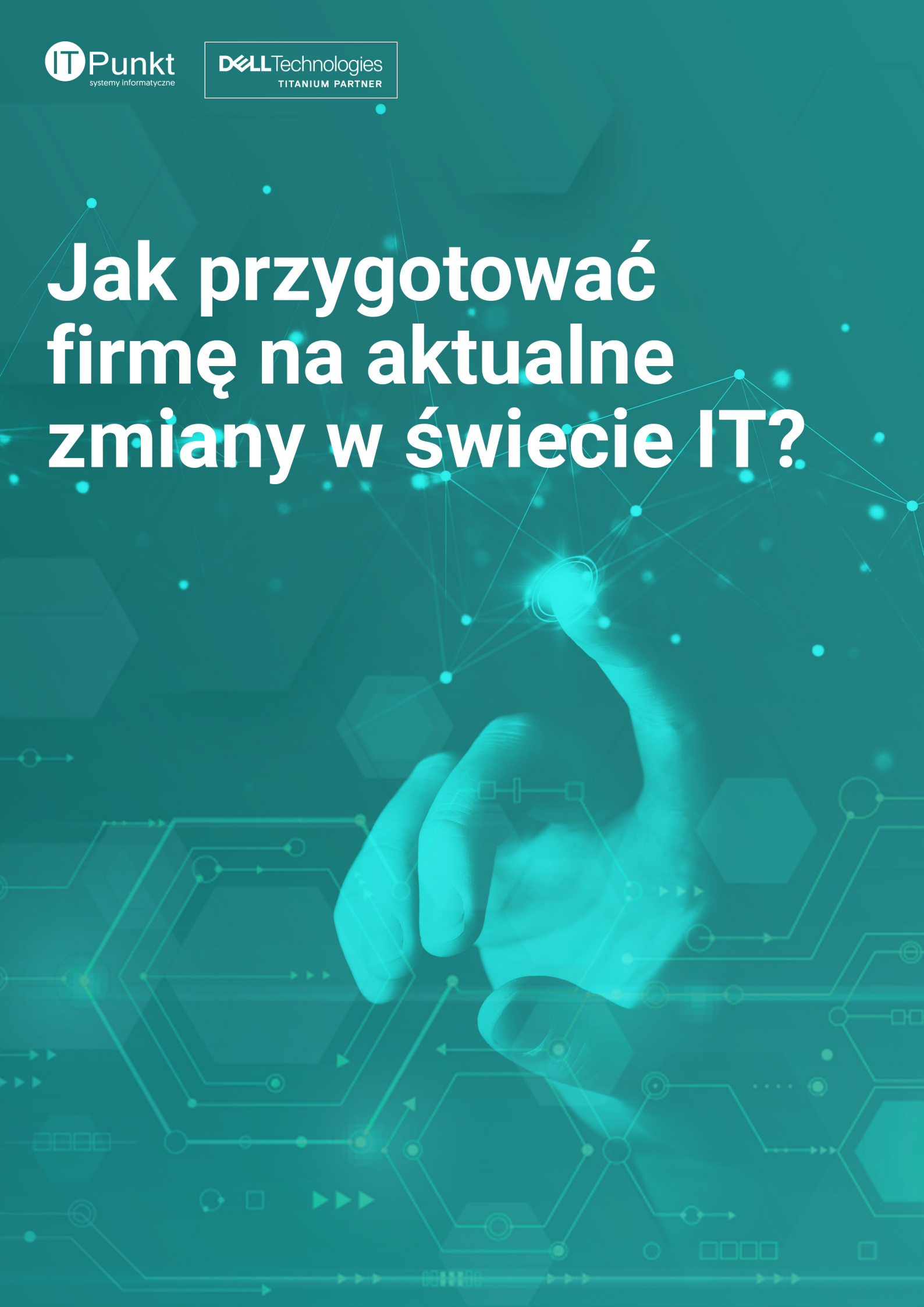
IT Punkt
systemy informatyczne

DELL Technologies
TITANIUM PARTNER

Jak przygotować firmę na aktualne zmiany w świecie IT?



SPIS TREŚCI

Jak zwiększyć swoją odporność?

Zwiększenie cyfryzacji firm i przedsiębiorstw było tylko kwestią czasu. Pandemia COVID-19 w wielu miejscach znacząco ją jednak przyspieszyła. Firmy chcą stać się bardziej odporne na nieprzewidziane sytuacje, lepiej reagować na zmiany, zapewnić sobie przewagę konkurencyjną i wzmocnić bezpieczeństwo swoich systemów. Rozwiązania, jakie zostały opisane w poniższym e-booku, wprost odpowiadają na te potrzeby. Zapewniają przedsiębiorstwom większą elastyczność infrastruktury, skuteczniejszą ochronę danych, niższe koszty obsługi informatycznej oraz, co równie istotne, lepszą komunikację i współpracę w zespołach.

