STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Grzegorz ŚLIWIŃSKI, Jerzy KOROSTIL
Politechnika Szczecińska, Wydział Informatyki

OKREŚLENIE BIEŻĄCEJ WARTOŚCI POZIOMU BEZPIECZEŃSTWA SIECI KORPORACYJNEJ

Streszczenie. W obecnym czasie występuje dość dużo różnych sposobów ochrony sieci korporacyjnej przed groźbą niepowołanej ingerencji w pracę na sieci. Przykładami takich sposobów mogą być: trasery sieciowe, systemu stwierdzające atak, środki przeciwdziałające atakom, inne specjalne środki ochrony[1] protokołów łączności. Środki te są ukierunkowane na wykonywanie odrębnych zadań w systemie bezpieczeństwa określonych sieci. Ich koszty są dość wysokie i dlatego nie każdy użytkownik sieci korporacyjnej może sobie pozwolić na ich nabycie i eksploatację.

DEFINING THE CURRENT VALUE OF SECURITY LEVEL IN CORPORATIVE NETWORK

Summary. Nowadays, there is a lot of different ways to secure corporate networks from some attacks. Good examples of such solutions can be network tracerouters, network attacks detection systems and preventives against such attacks and other special preventives of connections protocols. These elements are oriented for separated works in security system dedicated networks and because they are very expansive, not everyone can buy and use such a solution.

1. Wprowadzenie

Obecnie istnieje dość dużo sposobów ochrony sieci korporacyjnych przed niepowołaną ingerencją w pracę systemu. Ochrona ta to nie tylko zabezpieczenie przed niepowołanym dostępem do danych, ale również zapewnienie odpowiedniej jakości świadczenia usług w sieci. Coraz częstszym zagrożeniem systemów sieciowych jest doprowadzenie ich do stanu,

[1] Środek obrony – metoda, urządzenie lub program zabezpieczający system.

w którym są one całkowicie bezużyteczne, co świetnie określa definicja DoS[2] (Deny of Service). Należy również zwrócić uwagę na fakt, że wartość danych gromadzonych w pamięciach masowych może być nieadekwatna do wartości (kosztów) utraty tych danych lub wykorzystania ich poprzez niepowołane osoby.

Załóżmy, że można doprowadzić do stanu równowagi, gdzie stopień bezpieczeństwa systemu B(S) może być równy ryzyku pracy z systemem R(S). Równowaga taka oznaczać będzie, że system sieciowy (komputerowy) będący w takim stanie jest odpowiednio zabezpieczony w stosunku do zadań wykonywanych przez niego, które powinny być zabezpieczone przed niepowołanym dostępem do sieci [1].

$$B(S) = R(S) \tag{1}$$

Określmy również pewne współczynniki, które pozwolą na dokładniejsze przedstawienie zależności pomiędzy B(S) i R(S):

ξ - jako miara odporności (opisywana jako stosunek liczby prób zaburzenia systemu do czasu obsługi procesu klienta),

η - jako miara otwartości (opisywana zależnością części zasobu, które na moment t_i są stale dostępne, do całkowitej ilości posiadanych zasobów),

μ - możliwość przepustowości w jednym czasie (stosunek usług do całkowitego zapotrzebowania w czasie).

Zgodnie z zależnością (1) uwzględniając podane powyżej współczynniki: ξ, η i μ możemy rozpatrzyć taki system, który zachowa ten stan równowagi.

2. Definicja parametrów

2.1. Odporność systemu

Systemy komputerowe sieci korporacyjnych w chwili obecnej narażone są w sposób ciągły na próby zmiany stanu równowagi pomiędzy B(S) i R(S) poprzez różnego rodzaju nieuprawnione działania osób niepowołanych w tym systemie. Obecne korporacje nie mogą sobie pozwolić na ograniczanie czasowe dostępu do informacji poprzez zamykanie biur i wyłączanie serwerów o określonych porach oraz zamykanie swoich zasobów informatycznych przed klientem, w czasach kiedy działalność i wyniki korporacji kształtowane są przez prawa rynku.

