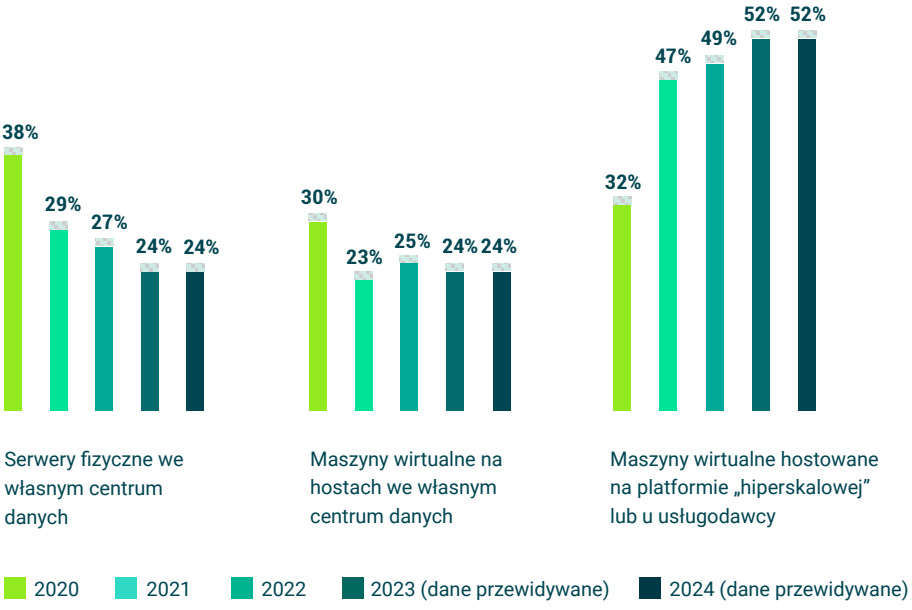
przedsiębiorstw jako podstawowy czynnik zmiany rozwiązania do backupu podaje chęć poprawy parametrów ekonomicznych, a 18% chce zwiększyć niezawodność i obniżyć wartości RPO/RTO

67%

przedsiębiorstw korzysta z usług chmurowych w ramach strategii ochrony danych

76%

przedsiębiorstw w ubiegłym roku było celem co najmniej jednego ataku ransomware



Ilustracja 1.1

Jak w Państwa przedsiębiorstwie obecnie wygląda odsetek serwerów w każdym z formatów i jak zgodnie z Państwa przewidywaniami odsetek ten będzie wyglądał za dwa lata?

W 2022 r. na terenie Europy Wschodniej, w tym Polski, Czech, Węgier, Rumunii itd., serwery fizyczne stanowią 28%, serwery wirtualne 25%, a serwery w chmurze 48%. Na postawie tych liczb można sformułować dwa najważniejsze wnioski:

- Centrum danych trwa i ma się dobrze. Uruchamianie obciążeń w środowisku lokalnym jest równie uzasadnione jak ich hostowanie w chmurze — nawet w przedsiębiorstwach realizujących strategię „cloud first".
- Firmowa strategia ochrony danych musi obejmować obciążenia fizyczne, wirtualne i działające w wielu chmurach.

Rozziew między oczekiwaniami jednostek biznesowych a ich spełnianiem przez dział IT jest najgorszy w historii

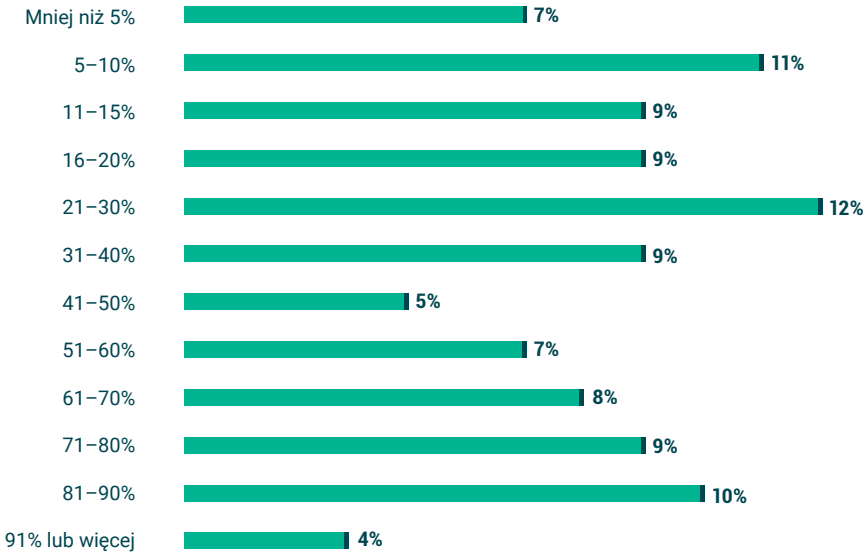
Jak wynika z danych gromadzonych w ramach tego projektu na przestrzeni ostatnich pięciu lat, w Europie Wschodniej — w tym w Polsce, w Czechach, na Węgrzech, w Rumunii itd. — stale rośnie rozziew między oczekiwaniami jednostek biznesowych i zdolnością do ich spełnienia przez dział IT.

