Jacek Wołoszyn

Bezpieczeństwo systemu informatycznego jako proces

Dydaktyka Informatyki 10, 160-165

2015

Dydaktyka Informatyki 10(2015)
ISSN 2083-3156
DOI: 10.15584/di.2015.10.19
http://www.di.univ.rzeszow.pl

Wydział
Matematyczno-Przyrodniczy UR
Laboratorium Zagadnień
Społeczeństwa Informacyjnego

Jacek WOŁOSZYN

Dr inż., Uniwersytet Technologiczno-Humanistyczny w Radomiu, Wydział Informatyki i Matematyki, Katedra Informatyki, ul. Malczewskiego 29, 26-600 Radom; jacek@delta.pl

BEZPIECZEŃSTWO SYSTEMU INFORMATYCZNEGO JAKO PROCES

SECURITY SYSTEM AS A PROCESS

Słowa kluczowe: bezpieczeństwo systemu, firewall, identyfikacja, szyfrowanie.
Keywords: system security, firewall, identification, encryption.

Streszczenie

Niniejszy artykuł stanowi krótkie wprowadzenie w zagadnienia bezpieczeństwa danych w systemach komputerowych. Zagadnienia te stanowią ważny element polityki bezpieczeństwa. Zwrócono szczególną uwagę na aspekt bezpieczeństwa do informacji elektronicznej jako procesu.

Summary

This article provides a brief introduction to data security in computer systems. These issues are an important part of security policy. Special attention was paid to the security aspect of electronic information as a process.

Wprowadzenie

Posiadanie informacji stało się jednym z najważniejszych celów we współczesnej globalnej gospodarce. Szybkie przemiany, nowoczesna technologia sprzyja wzrostowi konkurencji. Aby stanowić konkurencję trzeba działać szybciej i posiadać wiedzę, która daje możliwość uzyskania przewagi. Wcześniej wprowadzony produkt do sprzedaży, czy pozyskanie wyników kosztownych badań to duży krok do przodu, który zapewne będzie się przekładał na oczekiwane efekty finansowe.

Nowoczesne metody transmisji[1] oraz systemy sieciowe ułatwiają nie tylko wymianę informacji, ale także bardzo efektywne jej poszukiwanie, przetwarzanie i dystrybucję. Przy tak rozwiniętej sieci telekomunikacyjnej bezpieczeństwo przesyłania informacji jest istotne i niezbędne do prawidłowego, bezpiecznego funkcjonowania usług sieciowych.

1. Ochrona informacji

Sposób, w jaki traktowano zabezpieczenia informacji i dóbr na przestrzeni czasu bardzo się zmienił, podobnie jak ewoluowała cała technologia.

Zabezpieczanie informacji nie gwarantuje bezpieczeństwa firmy, czy systemów komputerowych, ponieważ nie może samo w sobie i samo z siebie zapewnić ochrony. Ustalając politykę bezpieczeństwa dla firmy należy rozważyć wszystkie możliwe zagrożenia[2], nie tylko elektroniczne. Zapewniając ochronę należy użyć prewencyjnie cały wachlarz dostępnych urządzeń, wiedzy i rozwiązań celem likwidacji słabych punktów w systemie. Doświadczenia wskazują, że żaden pojedynczy produkt nie może zapewnić firmie dobrego zabezpieczenia, ponieważ niezbędne są różne produkty o różnych typach działania, aby ochronić dobra informacyjne.

2. Bezpieczeństwo danych w systemie komputerowym jako proces

Jedną z części dobrego programu bezpieczeństwa jest program antywirusowy. Jest on przydatny i jeśli zostanie prawidłowo wprowadzony do użytku oraz skonfigurowany, ma możliwość znacznego zredukowania działania złośliwych programów i skryptów w systemie komputerowym. Skanuje jego zasoby, a także w wielu przypadkach aktywnie reaguje na próby nieautoryzowanego dostępu. Takie oprogramowanie chroni jednak wyłącznie przed złośliwymi programami, a nie przed osobami używającymi legalnego programu w celu uzyskania dostępu do systemu. Rozwiązanie to nie chroni również przed użytkownikami uprawnionymi, chcącymi uzyskać dostęp do plików, które są prawnie dla nich niedostępne.

