Droga do kompleksowego monitoringu środowiska IT

Zbudowanie odpowiedniego zestawu narzędzi dla działu IT jest kluczem do wydajnego monitorowania i zarządzania infrastrukturą informatyczną. Pozwala też maksymalnie wykorzystać potencjał zespołu IT.

Monitorowanie środowiska informatycznego może wydawać się wąską dziedziną, którą można obsłużyć jednym z wielu dostępnych na rynku rozwiązań. W czasach gdy IT jest nieodłączną częścią biznesu, jest to jednak rozumowanie błędne. Tylko odpowiednio dobrany zestaw narzędzi z obszaru monitorowania: infrastruktury, sieci, logów i aplikacji uprawnia do stwierdzenia, że nasze środowisko jest w pełni monitorowane, a co za tym idzie skutecznie zabezpieczone. Posłużmy się doświadczeniami jednej z dużych organizacji biznesowych. Jej problemy są dziś bowiem dość typowe dla wielu polskich przedsiębiorstw.

POWSZECHNE PROBLEMY W PRAKTYCE

W firmie X zespół kilkunastu specjalistów IT zarządza rozproszoną po wielu oddziałach infrastrukturą informatyczną zapewniającą usługi dla ponad tysiąca pracowników. Szybki rozwój działalności, a co za tym idzie przyrost różnego typu nowych usług i systemów informatycznych sprawiły, że dotychczas używane rozwiązania wspierające kontrolowanie sposobu działania środowiska IT przestały wystarczać. Przełożyło się to na problemy biznesowe – pojawiające się w coraz większej ilości zgłoszenia przestały być obsługiwane w sposób wydajny. Co ważniejsze, ze względu na szeroką integrację systemów biznesowych, zespół IT miał poważne trudności z poprawną identyfikacją źródeł problemów.

Szczególnie istotnym często powtarzającym się incydentem było zgłoszenie dotyczące braku wyświetlania formularza oferty w kluczowym systemie. Producent systemu nie doszukał się błędu w aplikacji, a administratorzy – wykorzystując wszelkie dostępne środki – nie byli w stanie wskazać źródła problemu w infrastrukturze. W tej sytuacji niezbędne było rozwiązanie, które pozwoli szerzej spojrzeć na infrastrukturę IT,

a skalą będzie odpowiadało posiadanym aplikacjom biznesowym.

MONITORING INFRASTRUKTURY

Odpowiedzią na potrzebę sprawnego monitorowania warstwy sieci okazało się wykorzystanie rozwiązania op5 Monitor. Oprogramowanie to wywodzi się z rozwijanego na zasadach open source systemu Nagios. Jedną z kwestii, które zadecydowały o wyborze tego właśnie narzędzia, była wysoka elastyczność i otwartość na infrastrukturę zróżnicowaną pod kątem sprzętu, producentów oraz wieku. Było to bardzo cenne, ponieważ nowe rozwiązanie pełnić miało rolę nadzorcy nad całością firmowej infrastruktury IT, a zarazem rozwiązania gromadzącego i centralizującego maksymalną ilość danych przydatnych dla osób zarządzających środowiskiem.

Wdrożenie jednolitego systemu monitorowania infrastruktury uświadomiło menedżerom, jak rozbudowanym środowiskiem IT dysponuje firma oraz jak bardzo jest ono istotne dla prawidłowo realizowanych, kluczowych procesów biznesowych. Zastosowanie jednego narzędzia wspierającego monitorowanie sieci pozwoliło też na usprawnienie współpracy rozproszonych zespołów administratorów. Okazało się, że osoby, które do tej pory nie komunikowały się ze sobą, rozwiązywały te same problemy i mają bardzo dużą wiedzę, którą chcą się dzielić. Centralny monitoring wpłynął doskonale na przepływ wiedzy i atmosferę pracy. Jednocześnie, pomimo całościowego spojrzenia na infrastrukturę, nie udało się rozwiązać problemu z krytyczną aplikacją. Chęć wyeliminowania tego problemu wymagała zastosowania narzędzia pozwalającego analizować ruch sieciowy.

