PORADNIKI

Przygotowanie sieciowych zasad bezpieczeństwa

I.Wprowadzenie

Świat komputerów zmienił się przez ostatnie 25 lat. Dwadzieścia pięć lat temu większość komputerów była scentralizowana i zarządzana w centrach danych. Komputery były trzymane w zamkniętych pokojach. Zagrożenia bezpieczeństwa komputerów były rzadkie i zasadniczo były związane z problemami wewnętrznymi. Zagrożenia te były dobrze zrozumiane i uporano się z nimi standardowymi technikami: komputery za zamkniętymi drzwiami i rozliczanie wszystkich zasobów. Dwadzieścia pięć lat później, wiele systemów jest połączonych z Internetem. Internet jest dużą siecią i nie ma granic. Biznes odczuwa coraz większe zapotrzebowanie na łączenie z Internetem aby wykorzystywać biznesowe okazje. Systemy bezpieczeństwa dla systemów dla połączeń internetowych są bardzo różne. Informacja w internecie może być dostępna z dowolnego miejsca na świecie w czasie rzeczywistym. Chociaż jest to dobre dla rozprzestrzeniania się informacji, pozwala również na rozprzestrzenianie się "złośliwych informacji" Narzędzia hackerskie są teraz szeroko dostępne w internecie. Niektóre strony WWW dostarczają nawet poradników jak hackować systemy, podając szczegóły słabości różnego rodzaju systemów. Nie potrzeba być programistą ekspertem aby włamać się do systemu. Każdy ze złymi intencjami może przeszukać internet pod kątem programów łąmiących system, który nie jest właściwie zabezpieczony. Jest zatem istotne dla firm aby ich połączenia intenetowe były odpowiednio zabezpieczone. Jest ważne zminimalizowanie ryzyka włamania zarówno ze strony wewnętrznej jak i z zewnątrz. Sieć z dobrym rozliczaniowymi i audytowanym systemem będzie zapewniała ,że wszystkie działania są rejestrowane aby wykrywać nieuprawnione działania.

II.Potrzeba zasad bezpieczeństwa sieciowego

Zanim zabezpieczymy sieć, musimy ustalić zasady bezpieczeństwa sieci. Zasady bezpieczeństwa sieci definiują oczekiwania organizacji co do właściwego używania komputera i sieci i procedur do zapobegania i reakcji na incydenty. Zasady bezpieczeństwa sieci są podstawą bezpieczeństwa ponieważ wymienia jakie aktywa są warte ochrony i jakie działania lub zaniechania zagrożą tym aktywom. Zasada rozważy ewentualne zagrożenia w stosunku do wartości osobistej produktywności i skuteczności oraz identyfikacji różnych zasobów korporacyjnych, które wymagają różnych poziomów ochrony. Bez zasad bezpieczeństwa sieci, nie można określić ram bezpieczeństwa .Pracownicy którzy nie będą stosować się do ustalonych standardów i kontroli bezpieczeństwa będą blokowani ze względu na wzrost produktywności. Zasady bezpieczeństwa sieci powinny być zakomunikowane każdemu kto używa sieci komputerowej, pracownicy lub zleceniobiorcy.

1.3 Ryzyko związane z podłączeniem do sieci

Przed ustanowieniemzasad bezpieczeństwa sieci,musimy przestudiować analizę ryzyka. Analiza ryzyka jest to proces identyfikacji jakiej potrzebujesz ochrony, czego potrzebujesz do jej ochrony i jak ją chronić. Jest to proces badania całego ryzyka, rankingu tych ryzyk przez poziom ciężkości. Dobrym sposobem oceny ryzyka związanego z łącznością sieciową jest najpierw ocenić jakie zaosby są warte ochrony i w jakim stopniu te zasoby powinny być chronione. Co do zasady, koszt ochrony poszczególnych zasobów nie powinien być większy niż samo aktywo. Szczegółowa list wszystkich aktywów, która obejmuje zarówno przedmioty materialne, takie jak serwery i stacj robocze, jak i niematerialne, takie jak oprogramowanie i dane, powinny być stworzona. Muszą być zidentyfikowane katalogi przechowujące poufne lub krytyczne pliki. Po zidentyfikowaniu tych zasobów, określenie ile kosztuje zastąpienie każdego zasobu, musi być priorytetem na liście zasobów. Kiedy zidentyfikowano aktywa wymagające ochrony, konieczna jest identyfikacja zagrożeń dla tych zasobów. Zagrożenia mogą być potem badane pod kątem określenia istnienia ryzyka utraty danych. Przykładami zagrożeń mogą być:

- Nieautoryzowany dostęp / użycie zasobów (uwierzytelnienie)
- Denial of Service (dostępność)

- Wyciek informacji (poufność)
- Zniekształcenie / nieautoryzowana zmiana danych (integralność)
- Klęski żywiołowe

Dokładna ocena ryzyka będzie najbardziej wartościowym narzędziem w kształtowaniu polityki bezpieczeństwa sieci. Dokładna analiza ryzyka wskazuje zarówno na najbardziej wartościowe jak i najsłabsze aktywa. Zasady bezpieczeństwa mogą ustalić skupienie się na środkach bezpieczeństwa które mogą identyfikować te zasoby.

