11. Procedura zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. Zabezpieczenie sprzętowe

1. Na styku sieci lokalnej z internetem powinny być zainstalowane firewall.
2. Firewall powinien mieć możliwość zdefiniowania wielu różnych zestawów reguł określających jaki ruch powinien być przez firewall przepuszczany a jaki blokowany.
3. Wszystkie komputery znajdujące się w sieci powinny znajdować się za firewall-em.
4. System informatyczny powinien być wyposażony w podstawowe usługi sieciowe (DHCP, DNS, SNMP, NTP)
5. Sieć lokalna powinna wykorzystywać serwer proxy umożliwiający filtrowanie URL dla wszystkich lub wybranych grup użytkowników definiowanych przez ASI.
6. Administracja firewall-em i serwerem proxy powinna odbywać się z wykorzystaniem konsoli konfiguracyjnej.

2. Zabezpieczenie programowe

1. Każda stacja robocza lub serwer podłączony do sieci komputerowej w CUWO i posiadający dostęp do internetu musi posiadać aktualne oprogramowanie antywirusowe oraz zaporę sieciową.
2. Oprogramowanie antywirusowe oraz zapora sieciowa muszą posiadać automatyczną aktualizację z sieci internet lub z lokalnego repozytorium.
3. Oprogramowanie antywirusowe powinno wykrywać poza wirusami jak największą liczbę złośliwych programów innego rodzaju (np. konie trojańskie, backdoory, exploity, niebezpieczne aplety Javy i ActiveX, spam, itp.). Ponadto powinno charakteryzować się dobrymi narzędziami do analizy heurystycznej, skanowaniem na żądanie całości systemu, bądź jego elementów, skanowaniem w czasie rzeczywistym i niskim obciążeniem systemu.
4. Oprogramowanie antywirusowe powinno posiadać funkcję automatycznego powiadamiania o wystąpieniu incydentu (np. pojawieniu się wirusa w poczcie, próby włamania do systemu, itp.), a także powinno monitorować system on-line i reagować na bieżąco na wszelkie incydenty wg stawionych przez ASI reguł.
5. Oprogramowanie antywirusowe powinno automatycznie sprawdzać wszelkie podłączane do systemu urządzenia.
6. Oprogramowanie antywirusowe oraz zapora sieciowa powinny być w języku polskim.
7. Administrator Danych Osobowych ma obowiązek przeznaczyć odpowiednie środki finansowe na bezpieczeństwo systemu informatycznego.

DOKUMENTACJA TYLKO DO UŻYTKU WEWNĘTRZNEGO - WSZELKIE KOPIOWANIE TYLKO ZA ZGODĄ DYREKTORA

3. Obowiązki ASI

1. ASI odpowiada za :
    a) za aktualizację oprogramowania i jego baz na serwerach oraz lokalnych repozytoriach.
    b) właściwą konfigurację oprogramowania antywirusowego oraz zapory sieciowej blokując wszystkie porty w zaporze sieciowej zezwalając tylko na komunikację aplikacji niezbędnych do pracy danemu Użytkownikowi
    c) przeglądania i zabezpieczenia elektronicznie logów oprogramowania antywirusowego oraz zapory sieciowej.
    d) przeszkolenie użytkowników mających w swoim zakresie obowiązków zabezpieczanie antywirusowe obsługi oprogramowania antywirusowego.
2. ASI ma obowiązek niezwłocznego reagowania na wszelkie powiadomienia o wystąpieniu incydentu, związanego z zainstalowanym oprogramowaniem antywirusowym i zaporą sieciową. zobowiązany jest podjąć właściwe działania dla danej sytuacji
3. IOD po otrzymaniu zgłoszenia o wystąpieniu incydentu od ASI i po zapoznaniu się ze sprawą, w wyniku której doszło do utraty (kradzieży)
4. ASI ma prawo wyłączyć użytkownikom mechanizm przeglądania i wysyłania treści wiadomości w formacie HTML w przeglądarce poczty. W przeglądarkach internetowych ma prawo ograniczyć możliwości otwierania się różnego rodzaju skryptów.
5. ASI jest zobowiązany do sporządzania zestawu programów freeware akceptowalnych w sieci przez niego zarządzanej.
6. ASI ma obowiązek odnotowywania w elektronicznym dzienniku wszelkich incydentów, w wyniku których doszło do utraty/kradzieży danych lub innego przestępstwa, a także niezwłocznego zgłaszania tego faktu IOD. Ponadto administrator ma obowiązek zabezpieczyć logi dla celów dowodowych.