MONITORING RUCHU SIECIOWEGO

Wobec faktu, że część infrastruktury nie obsługiwała standardu Netflow, zdecydowano o wykorzystaniu narzędzia, które będzie w stanie analizować ruch na podstawie pasywnych sond działających na kopii ruchu przechodzącego przez poszczególne przełączniki sieciowe. Po serii testów POC wybrano rozwiązanie Flowmon. Ze względu na unikalne potrzeby firmy X, zaletą tego oprogramowania okazał się moduł pozwalający na podejście do problemu monitorowania sieci z perspektywy analizy bezpieczeństwa i anomalii transmisji. Problemy często identyfikowane jako „wolno działająca" aplikacja nierzadko wywodzą się z naruszeń bezpieczeństwa sieci, które nie zostały zidentyfikowane przez firewall, a o których – wskutek braku odpowiednich narzędzi – administratorzy mogą się nigdy nie dowiedzieć. System zapewnił możliwość śledzenia i reagowania na automatycznie posegregowane problemy bez potrzeby ręcznego analizowania ruchu sieciowego, co okazało się cenne przy dość ograniczonych zasobach kadrowych.

Analiza ruchu sieciowego dostarczyła firmie X informacji o aktywnych incydentach zachodzących w sieci: atakach SSH, masowym skanowaniu portów, ruchu P2P oraz TOR, a także związanych z nimi opóźnieniach w działaniu sieci. Zidentyfikowane incydenty były realnym zagrożeniem nie tylko dla infrastruktury, ale groziły też wyciekiem danych wrażliwych – co mogło prowadzić do poważnych konsekwencji prawnych.

Dużo dokładniejsze spojrzenie na środowisko informatyczne, z perspektywy działu IT, przysporzyło wielu nowych dotychczas niezidentyfikowanych problemów, które mogły powodować istotne ryzyko dla bezpiecznego funkcjonowania przedsiębiorstwa. Otworzenie tej swoistej „Puszki Pandory" sprawiło, że zarząd spółki zaczął zupełnie inaczej postrzegać rolę zespołu IT, jaką realizujemy w organizacji. To z kolei ułatwiło pozyskanie finansowania na zakup wydajnego narzędzia do przetwarzania logów systemowych i zabezpieczenia infrastruktury.

ZARZĄDZANIE DANYMI I ZDARZENIAMI BEZPIECZEŃSTWA

Celem takiej inwestycji miało być wdrożenie rozwiązania, które będzie centralnym serwerem logów, ale zapewni również dodatkowe funkcje analityczne z naciskiem położonym na obszar bezpieczeństwa. Oprócz funkcjonalności standardowo przypisywanych rozwiązaniom klasy SIEM, poszukiwane narzędzie miało zapewniać możliwość szybkiego i ergonomicznego wyszukiwania analitycznego na bazie oceny korelacji. Ważna była również możliwość integracji rozwiązania z już istniejącymi systemami do monitorowania IT.

Rozwiązaniem spełniającym postawione wymagania okazał się system LogRhythm. Jego atutem było m.in. wykorzystanie narzędzia wyszukiwania opartego na projekcie Elasticsearch, co pozwoliło na uzyskanie precyzyjnych informacji o powiązaniach zjawisk w stosunkowo krótkim czasie. Oprogramowanie znalazło też zastosowanie w roli narzędzia, ułatwiającego działania administracyjne i operacje biznesowe.