- **88%** menedżerów IT uważa, że w ich przedsiębiorstwach występuje **„deficyt dostępności"**, czyli różnica między oczekiwanymi parametrami SLA i tym, jak szybko dział IT może przywrócić produktywność.
- **87%** menedżerów IT uważa, że w ich przedsiębiorstwach występuje **„deficyt ochrony"**, czyli różnica między ilością danych, na których utratę przedsiębiorstwo może sobie ochronić, a częstotliwością operacji ochrony.

Najbardziej prawdopodobną przyczyną tych deficytów jest rosnący stopień krytyczności coraz większej liczby obciążeń. Istnieje jednak oczywisty związek między najważniejszymi czynnikami zmian — poprawą parametrów RTO (dostępność) i RPO (ochrona) oraz niezawodności (ilustracja 1.3 w raporcie) — a tymi obserwowanymi deficytami. Deficyty postrzegane przez menedżerów IT oraz czynniki zmian związane z ograniczaniem strat danych i przestojów, którymi kierują się wdrożeniowcy technologii IT, stają się tym bardziej uzasadnione, jeśli wziąć pod uwagę, że **40%** serwerów (w ujęciu globalnym) miało w ciągu roku co najmniej jeden przestój.

40%

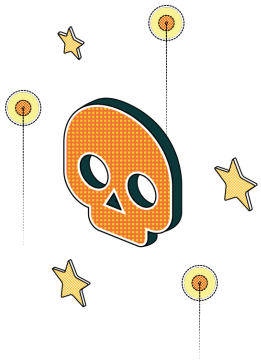
serwerów ma co najmniej jeden nieplanowany przestój



Ilustracja 1.2

Jaki odsetek Państwa serwerów miał co najmniej jeden nieplanowany przestój (choćby nieplanowany restart) w ciągu ostatnich 12 miesięcy?

Niewielka różnica między danymi „priorytetowymi" i „normalnymi"



Zawsze będą istnieć obciążenia lub dane, którym przypisuje się wyższy priorytet, jednak pod względem oczekiwań te ważne obciążenia nie różnią się zbytnio od reszty środowiska IT.

Utrata danych. W ujęciu globalnym w przypadku 56% danych priorytetowych i 49% danych normalnych tolerowana wielkość ich utraty wynosi maksymalnie godzinę. Jeśli chodzi o przedsiębiorstwa z Europy Środkowej — Polski, Czech, Węgier, Rumunii itd. — tolerowana wielkość utraty na poziomie maksymalnie godziny dotyczy 60% danych priorytetowych i 52% danych normalnych. Co to oznacza:

- Dane „priorytetowe" niewiele się różnią od pozostałych — wszystkie dane są ważne.
- Sam backup nie wystarczy, ponieważ nie jest wykonywany co godzinę. Dlatego tworzenie kopii zapasowych należy połączyć z wykonywaniem migawek i/lub replikacją.

Wskaźniki te wyglądają jeszcze ciekawiej na tle trzyletniego trendu, który wyłania się z kolejnych raportów „Trendy w ochronie danych". Poniżej przedstawiono średnią częstotliwość operacji ochrony danych (wyrażoną w minutach), które mają na celu złagodzenie skutków utraty danych priorytetowych i normalnych:

	2019	2020	2021
Częstotliwość ochrony danych priorytetowych	205 minut	198 minut	121 minut
Częstotliwość ochrony normalnych danych	663 minuty	423 minuty	171 minut

49%

przedsiębiorstw doświadczyło przestoju wskutek ataku ransomware. Drugi rok z rzędu cyberataki spowodowały najwięcej przestojów

To logiczne, że z upływem czasu przedsiębiorstwa polepszają ochronę danych priorytetowych: interwał operacji ochrony zmniejszył się z **205** minut w 2019 r. do **121** minut w 2021 r. Prawdziwym odkryciem jest jednak fakt, że w tym samym dwuletnim okresie przedsiębiorstwa radykalnie zwiększyły częstotliwość ochrony pozostałych danych: odstęp między operacjami ochrony spadł z **663** minut (operacje wykonywane w przybliżeniu co 8 godzin, czyli poza normalnymi godzinami pracy) do **171** minut (operacje wykonywane co 3 godziny, czyli również w normalnych godzinach pracy). Jest to poziom zbliżony do stopnia ochrony danych priorytetowych, co potwierdza tezę, że „wszystkie dane są ważne", a także atrakcyjność rozwiązań łączących (zazwyczaj tworzone w nocy) kopie zapasowe z migawkami i/lub replikacją.

