Zadanie weryfikacyjne (temat 2) Opracowanie planu asekuracyjnego.

(0) LP	(1) Ryzyko Podatność/Zagrożenie	(2) Poziom ryzyka	(3) Polecane mechanizmy kontrolne	(4) Priorytet akcji	(5) Wybrane mechanizmy kontrolne	(6) Wymagane zasoby	(7) Osoby odpowiedzialne	(8) Późniejsze wymagania
1.	Nieautoryzowani użytkownicy mogą się telnetować na serwer XYZ oraz przeglądać istotne(tajne) dane przy pomocy konta gościa	Wysoki	1. Uniemożliwić połączenie przychodzące typu telnet 2. Uniemożliwić dostęp do kluczowych plików (danych) 3. Dezaktywować konto gościa (zmienić hasło na skomplikowane)	Wysoki	1. Uniemożliwić połączenie przychodzące typu telnet 2. Uniemożliwić dostęp do kluczowych plików (danych) 3. zmienić hasło na skomplikowane	10h do rekonfiguracji i testu systemu	Jan Kowalski, XYZ server system administrator; Piotr Nowak, firmowy firewall administrator	Wykonać cykliczne przeglądy bezpieczeństwa system oraz testy sprawdzające czy odpowiednie mechanizmy kontrolne zostały wprowadzone w stosunku do serwera XYZ
2.	Nieupoważniony wstęp na teren firmy	Wysoki	1. Karty magnetyczne identyfikujące osoby (imienne) 2. Zamontować barierki wymagające identyfikacji poprzez kartę 3. Zastosować konieczność „odbicia" się, w przeciwnym wypadku karta nie powinna zadziałać 4. Polityka zabezpieczeń	Wysoki	1. Karty magnetyczne identyfikujące osoby (imienne) wręczyć każdemu pracownikowi 2. Zamontować barierki wymagające identyfikacji poprzez kartę 3. Zastosować konieczność „odbicia" się, w przeciwnym wypadku karta nie powinna zadziałać 4. Każdy pracownik ma obowiązek taką kartę nosić przy sobie, nie może jej nigdzie zostawiać	Wymagane wytworzenie kart, oraz około tydzień na wydanie pracownikom	Zespół od infrastruktury, wydający sprzęt komputerowy (w tym karty)	Nadzorować wymianę takich kart na nowe np. w przypadku zniszczeń, stare utylizować jak i dezaktywować, wymiana zabezpieczeń na samej karcie
3.	Dostęp do laptopa / danych przez osoby nie upoważnione	Wysoki	1. Szyfrowanie dysków na laptopach/komputerach stacjonarnych 2. Stacje dokujące plus blokady laptopów 4. Karty magnetyczne do laptopa	Wysoki	1. Zaszyfrowanie dysku wymagane na każdym urządzeniu, priorytetem urządzenia mobilne czyt. laptopy 2. Stacje dokujące dla każdego laptopa wraz z zabezpieczeniem (kłódką) oraz koniecznością przypięcia podczas pracy 3. Konieczność posiadania osobnej karty magnetycznej do laptopa	Wymagany duży nakład finansowy na zakup/umowę z dostarczycielem na laptopy z funkcją odczytu kart magnetycznych lub dokupienie urządzeń umożliwiających odczyt, kilka godzin na zaszyfrowanie dysków	Zespół od infrastruktury, wydający sprzęt komputerowy (w tym karty)	Zakup urządzeń (stacji dokujących) dla nowych pracowników, kontrole na terenie całej firmy.