Rozpatrzmy korporację, która udostępnia swoje strategiczne dane w sposób ciągły poprzez automatyczne usługi typu WWW, FTP, terminale itp. i jest otwarta dla klienta przez

[2] DoS (Deny of Service) – odmowa wykonania dostępu do usługi dla klienta spowodowana czynnikami zewnętrznymi.

większość dnia (załóżmy 12 godzin dziennie). Dobrym przykładem takiego działania może być praca uczelni.

W sytuacji takiej można dostrzec wiele zagrożeń i możliwości niepowołanego ingerowania w prawidłowe i bezpieczne działanie sieci korporacji. Z danych uzyskanych na podstawie bazy danych działania systemu monitorowania dostępu do zasobów informatycznych Wydziału Informatyki wynika, że np. stanowiska komputerowe Wydziału były użytkowane sumarycznie przez okres 806 dni 9 godzin i 44 minut (dane z działania w okresie od 20.03.2001 – 06.05.2001, wygenerowanych wpisów w bazie: 19 625, łączny czas w minutach: 1 161 224). W stosunku do pojedynczej maszyny daje to okres nieprzerwanego działania (24 godziny na dobę) średnio przez ponad 5 dni. W tym czasie do systemu sieciowego zalogowało się około 3 000 osób, gdyż tyle liczyła sieciowa baza użytkowników. W czasie tym zarejestrowano próby wpływania na QoS[3] oraz nieliczne (nieudane) próby złamania haseł, w tym administracyjnego.

Miarę odporności systemu można przedstawić za pomocą wzoru (2).

$$\xi = \frac{\sum_{i=0}^{n} k_i}{t(u)} \tag{2}$$

gdzie:

k_i – jednostkowa przewidywana próba niepowołanego dostępu,

t – czas obsługi danego procesu użytkownika u.

Przez stopień trwałości[4] środka obrony będziemy rozumieć ilość ataków, którym przeciwdziałać będzie rozpatrywany element obrony, w czasie obsługi przez użytkownika systemu zdalnego dostępu. Jak wynika z określenia (2), trwałość metody obrony może być określona na postawie badań eksperymentalnych albo w procesie eksploatacji. Jest oczywiste, że wartość początkowa tego parametru nie powinna być równa zeru. Dlatego przed włączeniem do systemu obrony oddzielnych elementów obrony każdy element powinien być poddany próbie na trwałość ilości zagrożeń. Naturalnie, w takich próbach należy symulować te zagrożenia, które są charakterystyczne dla systemu zdalnego.

2.2. Otwartość środków obrony

Fakt ten może zobrazować zależność (3), która mówi, że miarą otwartości środka obrony jest stosunek ilości otwartych komponentów środka obrony do ogólnej ilości ukrytych komponentów w danym środku obrony.

[3] QoS – Quality of Service – miara jakości i płynności dostarczanych usług.

[4] Trwałość – odporność w czasie, odporność na możliwe ataki.

$$\eta = \alpha * \sum_{i=1}^{n} \left(\frac{m}{M} \right)_i \tag{3}$$

gdzie:

m – ilość otwartych ukrytych komponentów,

M – całkowita ilość ukrytych komponentów,

i – ilość środków obrony,

α - współczynnik doprowadzenia stopnia otwartości środka obrony do jednostki pomiaru.

Największy system obrony składa się z rzędu oddzielnych podsystemów, które związane są ze sobą zgodnie z przestawionymi powyżej określeniami. Dlatego istnieją możliwości wykorzystania różnych środków obrony z jednego podsystemu do drugiego, zmieniając przy tym tajne komponenty. Doprowadza to do tego, że ten sam środek obrony, jeżeli wykorzystuje się go w różnych podsystemach ochranianego systemu, ma różny stopień otwartości. Ocena obciążających zdolności środków obrony jest ważną charakterystyką, o ile obciążenie tych środków jest jedną z szeroko stosowanych metod ataków [3].

