ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 878 STUDIA INFORMATICA NR 38 2015

DOI: 10.18276/si.2015.38-04

Tomasz Klasa*

MODEL GROMADZENIA DANYCH MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI W ORGANIZACJI WIRTUALNEJ

Streszczenie

Monitorowanie bezpieczeństwa informacji stanowi dość złożony proces w tradycyjnych organizacjach, a w przypadku organizacji wirtualnych jest jeszcze trudniejszy ze względu na zmienną strukturę i płynne granice organizacji. Oznacza to, że monitorowanie wymaga gromadzenia i kontroli stanu licznych parametrów, których lista może się często zmieniać. W rezultacie, choć pożądane jest gromadzenie i przetwarzanie danych w czasie niemal rzeczywistym, w praktyce jest to nieosiągalne ze względu na koszty operacyjne takiego postępowania. Gromadzenie gigabajtów danych z różnych źródeł może mieć wpływ na poprawne prowadzenie podstawowych procesów organizacji. Potrzebny jest więc mechanizm gromadzenia danych z wielu różnych źródeł o ograniczonym poziomie kosztów operacyjnych.

Słowa kluczowe: bezpieczeństwo informacji, monitorowanie bezpieczeństwa, organizacje wirtualne

Wprowadzenie

Organizacja wirtualna zwykle różni się istotnie od typowej, tradycyjnej organizacji wysoką elastycznością struktury, niewielką liczbą zasobów materialnych czy mocno rozproszoną strukturą. Wyróżnia się dwa stopnie organizacji wirtualnych. Poziom 1 charakteryzuje się tym, że (Appel i in., 1998; Brzozowski, 2006):

– posiada zdecentralizowaną organizację złożoną z wielu rozproszonych komórek współpracujących za pomocą narzędzi IT,
– nie istnieje jako całość w jednej lokalizacji,

* Tomasz Klasa, mgr inż., Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Wydział Informatyki, e-mail: tklasa@tksystemsecurity.pl

– wszystkie komórki mają fizyczne lokalizacje, ale wszystkie połączenia są wirtualne,
– posiada płaską strukturę zarządzania, z bardziej niezależnymi komórkami i częściowo niezależnymi zespołami.

Poziom 2 organizacji wirtualnej charakteryzuje się tym, że (Appel i in., 1998; Brzozowski, 2006):
– nie posiada fizycznej lokalizacji – istnieje tylko formalnie, łącząc przedsiębiorstwa, jednostki organizacyjne lub osoby w celu osiągnięcia określonych celów biznesowych,
– struktura istnieje tylko do osiągnięcia określonego celu, a nie by utrzymać i rozwijać organizację,
– osiągnięcie celu może oznaczać zamknięcie organizacji.

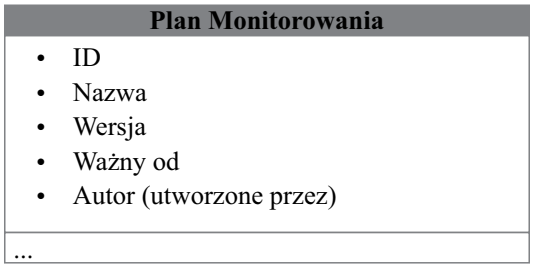
Biorąc powyższe cechy pod uwagę w kontekście bezpieczeństwa informacji, okazuje się, że podczas zarządzania bezpieczeństwem w organizacji wirtualnej występuje kilka dodatkowych problemów. Po pierwsze, mocno zdecentralizowana struktura lub wręcz brak fizycznej lokalizacji sprawia, że konieczne jest gromadzenie danych z licznych źródeł za pomocą tej samej infrastruktury teleinformatycznej, która zapewnia funkcjonowanie organizacji. W rezultacie, zwiększając ilość gromadzonych (a więc i przesyłanych) danych, trzeba mieć na uwadze, że ogranicza to pasmo dostępne dla podstawowej komunikacji. W skrajnym przypadku może to doprowadzić do zatorów komunikacyjnych w organizacji. Po drugie, mocno zmienna w czasie struktura organizacji sprawia, że poszczególne komponenty często zmieniają swoją rolę (funkcję). To z kolei utrudnia określenie, czy zebrane dane odpowiadają aktualnej strukturze – wskutek zmiany roli zasobu może on mieć udział w dodatkowych procesach, przez co zastosowanie starego profilu monitorowania nie pozwoli na wykrycie incydentu bezpieczeństwa w jednym z nowych obszarów.