Rozwiązania zaproponowane klientom ITPunkt są zawsze dobierane zgodnie z najlepszymi praktykami, wynikającymi z posiadanej wiedzy eksperckiej i doświadczenia zdobytego podczas realizacji wielu projektów. W każdym przypadku inżynierowie wykonują audyt środowiska produkcyjnego oraz przeprowadzają wywiad, by w szczegółach poznać potrzeby i oczekiwania klienta. Następnie, biorąc pod uwagę wszystkie zmienne, szyją dla niego system na miarę. Dodatkowo klienci otrzymują ofertę obsługi posprzedażowej, w tym usługi wdrożeń, monitoringu i serwisu środowiska.

Hiperkonwergencja odpowiedzią na wymóg wysokiej elastyczności

Jakub Kłoda

Tradycyjna architektura składająca się z serwerów, pamięci masowej, przełączników LAN i SAN jest nam wszystkim bardzo dobrze znana. Doskonale znane są również jej ograniczenia w zakresie elastyczności, skalowalności czy wydajności, które w wielu przypadkach kończą się wymianą części infrastruktury na zupełnie nową. Istnieją na rynku rozwiązania, które adresują powyższe ograniczenia, zmniejszając przy tym złożoność infrastruktury. Migracja obecnego środowiska może zostać przeprowadzona w sposób bezpieczny i bezprzerwowy. Rozwiązanie pozwala natywnie wykorzystać mechanizmy wysokiej dostępności zgodnie z naszymi potrzebami.

Brzmi sensownie? A to nie wszystkie korzyści wynikające z zastosowania architektury HCI (Hyper-Converged-Architecture). Architektura HCI wirtualizuje moc obliczeniową serwera (CPU/MEM), zasoby dyskowe (NVME, SSD, SAS) oraz obszar sieci (VSS, DVS). Rozwiązanie umożliwia rozbudowę zarówno w trybie Scale-Up, jak i w trybie Scale-Out – zgodnie z naszymi potrzebami. Proces rozbudowy w obu trybach odbywa się w sposób zautomatyzowany, a sama procedura rozbudowy jest bardzo dokładnie i w prosty sposób przedstawiona. Niewątpliwym atutem jest również ułatwienie procesu administracji infrastrukturą. Zarządzanie architekturą HCI odbywa się poprzez centralną konsolę i z jednego punktu umożliwia zarządzanie warstwą fizyczną, platformą wirtualizacji, warstwą sieciową czy nawet pojedynczą maszyną wirtualną. Czynności administracyjne nie wymagają wprowadzania zmian na pojedynczych elementach infrastruktury, co znacząco ułatwia i przyspiesza realizację zadań.

Architektura HCI w żaden sposób nie definiuje konkretnego obszaru zastosowania. Mając na uwadze elastyczność, skalowalność i wysoką wydajność, HCI jest wykorzystywane zarówno w środowiskach mieszanych, jak i bazodanowych, VDI, ROBO czy Hybrid-Cloud (VCF).

W ostatnim czasie zainteresowanie chmurą hybrydową znacząco wzrosło, gdyż takie podejście niweluje ograniczenia chmury publicznej, a jednocześnie pozwala na wykorzystanie jej zalet. Architektura HCI świetnie sprawdza się również w obsłudze środowisk VDI, czyli wirtualnych stacji roboczych. Platforma VDI - VMware Horizon to bardzo bezpieczne i efektywne rozwiązanie, które pozwala na wdrożenie i centralną administrację stacjami roboczymi.

Decydując się na infrastrukturę hiperkonwergentną, warto zwrócić uwagę na rozwiązanie Dell Technologies VxRail. Rozwiązanie VxRail bazuje na platformie VMware vSphere + VMware vSAN z bardzo funkcjonalnym i autorskim obszarem automatyzacji

Rozwiązanie VxRail jest efektem wieloletniej współpracy producenta sprzętu Dell Technologies oraz producenta oprogramowania VMware. Kolejną wartością dodaną rozwiązania VxRail jest pojedynczy punkt kontaktu serwisu producenta i wypracowane oraz sprawdzone procedury.

Bezpieczny dostęp do zasobów firmy

Tomasz Mrowiec

W czasach, gdy praca odbywała się wyłącznie w siedzibie firmy, dostęp do jej zasobów był dobrze chroniony. Przed zagrożeniami z zewnątrz broniły firewalle i inne zaawansowane zabezpieczenia. Potem biznes stał się bardziej mobilny i sytuacja zmieniła się diametralnie. Problem z bezpieczeństwem stał się jeszcze większy w ostatnich miesiącach, gdy pandemia COVID-19 wymusiła pracę zdalną. Obecnie do łączenia z firmą pracownicy wykorzystują domowe Wi-Fi lub sieć publiczną, które nie są dobrze zabezpieczone. W rezultacie cyberprzestępcom łatwo jest przechwycić dane przesyłane między komputerem pracownika i firmowym systemem. Pomyślmy o całej masie poufnych informacji, haseł, wiadomości e-mail itp., które codziennie krążą między urządzeniami pracowników a firmową infrastrukturą. Wszystko to może wpaść w czyjeś niepowołane ręce.

Zapobiec temu może umiejętnie wdrożona wirtualna sieć prywatna (VPN). To znane od lat rozwiązanie, które stworzono z myślą o pracownikach zdalnych i oddziałach firm, by zapewnić im bezpieczny dostęp do aplikacji i zasobów firmowych.