NIE TYLKO INFRASTRUKTURA

Implementacja trzech różnych, odmiennych rozwiązań wspierających monitorowanie istotnych aspektów funkcjonowania środowiska IT nie przyniosła jednak odpowiedzi na pytanie o dostępność formularza w głównym systemie biznesowym. Wdrażane kolejno rozwiązania nie zapewniały

Przykładowe efekty kompleksowej integracji rozwiązań monitoringu IT:

- Wzrost znaczenia IT w organizacji
- Szybsza identyfikacja problemów i zagrożeń
- Zwiększenie wydajności całego środowiska i optymalne wykorzystanie dostępnych zasobów
- Automatyzacja procesów i oszczędność czasu administratorów
- Lepsza i bardziej skoordynowana praca działu IT
- Rozwój kompetencji administratorów przy użyciu ulubionego narzędzia
- Większa satysfakcja użytkowników końcowych

Zastosowanie jednego narzędzia wspierającego monitorowanie sieci pozwoliło też na usprawnienie współpracy rozproszonych zespołów administratorów. Okazało się, że osoby, które do tej pory nie komunikowały się ze sobą, rozwiązywały te same problemy i mają bardzo dużą wiedzę, którą chcą się dzielić.

Zastosowanie parasola składającego się z rozwiązań o różnym profilu monitorowania środowiska doskonale wpisuje się w potrzebę zapewniania wydajnej i bezpiecznej zarazem platformy roboczej dla biznesu, a jednocześnie **pozwala osiągnąć efekt w postaci w pełni przejrzystego środowiska IT, w którym każdy incydent będzie natychmiast wychwycony i zneutralizowany.**

bowiem wglądu w funkcjonowanie aplikacji oraz reakcje jej użytkowników.

Niezidentyfikowane problemy leżące na pograniczu kompetencji poszczególnych działów oznaczały potrzebę wykorzystania narzędzia pozwalającego „zajrzeć" do aplikacji biznesowych. Jednak zróżnicowanie technologii, w jakich zostały wykonane używane w organizacji aplikacje biznesowe, wymagało zastosowania narzędzia o dużym stopniu uniwersalności. Rozwiązanie typu APM (Application Performance Management) miało przy tym wspierać przede wszystkim kluczowe oprogramowanie sprzedażowe – i wszystkie zintegrowane z nim aplikacje.

Jeśli zaś chodzi o funkcjonalności, to chęć rozwiązania wspomnianego na początku problemu wymagała m.in. wysokopoziomowego zarządzania wydajnością aplikacji, a także analizy funkcjonowania jej pod kątem luk w bezpieczeństwie oraz jakości kodu, aby zminimalizować możliwość pojawienia się niemożliwych do zidentyfikowania w przyszłości błędów. Rozwiązanie miało reagować na każdy przestój w działaniu aplikacji, wskazując na źródło problemu, niezależnie czy dotyczy ono warstwy systemu operacyjnego, bazy danych, czy też serwera. Dodatkowym wymaganiem była również możliwość analizy doświadczeń oraz zadowolenia użytkowników. Potrzebom tym odpowiadało rozwiązanie firmy Dynatrace.