2.3. Możliwość przeciążenia środków obrony

Obciążającą zdolnością elementów obrony informacji nazywa się wielkość charakteryzującą ilość usług, które mogą być przetwarzane środkami obrony w danym okresie czasu. Formalnie parametr ten będziemy określać poprzez następujący stosunek:

$$\mu = \frac{n * u_k}{\sum_{i=0}^{m} \left(z_i * t_i(u_k) \right)} \tag{4}$$

gdzie:

u_k – k-ta usługa,

n – ilość funkcjonalnych działań obsługi,

z_i – i-te zapotrzebowanie,

$t_i(u_k)$ – i-ty czas obsługi k-tej usługi

Niedostateczna możliwość przeciążenia może doprowadzić do większej wrażliwości na jakiekolwiek ataki spowodowane rozległymi możliwościami dostępu do k-tej usługi. DoS jest obecnie najpopularniejszą formą ataków na sieci korporacyjne. Obrona przed takimi rodzajami ataków w stosunku do sieci komputerowej nie może być prowadzona poprzez system sieciowy.

3. Gwarancja bezpieczeństwa

$$B(S) = \sum_{i=1}^{n} \xi_i + \sum_{j=1}^{m} \eta_j + \sum_{r=1}^{k} \mu_r \tag{5}$$

W celu przejścia do opisu gwarancji bezpieczeństwa należy w pierwszej kolejności przedstawić matematyczny obraz bezpieczeństwa systemu B(S) poprzez sumę cząstkową poszczególnych współczynników [1]. Przedstawia to wzór (5).

Pamiętając o założeniu (1) można zobrazować poziom gwarantowanego bezpieczeństwa G^*. Związane z tym wyliczenia kosztów utraty tajnych (niepublicznych) informacji przedstawimy za pomocą wskaźników zgodnych z B(S), czyli w zbliżonej jednostce miary. Wartość ryzyka R(S) dla każdego użytkownika, uzyskano na podstawie badań dotyczących liczby i rodzaju zagrożeń, które wystąpiły w sieciach korporacyjnych.

$$G^* = \min [\, B(S) - R(S) \,] \tag{6}$$

Jeżeli $G > G^*$, to poziom bezpieczeństwa jest zawyżony, jeżeli $G < G^*$, poziom ten jest niewystarczający. W rzeczywistych systemach zarządzanie bezpieczeństwem B(S), prowadzące do zmiany G (oprócz wymienionego powyżej przykładu) może polegać na zmniejszaniu czasu systemowego dla funkcjonowania środków wykrywania ataku, co prowadzi do podwyższenia efektywności systemu.

Celem możliwości zobrazowania poziomu gwarantowanego bezpieczeństwa doprowadzono przytaczane wcześniej współczynniki, które składają się na sumę (5), do wartości porównywalnych, i tak:

- Współczynnik ξ ze wzoru (2) ulega przekształceniu do ξ^*, gdzie jest on miarą rzeczywistego ξ przemnożonego przez stałą proporcjonalności celem ujednolicenia jednostki miary, jaką jest [%].
- Współczynnik η pozostaje w niezmienionej postaci, jego jednostką miary jest [%].
- Współczynnik μ ze wzoru (4) ulega przekształceniu do μ^*, gdzie jest on miarą rzeczywistego μ przemnożonego przez stałą proporcjonalności celem ujednolicenia jednostki miary, jaką jest [%].

$$B(S)^* = \sum_{i=1}^{n} \xi^*_i + \sum_{j=1}^{m} \eta_j + \sum_{r=1}^{k} \mu^*_r \tag{7}$$