W nazwie rozwiązania zawiera się idea jego działania. VPN rozszerza prywatną sieć firmową na komputery łączące się z nią zdalnie poprzez sieć publiczną. Powstaje bezpieczny tunel chroniący przesyłane dane przy użyciu szyfrowania. W rezultacie dane stają się bezużyteczne dla napastnika mogącego przechwycić komunikację. Dzięki uzyskanemu w ten sposób bezpośredniemu połączeniu z firmą użytkownicy zdalnych urządzeń mogą korzystać z pełnej ochrony i funkcjonalności firmowej sieci prywatnej. Najprościej mówiąc, osoby pracujące z domu mogą mieć taki dostęp do zasobów firmy, jakby wpinały swoje komputery do gniazdka sieciowego w biurze.

Gdy obecnie tak wielu pracowników łączy się z firmą poprzez współdzielone i publiczne sieci, użycie wirtualnych sieci prywatnych stało się koniecznością. Jednakże VPN wciąż nie wystarczy do zapewnienia rzeczywiście bezpiecznego dostępu do zasobów firmy. Nie obroni przed sytuacją, gdy napastnik w jakiś sposób wejdzie w posiadanie

danych uwierzytelniających – loginu i hasła do konta użytkownika. Sposobów na ich zdobycie cyberprzestępcy mają wiele, wykorzystując na dużą skalę socjotechnikę. Przede wszystkim w formie phishingu, czyli bardzo umiejętnie przygotowanych fałszywych wiadomości e-mail. Wysyłając je masowo, starają się obecnie wykorzystywać poczucie zagrożenia związanego z pandemią i podszywać się pod organizacje rządowe, instytucje ochrony zdrowia albo dostawców sprzętu medycznego.

Dlatego niezbędne jest dodanie kolejnej warstwy ochrony, którą jest uwierzytelnianie wieloskładnikowe (MFA). Jako drugi składnik, uzupełniający login i hasło, najczęściej wybierany jest sprzętowy token, który wyświetla dodatkowy kod uwierzytelniający, albo rozwiązanie oparte na oprogramowaniu, którym może być aplikacja na smartfonie

MFA to skuteczne narzędzie zabezpieczające przed kradzieżą tożsamości użytkownika

Gdy zostanie wdrożone, by przeprowadzić udany atak, napastnik musi nie tylko uzyskać dane logowania użytkownika, ale także mieć fizyczny dostęp do urządzenia służącego do dodatkowego uwierzytelniania. A to już nie jest proste.

Czy tego chcemy, czy nie, przyszłością jest elastyczna praca, wykonywana w dużej mierze poza biurem. Aby dostęp pracowników do firmowych zasobów pozostał bezproblemowy i bezpieczny, powinniśmy zadbać o zabezpieczenia, takie jak opisane VPN i MFA, które – co ważne – powinny iść ze sobą w parze.

Efektywna zdalna praca zespołowa

Piotr Sebastiański

Związana z koronawirusem konieczność przejścia na pracę zdalną (a następnie hybrydową) zmusiła zarówno duże, jak i małe organizacje ze wszystkich branż do ponownego przemyślenia sposobu, w jaki ich pracownicy oraz zespoły komunikują się ze sobą i współpracują. Choć była to potrzeba chwili, to pandemia tylko przyśpieszyła pewne trendy.

Już wcześniej różne badania pokazywały, że wielu pracowników ponad wyższą pensję przedkłada bardziej elastyczne podejście do pracy i brak konieczności codziennego wykonywania jej w biurze, w godzinach od 9:00 do 17:00. Oczekiwali oni takich narzędzi, które umożliwią im pracę z domu czy w ogóle z dowolnego miejsca.

Także jeszcze przed pandemią sporo firm próbowało zerwać z tradycyjnymi, hierarchicznymi strukturami organizacyjnymi, tworząc przestrzeń dla bardziej elastycznych form współpracy. Priorytetem dla nich stawała się taka praca zespołowa, w której zespoły mogły być szybko tworzone na potrzeby konkretnych projektów i pojawiających się idei. Powód był oczywisty: dzięki elastycznym i zmiennym strukturom udawało im się lepiej wykorzystywać indywidualne kompetencje swoich pracowników.

Zarówno pragnienie bardziej elastycznej pracy, jak i potrzebę tworzenia najbardziej kreatywnych w danym momencie i okolicznościach zespołów można łatwo spełnić, gdy dysponuje się odpowiednim narzędziem. Takim, które będzie hubem dla całej komunikacji i współpracy, realizowanych w czasie rzeczywistym. Narzędziem, które umożliwia prowadzenie audio- i wideokon-

ferencji oraz pozwala na zarządzanie spotkaniami i wspólną pracę nad dokumentami. Co więcej, do którego będzie łatwy dostęp – zarówno przez aplikację, jak i przeglądarkę internetową na dowolnym urządzeniu.