Zbieranie danych o stanie bezpieczeństwa systemu informacyjnego organizacji wirtualnej wiąże się więc z pozyskaniem, wstępnym przetworzeniem i zapisaniem w repozytorium bardzo dużych ilości danych pochodzących z wielu źródeł. Ponieważ mowa jest o systemie informacyjnym, a więc obejmującym zarówno system informatyczny, jak i obszary organizacyjne, źródła pochodzenia tych danych różnią się od siebie diametralnie. Ponadto, rozproszona struktura systemu wymusza zastosowanie agentów programowych lub sprzętowo-programowych. Proces gromadzenia danych wymaga więc skonstruowania odpowiedniego modelu komunikacji, zapewniającego adekwatny poziom bezpieczeństwa, oraz

opracowania modelu reprezentacji danych, czyli struktury repozytorium, dostosowanego do charakterystyki organizacji wirtualnej: zmienności i rozproszonej struktury.

Proponowany model reprezentacji danych

Punktem wyjścia jest zakres monitorowania. Określa on, które parametry zabezpieczeń i z jaką częstotliwością powinny być weryfikowane dla każdego z zasobów wymagających monitorowania bezpieczeństwa. Ponieważ plan monitorowania może ulegać zmianom, niezbędne jest zapewnienie jego wersjonowania, a także wyznaczenie okresu jego ważności. Dane te, wzorem terminologii stosowanej w systemie SAP R/3, stanowią część nagłówka dokumentu *Plan Monitorowania*. W skład nagłówka wchodzą także dane na temat czasu powstania dokumentu oraz jego pochodzenia. W rezultacie otrzymujemy nagłówek w postaci:

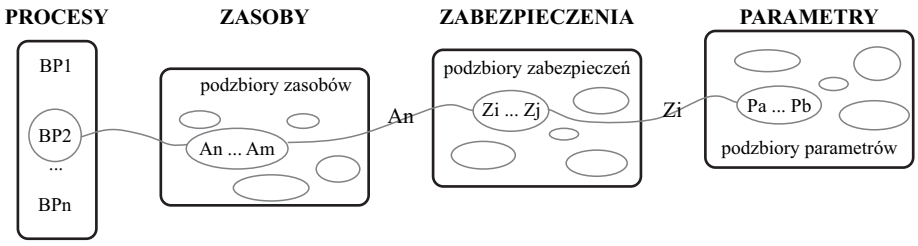


Rysunek 1. Plan monitorowania – struktura nagłówka
Źródło: opracowanie własne.

Plan monitorowania wskazuje parametry podlegające monitorowaniu dla poszczególnych zabezpieczeń, które z kolei dotyczą zasobów, a zasoby mają zastosowanie w określonych procesach biznesowych. W rezultacie powstaje struktura drzewiasta o następujących poziomach:

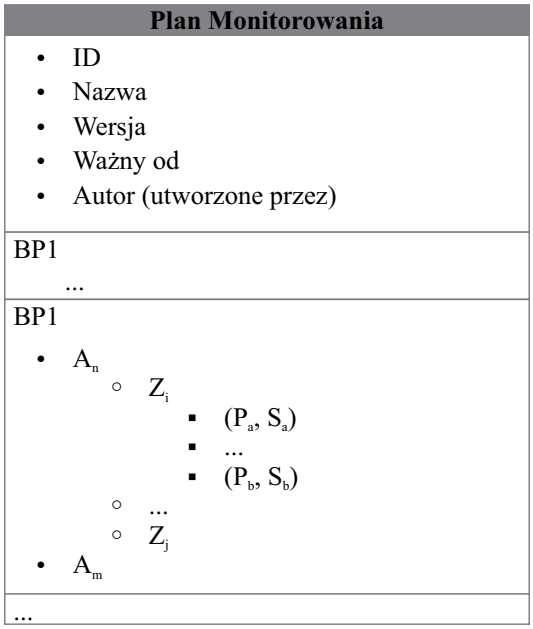
i Procesy
ii Zasoby
iii Zabezpieczenia
iv Parametry i sposoby monitorowania

Poziom n + 1 stanowi zbiór podzbiorów elementów powiązanych z elementem zbioru poziomu n odpowiadającym danemu podzbiorowi. Zależność tę przedstawiono na rysunku 2. Podział ten jest analogiczny do powszechnie stosowanego w zarządzaniu projektami schematu WBS (Department of Defense, 1999), który prezentuje złożone zadanie, jakim jest projekt (np. informatyczny) w postaci hierarchicznej struktury prostych zadań. Dla każdego z zadań łatwo określić wymagane zasoby czy czasochłonność, dzięki czemu znacznie łatwiejsze jest zaplanowanie działalności w ramach całego projektu. Proponowane rozwiązanie jest także analogiczne do funkcjonalności systemu projektowego SAP PS, który na bazie zasad budowy WBS pozwala zaplanować realizację złożonego projektu (np. budowy statku). Tak przygotowana struktura projektu stanowi podstawę i źródło danych do definiowania aktualnych potrzeb zakupowych, a nawet późniejszej dekretacji kosztów (SAP_PS).