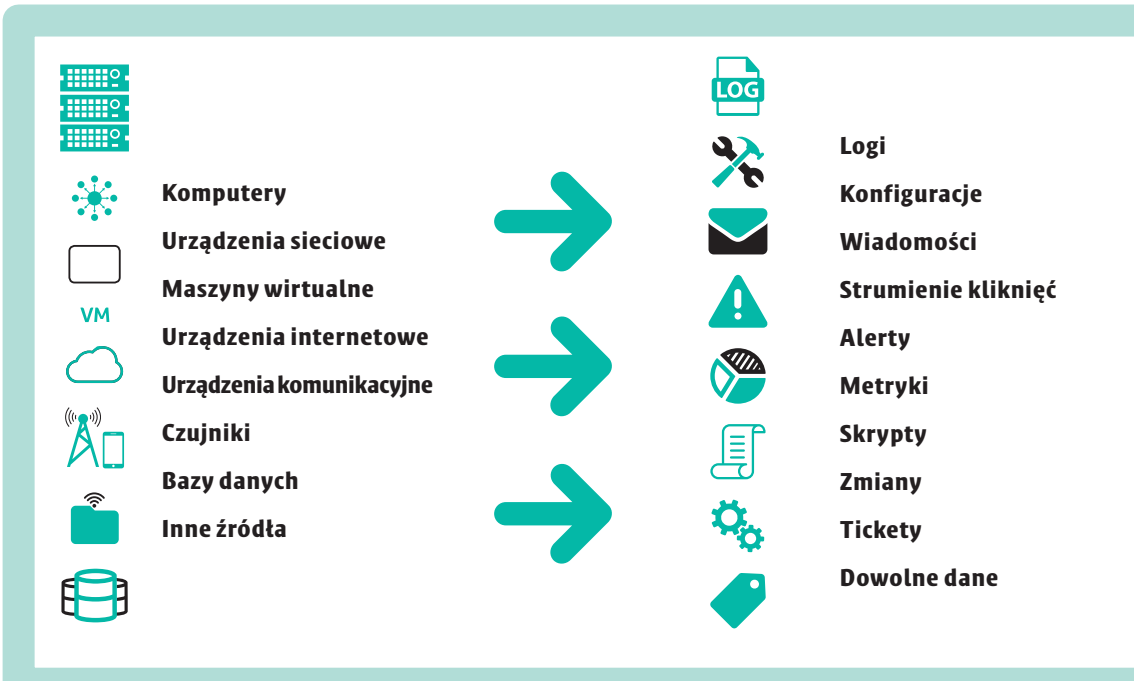
APLIKACJE POD LUPĄ

Oprogramowanie wspierające analizę wydajności aplikacji, po zainstalowaniu lekkich agentów zbierających informacje o stanie serwerów aplikacyjnych, pozwoliło – już po kilku godzinach – zlokalizować źródło problemu. Zastosowanie rozwiązania Dynatrace umożliwiło funkcjonalne rozbicie poszczególnych aplikacji na pojedyncze transakcje, zidentyfikowanie realizujących je fragmentów kodu oprogramowania, a także przypisanie precyzyjnie zmierzonych czasów wykonania każdej iteracji. Dużo łatwiejsze stało się też wychwycenie elementów pośredniczących w działaniu aplikacji – połączeń z bazą danych, czy odwołań do systemów zewnętrznych, które ostatecznie były odpowiedzialne za dotychczas nierozwiązywalny problem. Okazało się, że za tym zamieszaniem stał stosunkowo nieduży, zintegrowany z główną aplikacją sprzedażową system odpowiedzialny za przygotowywanie wycen pod oferty.

Firma X zyskała również szczegółowe informacje o tym, jak wykorzystywana jest farma serwerów, na których działa aplikacja, które serwery są najbardziej obciążone oraz jak rozkłada się poziom satysfakcji użytkowników z poszczególnych oddziałów terenowych. Doświadczenia firmy X pokazały też, że wykorzystanie rozwiązania klasy APM wpłynęło na zwiększenie efektywności działania IT oraz poprawę wskaźników biznesowych. Przyczyniła się do tego m.in. funkcjonalność eksportu danych – wraz z funkcją ich anonimizacji – do celów dalszej analizy. Dzięki temu dostawcy oprogramowania dla firmy X otrzymali zestaw narzędzi i dane pozwalające na analizę problemów z oferowanymi przez nich aplikacjami.

WYMIERNE EFEKTY TAKŻE DLA BIZNESU

Wdrożone w firmie X rozwiązania do monitorowania środowiska IT przyczyniły się do wielu pozytywnych zmian w organizacji pracy działu IT oraz całej firmy. Umożliwiły m.in. skrócenie czasu identyfikacji problemów oraz zagrożeń w obszarze IT, zautomatyzowanie procesów administracyjnych i lepszą koordynację prac. Wpłynęły też na zwiększenie wydajności środowiska oraz optymalizację wykorzystania dostępnych zasobów, a jednocześnie – przyczyniły się do wzmocnienia efektywnej roli IT w organizacji oraz podniesienia poziomu satysfakcji użytkowników biznesowych.