Narzędziem, które spełnia powyższe kryteria jest Microsoft Teams. Zrywa ono z tradycyjnym sposobem współpracy, polegającym na częstym sięganiu po telefon, korzystaniu z poczty elektronicznej i wysyłaniu załączników z kolejnymi wersjami tego samego dokumentu (a potem czekaniu na odpowiedź) oraz na spotkaniach wyłącznie twarzą w twarz.

Zamiast tego Teams oferują szybkie i sprawne przełączanie się w jednym oknie pomiędzy wybranymi kanałami komunikacji, w tym wideokonferencjami i czatami, współpracę nad dokumentami w czasie rzeczywistym, współdzielenie plików i działania w mniejszych i większych grupach.

Teams mają intuicyjny interfejs i są proste w obsłudze, więc praca przy ich użyciu staje się wydajniejsza. Jednym lub dwoma kliknięciami można skonfigurować wiele kanałów komunikacji, konwersacje są prowadzone w wątkach, co ułatwia ich śledzenie, a nowe powiadomienia pojawiają się na ekranie. Także jedno kliknięcie wystarczy, by rozpocząć rozmowę głosową lub wideo.

Platforma nie jest prostym hubem różnych kanałów komunikacji. Ponieważ jest zintegrowana z Office 365, daje użytkownikom łatwy dostęp do aplikacji biurowych, takich jak Excel i Word, a także do plików w chmurze i rozwiązań synchronizujących informacje, takich jak SharePoint, Power BI czy Delve. Użytkownicy Teams mogą płynnie przełączać się pomiędzy czatem wideo, komunikatorem, pocztą e-mail i jednocześnie razem pracować nad dokumentami.

W dodatku Teams to nieustannie rozwijane rozwiązanie, które oferuje coraz więcej aplikacji, lepszą ich integrację i kolejne usprawnienia. Nie ogranicza się przy tym do programów Office 365, umożliwiając także korzystanie z aplikacji zewnętrznych dostawców. By wybrać potrzebne do pracy narzędzia, użytkownicy mogą skorzystać ze sklepu z aplikacjami Teams.

Zabezpieczenie urządzeń mobilnych poza firmą

Paweł Soból

Wyciek danych może w każdej organizacji doprowadzić do strat finansowych i utraty wiarygodności. Likwidowanie jego skutków może kosztować dużo pieniędzy, czasu i wysiłku. Co ciekawe, gdy mowa o kradzieży danych, najczęściej myśli się o hakerach wnikających do sieci i przełamujących zabezpieczenia systemów oraz aplikacji przy użyciu wyrafinowanych technik. Ponieważ o cyber-atakach mówi się coraz więcej, organizacje dobrze wiedzą, że trzeba zabezpieczyć przed nimi firmową infrastrukturę. Dokonać tego można: wdrażając firewalle, instalując oprogramowanie chroniące urządzenia końcowe przed złośliwym oprogramowaniem, ostrzegając pracowników przed phishingiem itp.

W rzeczywistości, wiele przypadków wycieku informacji, które skutkują poważnymi konsekwencjami, dotyczy źle zabezpieczonych urządzeń przenośnych, które są gubione lub kradzione. O ochronie laptopów przed wyciekiem danych przy użyciu szyfrowania dysków najczęściej się zapomina lub odsuwa się takie wdrożenie na później. Tymczasem powinna być to sprawa priorytetowa, będąca jednym z kluczowych narzędzi bezpieczeństwa składających się na zabezpieczenie naszych danych.

Według zleconego przez firmę Kensington badania, przeprowadzonego w 2018 r. wśród osób zarządzających IT, aż 61% ankietowanych firm odnotowało zgubienie lub kradzież laptopa albo tabletu, na których znajdowały się cenne informacje firmowe lub dane osobowe.

Można zakładać, że po dwóch latach, gdy w firmach przybyło urządzeń mobilnych, może być tylko gorzej. Tym bardziej że koronawirus zmusił zarówno biznes, jak i sektor publiczny do pracy poza biurem i już wiadomo, że tryb zdalny (mobilny) także po pandemii stanie się powszechny. Dlatego praktycznie w każdej organizacji prędzej czy później dojdzie do tego rodzaju incydentu.

Idealnym przykładem będzie zdarzenie, o którym można było usłyszeć w serwisach informacyjnych. Pod koniec ubiegłego roku na warszawskiej SGGW zaginął laptop, na którym przechowywano szczegółowe dane wszystkich kandydatów na studentów, w tym ich numery PESEL, serie i numery dowodów osobistych oraz adresy. Studenci zarzucili uczelni brak rozwiązań zgodnych z RODO i jeśli w wyniku pozwu dojdzie do odszkodowań, uczelnia będzie musiała znaleźć na nie wiele milionów złotych.

Cała sytuacja byłaby mniej poważna, gdyby laptop posiadał zabezpieczenie niepozwalające niepowołanej osobie na dostęp do zapisanych w nim

danych. Skuteczną ochronę zapewnia szyfrowanie dysku i takie narzędzie jak Bitlocker. Łatwo dostępne, bo dostarczane wraz z systemem Windows.