Rysunek 2. Zależność między procesami a parametrami
Źródło: opracowanie własne.

W odróżnieniu od rozwiązania SAP PS, w którym projekt nie jest zdefiniowany jako pojedynczy dokument, a jako rozproszona struktura dokumentów o określonych relacjach wzajemnych, struktura zawarta w *Planie Monitorowania* została zdefiniowana w postaci jednego dokumentu podzielonego na pozycje lub segmenty (ponownie, zgodnie z terminologią SAP). Pozycją jest opis struktury dla pojedynczego procesu (albo jednej grupy procesów), wraz z relacjami do definicji powiązanych elementów na niższych poziomach. W rezultacie otrzymujemy więc postać dokumentu:



Rysunek 3. Plan monitorowania – struktura dokumentu
Źródło: opracowanie własne.

Analogicznie do systemu projektowego SAP PS, w którym na podstawie poszczególnych elementów planu generuje się zapotrzebowania (SAP_PS), plan monitorowania jest podstawą określenia zapotrzebowania na czynności monitorujące w wyznaczonych punktach systemu informacyjnego, związane z koniecznością osiągnięcia określonych celów zabezpieczeń. Zapotrzebowanie takie stanowi więc wskazanie parametru, który ma być monitorowany (wraz ze sposobem monitorowania go) z zachowaniem jego „ścieżki dostępu", czyli wskazaniem przypisanego mu zabezpieczenia, zasobu i procesu biznesowego. Zgodnie z zasadami właściwymi dla drzew FTA (IEC, 1990; NASA, 2002), analogicznie do wyznaczania prawdopodobieństwa całkowitego zdarzeń tworzących drzewo stochastyczne (Bean, 2001), pomiędzy elementami składowymi zapotrzebowania występuje relacja AND. Dokument *Zapotrzebowanie* dzieli się na część nagłówkową oraz opis pozycji:

Zapotrzebowanie
ź ID ź Ważny od ź Autor (utworzone przez)
ź Parametr (ref.) ź Zabezpieczenie (ref.) ź Zasób (ref.) ź Proces biznesowy (ref.)

Rysunek 4. Zapotrzebowanie – struktura dokumentu
Źródło: opracowanie własne.

Jeśli parametr dotyczy wielu zabezpieczeń, zasobów lub procesów biznesowych, to zapotrzebowanie może zawierać w swojej definicji odwołanie do grupy obiektów w miejscu odwołania do jednego obiektu. Na przykład, jeśli parametr występuje w kilku zabezpieczeniach dla tego samego zasobu i procesu biznesowego, zapotrzebowanie przyjmie ogólną postać:

Zapotrzebowanie
• ID • Ważny od • Autor (utworzone przez)
• Parametr (ref.) • Zabezpieczenie (ref.), ... • Zasób (ref.) • Proces biznesowy (ref.)

Rysunek 5. Zapotrzebowanie z referencją do grupy zabezpieczeń – struktura dokumentu
Źródło: opracowanie własne.

Analogicznie do zarządzania projektem, gdzie – aby zrealizować przedsięwzięcie zgodnie z założeniami – należy zaadresować wszystkie zadania opisane w diagramie WBS (Department of Defense, 1999), w przypadku planowania monitorowania bezpieczeństwa wyznaczone zapotrzebowania powinny realizować całość planu monitorowania. Stąd, zbiór wszystkich zapotrzebowań, który można przedstawić w postaci

$$ZZap = \{Zap_1, Zap_2, \ldots, Zap_i\},$$

powinien dla każdego parametru opisanego w planie monitorowania (niepowtarzalnego dla zestawu „zabezpieczenie, zasób i proces biznesowy") zawierać dokładnie jedno zapotrzebowanie ważne w danej chwili. Jeśli warunek ten nie zostanie spełniony, oznacza to, że nie zaplanowano śledzenia wszystkich parametrów zawartych w *Planie Monitorowania*, a więc prowadzone działania będą niekompletne i mogą być nieskuteczne.