Chociaż firma X istnieje tylko w teorii, to problem z dostępnością formularza w aplikacji sprzedażowej oraz jego źródło w postaci elementu zewnętrznego rozwiązania – jest typowy dla wielu przedsiębiorstw. Wdrożenie poszczególnych rozwiązań monitoringu IT jest naturalną konsekwencją szybkiego rozwoju organizacji oraz potrzeby zapewniania wydajnej i bezpiecznej zarazem platformy roboczej dla biznesu.

Zastosowanie parasola składającego się z rozwiązań o różnym profilu monitorowania środowiska doskonale wpisuje się w taką potrzebę i pozwala osiągnąć efekt w postaci w pełni przejrzystego środowiska IT, w którym każdy incydent będzie natychmiast wychwycony i zneutralizowany. Dodatkowym, bardzo pozytywnym efektem wdrożenia kompleksowych rozwiązań wspierających monitorowanie funkcjonowania środowisk IT jest rozwój kompetencji. Narzędzia te znacząco ułatwiają pracę wielu pracownikom działu IT, wręcz budzą ich entuzjazm i zachęcają do poznawania zależności pomiędzy konkretnymi elementami środowiska oraz rozwoju kompetencji w całym obszarze IT.

Warto jednak podkreślić, że każda organizacja na swojej drodze do kompleksowego monitorowania środowisk IT będzie kłaść nacisk na różne elementy funkcjonalne. Ważne jest, aby już na etapie planowania tego rodzaju inwestycji skorzystać z pomocy partnera, który pomoże zrozumieć ideę monitorowania, zdefiniować potrzeby i obrać najbardziej efektywną drogę do ich realizacji.

Artur Bicki,
dyrektor wydziału wdrożeń technologii IT w firmie EM&CA
Łukasz Nieborek,
Key Account Manager w firmie EM&CA

Przykładowe rozwiązania tworzące kompletne środowisko monitoringu oraz ich efekty:

op5 Monitor

Pozwala na przeprowadzenie kompleksowej inwentaryzacji środowiska wysokodostępnego, włączając w to wszystkie oddziały terenowe. Wszystkie systemy IT, bez względu na architekturę, mogą zostać objęte dedykowanymi pomiarami, dzięki czemu w przypadku przestoju lub groźby jego wystąpienia administrator ma w ciągu kilku minut wiedzę, gdzie leży potencjalne źródło problemu. Raportowanie stanu infrastruktury oraz kontrola SLA pozwalają szybko uzyskiwać komplet informacji zarządczej.

Flowmon

Ułatwia zdobycie informacji na temat sposobu rzeczywistego wykorzystywania sieci oraz łączy szerokopasmowych, a także – sposobu realizacji połączeń pomiędzy poszczególnymi komponentami infrastruktury. Analiza funkcjonowania sieci pozwala na uzyskanie uporządkowanych informacji na temat potencjalnych zagrożeń i niestandardowych zachowań sieci.

LogRhythm

Zapewnia możliwość szybkiego wyszukiwania analitycznego zdarzeń związanych z bezpieczeństwem – oraz działaniem infrastruktury – na podstawie oceny korelacji obserwowanych zjawisk.

Dynatrace

Daje możliwość przeanalizowania sposobu funkcjonowania poszczególnych aplikacji, w rozbiciu na konkretne transakcje lub iteracje wewnętrznych procesów i wykonania elementów kodu źródłowego. Umożliwia też śledzenie wpływu sposobu działania aplikacji na doświadczenia i zachowania użytkowników. Sprzyja również eliminacji procesów w warstwie aplikacyjnej, komunikacji pomiędzy różnymi grupami interesariuszy zaangażowanych w procesy dotyczące konkretnych aplikacji, a także zwiększeniu wydajności systemów za sprawą ich optymalizacji i lepszemu wykorzystaniu posiadanej infrastruktury. APM dostarcza niepodważalnych argumentów w różnego rodzaju sporach z dostawcami aplikacji, a dzięki funkcjom monitoringu daje możliwość śledzenia na bieżąco jakości nowo wdrażanych aplikacji, co pozwala eliminować potencjalne koszty ich poprawy w przyszłości.