Oczywiście stopień skomplikowania wdrożenia tego rozwiązania będzie zależał od jego skali. W przypadku małej firmy i kilku komputerów można ręcznie uruchomić narzędzie na każdej maszynie wymagającej zabezpieczenia. W organizacjach, w których urządzeń mobilnych z dyskami do zaszyfrowania może być 100 albo więcej, konieczne będzie systemowe podejście, uwzględniające kontrolę działania tej warstwy ochrony, zarządzanie nią, zapewnienie możliwości odzyskiwania danych w razie awarii systemu. Dobrą praktyką przy wdrożeniu będzie wykorzystanie komputerów przenośnych wyposażonych w sprzętowy moduł szyfrujący TPM. Dzięki temu szyfrowanie stanie się transparentne dla ich użytkowników.

Wdrożenia Bitlockera, zwłaszcza na większą skalę, muszą zostać szczegółowo zaplanowane. Pozwoli to uniknąć błędów mogących doprowadzić nawet do paraliżu działalności organizacji. Przecież skutki nieumiejętnego użycia szyfrowania dysków mogą być podobne do ataku ransomware! Dlatego warto skorzystać ze wsparcia doświadczonego partnera, który pomoże wdrożyć narzędzie ochrony w taki sposób, by zapewniało ono najwyższy możliwy poziom bezpieczeństwa bez zbędnego ryzyka.

Centralne zarządzenie urządzeniami w centrum danych

Marcin Baldy

Coraz więcej urządzeń wokoło działa automatycznie. Czy nie jest więc zaskakujące, że w tym samym czasie, gdy na drogach testuje się autonomiczne pojazdy, olbrzymią część zarządzania serwerami, ich konfigurowania, wdrażania i utrzymania przeprowadza się wciąż manualnie, marnując na to długie godziny pracy? Przecież ręcznie wykonywane procesy angażują cenne zasoby ludzkie i skutkują błędami, których wynikiem są awarie i przestoje.

To poważny problem, ponieważ różne badania wykazują, że aż 70-75% przestojów w centrum danych jest wynikiem ludzkiego błędu. Jego przyczyną wcale nie musi być brak umiejętności, ponieważ nawet doświadczony administrator może być przemęczony lub działać w pośpiechu. Sytuacji na pewno nie poprawia fakt, że zespoły IT są coraz bardziej obciążone pracą i ograniczone budżetami. Dlatego administratorzy potrzebują inteligentnego wsparcia w postaci narzędzia,

które zwiększy ich wydajność, ograniczając pracę do wykonania. Zaoszczędzi ich czas i energię na realizację tych zadań w ramach zarządzania złożoną infrastrukturą IT, które są ważniejsze od prostych, uciążliwych i powtarzalnych czynności. Dobrze będzie, jeśli to narzędzie – zapewniając centralne zarządzania serwerami – dodatkowo umożliwi kontrolowanie innych elementów infrastruktury. Wręcz idealnie, jeśli – z uwagi na wspomniane ograniczenia budżetowe – będzie jeszcze dostarczane wraz z serwerami za darmo.

Właśnie takim narzędziem, które jest łatwe w użyciu, integruje zarządzanie i monitorowanie różnych systemów oraz automatyzuje procesy administracyjne jest OpenManage Enterprise (OME) firmy Dell Technologies.

Dzięki OpenManage Enterprise administrator nie musi sięgać po wiele różnych narzędzi do zarządzania. Zamiast tego może wdrożyć jedną konsolę w formie urządzenia wirtualnego w środowiskach VMware, Microsoft Hyper-V czy KVM. OME ma nowoczesny (oparty na HTML5) interfejs użytkownika, a użyty w konsoli mechanizm wyszukiwania sprawia, że jej obsługa staje się intuicyjna. Dlatego nie potrzeba długich szkoleń, by zacząć używać OME.

Jako jedna konsola do zarządzania wieloma systemami OpenManage Enterprise obsługuje blisko 8000 różnego rodzaju urządzeń, w tym serwery rackowe, towerowe i modularne serii PowerEdge, a także rozwiązania pamięci masowej PowerVault MD3 i ME4 oraz Storage Center. Co ważne, monitoruje ono również urządzenia dostawców innych niż Dell Technologies i generuje dla nich alerty. Oczywiście, OME umożliwia także zdalne zarządzanie.

Chroniąc infrastrukturę, OpenManage Enterprise umożliwia utrzymywanie zgodności z ustalonymi standardami konfiguracji, stworzonymi wcześniej przy użyciu szablonów. Oprogramowanie może wykryć odchylenia od uprzednio zdefiniowanych ustawień, ostrzec administratora i pomóc mu skorygować błędy.

OME automatyzuje działania związane z zarządzaniem cyklem życia urządzenia. Od jego wykrycia w sieci aż po wyłączenie z użytku jest ono zarządzane z jednej konsoli. Bardzo niewiele czasu zabiera automatyczne wdrożenie urządzenia w oparciu o jego znacznik serwisowy albo identyfikator. Zapewniając centralne zarządzanie i wprowadzając automatyzację, narzędzie znacząco zmniejsza koszty administrowania, oszczędza czas oraz ogranicza ryzyko ludzkich błędów i strat wynikających z nieplanowanych przestojów.