W wielu zintegrowanych systemach logistycznych, m.in. SAP, kolejnym krokiem procesu zaopatrzeniowego jest zlecenie, na podstawie zapotrzebowania, dostawy określonych towarów lub usług wybranemu kontrahentowi (SAP_MM). W przypadku systemu monitorowania bezpieczeństwa rolę kontrahentów pełnią wskazane w planie monitorowania podsystemy agentowe, formularze oraz inne automaty przekazujące raporty o stanie komponentów systemu, w tym np. komunikaty błędów. Dla pewnego uproszczenia przyjmijmy, że każde źródło jest agentem o pewnym unikatowym identyfikatorze, pozwalającym na identyfikację adresata zamówienia przez każdą ze stron (nadawca i odbiorca zamówienia).

Wystawienie zamówienia na podstawie zapotrzebowania wymaga zmiany sposobu identyfikacji parametrów oraz zabezpieczeń, których dotyczą, z identyfikatorów parametrów i zabezpieczeń na poziomie agregatów (np. firewall, data ostatniej aktualizacji) na identyfikatory rzeczywistych zabezpieczeń (np. firewall, system wykrywania włamań IDS) i parametrów tych zabezpieczeń (np. data aktualizacji wzorców IDS). Jeden mechanizm zabezpieczający (np. firewall) może występować w wielu instancjach, przy czym każda z nich zwykle może być powiązana z innym podzbiorem zasobów. W istniejących rozwiązaniach konwersja ta odbywa się poprzez przyporządkowanie agentów (czasem zwanych konektorami) dedykowanych obsłudze określonych urządzeń (Muszyński i in., 2011). W rezultacie, rzeczywisty identyfikator zabezpieczenia można uzyskać w oparciu o relację uogólnionego zabezpieczenia z konkretnym wystąpieniem zasobu, a nie jego ogólną definicją (lub ich grupą). Dla rozróżnienia zasobu w ujęciu ogólnym od jego konkretnego egzemplarza ten ostatni oznaczono dodatkowo gwiazdką. Zbiór zasobów jednego typu można przedstawić jako:

$$\text{Zasób} = \{\text{Zasób}^*, \text{Zasób}^*, \dots\}.$$

Analogicznie, relację dla zabezpieczenia można przedstawić w postaci:

$$\text{Zabezpieczenie}^* = \text{zabezpieczenie}(\text{Zasób}^*).$$

W zależności od modelu lub wersji zabezpieczenia, zastosowanej wersji oprogramowania etc. oznaczenia techniczne poszczególnych parametrów mogą być różne. Ten sam parametr w różnych urządzeniach lub programach tego samego rodzaju może mieć (i zwykle ma) odmienny identyfikator lub nazwę techniczną, do której trzeba się odwołać, by uzyskać wartość tego parametru. Ponieważ plan monitorowania wskazuje parametry w ujęciu ogólnym, konieczna jest konwersja ich identyfikatorów na rozpoznawalne na poziomie konkretnego zabezpieczenia. W rezultacie otrzymujemy więc zależność, którą w pewnym uproszczeniu można przedstawić w postaci:

Parametr* = parametr (Zabezpieczenie*).

Opisana konwersja pełni istotną rolę: umożliwia uniwersalnemu agentowi identyfikację parametru właściwego dla określonego egzemplarza zabezpieczenia, zachowując jednocześnie spójny sposób obsługi parametrów dla wszystkich analogicznych egzemplarzy zabezpieczeń powiązanych z danym zasobem.

Zamówienie
• ID • Ważny od • Autor (utworzone przez) • Agent ID • Format odpowiedzi (schema)
• Zapotrzebowanie 1 ◦ ID, ◦ Parametr*, ◦ Zabezpieczenie*, ..., ◦ Zasób*, ◦ Próbkowanie, ◦ Format opisu (ref.)
• Zapotrzebowanie 2 ...
...

Rysunek 6. Zamówienie – struktura dokumentu

Źródło: opracowanie własne.

Dwa kolejne istotne komponenty dokumentu zamówienia to definicje formatów komunikacji oraz definicja formatu odpowiedzi. Ponieważ agent, konwertując format opisu, pełni funkcję analogiczną do bramy w sieciach komputerowych (Tanenbaum, 2004), niezbędne jest wskazanie, w jakim języku powinien komunikować się z danym egzemplarzem zabezpieczenia, a także w jakiej postaci ma udzielić odpowiedzi. Sposobem na możliwie duże ograniczenie nadmiarowości opisu w komunikacji jest tworzenie zamówień na podstawie wielu dokumentów zapotrzebowania. W rezultacie jeden agent, za pomocą jednego dokumentu zamówienia, może otrzymać zlecenie działań w odniesieniu do wszystkich zabezpieczeń (a więc i zasobów), które ma obsłużyć.

