Piotr Kijewski, Krzysztof Szczypiorski
Politechnika Warszawska
Instytut Telekomunikacji
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

Ograniczenia systemów wykrywania włamań

W artykule przedstawiono ograniczenia występujące w systemach wykrywania włamań w sieciach teleinformatycznych. Omówiono kluczowe dla tych systemów zagadnienia: definicję włamania, rozpoznanie włamania, informację o włamaniu, reakcję na tę informację. Zaprezentowano m.in. problem fałszywych alarmów (niską liczbę prawdziwych włamań, w stosunku do podejrzanie wyglądających zdarzeń w sieci), metodę analizowania zaszyfrowanego ruchu sieciowego opartą na zaufanych trzecich stronach i kwestie zarządzania personelem kontrolującym zabezpieczenia sieci.

Piotr Kijewski, Krzysztof Szczypiorski
Warsaw University of Technology, Poland
Institute of Telecommunications
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

Limitations of Intrusion Detection Systems

The article presents several limitations inherent to network intrusion detection systems. Key intrusion detection concepts are outlined: the definition of an intrusion, recognizing an intrusion, intrusion reporting and response. The effectiveness aspect of intrusion detection is discussed and the problem of false alarms (so called false positives) explained. Solutions including trusted third parties are proposed for dealing with encrypted traffic. Problems with the management of personnel operating the intrusion detected system are also discussed.

Piotr Kijewski, Krzysztof Szczypiorski
Politechnika Warszawska
Instytut Telekomunikacji
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

Ograniczenia systemów wykrywania włamań

W artykule przedstawiono ograniczenia występujące w systemach wykrywania włamań w sieciach teleinformatycznych. Omówiono kluczowe dla tych systemów zagadnienia: definicję włamania, rozpoznanie włamania, informację o włamaniu, reakcję na tę informację. Zaprezentowano m.in. problem fałszywych alarmów (niską liczbę prawdziwych włamań, w stosunku do podejrzanie wyglądających zdarzeń w sieci), metodę analizowania zaszyfrowanego ruchu sieciowego opartą na zaufanych trzecich stronach i kwestie zarządzania personelem kontrolującym zabezpieczenia sieci.

0. Wstęp

Głównym celem artykułu jest przedstawienie ograniczeń występujących w rzeczywistych systemach wykrywania włamań. Systemy wykrywania włamań (*intrusion detection systems*) są coraz powszechniej stosowane w sieciach teleinformatycznych w szczególności w środowisku TCP/IP.

Na początku spróbujmy wyobrazić sobie działanie **idealnego systemu wykrywania włama ń.** W momencie zajścia **zdarzenia wyglądającego na włamanie**, system wykrywania włamań na podstawie danych odebranych z sensorów **wykrywa** to zdarzenie. Następnie system wykrywania włamań **informuje** o tym zdarzeniu, a na samym końcu **podejmuje** odpowiednią **reakcję**.

W idealnym systemie wykrywania włamań każde **zdarzenie wyglądające na włamanie** jest wykrywane, zawsze następuje powiadomienie i zachodzi właściwa reakcja.

W kontekście idealnego systemu wykrywania włamań sformułujmy **cztery** problemy:

1. co to jest zdarzenie wyglądające na włamanie?
2. jak rozpoznać zdarzenie wyglądające na włamanie?
3. o czym system powinien informować?
4. jak należy reagować na te informacje?

Omawiając każdy z powyższych problemów krok po kroku, wykażemy, że zrealizowanie systemu idealnego nawet jeżeli byłoby możliwe nie doprowadzi do sytuacji, w której system wykrywania włamań, będzie systemem dającym detekcję o 100% wiarygodności.

1. Co to jest zdarzenie wyglądające na włamanie?

Odpowiedź na pierwsze pytanie jest prosta: **zdarzenie wyglądające na włamanie** jest **nadużyciem** lub **anomalią**. Nadużycie jest rodzajem zachowania, które system wykrywania włamań rozpoznaje jako konkretny (a więc znany, skatalogowany) atak na system. Wszelkie zachowania niezgodne z przyjętymi zasadami („polityką" zachowania) są uznawane za anomalie (np. większe wykorzystanie mocy obliczeniowej, niestandardowa sekwencja komend użytkownika, wykorzystanie przez aplikację nietypowego dla niej wywołania systemowego lub ich sekwencji).

