Analiza ryzyka zgodna z ISO 27001
SZPITAL

Bieńkowski Mikołaj (s6020)
Domański Jakub (s4711)
Graczyk Hubert (s6215)
Kwit Przemysław (s6190)

17 czerwca 2013

Spis treści

Rozdział 1

Mapowanie zasobów

W związku z brakiem identyfikatorów nazw zasobów, w celu ułatwienia dalszych prac zastosowaliśmy następujące, własne, mapowania.

1.1 Informacje

Nazwa zasobu	**Identyfikator zasobu**
Baza danych pacjentów	I_1
Terminarz wizyt	I_2
Baza danych wystawionych recept	I_3
Baza danych wystawionych rachunków	I_4
Baza danych przeprowadzonych zabiegów	I_5
Baza danych historii rozmów telefonicznych z klientami	I_6
Baza danych historii opieki nad pacjentami	I_7

1.2 Oprogramowanie

Nazwa zasobu	**Identyfikator zasobu**
Serwer aplikacji firmy ds. rejestracji	O_1
Serwer wykrywania włamań na WEB_Serw	O_2
Serwer archiwizacji danych	O_3
MS Windows 7 Enterprise Edition	O_4
Norton AntyVirus 2013	O_5
MS Windows SQL Serwer	O_6

1.3 Urządzenia usługowe

Nazwa zasobu	**Identyfikator zasobu**
Firewall Cisco ASA5525X Firewall Edition	Z_1
Routery Cisco 3945 with 3 onboard GE	Z_2
Switche core'oweWSC3750 X48PS	Z_3
Switche dostępowe WSC2960 S48LPDL	Z_4
SerweryDell PowerEdge R720 z VMware 5	Z_5
Macierze EMC VNX5100	Z_6

1.4 Zasoby fizyczne

Nazwa zasobu	**Identyfikator zasobu**
Agregat prądotwórczy	U_1
Klimatyzacja serwerowni	U_2
Panele słoneczne	U_3
Oczyszczacz powietrza	U_4
Klimatyzacja / ogrzewanie	U_5
Wentylacja szpitala	U_6

Rozdział 2

Opis zagrożeń dla zasobów

Braki i uwagi ogólne:

1. W chwili uszkodzenia switcha na którymkolwiek z pięter infrastruktura sieci na danym piętrze i piętrach poniższych straci połączenie.
2. Drukarki sieciowe są niewymienione w liscie zasobów, a znajdują się na schemacie. Zakładamy że drukarki sieciowe mają ID U_7
3. Brak informacji o zastosowanym w macierzach systemie RAID.
4. W obecnej konfiguracji macierze dysków są zbędne. Dyski są umieszczone bezpośrednio w serwerze.
5. Na diagramie struktury teleinformatycznej brak umieszczonych urządzeń usługowych co utrudnia identyfikacje zagrożeń.
6. Komputery są niewymienione w liście zasobów, a znajdują się na schemacie. Zakładamy, że komputery mają ID Z_7

2.1 Informacje

Id_zas.	**Zagrożenie**	**Podatność**	**Skutek**	**Id_zagr.**
I_1	Uzyskanie danych osobowych klienta przesyłanych w procesie	Urządzenia sieciowe - atak typu „APR spoof" + man in the middle - brak kontroli protokołu APR	Poufność	ZAG_1
I_2	Zmiana terminów wizyt spotkań pacjentów	Brak aktualnych sygnatur złośliwego oprogramowania	Integralność	ZAG_2