Podstawowym zadaniem systemu monitorowania bezpieczeństwa jest gromadzenie danych w celu ich dalszego przetworzenia. Ponieważ zamówienie zostało przewidziane jako dokument o otwartym czasie ważności (tj. ważne jest od podanego punktu w czasie aż do punktu w czasie wskazanym w wystawionym kolejnym zamówieniu), nie ma potrzeby stałego przesyłania go do agenta (cyklicznego odświeżania). Oczywiście w konsekwencji sam agent musi być w stanie przechować i obsłużyć zamówienie aż do wygaśnięcia jego terminu ważności (otrzymania nowego). W takiej sytuacji największy ruch będzie powodowany przez komunikację zwrotną (przesyłanie danych przez agenta do repozytorium). Dzięki wprowadzeniu dokumentu zapotrzebowania, możliwe jest ograniczenie się do następującej struktury:

Raport
• ID raportu • Data i czas wygenerowania • Agent ID • Zamówienie (ID)
• Zapotrzebowanie (ID) ◦ (Zabezpieczenie*, Wartość, timestamp) ◦ (Zabezpieczenie*, Wartość, timestamp) ◦ ...
• Zapotrzebowanie (ID) ...
...

Rysunek 7. Raport – struktura dokumentu

Źródło: opracowanie własne.

Ponieważ zapotrzebowanie dotyczy określonego parametru w ujęciu ogólnym i jest powiązane z dokładnie jednym zamówieniem w danej chwili, to tak opisaną wartość można łatwo powiązać zarówno z konkretnym egzemplarzem zasobu, jak i zabezpieczenia czy zasobu w ujęciu ogólnym. Jest to rozwiązanie w znacznym stopniu analogiczne do zastosowanego w systemie SAP, gdzie zapotrzebowanie może być podstawą do wystawienia zamówienia dla konkretnego kontrahenta (dostawcy), a realizacja zamówienia (dostawa, faktura) jest dekretowana na zamówienie (SAP_MM). W przypadku opisanego modelu, agent może obsługiwać tylko jedno ważne zamówienie w danej chwili (wystawienie nowego zamówienia zastępuje jego poprzednią wersję). Ponieważ zamówienie, na poziomie pozycji, zawiera odwołania do zapotrzebowania, za pomocą jednego zamówienia zlecane jest monitorowanie wielu parametrów, a nawet szeregu zabezpieczeń lub zasobów. Aby więc jednoznacznie zidentyfikować przekazywane dane, na etapie raportowania wystarczy podać referencję do zamówienia na poziomie nagłówka raportu, a na poziomie pozycji wskazać zapotrzebowanie, którego dane dotyczą. W systemie SAP dokument potwierdzający realizację zamówienia nie zawiera już referencji do zapotrzebowania. W rezultacie dokument zamówienia powiela niezbędne dane z zapotrzebowania, uzupełniając je nowymi polami (SAP_MM). W zaproponowanym modelu, dzięki zachowaniu referencji do zapotrzebowania, można było ograniczyć liczbę pól przekazywanych razem z raportem, ponieważ są one zawarte w definicji zapotrzebowania dostępnej w repozytorium.

Wyniki

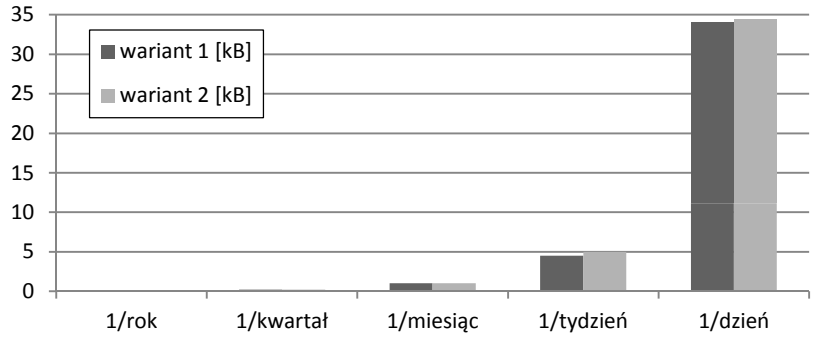
Biorąc pod uwagę możliwe wartości poszczególnych identyfikatorów, wynikające z liczby tego typu elementów, jakie mogą występować w dużej organizacji wirtualnej, wyznaczono rozmiar metadanych. Przyjmując, że jeden znak jest reprezentowany za pomocą 1 bajta oraz że każdy identyfikator jest unikatowy w skali systemu, otrzymano wartości:

– id raportu – 15 B,
– data i czas – 20 B,
– id agenta – 6 B,
– id zabezpieczenia lub sposobu postępowania z ryzykiem – 6 B,
– id zasobu – 6 B,
– id parametru – 6 B,
– id formatu opisu – 3 B.