2. Jak rozpoznać zdarzenie wyglądające na włamanie?

Odpowiedź na drugie pytanie jest już trudniejsza. **Wykrywanie nadużyć** w najprostszym przypadku wymaga posiadania wiedzy w postaci bazy danych o typowych atakach, w tym typowych sekwencji pojawiających się w okolicznościach ataku. Obserwację nadużyć niekiedy utrudnia fakt, że źródło ataku jest rozproszone lub też atak jest rozciągnięty w czasie. Atakujący dążąc do zamazania korelacji pomiędzy typowymi krokami (np. skanowanie portu, skanowanie usługi uruchomionej na aktywnym porcie, skanowanie dziury w tej usłudze) może korzystać z maszyn o różnych adresach sieciowych lub wprowadzić pomiędzy poszczególnymi etapami włamania długie przerwy (np. tygodniowe). Warto zdać sobie sprawę, że sekwencja zdarzeń składająca się na jeden atak może być skonstruowana na wiele sposobów. Wynika to z cech poszczególnych protokołów, reprezentacji danych oraz ich interpretacji. Jako przykład można podać manipulację polami nagłówka protokołu TCP/IP, ustawienia nielegalnych wartości pól (np. długości) bądź opcji. Za przykład na poziomie warstwy aplikacji może posłużyć system kodowania znaków Unicode, który dopuszcza wiele reprezentacji tego samego znaku. Zatem idealny system wykrywania włamań powinien znać sposób, w jaki wszystkie systemy teleinformatyczne, które chroni, interpretują dane i protokoły. W przypadku, gdy mamy do czynienia z zaszyfrowanymi danymi (np. połączenie SSL/TLS) jest jeszcze gorzej – system wykrywania włamań musi być zaufaną trzecią stroną – znać klucze sesyjne, aby odszyfrowywać strumień danych i wykrywać niepożądane znaczenia. Oprócz zwiększenia mocy obliczeniowej koniecznej do intensywnych operacji matematycznych, przejęcie funkcji zaufanej trzeciej strony uderza w podstawowe założenia niektórych systemów bezpieczeństwa (SSL/TLS jest przeznaczony do zapewnienia poufności i uwierzytelnienia w bezpośrednim połączeniu klienta z serwerem, bez żadnych systemów pośredniczących). Co jednak będzie wtedy, gdy system wykrywania włamań jako zaufana strona będzie narażony na wyciek informacji? Czy nie prowadzi to do absurdalnej sytuacji: wprowadzając nowy system zabezpieczeń, znacząco obniża się bezpieczeństwo istniejących systemów ochrony informacji?

Podstawowym zagadnieniem **w wykrywaniu anomalii** jest niemożność zbudowania uniwersalnego modelu zachowania systemu teleinformatycznego. Zdefiniowanie anomalii wymaga określenia parametrów (zmiennych), które system wykrywania włamań może śledzić. Dla zdefiniowanych parametrów należy określić progi, które odróżniają zachowanie typowe od uznawanego za anomalię. Określenie parametrów jak i progów nie jest zadaniem trywialnym. Wyobraźmy sobie prymitywny system wykrywania włamań, który uczy się skąd użytkownik loguje się do systemu. Określono parametr: liczba nowych hostów w ciągu określonego czasu, próg: dwa nowe hosty w ciągu 24 godzin. Wykrycie dwóch nowych hostów z których użytkownik się zalogował w ciągu 2

godzin prowadzi do rozpoznania takiego zachowania jako anomalii. Nie musi to jednak wcale oznaczać rzeczywistego włamania.

3. O czym system wykrywania włama ń powinien informować?

W ten sposób dochodząc do naszego trzeciego pytania i udzielając odpowiedzi: „idealny system powinien informować o wszystkich zdarzeniach, które są uznane za anomalię lub nadużycie", popadamy w pułapkę **fałszywych alarmów.** Zilustrujmy to z pozoru paradoksalnym przykładem: lekarz używa testu na obecność pewnej rzadkiej bakterii występującej u jednego pacjenta na milion badanych (1/1.000.000). Skuteczność testu jest bardzo wysoka - wynosi 99,99%. Oznacza to, że jeśli ktoś ma tę bakterię to test wykaże to w 99,99% przypadków, a jeżeli jej nie ma - wykaże jej nieobecność również w 99,99%. przypadków. Prawdopodobieństwo posiadania tej bakterii pod warunkiem otrzymania pozytywnego wyniku testu wynosi zaledwie 1%! Mając test tej samej skuteczności na inną powszechniejszą bakterię, występującą u jednego pacjenta na tysiąc badanych (1/1.000), prawdopodobieństwo posiadania tej bakterii pod warunkiem otrzymania pozytywnego wyniku osiąga wartość zaledwie 91%. Prawdopodobieństwa te wynikają z proporcji pomiędzy liczbą osób chorych, a liczbą osób zdrowych. Wyliczenia są oparte na znanym wzorze Bayesa na prawdopodobieństwa warunkowe (por. [Axelsson1999]).

Podobne wyliczenia odnoszą się do systemów wykrywania włamań - ataki są stosunkowo rzadkie w porównaniu do normalnych zdarzeń, które przez te systemy są analizowane

Wnioski dla twórców systemów wykrywania włamań nie są jednoznaczne: z jednej strony zestaw reguł wykrywających nadużycia powinien być bardzo precyzyjny, z drugiej przesadna dokładność może doprowadzić do tego, że niektóre działania (np. skanowanie sieci) pozostaną nie wykryte. Wniosków tych nie można w prosty sposób rozszerzyć na systemy wykrywające anomalie, gdyż posiadają one różne cechy w zależności od przyjętych modeli zachowania systemu teleinformatycznego, a co za tym idzie różnych parametrów, progów i zależności między nimi.