Kontynuacja na następnej stronie

Kontynuacja z poprzedniej strony

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
I_3	Zafałszowanie informacji dotyczących wystawionych recept - skutek: problemy z urzędem skarbowym, niezgodność przychodów szpitala	Urządzenia sieciowe - atak typu „APR spoof" + man in the middle - brak kontroli protokołu APR	Integralność	ZAG_3
I_4	Zmienione dane (zafałszowane) na fakturze w procesie przesyłania danych do faktury	Urządzenia sieciowe - atak typu „APR spoof" + man in the middle - brak kontroli protokołu APR	Integralność	ZAG_4
I_5	Uzyskanie konta administratora w serwerze bazy danych przeprowadzonych zabiegów - skutek : ujawnienie historii przeprowadzonych zabiegów	Atak słownikowy z sieci wewnętrznej na konto roota	Integralność	ZAG_5
I_6	Uzyskanie konta administratora w serwerze bazy danych przeprowadzonych rozmów telefonicznych - skutek: utrata poufnych danych	Atak słownikowy z sieci wewnętrznej na konto roota	Poufność	ZAG_6
I_7	Uzyskanie konta administratora w serwerze bazy danych pacjentów - skutek : ujawnienie historii pacjentów szpitala	Atak słownikowy z sieci wewnętrznej na konto roota	Poufność	ZAG_7

2.2 Oprogramowanie

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
O_1	Uzyskanie danych osobowych pacjentów przesyłanych w procesie	Urządzenia sieciowe - atak typu „APR spoof" + man in the middle - brak kontroli protokołu APR	Poufność	ZAG_8

Kontynuacja na następnej stronie

Kontynuacja z poprzedniej strony

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
O_2	Uzyskanie dostępu do konta administratora - skutek: wyłączenie zabezpieczeń, przekłamanie serwera	Systemy teleinformatyczne – system użytkowe – atak słownikowy z sieci wewnętrznej na konto roota	Poufność	ZAG_9
O_3	Uzyskanie dostępu do konta administratora - skutek: wyłączenie zabezpieczeń, przekłamanie serwera	Systemy teleinformatyczne – system użytkowe – atak słownikowy z sieci wewnętrznej na konto roota	Poufność	ZAG_10
O_4	Podatność na wirusy - skutek: kradzież danych, przejęcie kontroli, odmowa działania	Brak aktualizacji oprogramowania	Poufność	ZAG_11
O_5	Podatność na wirusy - skutek: kradzież danych, przejęcie kontroli, odmowa działania	Brak aktualizacji oprogramowania	Poufność	ZAG_12
O_6	Podatność na wirusy - skutek: kradzież danych, przejęcie kontroli, odmowa działania	Brak aktualizacji oprogramowania	Poufność	ZAG_13

2.3 Zasoby fizyczne

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
Z_1	Modyfikacja konfiguracji firewalla z sieci wewnętrznej	Systemy teleinformatyczne – system operacyjny – brak aktualizacji firmwaru	Poufność	ZAG_14
Z_2	Modyfikacja konfiguracji routera sieci internet lub wewnętrznej	Systemy teleinformatyczne – system operacyjny – brak aktualizacji firmwaru	Poufność	ZAG_15
Z_3	Modyfikacja konfiguracji switcha z sieci wewnętrznej	Systemy teleinformatyczne – system operacyjny – brak aktualizacji firmwaru	Poufność	ZAG_16
Z_4	Modyfikacja konfiguracji switcha z sieci wewnętrznej	Systemy teleinformatyczne – system operacyjny – brak aktualizacji firmwaru	Poufność	ZAG_17

Kontynuacja na następnej stronie

Kontynuacja z poprzedniej strony

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
Z_5	Uzyskanie konta administratora na serwerze, ataki z sieci wewnętrznej	Systemy teleinformatyczne – system użytkowe – atak słownikowy z sieci wewnętrznej na konto roota	Poufność	ZAG_18