Backup środowisk produkcyjnych *Jacek Tomczak*

Mówi się, że ludzie dzielą się na takich, którzy już robią backup, będą go robić (bo przekonają się na własnej skórze, co oznacza jego brak) oraz tych, którzy myślą, że robią kopię zapasową swoich danych (a w rzeczywistości, z powodu jakiegoś błędu, backup się nie wykonuje).

Zabezpieczanie danych przed ich utratą – niezależnie od jej przyczyny, którą może być zaszyfrowanie dysku, awaria macierzy czy serwera albo po prostu nieumyślne skasowanie pliku – to dziś oczywistość. Musimy jednak zdawać sobie sprawę z wyzwań, jakie niesie stworzenie prawidłowo działającego rozwiązania do backupu i nie popełniać błędów.

Jednym z podstawowych błędów jest brak odpowiedniej polityki tworzenia kopii zapasowych. Rezultatem jest trudny do opanowania chaos, objawiający się np. tym, że dane z urządzeń końcowych są zabezpieczane jednym systemem backupu, a dane z serwerów innym. Często kopie zapasowe są porozrzucane na różnych urządzeniach. Zdarza się nawet, że backup jest składowany na tych samych zasobach, z których korzysta środowisko produkcyjne (które przecież ma być chronione).

> **Dobrze wykonany backup pozwoli odtworzyć dane w razie awarii lub potrzeby cofnięcia się do konkretnego momentu z przeszłości.**

Takie odtworzenie może dotyczyć zarówno pojedynczego pliku, jak i całego serwera, który trzeba szybko uruchomić. Ważnym zadaniem systemów backupowych jest również archiwizacja danych – tych, które powinny być przechowywane przez dłuższy czas, ale do których niekoniecznie musimy mieć natychmiastowy dostęp.

> **W zapanowaniu nad wspomnianym chaosem i uniknięciu błędów pomoże nam odpowiednie rozwiązanie do backupu. Takie, jak DPS (Data Protection Suite) firmy Dell Technologies, dzięki któremu jesteśmy w stanie zabezpieczać dane znajdujące się na urządzeniach końcowych, serwerach i macierzach**

DPS to zestaw programowych narzędzi zapewniających ciągłą ochronę danych na potrzeby odzyskiwania operacyjnego i przywracania po awarii. I tak aplikacja PowerProtect Data Manager zapewnia zarządzanie

danymi i backupami z jednego miejsca. Z kolei Avamar to narzędzie zoptymalizowane pod kątem codziennych pełnych kopii zapasowych środowisk fizycznych i wirtualnych, serwerów NAS, aplikacji korporacyjnych, zdalnych biur i komputerów stacjonarnych oraz mobilnych. Dell EMC Recovery Point umożliwia natomiast szybkie przywracanie maszyn wirtualnych VMware do dowolnego punktu w czasie.

Oczywiście oprócz oprogramowania do wykonania kopii zapasowej potrzebny jest również sprzęt, na którym uruchomiony zostanie system do backupu, oraz medium umożliwiające zapisywanie, oraz składowanie chronionych danych. Choć na rynku dostępnych jest wiele rozwiązań, to naturalnym wyborem dla DPS będzie hardware Dell Technologies, zoptymalizowany pod kątem tego oprogramowania i oparty na najnowszych technologiach. Wśród mediów do backupu warto zwrócić uwagę na PowerProtect DD (DataDomain), które – dzięki globalnej deduplikacji danych – skróci nam czas wykonywania kopii, zmniejszy obciążenie sieci oraz zaoszczędzi miejsce na dane.

Bardzo wygodnym rozwiązaniem może okazać się IDPA (Integrated Data Protection Appliance), czyli urządzenie typu „wszystko w jednym”.

Zapewnia ono zarówno fizyczną warstwę serwerową z medium do przechowywania danych, jak i cały pakiet oprogramowania Data Protection Suite. Wygoda zastosowania IDPA polega m.in. na uwolnieniu użytkownika od uciążliwego rozwiązania, jakim są taśmy – poprzez umożliwienie składowania backupów LTR (Long Term Retention) w chmurze.

Środowisko chmury hybrydowej jako przyszłość nowoczesnego IT

Jakub Kłoda

Popularyzacja środowisk chmurowych stawia przed nami nowe wyzwanie – co będzie odpowiednim wyborem dla naszego środowiska. Wybór nie jest prosty i oczywisty, ponieważ do dyspozycji mamy chmurę publiczną, chmurę prywatną, chmurę hybrydową i oczywiście infrastrukturę lokalną tzw. on-premises. Infrastruktura lokalna wciąż zapewnia wyższy poziom kontroli, bezpieczeństwa czy personalizacji rozwiązania. Chmura publiczna ma istotne zalety w zakresie skalowalności, dostępu do najnowszych technologii, a także nie wymaga zakupu i utrzymania infrastruktury.

