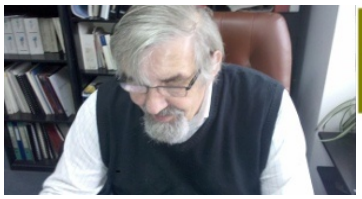


Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Numer 39/2013 26 czerwiec 2013

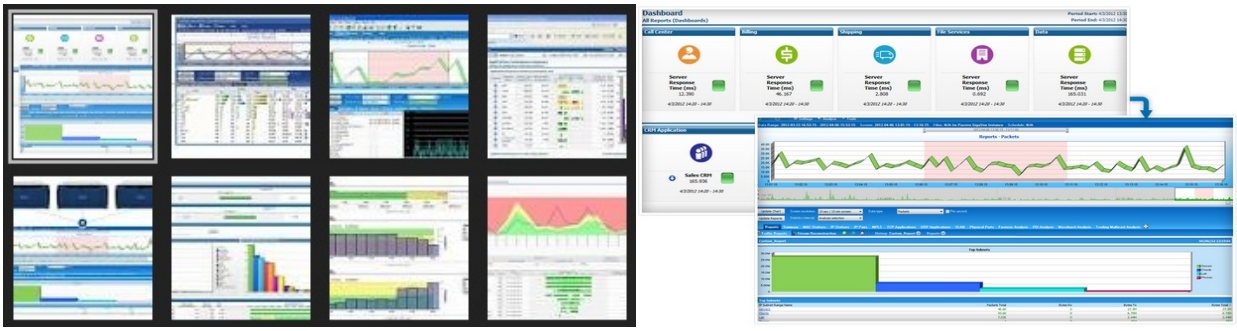
Do napisania tego tekstu zainspirowały mnie różne opinie dotyczące śladów pozostawianych w sieci przez „złych chłopców” oraz możliwości monitorowania ich działalności. Wiele osób wygłasza publicznie swe opinie na ten temat. Opinie te mają bardzo różną wartość merytoryczną, postanowiłem poświęcić tej sprawie kolejny numer „Guru” - tym bardziej, że już od 1995 r. zajmuję się dystrybucją produktów firmy Network Instruments, która specjalizuje się w produktach realizujących monitorowanie sieci komputerowych.

Ogólnoświatowa sieć komputerowa jest czymś wspaniałym i wywarła ogromny wpływ na całe nasze życie. Niestety, sieć jest zwierciadłem, w którym przeglądamy się wszyscy. Dzięki sieci poznaliśmy, jacy naprawdę jesteśmy – i piękni i równocześnie okropni. Sieć pozwala na swobodną wymianę wzniosłych idei – ale równocześnie spowodowała powstanie nowych rodzajów przestępstw.

Nadzór nad przestrzenią publiczną (także wirtualną) wydaje się być konieczny. Możliwe jest wiele sposobów jego realizacji – można i trzeba budować ogrodzenia (różne „ściany ogniowe”, systemy IDS, programy antywirusowe), jednak sprawdzonym w praktyce rozwiązaniem jest ciągły monitoring. Stosuje się go coraz częściej na ulicach naszych miast, a coraz więcej kierowców (zwłaszcza zawodowych) instaluje w swych samochodach kamery monitorujące sytuacje drogowe. Dzięki monitoringowi udaje się „namierzyć” coraz więcej przestępców.

Stacja monitorowania ruchu na autostradzie – źródło: Wikimedia Commons

Przestrzeń wirtualna wbrew pozorom niewiele różni się od przestrzeni rzeczywistej i zasady jej monitoringu powinny być podobne:



1. Monitoring powinien być ciągły!

O przestępstwie lub wypadku dowiadujemy się z zasady po fakcie. Jeśli monitoring ma pomóc w odtworzeniu ich przebiegu musimy dysponować informacjami historycznymi. Aby kamera w samochodzie lub na ulicy była skuteczna musi być cały czas włączona i zapisywać dane w taki sposób, aby było możliwe odtworzenie przebiegu zdarzenia.

Monitoring sieci komputerowej musi być również ciągły, ponieważ tylko taki sposób monitorowania umożliwi poznanie natury zdarzenia oraz zastosowanych metod ataku i ułatwi dotarcie do jego źródła lub źródeł (a więc tym samym do samego atakującego). Ciągły monitoring umożliwia także przeprowadzenie analizy skuteczności stosowanych zabezpieczeń i tym samym ich skorygowanie.