Redukcję fałszywych alarmów utrudniają także prozaiczne powody: awarie w działaniu sieci, niepoprawnie zaimplementowane protokoły i aplikacje, błędy systemu operacyjnego. Generowanie przez włamywaczy fałszywych alarmów może stać się nową metodą ataku na system wykrywania włamań.

Można zaryzykować stwierdzenie, że systemy wykrywania włamań są w obecnej formie **systemami wykrywania zdarzeń wyglądających na włamanie.**

4. Jak należy reagować na informacje o zdarzeniach wygl ądających na włamanie?

Pozostaje ostatnie czwarte pytanie. Przypomina się tu bajka Ezopa o młodym pastuchu, owcach i wilku. Pastuch wielokrotnie (z nudów? dla zabawy?) alarmował wieś, twierdząc że wilk napada na jego owce - czujni mieszkańcy zbiegali się na pastwisko, aby pomóc pastuchowi ochronić stado owiec - odgonić szkodnika. Na miejscu okazywało się, że zagrożenia nie ma. Pewnego dnia wilk

rzeczywiście napadł na stado owiec, ale nikt po serii fałszywych alarmów nie zareagował na rozpaczliwe wezwania pastucha.

Powyższy problem - utraty wiarygodności w detekcję zdarzeń jako włamań - staje się poważniejszy, jeżeli system wykrywania włamań jest skonfigurowany jako wyrafinowany mechanizm kontroli dostępu (tzn. nie ogranicza się jedynie do wysłania komunikatu do operatora o włamaniu). Fałszywe alarmy mogą wtedy stać się powodem nieuzasadnionego odcięcia dostępu do zasobu.

Z drugiej strony interpretacją informacji o zdarzeniach wyglądających na włamanie powinien zająć się wyspecjalizowany personel świadomy zjawiska przyzwyczajenia, które często powoduje poczucie bezsensownej straty czasu, obniża morale zespołu. Przyzwyczajenie może doprowadzić do tego, że w razie rzeczywistego włamania ludzie nie zareagują adekwatnie do sytuacji.

Także z dużą rezerwą należy się odnieść do pomysłu dzielenia się informacjami o włamaniach przez systemy wykrywania włamań działające w różnych organizacjach. Abstrahując od zapewne różnych polityk bezpieczeństwa, a co za tym idzie definicji włamań, wiara w chęć bezpośredniego dzielenia się wiedzą o tego typu zdarzeniach może być w praktyce nierealizowalna. Dopiero analiza zdarzeń w specjalizowanych niezależnych zespołach wykrywania włamań i wydawanie „biuletynów" uczących systemy wykrywania włamań ma rację bytu.

Na koniec warto też wspomnieć o działaniu wspomagającym systemy wykrywania włamań – przykładem może być zastosowanie techniki typu *honeypot* („garnek z miodem", przynęta), czyli umieszczenie w sieci zasobu celem przyciągnięcia uwagi atakującego, z założeniem, że zasób może zostać skompromitowany. System wykrywania włamań monitorujący zasób jest w tym wypadku w mniejszym stopniu podatny na fałszywe alarmy - proporcje między atakami a normalnymi zdarzeniami ulegają zmianie na korzyść ataków.

5. Podsumowanie

Systemy wykrywania włamań w obecnej formie są ułomne, a ich praktyczne zastosowanie jako narzędzi automatycznych jest wątpliwe. Nie ulega wątpliwości, że do obsługi tych systemów i podejmowania decyzji jak zareagować na zdarzenie wyglądające na włamanie wymagany jest przeszkolony personel. Kłopotliwe wydaje się wykrywanie i definiowanie anomalii. Niejednoznaczność semantyczna wciąż umożliwia wprowadzanie omawianych systemów w błąd. W przypadku ruchu szyfrowanego, system wykrywania powinien stać się zaufaną trzecią stroną, jednak pojawia się tu ryzyko wycieku informacji, a więc osłabienia bezpieczeństwa całego systemu teleinformatycznego. Pułapka fałszywych alarmów – niska liczba prawdziwych włamań, w stosunku do podejrzanie wyglądających zdarzeń w sieci – prowadzi do niskiej wiarygodności detekowanych zdarzeń. Dodatkowo przyzwyczajenie ze strony personelu obsługującego może doprowadzić do zignorowania właściwego ataku.

Literatura

[Amoroso1999] E. Amoroso - *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response* - Intrusion.net, 1999

[Axelsson1999] S. Axelsson, - *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection* - Chalmers University of Technology, Second International Workshop on Recent Advances in Intrusion Detection, RAID'1999

[Ptacek1998] T. Ptacek, T. Newsham - *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection* - Secure Networks Inc., January 1998

[Schneier2000] B. Schneier - *Secrets & Lies: Digital Security in a Networked World* - John Wiley & Sons, Inc., 2000

[Schneier2001] B. Schneier - *The „Death" of IDS?* - Crypto-Gram, March 15, 2001