[1] J. Faircloth, *Penetration Tester's Open Source Toolkit*, Syngress 2011; K.R. Fall, W.R. Stevens, *TCP/IP od środka. Protokoły*, wyd. II, Helion, Gliwice 2013; R. Stevens, *TCP/IP Illustrated Volume 1*, Pretence Hall 2010.

[2] J.C. Huang, *Software error detection*, Wiley 2009; Ch. McNab, *Network Security Assessment*, O'Reilly 2007.

Dlatego też konsekwencją tego systemy komputerowe[3], które funkcjonują w firmie powinny posiadać możliwość ochrony plików przy pomocy identyfikacji użytkownika, który chce uzyskać do nich dostęp. W przypadku, gdy system jest prawidłowo skonfigurowany i uprawnienia plików są odpowiednio ustawione wówczas kontrola dostępu do systemu zapewnia hierarchiczny autoryzowany dostęp. Atak może wyglądać dla systemu kontroli dostępu tak samo jak działanie uprawnionego administratora, który chce się dostać do plików, do których posiada dostęp.

Ochronę wewnętrznej sieci firmy powinny również wspomagać firewalle[4], zwane też zaporami ogniowymi. Są to urządzenia sieciowe kontroli dostępu i mają za zadanie chronić sieci przed atakami z zewnątrz. Firewalle funkcjonują na granicy sieci wewnętrznej oraz zewnętrznej, czyli są one produktami bezpieczeństwa granicznego, a odpowiednia konfiguracja zapewnia poważne utrudnienie w przypadku nieautoryzowanego dostępu do systemu. Firewall nie ma możliwości powstrzymania osób, które chcą zaatakować system przed wykorzystaniem uprawnionego połączenia. Jeśli więc konfiguracja firewalla zezwala na dostęp z zewnątrz, to system jest narażony na atak Firewall nie ma także możliwości ochronienia firmy przed wewnętrznym użytkownikiem, ze względu na to, że użytkownik ten jest już w wewnętrznej sieci i jego transmisja nie podlega kontroli. Firewall[5] to nic innego jak filtr pakietów, który odpowiednio skonfigurowany zezwala na przepuszczenie pakietów spełniających reguły i odrzucenie pakietów niespełniających reguł.

W przeszłości i obecnie w celu identyfikacji danej osoby przez system komputerowy używano haseł. Identyfikacja osoby może opierać się na kombinacji czegoś, co się zna, co się ma lub czymś się jest. Hasło było więc tu czymś co się zna. Jednak okazało się, że nie jest dobrym sposobem, aby polegać na czymś, co się zna. Hasła do sytemu mogą również być przez użytkowników zapisane, czy też odgadnięte przez inne osoby.

Aby zaradzić takim sytuacjom zaczęły pojawiać się coraz to nowsze metody identyfikacji użytkowników. Oparte były one na tym, co się ma bądź na tym, czym się jest. Wówczas do identyfikacji można było używać elektronicznych kart identyfikacyjnych. Dzięki nim ryzyko odgadnięcia hasła przez osoby trzecie było mniejsze. Jednak dużym ryzykiem jest zagubienie karty, ponieważ wtedy intruz może podszyć się pod legalnego użytkownika systemu. W tej sytuacji nie

[3] E. Nemeth, G. Snyder, R. Trent, H. Whaley, *Ben Unix and Linux system administration handbook fourth edition*, Pretence Hall 2010; R. Pinkal Pollei, *Debian 7 System Administration Best Practices*, Packt 2013.

[4] Ch. Negus, *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012; M. Rash, *Linux firewalls Attack Detection and Response with iptables, psad, and fwsnort*, No Starch Press 2007.

[5] M. Rash, *Linux firewalls...*

ma możliwości, aby zapobiec atakowi za pomocą systemu elektronicznej identyfikacji, gdyż polega ona głównie na skorzystaniu przez użytkownika z właściwej ścieżki dostępu do systemu komputerowego.