Ponadto, przyjęto następujące wielkości dla identyfikatorów zaproponowanych dodatkowych struktur pomocniczych (dokumentów):
– zamówienie – 10 B,
– zapotrzebowanie – 10 B.

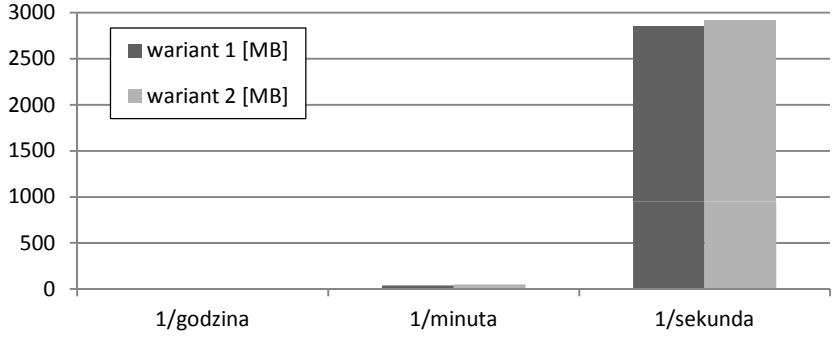
Na potrzeby porównania zdefiniowano dwa skrajne warianty gromadzenia danych:
– wariant 1 – gromadzenie indywidualnych raportów dla każdego parametru przypisanego do określonego (jednego) zabezpieczenia jednego zasobu,
– wariant 2 – gromadzenie raportów zbiorczych na podstawie zapotrzebowania i zamówienia.

W pierwszej kolejności porównano rozmiar raportu dla obu powyższych wariantów, przy założeniu, że raport zawiera jeden odczyt jednego parametru z jednego zabezpieczenia dla jednego zasobu.



Rysunek 8. Porównanie rozmiaru raportu, gdy raport zawiera jeden odczyt – niskie częstotliwości

Źródło: opracowanie własne.

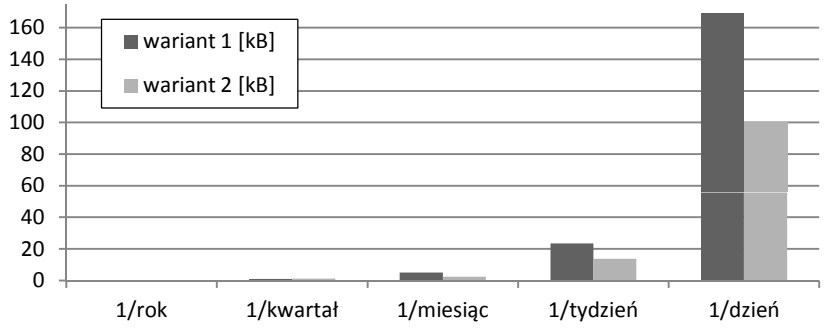


Rysunek 9. Porównanie rozmiaru raportu, gdy raport zawiera jeden odczyt – wysokie częstotliwości

Źródło: opracowanie własne.

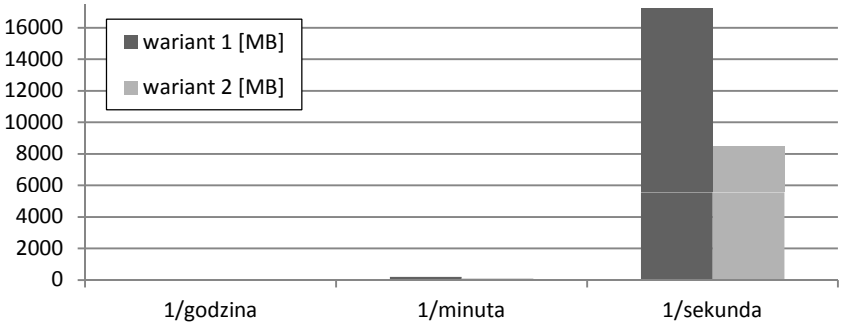
Proponowany model organizacji metadanych nie przynosi korzyści, gdy raport zawiera wartość tylko jednego parametru – otrzymany rozmiar raportu jest w pełni porównywalny. Ponadto, po zwiększeniu częstotliwości próbkowania, widać możliwe problemy wydajnościowe dla obu wariantów – monitorowanie jednego parametru z częstotliwością $f = 1/s$ wymaga przesłania niemal 3 GB danych, z czego ok. 600 MB to wartości parametru, a 2,4 GB to metadane.