2.4 Urządzenia usługowe

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
U_1	Restart wszystkich serwerów	System zasilania - nagły spadek mocy	Dostępność	ZAG_20
U_2	Podgrzewanie się urządzeń w serwerowni	System wentylacji / klimatyzacji - awaria klimatyzatora / wentylatora	Dostępność	ZAG_21
U_3	Uszkodzenia mechaniczne	Uszkodzenie fizyczne w wyniku zjawisk pogodowych (silne wiatry, grad)	Dostępność	ZAG_22
U_4	Uszkodzony filtr	Zanieczyszczenie może spowodować zniszczenie filtru.	Dostępność	ZAG_23
U_5	Uszkodzenie mechaniczne klimatyzatora	Uszkodzenie fizyczne w wyniku zjawisk pogodowych (silne wiatry, grad, zamarznięcie wymiennika)	Dostępność	ZAG_24
U_6	Rozprzestrzenie się bakterii / skażenia	Poprzez przewody wentylacyjne możliwe jest przenoszenie się zarazków/ materiałów skażonych	Integralność	ZAG_25

2.5 Dodatkowe niewymienione zasoby

Id_zas.	Zagrożenie	Podatność	Skutek	Id_zagr.
U_7	Uzyskanie dostępu do drukarek poprzez sieć Wi-Fi	Podłączając się poprzez Wi-Fi do sieci każdy użytkownik ma dostęp do drukarki - brak informacji o jakiejkolwiek ochronie przed użyciem drukarki sieciowej (np. hasło)	Dostępność	ZAG_26
Brak	Brak wykwalifikowanej kadry w szpitalu w chwili zdarzenia.	W systemie informatycznym szpitala brak jest jakiegokolwiek systemu umożliwiającego synchronizację zwolnień/urlopów lekarzy. Możliwe jest więc, że podczas zdarzenia (np. wypadek samochodowy) w szpitalu nie będzie lekarza, który mógłby udzielić natychmiastowej pomocy (np operacji).	Integralność	ZAG_27

Kontynuacja na następnej stronie

Kontynuacja z poprzedniej strony

Id_zas.	**Zagrożenie**	**Podatność**	**Skutek**	**Id_zagr.**
Brak	Wysłanie karetki pod zły adres.	W systemie teleinformatycznym szpitala brak jest systemu umożliwiającego nagrywanie rozmów. W chwili stresowej dyspozytor może zapomnieć gdzie miał wysłać pomoc i brak takiego systemu uniemożliwi mu szybką reakcję. Dodatkowo w systemie brak jakiejkolwiek informacji o zastosowanych telefonach - nie wiemy czy dyspozytor w takiej sytuacji mógłby oddzwonić na numer osoby wzywającej pomoc (może nie mieć danego numeru).	Integralność	ZAG_28
Brak	Brak systemu monitorującego	Brak informacji o jakimkolwiek systemie monitorującym. Urządzenia takie mogłyby być wykorzystane do monitoringu np sali operacyjnej - w chwili wypadku można by było stwierdzić czy kadra zareagowała zgodnie z obowiązującym ich prawem. Kamery mogłyby być także umieszczone nad pokojami z lekami, przez co zmalałoby ryzyko wykradnięcia leków.	Poufność	ZAG_29

Kontynuacja na następnej stronie

Kontynuacja z poprzedniej strony

Id_zas.	**Zagrożenie**	**Podatność**	**Skutek**	**Id_zagr.**
Z_7	Brak osoby odpowiedzialnej za jeden z głównych zasobów - komputery	W chwili awarii komputera brak jest osoby, która zajełaby się naprawą danej szkody. W chwili jednoczesnej dużej awarii (przepięcie w układzie elektrycznym szpitala co spowoduje przepalenie kilku komputerów) niemożliwe będzie zapisywanie nowych pacjentów, bądź sprawdzanie historii leczenia pacjenta.	Integralność	ZAG_30

Rozdział 3

Szacowanie ryzyka

3.1 Określenie możliwości wystąpienia zagrożeń wg. NIST

1. **Poziom wysoki (1)** - Czynnik o wysokiej motywacji, posiadający potencjał do dużego rażenia, zabezpieczenia mające chronić przed wykorzystaniem podatności są niesktuczne.