Pamiętajmy, że mamy możliwość wyboru i nie ma wymogu wykorzystywania pojedynczej technologii czy rozwiązania. Warto również rozważyć opcję chmury hybrydowej. Pozwala ona na wykorzystanie zalet infrastruktury lokalnej lub chmury prywatnej z zaletami chmury publicznej, minimalizując tym samym wady obu rozwiązań. Takie rozwiązanie daje możliwość zaadresowania wymagań i potrzeb bez ustępstw, z którymi musimy się liczyć, decydując się np. na chmurę publiczną.

Jedną z korzyści wynikających z wdrożenia chmury hybrydowej są oszczędności.

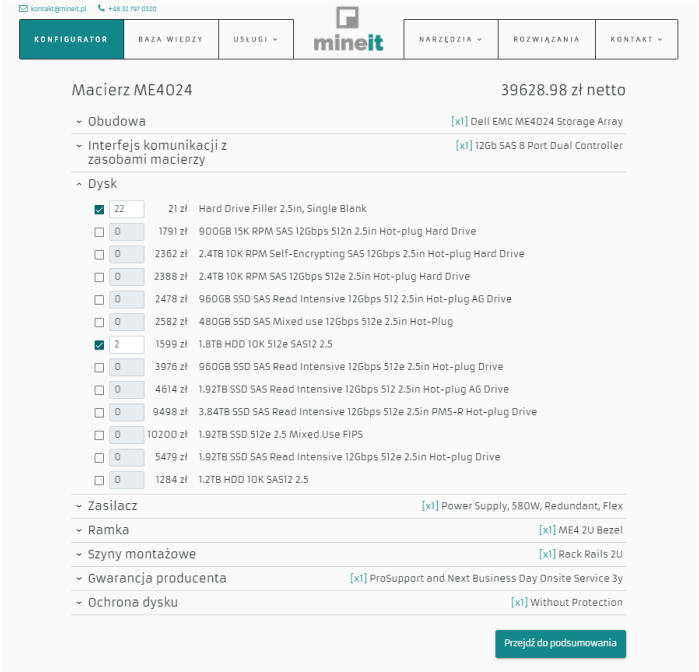
Obsługa wzmożonego i okresowego zapotrzebowania na moc obliczeniową oraz pamięć masową, nie wymusza na nas inwestycji w rozbudowę obecnej infrastruktury i przeskalowania środowiska na pozostałe 90% czasu.

Możemy ten problem rozwiązać poprzez parametryzację naszego środowiska w chmurze publicznej w określonym czasie, a koszt obsługi tego zapotrzebowania rozliczyć zgodnie z użyciem. Działając w ten sposób, dodatkowo zmniejszamy ryzyko niedostępności usług spowodowanych przeciążeniem systemów. Chmura publiczna doskonale sprawdza się także w przypadku tworzenia i testowania nowych aplikacji (DEV/TEST). Zasoby obiektowe chmury publicznej mogą być również wykorzystywane jako cel replikacji kopii zapasowych w celu realizacji zasady 3-2-1. Dodatkowo chmura publiczna znacznie ułatwia realizację inicjatyw BCP (Business Continuity Plan) i DRP (Disaster Recovery Plan).

Nie jest jednak tak, że koegzystencja chmury publicznej i prywatnej jest zupełnie bezproblemowa. Wdrożenie chmury hybrydowej wymaga kompetencji i doświadczenia, aby integracja obu środowisk była zrealizowana w sposób właściwy i zgodny z najlepszymi praktykami. Niewłaściwa integracja z wykorzystaniem niewłaściwych rozwiązań może skutecznie ograniczyć zalety obu rozwiązań i utrudnić administrację środowiska. Niezależnie od wybranej opcji, każdy projekt wymaga rzetelnej analizy obecnego środowiska i zaproponowania dedykowanego rozwiązania.

Chmura hybrydowa, oprócz niewątpliwych korzyści, przynosi także wyzwania. Stworzenie złożonego środowiska wymaga bardzo dobrego projektu, znajomości wielu rozwiązań, kompetencji i doświadczenia.

Pozostaje tylko wybrać, w czym pomoże konfigurator mineIT *Piotr Gigoń*



Kolejne strony tego e-booka pokazały, jakie korzyści może dać nam nowoczesna infrastruktura IT. Trzeba tylko wybrać takie rozwiązanie, które będzie najlepiej odpowiadało na nasze potrzeby. Kłopot w tym, że to wcale nie musi być łatwe. Przecież musimy się dobrze zastanowić, czy ważniejsze są w tym momencie oszczędności (godząc się na skromniejszą konfigurację), czy może powinniśmy wybrać produkt, który będzie bardziej perspektywiczny. Większość z nas, planując ważny zakup, poświęca sporo czasu na znalezienie optymalnego wariantu. Bez wątpienia największą przeszkodą jest wtedy brak dostępu do informacji. Nie możemy przecież wybierać, nie mając pewności co do cech, funkcji, możliwości czy wreszcie ceny produktu.

Na szczęście dostępne są narzędzia, które mogą żmudny i czasochłonny proces dochodzenia do właściwej decyzji usprawnić tak, by stał się szybki i wygodny.