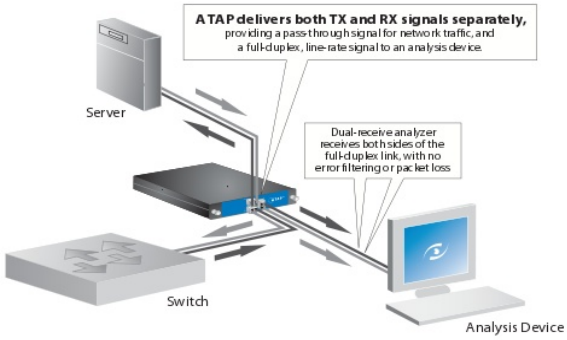
Zestaw dysków dla urządzenia NI GigaStor

2. Monitoring powinien być kompletny!

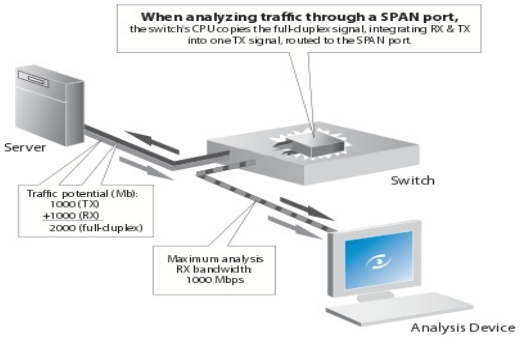
Kontrole wyrywkowe mogą dawać jedynie pewność statystyczną. Jeśli monitoring sieci komputerowej będzie dotyczył jedynie części transmisji to nie będzie możliwe pełne odtworzenie przebiegu zdarzeń. Współczesne sieci komputerowe są szybkie – powszechnie stosowana jest sieć ethernet o prędkości 1 Gbps, a w sieciach szkieletowych 10 Gbps. Wdrażane są już sieci o prędkości 40 Gbps i 100 Gbps. Monitorowanie takie sieci to prawdziwe wyzwanie tym bardziej, że pracują one w trybie Full Duplex – a więc dla skutecznego monitorowania sieci 10 Gbps musimy dysponować możliwością równoczesnego zapisu informacji z 2 kanałów z prędkością 20 Gbps (10 Gbps dla kanału Tx oraz 10 Gbps dla kanału Rx). Tylko takie urządzenie monitorujące może zapewnić przechwycenie wszystkich informacji przesyłanych siecią, a więc kompletność jej monitoringu.

Drugim problemem jest konieczna pojemność pamięci przeznaczonej do zapisu danych. Dla w pełni wykorzystywanej sieci 1 Gbps pracującej w trybie Full Duplex przez 2 godziny potrzebny nam będzie dysk twardy o pojemności 2 TB. Aby uzyskać taki sam czas zapisu dla sieci 10 Gbps będzie potrzebny zestaw dysków o pojemności 24 TB zaś dla sieci 40 Gbps - 96 TB.

Oczywiście same dyski, jak i oprogramowanie ja obsługujące muszą zapewnić odpowiednią prędkość zapisu.



Bezpośredni pobór sygnałów Tx i Rx (Full Duplex)



Wykorzystanie portu SPAN

3. Monitoring musi być skutecznie zabezpieczony przed wyłączeniem lub ominięciem!

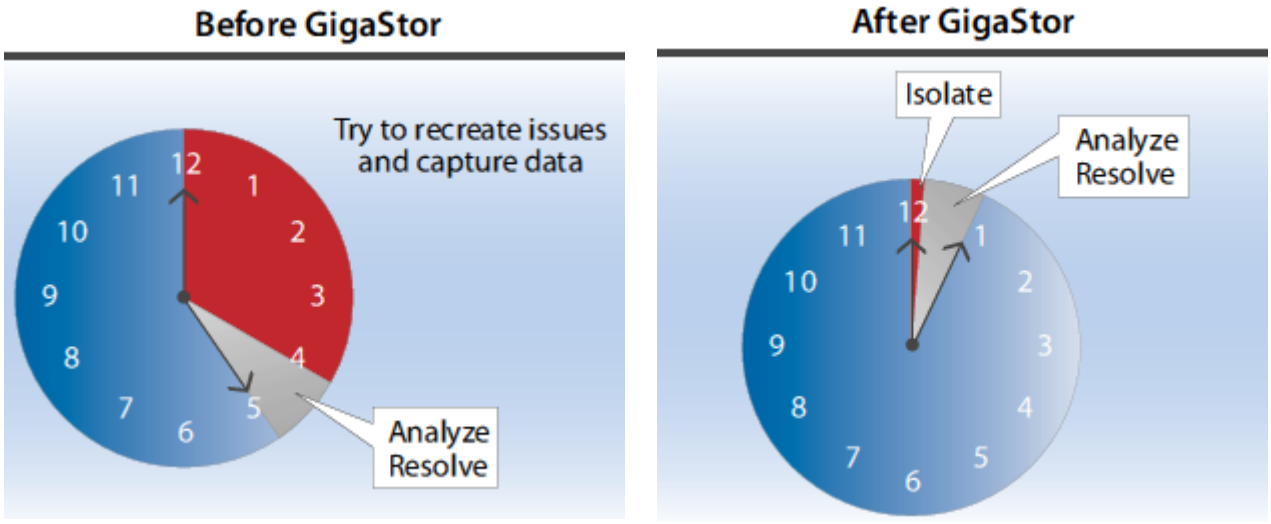
Po wprowadzeniu automatycznych radarów drogowych dość popularnym „sportem" było zamalowywanie „sprayem" okienka kamery. Metoda prosta, która skutecznie uniemożliwia identyfikację pojazdu przekraczającego dozwoloną prędkość.