2. **Poziom średni (0,5)** - Czynnik sprawczy o średniej motywacji, posiadający możliwości, zabezpieczenia są w stanie skutecznie przecistawić się wykorzystaniu podatności.

3. **Poziom niski (0,1)** - Czynnik niski nie posiada motywacji lubnie posiada wystarczającego potencjału rażeni. Zabezpieczenia są skuteczne albo przynajmniej spełniają swoje zadania

3.2 Określenie poziomu podatności skutków zagrożeń według NIST

1. **Poziom bardzo wysoki (100)** - Wykorzystanie podatności może:

   - spowodować najwyższe możliwe straty dla ważnych zasobów
   - zakłócić realizację ciągłości funkcjonowania
   - wstrzymać realizację ciągłości funkcjonowania
   - zaszkodzić w dużym stopniu reputacji szpitala
   - spowodować utratę życia
   - spowodować utratę zdrowia

2. **Poziom wysoki (75)**

3. **Poziom średni (50)** - Wykorzystanie podatności może:

   - spowodować duże straty w zakresie ważnych zasobów
   - zakłócić realizację celów organizacji

- zaszkodzić interesom
- zaszkodzić reputacji szpitala
- spowodować utratę zdrowia

4. **Poziom niski (30)** - Wykorzystanie podatności może:
   - spowodować stratę niektórych ważnych zasobów
   - zakłócić w sposób zauważalny realizację celów szpitala
   - wpłynąć negatywnie na reputację szpitala
   - wpłynąć negatywnie na interesy szpitala
5. **Poziom bardzo niski (10)**

3.3 Macierz ryzyka według NIST

Możliwe zagrożenie	**Poziom bardzo niski (10)**	**Poziom niski (30)**	**Poziom średni (50)**	**Poziom wysoki (75)**	**Poziom bardzo wysoki (100)**
wysokie (1)	$1 \times 10 =$ **10**	$1 \times 30 =$ **30**	$1 \times 50 =$ **50**	$1 \times 75 =$ **75**	$1 \times 100 =$ **100**
Średnie (0.5)	$0,5 \times 10 =$ **5**	$0,5 \times 30 =$ **15**	$0,5 \times 50 =$ **25**	$0,5 \times 75 =$ **37,5**	$0,5 \times 100 =$ **50**
Niskie (0.1)	$0,1 \times 10 =$ **1**	$0,1 \times 30 =$ **3**	$0,1 \times 50 =$ **5**	$0,1 \times 75 =$ **7,5**	$0,1 \times 100 =$ **10**

3.4 Poziom bezpieczeństwa według NIST

- **Poziom wysoki**
  Następuje silna potrzeba redukcji działań korygujących, wdrożenia systemu zabezpieczeń. System mógłby działać dalej jednak plan bezpieczeństwa / zabezpieczeń powinien być wdrożony w trybie natychmiastowym.

- **Poziom średni**
  Działania korygujące są konieczne. System mógłby działać dalej jednak plan bezpieczeństwa / zabezpieczeń powinien być wdrożony w rozsądnym przedziale czasowym.

- **Poziom niski**
  Osoba odpowiedzialna za bezpieczeństwo systemu powinna niezwłoczenie podjąć decyzję o podjęciu działań korygujących ewentualnie akceptacji ryzyka o dopuszczeniu systemu do eksploatacji.