4. Obowiązki użytkownika

1. Użytkownicy nie mogą instalować żadnego oprogramowania bez wiedzy i pisemnej zgody ASI lokalnej sieci komputerowej.
2. Użytkownicy nie mają prawa podłączać do sieci lokalnej żadnych urządzeń (np. routery, access pointy, switche, notebooki, palmtopy, kamery, aparaty fotograficzne, dyktafony cyfrowe, telefony komórkowe, pendrive, itp.), za wyjątkiem urządzeń służbowych, bez wiedzy i pisemnej zgody ASI ich sieci lokalnej.
3. Użytkownicy nie powinni otwierać poczty, załączników poczty oraz plików nieznanego pochodzenia. Dotyczy to również plików pobranych ze stron WWW (np. aplikacji flash, muzyki, krótkiego filmiku, itp.).
4. Każdy użytkownik powinien zostać przeszkolony w zakresie obsługi oprogramowania antywirusowego oraz zapory sieciowej, a także sposobów powiadamiania administratora sieci lokalnej o wystąpieniu incydentów (np. wirusów) wykrytych przez oprogramowanie antywirusowe. Użytkownicy nieprzeszkoleni mogą żądać przeprowadzenia stosownego szkolenia w ustalonym z administratorem terminie.

DOKUMENTACJA TYLKO DO UŻYTKU WEWNĘTRZNEGO - WSZELKIE KOPIOWANIE TYLKO ZA ZGODĄ DYREKTORA

5. Po włożeniu zewnętrznego nośnika danych, jeśli nie zostanie on sprawdzony automatycznie przez oprogramowanie antywirusowe lub inne oprogramowanie chroniące, użytkownik ma obowiązek sprawdzenia go ręcznie przy pomocy w/w oprogramowania.
6. System informatyczny powinien być tak zabezpieczony aby uniemożliwić użytkownikowi korzystanie z zewnętrznych pamięci USB jak również płyt CD/DVD.
7. W przypadku, gdy oprogramowanie powiadomi użytkownika o wystąpieniu incydentu (np. pojawieniu się wirusa, próbie włamania do systemu, itp.), użytkownik ma obowiązek postępować zgodnie z ustaleniami jakie uzyskał od administratora sieci lokalnej podczas szkolenia.

5. Zasady bezpieczeństwa antywirusowego

Aby ograniczyć możliwość działania wirusów należy:

1. Diagnozować istnienie szkodliwego oprogramowania w trybie awaryjnym.
2. Sprawdzać listę uruchomionych programów i usług w menedżerze zadań.
3. Ograniczać listę uruchamianych usług, z których korzysta się za pomocą sieci do minimum, tzn. do tych, z których rzeczywiście będzie się korzystać.
4. Stosować program antywirusowy i włączyć zaporę i aktualizacje.
5. Szyfrować informacje.
6. Włącz automatyczne aktualizacje używanych programów, w szczególności systemu operacyjnego.
7. Nie udostępniać konta administratora użytkownikom.
8. Instalować oprogramowanie pochodzące z legalnego źródła oraz starać się, aby było ono jak najbardziej aktualne.
9. Instalować system operacyjny, gdy komputer jest odłączony od sieci i internetu.
10. Podłączać komputer do internetu dopiero wtedy, gdy sprawdzony ma skonfigurowane zabezpieczenia
11. Utworzone konta użytkowników zabezpieczać hasłem oraz ograniczyć ich uprawnienia
12. Zmienić konto Administrator na inną nazwę lub wyłączyć konto Administrator, a jednemu z nowo utworzonych kont nadać uprawnienia administracyjne.
13. Ograniczyć do minimum współużytkowanie plików i drukarek w sieci
14. Włączyć podstawowe zabezpieczenia systemu Windows - zaporę sieciową
15. Ustawienie bezpiecznych stref bezpieczeństwa w przeglądarkach internetowych
16. Stosowanie bezpiecznych haseł dostępu i innych rozwiązań uwierzytelniających wszędzie tam, gdzie jest to konieczne
17. Bezpieczne usuwanie danych, których już się nie przetwarza (np. zastosowanie programu do bezpiecznego usuwania danych z nośników elektronicznych)
18. Regularnie archiwizować istotne dane (tworzenie kopii bezpieczeństwa).

DOKUMENTACJA TYLKO DO UŻYTKU WEWNĘTRZNEGO - WSZELKIE KOPIOWANIE TYLKO ZA ZGODĄ DYREKTORA