W przypadku monitoringu sieci komputerowych urządzenie monitorujące powinno być podłączone w taki sposób, aby nie było możliwe jego „oślepienie" lub wyłączenie. Wyklucza to w praktyce możliwość podłączenia takiego urządzenia do portu urządzenia, które może być zdalnie zarządzane sieciowo, ponieważ zawsze należy się liczyć z możliwością przejęcia kontroli nad takim urządzeniem (np. przełącznikiem lub routerem) przez atakującego. Wyłączenie portu (SPAN port), z którego korzysta urządzenie monitorujące spowoduje natychmiastowe jego „oślepienie".

Najkorzystniejszym sposobem podłączenia urządzenia monitorującego do sieci komputerowej jest możliwe bezpośrednie podłączenie go do okablowania (miedzianego lub światłowodowego) za pomocą rozgałęźników nTAP (Network Testing Access Point). Urządzenia tego typu mogą być całkowicie niewidoczne oraz co bardzo ważne rozgałęziają sygnały z obu kanałów Rx i Tx przekazując je do urządzenia monitorującego. Rozgałęźniki nTAP przekazują sygnały tylko w jedną stronę – z sieci do urządzenia monitorującego. Nie mogą przekazać żadnego sygnału z urządzenia monitorującego do sieci, co uniemożliwia wykrycie jego obecności oraz przy zastosowaniu odpowiedniej ochrony fizycznej skutecznie uniemożliwia wyłączenie lub ominięcie monitoringu.

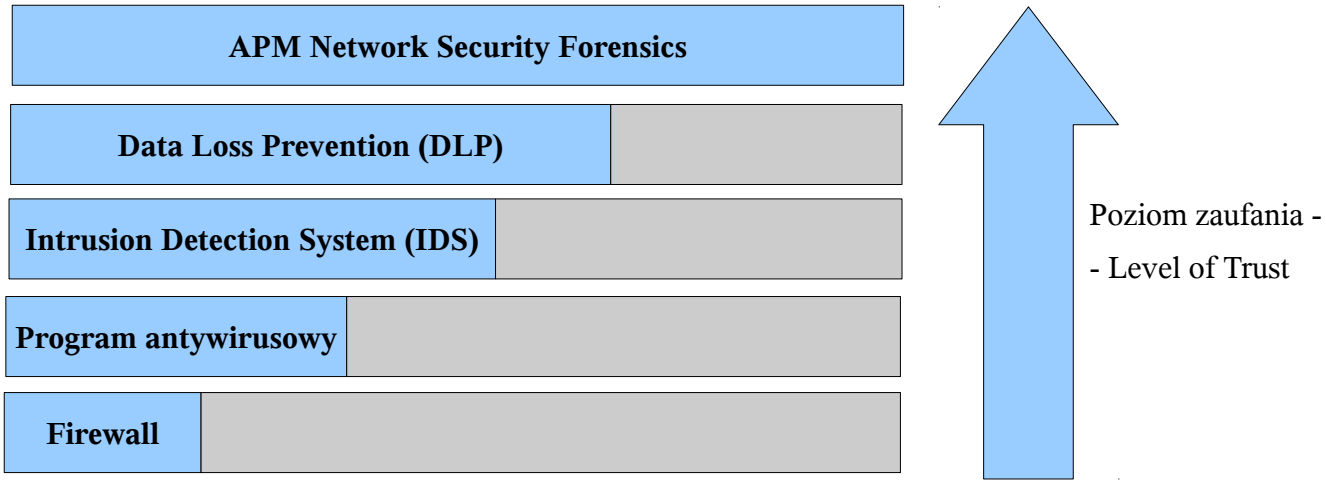
Dzięki monitoringowi dysponujemy zapisem transmisji sieciowych – np. realizowanych w ciągu ostatniej nocy. Przegląd zapisanych danych umożliwia błyskawiczne wykrycie oraz wyizolowanie ewentualnych incydentów i natychmiastowe podjęcie analizy i podjęcie odpowiednich akcji.

W przypadku działań przestępców komputerowych profesjonalny monitoring umożliwia nam przedstawienie odpowiednich i wiarygodnych dowodów.



4. Dane z monitoringu powinny być łatwe do przeanalizowania.

W przypadku wystąpienia zakłóceń w pracy sieci komputerowej (nie tylko w wyniku ataku, ale również błędów użytkowników, oprogramowania lub niepoprawnej konfiguracji) monitoring umożliwi nam „cofnięcie się wstecz" i przeprowadzenie analizy przebiegu zdarzeń. Najczęściej będziemy mieli do czynienia z koniecznością wyselekcjonowania interesujących nas danych z bardzo dużej ilości transmisji sieciowych. Konieczny będzie więc efektywny system filtrowania oraz prezentowania informacji. W wielu przypadkach urządzenia monitorujące umieszcza się w różnych segmentach sieci – system analizy danych powinien umożliwiać sprawdzenie, czy występują korelacje pomiędzy danymi z różnych urządzeń monitorujących.



Więcej informacji o rozwiązaniach Network Instruments znajdą Państwo na stronie www.aba.krakow.pl/NI lub www.networkinstruments.com . Z przyjemnością odpowiem również na wszystkie pytania.