Następnie powtórzono test zakładając, że w ramach wariantu 2 jeden raport realizuje jedno zamówienie wynikające z pięciu zgłoszeń zapotrzebowania. Odpowiednikiem tej sytuacji jest przesłanie pięciu odrębnych raportów w wariancie 1.



Rysunek 10. Porównanie rozmiaru raportu – raport dla pięciu zgłoszeń zapotrzebowania – niskie częstotliwości

Źródło: opracowanie własne.



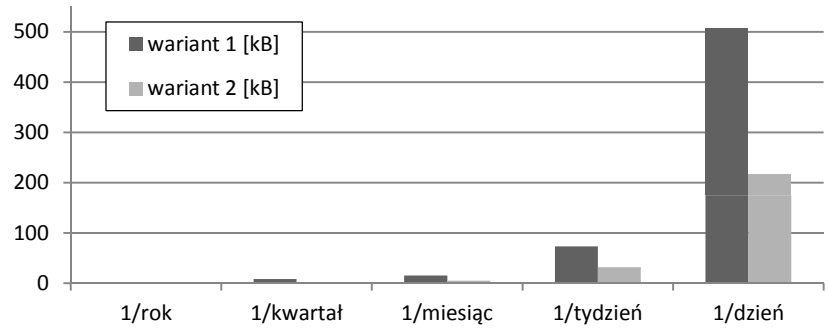
Rysunek 11. Porównanie rozmiaru raportu – raport dla pięciu zgłoszeń zapotrzebowania – wysokie częstotliwości

Źródło: opracowanie własne.

Jak widać, zastosowanie proponowanego modelu metadanych pozwala na znaczne ograniczenie sumarycznego rozmiaru przesyłanych raportów. Prezentowane wartości dotyczą raportów wzorcowych, ale odzwierciedlają skalę możliwych rzeczywistych różnic, jakie można osiągnąć przez zastąpienie części metadanych referencjami do opisujących je dokumentów (zapotrzebowanie, zamówienie). W ujęciu ilościowym największą różnicę można zaobserwować przy raportowaniu z przedziałem sekundowym – sumaryczna ilość przesyłanych danych została zredukowana z ok. 17 GB rocznie do ok. 8,5 GB rocznie. Liczby te dotyczą raportowania pięciu parametrów (po jednym na zgłoszenie zapotrzebowania).

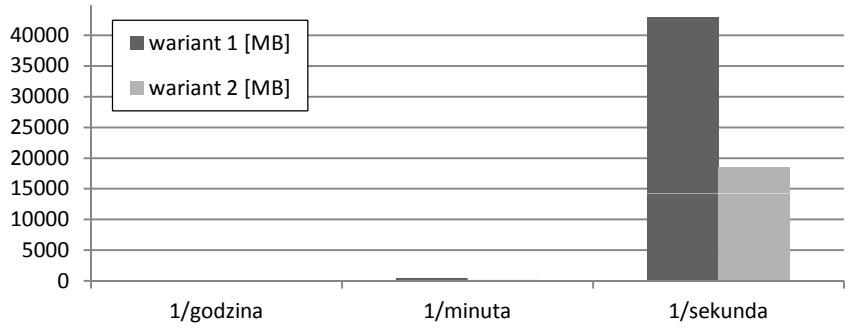
Trzeci przeprowadzony test miał na celu zobrazowanie różnicy w warunkach bardziej zbliżonych do rzeczywistych. W tym przypadku przyjęto, że jeden agent gromadzi wartości trzech parametrów (A, B, C):

– parametr A jest powiązany z trzema zabezpieczeniami, a każde z nich dotyczy dwóch zasobów, więc znajdzie się w dwóch odrębnych dokumentach zapotrzebowania (dla wariantu 2),
– parametr B jest związany z 1 zabezpieczeniem, które dotyczy 3 zasobów, więc znajdzie się w trzech odrębnych dokumentach zapotrzebowania (dla wariantu 2),
– parametr C jest związany z 5 zabezpieczeniami, dotyczy 1 zasobu, więc znajdzie się w jednym dokumencie zapotrzebowania (dla wariantu 2).