Przestoje. Tutaj sytuacja wygląda podobnie jak w kwestii utraty danych: pod względem tolerowanej długości przestoju wynoszącej maksymalnie godzinę aplikacje priorytetowe i aplikacje normalne różnią się zaledwie o **8%**. Jest to kolejne potwierdzenie obserwacji, że wszystkie dane są ważne i potrzebne są lepsze rozwiązania niż tworzone raz na dobę kopie zapasowe.

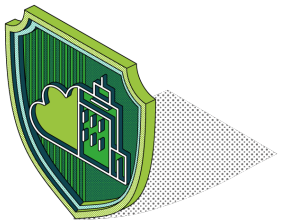
36%

danych (średnio) nie można było odzyskać po ataku ransomware

Co to oznacza na 2022 r.?

Od dwóch lat obserwujemy znaczącą modernizację środowisk IT, zwłaszcza tam, gdzie można wykorzystać usługi hostowane w chmurze. Wynika to z bieżących inicjatyw z zakresu transformacji cyfrowej, a także szybszego tempa wdrażania chmury podczas ogólnoświatowej pandemii. **Dynamiczna modernizacja środowisk produkcyjnych zmusiła wiele przedsiębiorstw do przyznania, że ich systemy ochrony nie są unowocześniane w równie szybkim tempie, mimo że stopień ich uzależnienia od danych i niezadowolenie z obecnego stanu notują historyczne rekordy. Z tej sytuacji wyłaniają się trzy najważniejsze trendy na 2022 r.:**

- Ochrona danych będzie obszarem kolejnych inwestycji, których celem będzie zabezpieczenie nowoczesnych obciążeń już działających w środowisku produkcyjnym, a często hostowanych w chmurze.
- Głównym czynnikiem wymuszającym zmiany będzie dążenie do jakościowej poprawy niezawodności, częstotliwości ochrony i sprawności odzyskiwania, przekładającej się na polepszenie wskaźników RPO i RTO. Bardzo ważna będzie też chęć zwiększenia korzyści ekonomicznych i podwyższenia stopnia konsumpcji, ochrony środowisk IaaS, SaaS i kontenerowych oraz wykorzystywania chmury do operacyjnego backupu i odzyskiwania po awarii.
- Doskonalenie ochrony danych w dużej mierze wynika z uznania faktu, że w większości przedsiębiorstw cyberataki, w szczególności ataki ransomware, to kwestia nie „czy", ale „kiedy", a ważnym elementem strategii gotowości cybernetycznej jest niezawodne odzyskiwanie pozwalające usunąć skutki ewentualnego ataku. Każde przedsiębiorstwo rozumie, że atak ransomware jest katastrofą, a zorkiestrowane odzyskiwanie danych z kopii zapasowych to krytyczny element każdego planu zachowania ciągłości działania / odzyskiwania po awarii.



42%

menedżerów IT na świecie za najważniejszy aspekt rozwiązania do backupu klasy „korporacyjnej" uważa zakres chronionych obciążeń

Perspektywa firmy Veeam

Platforma firmy Veeam do backupu i zarządzania danymi

Obecnie firmom szczególnie zależy na stałej pewności, że ich dane są chronione i zawsze dostępne — niezależnie od tego, czy znajdują się w środowisku lokalnym, na brzegu sieci czy w chmurze. Firma Veeam udostępnia kompleksową platformę przeznaczoną do środowisk chmurowych, wirtualnych, fizycznych, SaaS i Kubernetes. Nasi klienci mają pewność, że ich dane są chronione przed atakami ransomware, awariami i złośliwymi podmiotami oraz zawsze dostępne dzięki najprostszej oraz najbardziej elastycznej, niezawodnej i wydajnej platformie w branży.

Zapewniając stałą ochronę i dostępność danych, rozwiązania Veeam dają klientom pewność, która ułatwia szybsze wdrażanie transformacji cyfrowej, ochronę przed cyberprzestępczością i zwiększanie odporności biznesowej. Również Twoja firma może obniżyć koszty i stopień złożoności oraz osiągnąć cele biznesowe, jeśli wdroży Veeam — nr 1 do backupu i odzyskiwania.

Więcej informacji jest dostępnych na stronie **https://www.veeam.com/pl**.

Kliknij tutaj, aby wyświetlić pełny raport z badania globalnego

Pytania dotyczące przedstawionych danych i spostrzeżeń badawczych można kierować na adres StrategicResearch@veeam.com