1.4 Elementy zasad bezpieczeństwa sieciowego

Chociaż zasady bezpieczeństwa sieci są subiektywne i mogą być bardzo różne dla różnych organizacji,są pewne kwestie, które są istotne w większości zasad. Ta częśćwyjaśni niektóre wspólne elementy zasad bezpieczeństwa sieci.

Bezpieczeństwo Fizyczne

Bezpieczeństwo sieci współgra z bezpieczeństwem fizycznym ponieważ rozmiar lub kształt "maszyny" sieciowej lub jednostki może obejmować budynek, kampus, kraj lub świat ze względu na wzajemne powiązania i relacje zaufania. Bez fizycznego bezpieczeństwa,pozostałe składniki bezpieczeństwa sieciowego takie jak poufność, dostępność czy integralność byłyby bardzo zgrożone. Bezpieczeństwo fizyczne stanowi o tym jak wyposażenie czy sprzęt powinny być chronione. Definiuje również jacy pracownicy powinni mieć dostęp do ograniczonych obszarów takich jak serwerownie czy powieszczenia z okablowaniem.

Bezpieczeństwo Sieci

Bezpieczeństwo sieci stanowi jak aktywa przechowywane w sieci będą chronione. Może obejmować środki bezpieczeństwa dotyczące kontroli dostępu, firewall, kontroli sieci, zdalnego dostępu do usług katalogowych, usługi internetowe, oraz struktury systemu plików w katalogu.

Kontrola Dostępu

Kontrola dostępu określa kto ma dostęp do czego. Musi być właściwa procedura aby zapewnić ,że tylko uprawnione osoby mają dostęp do uprawnionych dokumentów lub usług. Dobra kontrola dostępu obejmuje zarządzanie zdalnym dostępem i pozwala administratorom na wydajną pracę. Nie powinno być to tak złożone aby nie było podatne na błędy.

Uwierzytelnianie

Uwierzytelnianie to sposób w jaki użytkownik mówi sieci kim jest. Używany typ uwierzytelniania różni się w zależności od tego gdzie użytkownik jest uwierzytelniany. Z komputera osobistego, prosta nazwa użytkownika i hasło mogą być wystarczające ze względu na towarzyszące bezpieczeństwo fizyczne. Kiedy łączymy się z Internetem, może być konieczne bardziej bezpieczne, 2 czynnikowe uwierzytelnianie (autoryzacja z tokenem)

Szyfrowanie

Szyfrowanie może zapewnić integralność danych lub ochronę wrażliwych informacji wysyłanych przez niezbezpieczone linie. Takie zabezpieczenie jest zazwyczaj niezbędne dla zdalnego dostępu do ważnych aktywów lub dodatkowej ochrony kiedy używamy intranetu firmowego

Zarządzanie kluczami

Klucze są wykorzystywane do szyfrowania i deszyfrowania danych. Poważną kwestią przy szyfrowaniu jest zarządzanie kluczami. Właściwa zasada musi być ustanowiona, rozwiązując kwestię ,jak będzie to wpływać na skuteczność szyfrowania.

1) Długość klucza – jak długi

2) Zmiana klucza – jak często
3) Przechowywanie klucza – mieć lub nie mieć, jeśli tak, to jak
4) Generowanie klucza – kto , jak
5) Dystrybucja klucza – kto , jak

Zastosowanie
Zastosowanie wyjaśnia jak wymusić aby zasady bezpieczeństwa sieci były zrobione. Może również stanowić o metodzie jaka będzie użyta do zbadania naruszeń zasady. W tym miejscu można również podać kary za naruszenie zasad.

Audyt i weryfikacja
Kiedy zasady bezpieczeństwa zostaną zaimplementowane, trzeba sprawdzić aby upewnić się,że wszystkie elementy i pacownicy są zgodni. Bez wystarczającej kontroli, organizacje mogą nie mieć mocy prawnej odwołania jeśli nastąpi naruszenie bezpieczeństwa. Audyt może również zidentyfikować problemy przed tym nim wystąpi naruszenie bezpieczeństwa. Zasady muszą również być weryfikowane regularnie aby upewnić się ,że są jeszcze istotne.

Świadomość bezpieczeństwa
"Ciemni użytkownicy to szeroko rozpoznana grupa najpoważniejszego zagrożenia bezpieczeństwa sieci. Jeśli pracownicy nie zrozumieją ,siły i właściwego korzystania z sieci,mogą niechcący narazić na szwank bezpieczeństwo. W szczególności, pracownicy muszą odpowiednio zarządzać hasłem i być odporni na ataki "social engineering".