Rysunek 12. Porównanie dla agenta obsługującego trzy parametry – niskie częstotliwości

Źródło: opracowanie własne.



Rysunek 13. Porównanie dla agenta obsługującego trzy parametry – wysokie częstotliwości

Źródło: opracowanie własne.

Warte podkreślenia jest zmniejszenie całkowitego rozmiaru przesłanych raportów z ok. 500 kB do ponad 200 kB, a więc o ok. 55%. Takie same różnice widać także przy wyższych częstotliwościach raportowania. Ponownie potwierdza się, że gromadzenie danych o stanie elementów złożonego systemu z wysoką częstotliwością wiąże się z przesyłaniem bardzo dużych ilości danych. Jest to potwierdzenie wniosków, które w przypadku systemów Smart-Grid postawili Aiello i Pagani (Aiello i in., 2014). Podobnie jak w przypadku systemu Smart-Grid, poszukiwanie sposobów ograniczenia ilości przesyłanych danych jest koniecznością, jeśli ma być zastosowana większa częstotliwość próbkowania.

Podsumowanie

Na podstawie przeprowadzonych testów pokazano, że wprowadzenie dokumentów zgłoszenia zapotrzebowania oraz zamówienia pozwala na znaczące zredukowanie całkowitej ilości danych przesyłanych do centralnego repozytorium powiązanego z systemem wnioskowania o stanie bezpieczeństwa. Wprowadzenie, wzorowanego na procesie logistycznym SAP, modelu obsługi procesu gromadzenia danych, w którym źródła danych (agenci) otrzymują zamówienie wynikające z określonego zapotrzebowania na dane, pozwala na grupowanie danych w bloki (pakiety), które mają wspólny termin raportowania (odwołując się do terminologii logistycznej: dostawy). W rezultacie możliwe jest przesyłanie pakietów zbiorczych, dla których część metadanych jest wspólna, a więc nie jest powielana dla każdego przekazywanego odczytu.

Pomimo to wartość informacyjna tak przekazywanych informacji nie ulega pogorszeniu.

Bibliografia

Aiello M., Pagani G.A. (2014), *The Smart Grid's Data Generating Potentials*, „Annals of Computer Science and Information Systems", vol. 2, s. 9–16.

Appel W., Behr R. (1998), *Towards the theory of Virtual Organizations: A description of their formation and figure*, „Newsletter", no. 2.

Bean M.A. (2001), *Probability: The Science of Uncertainty with Applications to Investments, Insurance, and Engineering*, American Mathematical Society, Providence.

Brzozowski M. (2006), *Ewolucja pojmowania wirtualności i definiowanie organizacji wirtualnej*, w: *Wybory strategiczne firm – nowe instrumenty analizy i wdrażania*, red. P. Płoszajski, G. Bełza, Oficyna Wydawnicza Szkoły Głównej Handlowej, Warszawa.

Department of Defense (1999), *Systems Engineering Fundamentals*, Defense Systems Management College Press, Fort Belvoir.

IEC (1990), *Fault Tree Analysis (FTA)*, International Technical Commission, IEC Standard, Publication 1025.

Muszyński J., Grimes R. (2011), *Rozwiązania do zarządzania logami*, NetWorld, http://www.networld.pl/artykuly/366992_1/Rozwiazania.do.zarzadzania.logami.html.

NASA (2002), *Fault Tree Handbook with Aerospace Applications', Version 1.1*, NASA Publication.

SAP_MM, materiały szkoleniowe systemu SAP ECCv6.0, moduł MM.

SAP_PS, materiały szkoleniowe systemu SAP ECC 6.0, moduł PS.

Tanenbaum A.S. (2004), *Sieci komputerowe*, Helion, Gliwice.

INFORMATION SECURITY MONITORING DATA RETENTION MODEL FOR VIRTUAL ORGANIZATIONS

Summary

Information security monitoring in traditional organizations is quite a sophisticated process. In the case of virtual organization, however, it becomes even more difficult as its structure is very dynamic and borders flexible. This means that monitoring requires gathering and controlling status of numerous parameters, while list of them may change on

a regular basis. As a result, although it is desired to gather and process data in-near-real--time mode, in practice it is not possible due to operational costs connected with such an activity. Gathering gigabytes of data from various sources may influence regular operation of organization's basic services. Thus it is necessary to provide a mechanism of data acquisition that will reduce operational costs associated with gathering information security data from various remote sources.

Translated by Tomasz Klasa

Keywords: information security, security monitoring, virtual organizations