Dostępny na stronie **mineit.pl** konfigurator pozwala w banalnie prosty sposób wybrać, a następnie skonfigurować dowolny serwer, macierz lub przełącznik sieciowy z oferty Dell Technologies. Tym, co czyni konfigurator mineIT narzędziem nie tylko potężnym, ale także przystępnym i łatwym w obsłudze, jest ukrywająca się za intuicyjnym interfejsem logika.

Wystarczy wybrać interesującą nas kategorię – np. „Serwery Dell EMC PowerEdge" – następnie podkategorię, w której decydujemy, czy interesują nas serwery rackowe, czy w obudowach typu tower, wreszcie w trzecim kroku, zdecydować się na konkretny produkt. Na jego stronie znajdziemy wyczerpującą listę wszystkich komponentów, poczynając od obudowy, poprzez procesor, pamięć RAM, moduły SD, kontrolery RAID, dyski, karty sieciowe i wiele innych, aż do zasilacza. Uzupełniają ją takie elementy jak system operacyjny, licencje CAL, licencje na dodatkowe oprogramowanie czy gwarancja. Absolutnie każdy punkt tej listy możemy zmieniać, dopasowując ostateczną konfigurację do swoich potrzeb.

Żeby uwolnić klienta od konieczności uważnego sprawdzania specyfikacji każdego komponentu i żmudnego dobierania opcji w taki sposób, żeby nie doprowadzić do żadnych konfliktów, konfigurator nie pozwala zestawiać niepasujących elementów. Umożliwia więc nie tylko sprawdzenie, ile kosztowałaby konfiguracja serwera, o jakiej myślimy, ale też, czy jest ona w ogóle możliwa. Dzięki temu możemy skupić się na doborze optymalnego do naszych potrzeb zestawu, który zmieści się w założonym budżecie. Co więcej, ceny podane w mineIT nie są cenami docelowymi. Choć zawierają one już wstępny rabat, to wciąż podlegają możliwym negocjacjom, dzięki czemu ostatecznie są niższe niż ceny katalogowe.

Ktoś mógłby jednak zapytać – po co taki konfigurator, jeśli do każdego dystrybutora można po prostu zadzwonić albo napisać mail z pytaniem

o dostępność i cenę potrzebnej nam konfiguracji? Odpowiedzią są: **czas, wygoda i elastyczność.**

Po pierwsze, wysłane mailem pytanie o cenę określonego serwera nawet przy najsprawniejszej obsłudze ma szansę doczekać się konkretnej odpowiedzi nie prędzej, niż w ciągu kilku godzin, a jeśli przypadkiem zaczyna się właśnie weekend, to na informacje poczekamy nawet i kilka dni.

Po drugie, jeśli chcielibyśmy sprawdzić ceny i dostępność kilku różnych wariantów sprzętu, trzeba je zawczasu przemyśleć i opisać, a czas, jakiego dostawca będzie potrzebować na przygotowanie rzetelnej odpowiedzi, wzrośnie kilkukrotnie.

Po trzecie wreszcie, tradycyjne podejście pozbawia nas swobody – przestrzeni na olśnienia i zmianę decyzji. W konfiguratorze mineIT możemy błyskawicznie sprawdzić wiele opcji i wariantów, także tych, których nie bralibyśmy pod uwagę. Może się okazać, że któraś z konfiguracji będzie lepsza, niż nam się wydawało, i tańsza, niż się spodziewaliśmy.

Pozostaje już tylko sprawdzić **mineIT** w praktyce i stworzyć własną konfigurację.

Autorzy:

- Backup środowisk produkcyjnych – **Jacek Tomczak**
- Bezpieczny dostęp do zasobów firmy – **Tomasz Mrowiec**
- Hiperkonwergencja jako odpowiedź na wymóg obecnej elastyczności – **Jakub Kłoda**
- Środowisko chmury hybrydowej jako przyszłość nowoczesnego IT – **Jakub Kłoda**
- Efektywna zdalna praca zespołowa ¬– **Piotr Sebastiański**
- Zabezpieczenie urządzeń mobilnych poza firmą – **Paweł Soból**
- Centralne zarządzenie urządzeniami – **Marcin Baldy**
- Pozostaje tylko wybrać, w czym pomoże konfigurator mineIT – **Piotr Gigoń**

Jacek Tomczak
Wiceprezes Zarządu
jacek.tomczak@itpunkt.pl

Tomasz Mrowiec
Wiceprezes Zarządu
tomasz.mrowiec@itpunkt.pl

Piotr Sebastiański
Inżynier IT
piotr.sebastianski@itpunkt.pl

Paweł Soból
Inżynier IT
pawel.sobol@itpunkt.pl

Marcin Baldy
Inżynier IT
marcin.baldy@itpunkt.pl

Jakub Kłoda
Inżynier IT
jakub.kloda@itpunkt.pl

Piotr Gigoń
Dyrektor Sprzedaży
piotr.gigon@itpunkt.pl

IT Punkt
systemy informatyczne

ITPunkt Sp z o.o. Centrala
ul. Wandy 18A
40-322 Katowice
tel.: +48 32 797 0320
fax: +48 32 797 0319
e-mail: handel@itpunkt.pl