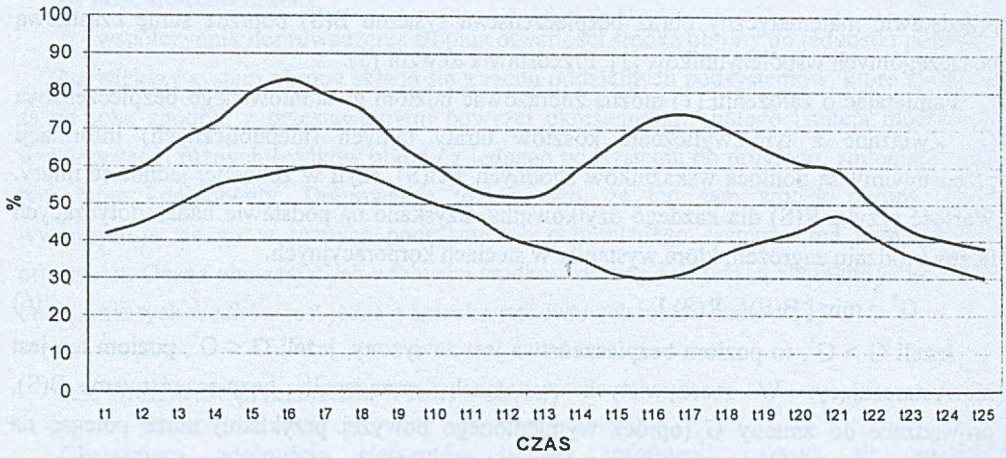
Wynikiem takiego działania będzie zmiana wzoru (5) do postaci zapisanej w zależności (7).

Po takich zmianach można przedstawić następujące dane (tabela 1), będące wynikiem obliczenia podanych wcześniej współczynników, które następnie posłużyły do obliczenia B(S)*.

Tabela 1

Zestawienie danych B(S)* i R(S)

Czas	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10	t11	t12	t13	t14	t15	t16	t17	t18	t19	t20	t21	t22	t23	t24	t25
B(S)*	57	60	67	72	80	83	79	75	66	60	54	52	53	60	67	73	74	70	65	61	59	50	43	40	38
R(S)	42	45	50	55	57	59	60	58	54	50	47	41	38	35	31	30	32	37	40	43	47	41	36	33	30



Rys. 1. Zależność B(S)* i R(S) w czasie
Fig. 1. Interdependence between B(S)* and R(S) in time

4. Podsumowanie

Określenie prawidłowych parametrów podanych powyżej jest procesem mocno złożonym, który zależy od wielu czynników. Uproszczenie podanych w toku rozumowania współczynników jest jednym ze sposobów na znalezienie punktu odniesienia do prawidłowego i zbilansowanego określenia stopnia zabezpieczeń, a następnie stopnia bezpieczeństwa. Głównym celem tej pracy było zobrazowanie problemu oraz przedstawienia pewnego rozwiązania tego problemu poprzez określenie parametrów strategicznych dla bezpieczeństwa dowolnego systemu sieciowego, co zostało przedstawione w tej pracy.

LITERATURA

1. Grzywaka A. (red.): Bezpieczeństwo systemów komputerowych. Wydawnictwo Pracowni Komputerowej Jacka Skalmerskiego, Gliwice 2000.
2. Robling Denning D. E.: Kryptografia i ochrona danych. WNT, Warszawa 1999.

3. Anderson R. J.: Security Engineering – A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, New York 2001.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 26 marca 2002 r.

Abstract

Nowadays, there is a lot of different ways to secure corporate networks from some attacks. Good examples of such solutions can be network tracerouters, network attacks detection systems and preventives against such attacks and other special preventives of connections protocols. These elements are oriented for separated works in security system dedicated networks and because they are very expansive, not everyone can buy and use such a solution.

This paper is written to show some possibilities of defining users' needs of data security, which are located on servers hard disks, and of sufficient security of network systems to satisfy the users. As a result of this paper author has determined the minimal security level that points the most menaced security element of a system and called it G^* (6) and approximately defined the time of a possible attack (Fig. 1.).

Publication of this work is the initial fragment of the doctorate, the main target of which is to find the algorithm of replacing users' needs with possible solutions of system's security (to secure their data) [3].

Additionally this paper defines few coefficients such as ξ (2), η (3) or μ (4), which allow fragmentarily describing possible critical points of securing corporate networks.