Kolejnym mechanizmem identyfikacji są dane biometryczne. Przyczyniają się one również do obniżenia ryzyka odgadnięcia hasła przez osoby trzecie. Również w tym przypadku, aby ten mechanizm był skuteczny to uzyskanie dostępu do systemu musi być uzależnione od skorzystania z właściwej ścieżki dostępu. Jeśli ktoś potrafi znaleźć sposób, aby obejść system danych biometrycznych wówczas ta metoda nie umocni w żaden sposób zabezpieczenia.

Głównym punktem dla dobrego programu zabezpieczeń jest strategia bezpieczeństwa firmy wraz z odpowiednimi procedurami oraz właściwe zarządzanie nimi na poziomie różnych systemów komputerowych[6]. Firma, która posiada system zarządzania strategią może być świadoma systemu niepodporządkowującego się. Jednak takie zarządzanie strategią może nie obejmować błędnego skonfigurowania oprogramowania użytkowego lub słabych punktów występujących w systemie. Czynniki te mogą być przyczyną udanego włamania do systemu. Takie zabezpieczenie również nie jest gwarancją tego, że użytkownicy tego systemu nie będą zapisywać swoich haseł, czy też udostępniać je osobom trzecim co w konsekwencji doprowadzi do włamania.

Istotnym czynnikiem dobrego programu zabezpieczeń jest przeszukiwanie systemów komputerowych na okoliczność wystąpienia słabych punktów. Pomaga to w ustaleniu potencjalnych furtek w systemie dla włamywaczy. Tropienie słabych punktów nie ochroni jednak systemów całkowicie, ale znacznie je wzmacnia. Powinny po wykryciu być natychmiast skorygowane.

Szyfrowanie należy do podstawowego mechanizmu zabezpieczenia komunikacji. Treść transmisji szyfrowanej, czy też zapisane w takiej postaci pliki są bezużyteczne dla intruza, chyba że zna on klucz, za pomocą którego można przechwycone pliki przywrócić do postaci jawnej. Aby mieć możliwość korzystania z szyfrowania trzeba pamiętać, że użytkownicy muszą posiadać dostęp do tych plików i kluczy.

3. Możliwe scenariusze zagrożeń

Atak na system komputerowy firmy może być wyrządzony przez przypadek bądź z premedytacją. Niezależnie od tego, jakie będą przyczyny ataku to firma ponosi straty z tego powodu. Atak na system komputerowy może być przeprowadzony przy pomocy środków technicznych lub inżynierii społecznej, które polega na użyciu nietechnicznych metod uzyskania autoryzowanego dostępu

[6] G. Stepanek, *Software Project Secrets*, Apress 2012.

bądź wejścia na teren firmy podając się np. za pracownika. To właśnie ten typ ataku może być najbardziej niebezpieczny. Występują również ataki na informację w formie elektronicznej. Są one dość specyficzne głównie z tego względu, że ich cechą jest to, że tych informacji się nie kradnie, a tylko kopiuje. W tej sytuacji osoba trzecia może dostać się do danych, podczas, gdy pierwotny właściciel tych informacji nie traci. Taki atak jest dość trudny do wykrycia, ponieważ nie ma żadnych przesłanek, że ktoś posiada kopię informacji.

Można wyróżnić cztery kategorie ataków: Dostęp (ang. *Access*), Modyfikacja (ang. *Modification*), Pozbawienie usługi (ang. *Denial of service*), Zaprzeczenie (ang. *Repudiation*).