4.	Możliwe monitorowanie aktywności na laptopie użytkownika przez osoby nieupoważnione/ inne programy	Średni	1. Odizolowany dostęp do danych/systemów firmy	Średni	1. Praca wymagana poprzez system pośredniczący np. Citrix, co pozwoli uchronić przed potencjalnym zagrożeniem płynącym ze źródła (laptopa)	Dodatkowe urządzenia	Team odpowiedzialny za konfigurowanie dostępnych aplikacji/zdalnych pulpitów z serwera pośredniczącego	Kontrolowanie działania, wprowadzanie poprawek, aktualizacji software jak i zabezpieczeń

5.	Brak kontroli dostępu na dany serwer	Wysoki	1. Wprowadzić system generowania sesji/haseł 2. Wprowadzić autoryzację przez klucz SSH 3. Dodatkowe zabezpieczenie dla kont administracyjnych	Wysoki	1. System który za każdym razem generuje pracownikowi sesje na zdalnym pulpicie lub generuje hasło na system operacyjny/ do aplikacji, co pozwoli na zidentyfikowania osoby odpowiedzialnej za incydent 2. Autoryzacja przez klucz SSH, głównie na systemach z rodziny Unix 3. Dodatkowa autoryzacja kont administratorskich, poprzez wystosowanie – potwierdzenie requestu	Dodatkowe urządzenia służące jako kolejne serwery pośredniczące	Osobny team odpowiedzialny za akceptacje requestów, jak i dbający o infrastrukturę (serwery pośredniczące)	Dodawanie nowych systemów, osób (klucze SSH), administracja aktualnymi zasobami
6.	Brak kontroli poczynań na danym hoście	Niski	1. Nagrywanie sesji	Średni	1. Nagrywanie sesji na serwerach pośredniczących	Dodatkowe miejsce na przetrzymywanie multimediów (filmów) czy też samych wywołanych komend	Ten sam zespół co odpowiedzialny za serwery pośredniczące, gdyż to właśnie generowane tam sesje powinny być kontrolowane	Regularne usuwanie starej zawartości
7.	Brak analiz , w przypadku ewentualnych incydentów,	Niski	1. Zorganizowanie bazy logów 2. Dokumentacje RCA	Wysoki	1. W miejscach gdzie to możliwe zorganizować/podnieść poziom trace/logów by przeciwdziałać ewentualnym problemom z systemami 2. Po ewentualnym incydencie tworzenie dokumentacji RCA analizując dokładnie przyczynę	Dodatkowe miejsce na przetrzymywanie zebranych logów, organizacja ich może zająć kilka dni	Zespół odpowiedzialny za przeglądanie logów i wyłapujących odpowiednie błędy, team administrujących do tworzenia dokumentacji RCA	Regularne usprawnianie infrastruktury poprzez eliminacje pojawiających się błędów
8.	Możliwość przenoszenia szkodliwych plików pomiędzy systemami	Średni	1. Zablokowanie możliwości przenoszenia plików pomiędzy systemami 2. Wszelki import/export plików kontrolować	Średni	1. Ograniczyć do minimum możliwość przenoszenia plików pomiędzy systemami – poprzez blokadę połączeń SSH pomiędzy systemami 2. Wprowadzić serwer pośredniczący gdzie wszystkie pliki wprowadzane/wyprowadzane z systemów będą sprawdzane	Implementacja reguł w firewallu, kilka dni na testy. Dodatkowy serwer pośredniczący	Zespół odpowiedzialny za dostępy na systemy	Ciągła kontrola plików importowanych/ eksportowanych
9.	Szeroki dostęp do systemów z różnych portów/IP	Wysoki	1. Zablokować dostęp do systemów przez niepożądane hosty/usługi	Średni	1. Dla tych usług gdzie to możliwe wprowadzić ograniczenia poprzez listy kontrolne dostępu (ACL), gdzie można dokładnie zdefiniować jak ma przebiegać dostęp.	Zdefiniowanie usług, stworzenie szablonów ACL'ek oraz implementacja powinny zająć około tygodnia	Zespół administratorów systemów	Monitorowanie list kontrolnych dostępu oraz ich ewentualne rozszerzanie o nowe hosty
10.	Zbyt szeroki dostęp do Internetu	Wysoki	1. Serwer pośredniczący proxy 2. Konieczność komunikacji przez	Średni	1. Zorganizować osobny serwer, gdzie działać będzie proxy	Serwer proxy oraz zaprogramowanie i	Informatyk odpowiedzialny za	Dodawanie nowych wykluczeni.