Reagowanie na incydenty i plan awaryjny po awarii
Organizacja jest najbardziej narażona kiedy wykryje intruza lub kiedy mamy do czynienia z katastrofą.Co się wydarzy w ciagu kliku minut i godzin może określić ile miliardów dolarów własności intelektualnej podlega zwrotowi. Plan awaryjny po katastrofie wyjaśnia jak organizacja będzie odzyskiwała siły po wszelkiego rodzaju klęsce żywiołowej lub atakach, w tym ze strony hackerów i pracowników. Na przykład może on zawierać środki bezpieczeństwa do tworzenia kopii zapasowych serwerów, określające, jak często kopie zapasowe muszą być wykonywane i jak kopie zapasowe muszą być przechowywane poza miejscem pracy. Może również zawierać listę członków zespołu reagowania kryzysowego,któy zajmuje się klęską żywiołową i atakami. Dodatkowo, plan może zawierać środki bezpieczeństwa dla prowadzenia ćwiczeń aby upewnić się ,że wszyscy użytkownicy i pracownicy wiedzą co robić w przypadku klęski lub ataku.

Akceptowalne zasady użytkowania
Akceptowalne zasady użytkowania stanowią jak użytkownicy będą mogli używać zasobów sieciowych. Na przykład, mogą opisywać typy informacji jakie mogą być zawarte w wiadmościach e-mail i wyjaśniać kiedy wiadomość e-mail musi być szyfrowana. Może również rozwiązywać kwestie takie jak czy lub nie użytkownicy mogą grać w gry lub używać zasobów takich jak e-mail i dostęp do Internetu dla osobistego użytku.

Oprogramowanie bezpieczeństwa
Oprogramowanie bezpieczeństwa wyjaśnia jak oganizacja będzie używała komercyjnego i niekomercyjnego oprogramowania na serwerach, stacjach roboczych i sieci. Może również identyfikować kto może kupować i instalować oprogramowanie i środki bezpieczeństwa dla ściągania oprogramowania z Internetu.

1.5 Kroki w celu opracowania zasad bezpieczeństwa sieci

Cel
Przed rozpoczęciem pracy nad zasadami, musimy zdefiniować wyraźne cele zasad. Zapewni to ,że

zasady nie odbiegną od pierwotnego celu. Cele definiują podejście do bezpieczeństwa sieci. Typowym celem może być to ,że informacja jest ważnym zasobem i że organizacja będzie implementował środki bezpieczeństwa do ochrony tego zasobu.

Zakres
Zakres definiuje zasoby, które będą chronione przez zasady bezpieczeństwa sieci. Bezpieczeństwo sieci może pokrywać szeroki zakres kwestii od bezpieczeństwa sieci przez bezpieczeństwo osobiste so bezpieczeństwo proceduralne. Zakres może definiować czy zasady obejmują tylko bezpieczeństwo sieciowe lub obejmują inne obszary bezpieczeństwa. Zakes również definiuje kto musi postępować według zasad bezpieczeństwa sieci.Czy zasady te obejmują tylko pracowników? Czy też polityka obejmuje kontrahentów, klientów i dostawców, którzy mogą być zobowiązani do przestrzegania zasad, jeśli zostanie podłączone do sieci organizacji?

Wsparcie ze strony wyższego kierownictwa
Po zdefiniowaniu zakresu i celu. Wsparcie powinno przyjść ze strony zarządzających wyższego szczebla zanim przystąpi się do projektowania zasad. Bez wsparcia wyższej kadry będzie bardzo trudno zapewnić zgodność zasad bezpieczeństwa sieci. Jeśli to możliwe,komitet bezpieczeństwa powinien również objąć zarządzających wyższego szczebla

Odniesienia do innych zasad
Aby wiedzie jak powinny wyglądać zasady bezpieczeństwa sieci. Mogą byś stworzone odniesienia do innych zasad. Pomaga to również rdefiniować zakres i cele zasad.

Ocena ryzyka
Przed rozpoczęciem zapisywania zasad, powinna być wykonana ocena ryzyka. Oceny ryzyka będą określać jakie kwestie należy rozwiązać. Sprawozdanie z oceny ryzyka będzie cennym narzędziem w kształtowaniu polityki bezpieczeństwa sieci.

Określenie elementów i zapisywanie zasad
Powinny być określowne elementy Zasad Bezpieczeństwa . To będzie uzależnione od sprawozdania oceny ryzyka. Nie wszystkie elementy muszą być zawarte. Zależą od struktury sieci, położenia i struktury organizacji. Zasady powinny dotyczyć wszystkich stanów ryzyka w sprawozdaniu oceny ryzyka. W przypadku pewnych zgrożeń które nie mogą być rozwiązane, powinny być odnotowane.

Ocena
Po zaprojektowaniu zasad, powinna zostać dokonana ocena zasad aby przekonać się czy cele zostały osiągnięte.Nietóre z pytań jakie należy uwzględnić:

1) Czy zasady są zgodne z prawem i obowiązkami osób trzecich?
2) Czy zasady narażają na szwank interes pracowników, organizacji lub osób trzecich?
3) Czy zasady są praktyczne, realne i mogą być egzekwowane?
4) Czy zasady wypełniają wszystkie formy komunikacji i prowadzenia dokumentacji wewnątrz orgranizacji
5) Czy zasady zostały właściwie przedstawione i zatwierdzone przez wszystkie zainteresowane strony?