Atak dostępu polega na zdobyciu informacji, do których atakujący nie ma uprawnień. Może on być przeprowadzony na miejsce przechowywania informacji lub podczas jej transmisji. Istnieje również węszenie, które polega na przeglądaniu informacji w systemie w celu znalezienia czegoś interesującego. Osoba, która się włamuje przegląda pliki po kolei, aż do momentu znalezienia informacji, którą chce uzyskać. Można także zdobyć informację poprzez podsłuchiwanie rozmowy nie biorąc w niej czynnego udziału. Intruz chcąc przechwycić informację może „podsłuchiwać" sesję komputera roboczego, który podłączony jest do tej samej sieci lokalnej. Jest możliwe również przechwycenie informacji, które jest aktywnym atakiem. Przechwycenie następuje, gdy osoba trzecia umieszcza siebie na drodze przepływu informacji i wyłapuje ją zanim ona jeszcze dotrze na miejsce przeznaczenia. Ataki dostępu mogą być w różnej formie, w zależności głównie od tego czy informacja przechowywana jest w formie papierowej czy elektronicznej. Jeśli dana informacja jest w formie papierowej to można ją znaleźć m.in.: w szafach, w faksach, w drukarkach, na biurkach czy nawet w śmieciach. Szafki w firmie mogą być niezamknięte przez pracowników na noc, faksy czy drukarki zazwyczaj są w miejscach publicznych i często w nich są pozostawione informacje. W koszach na śmieci również mogą znajdować się cenne informację, ponieważ codziennie kosze nie są opróżniane. Zamykanie szafek na klucz może być w jakimś rodzaju środkiem ostrożności, jednak włamywacz może w szybki sposób je otworzyć. Aby mieć dostęp do informacji w tej formie włamywacz musi mieć dostęp fizyczny do tych miejsc, w których może je znaleźć. Może on być pracownikiem firmy lub może mieć od kogoś dostęp do pomieszczeń biurowych, w których być może będą przechowywane dokumenty. Dostęp do dokumentacji może być niemożliwy w sytuacji, gdy firma je przechowuje poza siedzibą. W przypadku zapisu informacji elektronicznej może być przechowywana na: pojedynczych komputerach, serwerach, komputerach przenośnych dyskach, dyskach optycznych, pamięci masowej czy backupie. W większości tych przypadków poprzez fizyczną kradzież nośników można uzyskać dostęp do informacji i taki sposób może być dużo łatwiejszy w porównaniu z dotarciem do plików elektronicznych na terenie firmy. W sytuacji, gdy osoba trzecia posiada uprawnienia

do systemu może przeglądać informację poprzez otwarcie plików. W celu wyeliminowania takiej sytuacji powinny być właściwie ustawione uprawnienia kontroli dostępu by osoba nieuprawniona nie miała do nich dostępu, a próby dotarcia do nich powinny być zarejestrowane w logach. Eliminacja wszystkich słabych punktów w systemie informatycznym jest procesem długotrwałym i tylko ciągły monitoring pozwoli na efektywną eliminację takich zagrożeń.

Wnioski

Całkowite bezpieczeństwo systemów komputerowych jest procesem składającym się z wielu płaszczyzn. Zastosowanie doskonałej konfiguracji monitorującej wszystkie ruchy nieautoryzowanego dostępu przez nieuprawnionych użytkowników nie rozwiązuje problemu. Pozostaje kwestia stosowania metod socjotechnicznych i słabości ludzkich, jak również klasycznego dostępu fizycznego do zasobów.

Całkowite bezpieczeństwo, o ile w ogóle takie istnieje, polega na procesie, a nie na pojedynczych produktach. Nie można używać tylko jednego typu ochrony dla zapewnienia dostępu do zasobów informacji firmy. Skuteczne zabezpieczenie systemu składa się z wielu typów produktów, by właściwie ochronić system przed osobami trzecimi i nieustannie monitorować stan poziomu bezpieczeństwa. Nadzór nad całością powinna sprawować zaufana osoba zwana netofficerem lub w przypadku dużych przedsiębiorstw odpowiednia komórka podlegająca bezpośrednio pod zarząd.

Bibliografia

Faircloth J., *Penetration Tester's Open Source Toolkit*, Syngress 2011.

Fall K.R., Stevens W.R., *TCP/IP od środka. Protokoły*, wyd. II, Helion, Gliwice 2013.

Huang J.C, *Software error detection*, Wiley 2009.

McNab Ch., *Network Security Assessment*, O'Reilly 2007.

Negus Ch., *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012.

Nemeth E., Snyder G., Trent R. Whaley H., *Ben Unix and Linux system administration handbook fourth edition*, Pretence Hall 2010.

Pollei Pinkal R., *Debian 7 System Administration Best Practices*, Packt 2013.

Rash M., *Linux firewalls Attack Detection and Response with iptables, psad, and fwsnort*, No Starch Press 2007.

Stepanek G., *Software Project Secrets*, Apress 2012.

Stevens R., *TCP/IP Illustrated Volume 1*, Pretence Hall 2010.