			wewnętrzną sieć firmy		transparentne tzn. przez ten serwer będzie przechodzić cały ruch sieciowy 2. Zorganizowanie dostępu do sieci wewnętrznej firmy	implementacja ruchu sieciowego co wiąże się z całkowitą zmianą routingu, czas niemierzalny	nadzorowanie serwera proxy	
11.	Zbyt szeroki dostęp do aplikacji	Średni	1. Ograniczyć dostęp do aplikacji	Średni	1. Gdzie możliwe wprowadzić autoryzacje przez kartę – certyfikaty SNC	Utworzenie własnych certyfikatów, rozdystrybuowanie danych certyfikatów na poszczególne używane aplikacje	Zespół administratorów systemów	Dodawanie nowych szyfrowań do certyfikatów, odświeżanie certyfikatów w momencie wygaśnięcia
12.	Możliwość odcięcia zasilania w skutek awarii	Wysoki	1. Zapasowe zasilanie	Wysoki	1. Zorganizować zapasowe zasilanie, oraz wyznaczyć strefy o wyższym priorytecie gdzie ma być kierowane	Wykupienie agregatów, tydzień na przeanalizowanie, stworzenie planu organizacji zasilania awaryjnego	Ewentualny właściciel placówki wynajmowanej przez firmę	Nadzorowanie odpowiedniej ilości pokładów zasilania, na czas wymagany do naprawnienia usterki
13.	Ogólnodostępne hasła, w wersji tekstowej	Wysoki	1. Szyfrowanie haseł 2. W przypadku dużych ilości potrzebnych haseł wprowadzenie aplikacji/ mini bazy zaszyfrowanej 3. Polityki haseł	Wysoki	1. Konieczność szyfrowania haseł 2. Używanie aplikacji do przetrzymywania haseł, aplikacja ta powinna je szyfrować jak i dostęp do samej aplikacji powinien być ograniczony 3. Ustalić polityki haseł	Brak	Zespół od kontrolowania zabezpieczeń	Wprowadzić częste kontrole
14.	Dostęp do baz danych	Średni	1. Ograniczanie ról 2. Udostępnienie poszczególnych widoków bazy	Średni	1. Ograniczenie ról, poprzez zabranie tych niepotrzebnych 2. Udostępnienie tylko najpotrzebniejszych widoków	Czas potrzebny na zdefiniowanie szablonu z potrzebnymi rolami – czas potrzebny na implementacje zależny od ilości systemów	Zespół administratorów systemów	Konfiguracja nowych systemów
15.	Możliwość zainfekowania laptopa	Średni	1. Zablokować możliwość instalacji nieznanego oprogramowania 2. Zablokować możliwość automatycznej aktualizacji	Średni	1. Tylko potwierdzone oprogramowanie wraz z dostarczonymi wcześniej instalatorami powinno być zezwalane do instalacji 2. Paczki do aktualizacji powinny być wyznaczane i rozdystrybuowane	Czas potrzebny na selekcje odpowiednich paczek, około kilku dni	Team OS – odpowiedzialny za systemy operacyjne	Zatwierdzanie kolejnych paczek z aktualizacjami i udostępnianie ich
16.	Stare oprogramowanie, brak optymalizacji pracy	Średni	1. Na administrowanych systemach realizacja projektów aktualizujących oprogramowanie	Średni	1. Regularne realizowanie projektów aktualizujących oprogramowanie np. baz danych,	Czas potrzebny na wyrównanie wersji na wszystkich	Zespół administratorów systemów	Kontrolowanie wychodzących nowych wersji oprogramowania,

			2. Wprowadzenie łatek producentów		usprawniających działanie 2. Wprowadzanie dodatkowych zabezpieczeń, uprzedzonych wcześniej poprzez oficjalną informację od producenta	administrowanych systemach może być ogromny i sięgnąć około miesiąca		testowanie i wdrażanie
17.	Niepowodzenia implementacji nowego oprogramowania	Wysoki	1. Regularny zabezpieczanie zasobów, poprzez kopie zapasowe	Wysoki	1. Regularne zabezpieczanie (backup) najważniejszych danych dla firmy/klienta, czy to podczas codziennego działania czy też w skutek niepowodzenia projektu	Zapewnienie nowych hostów przytrzymujących kopie bezpieczeństwa, zaplanowanie tworzenia kopii może zająć do tygodnia	Zespół od organizowania „grafiku" kopii zapasowych	Nadzorowanie wykonywania kopii w szczególności systemów o wysokim priorytecie
18.	Bezmyślne przesyłanie ważnych informacji	Wysoki	1. Szyfrowanie maili 2. Brak możliwości nagrywania sesji na konferencjach przez osoby niepowołane	Wysoki	1. Szyfrowanie maili posiadających ważne informacje np. hasła 2. Zabranie możliwości nagrywania niektórych sesji szkoleniowych, w celu dalszej propagacji	Dodawanie osób odpowiedzialnych za kontrolę do list dystrybucyjnych aby widziały co jest wysyłane, czas potrzebny około 1 dzień	Team od zabezpieczeń	Kontrolowanie przepływu maili