3.5 Ocena ryzyka

Zagrożenie	Waga szkody	Możliwość wystąpienia szkody	Wyliczone ryzko
ZAG_1	100	0,1	10
ZAG_2	100	0,1	10
ZAG_3	100	0,1	10
ZAG_4	50	0,1	5
ZAG_5	100	0,1	10
ZAG_6	25	0,1	2,5
ZAG_7	100	0,1	10
ZAG_8	100	0,1	10
ZAG_9	100	0,1	10
ZAG_10	100	0,1	10
ZAG_11	100	0,5	50
ZAG_12	100	0,5	50
ZAG_13	100	0,5	50
ZAG_14	50	0,1	5
ZAG_15	50	0,1	5
ZAG_16	50	0,1	5
ZAG_17	50	0,1	5
ZAG_18	100	0,1	10
ZAG_20	75	0,1	7,5
ZAG_21	75	0,5	37,5
ZAG_22	50	0,1	5
ZAG_23	75	0.1	7,5
ZAG_24	75	0,5	37,5
ZAG_25	100	0,1	10
ZAG_26	10	1	10
ZAG_27	100	0,5	50
ZAG_28	100	0,1	10
ZAG_29	50	0,5	25
ZAG_30	50	0,1	5

3.6 Definiowanie poziomów ryzyka

Poziom wysoki (51 - 100):
ZAG_11, ZAG_12, ZAG_13, ZAG_27
Poziom średni (11 - 50):
ZAG_21, ZAG_24, ZAG_29
Poziom niski (0 - 10):
ZAG_1, ZAG_2, ZAG_3, ZAG_4, ZAG_5, ZAG_6, ZAG_7, ZAG_8, ZAG_9, ZAG_10, ZAG_14, ZAG_15, ZAG_16, ZAG_17, ZAG_18, ZAG_20, ZAG_22, ZAG_23, ZAG_25, ZAG_26, ZAG_28, ZAG_30.

Rozdział 4

Wnioski

Ocena ryzyka wykryła trzy najgroźniejsze zagrożenia , które oznaczone są następująco: ZAG_11, ZAG_12, ZAG_13, ZAG_27. Podatność na ataki wirusowe jest duża ze względu na brak aktualizacji oprogramowania. Skutkiem może być wykradnięcie danych między innymi: historia zabiegów, wydane recepty (zwłaszcza, które opierają na leki nie dostępne bez recepty), baza i historia leczenia pacjentów co nie jest korzystne dla szpitala. Do tej grupy groźnych zagrożeń również zalicza się brak wykwalifikowanej kadry w szpitalu w chwili zdarzenia co spowodowane jest brakiem systemu do obsługi grafiku szpitala.

Do średnich zagrożeń zaliczamy jedynie dwa oznaczone następująco: ZAG_21, ZAG_24, ZAG_29. Zagrożenia nie są niskiego poziomu więc im również należy poświęcić więcej uwagi aby ich działanie nie przeszkodziło w funkcjonowaniu szpitala. Podgrzewanie się urządzeń w serwerowni jest poważnym zagrożeniem , ponieważ niesie za sobą nieprzewidziane skutki tak samo klimatyzator , który powinien być niezawodny. Szpital jest miejscem gdzie przechowywane są różne zasoby , które powinny mieć odpowiednią temperaturę i stosowne miejsce przechowywania.

Osoba odpowiedzialna za bezpieczeństwo, agregująca dane powinna jak najszybciej podjąć stosowne kroki w celu wyeliminowania powyższych zagrożeń.

Rozdział 5

Uwagi do raportu

- Brak identyfikatórów nazw: wprowadzono własną mapę.
- Wprowdzono dodatkowe zasoby, które są uwzględnione w tabeli zasobów jednak na diagramie istnieją

Rozdział 6

Korespondencja z klientem

6.1 Pytanie 1

Nadawca: mykhi@pjwstk.edu.pl
Odbiorca: lukasz.leszko@gmail.com
Data: 13 czerwca 2013, 18:11
Temat: Pytanie macierze dyskowe - projekt Szpital ZMI
Treść pytania:
Witam,
Proszę o wyjaśnienie zawartości dokumentacji. Dyski twarde znajdują się bezpośrednio w serwerze a nie w macierzy. Innymi słowy Macierz jest pusta. Czy tak jest w rzeczywistości czy może jest to błąd w dokumentacji.
Proszę o wyjaśnienie.

Nadawca: lukasz.leszko@gmail.com
Odbiorca: mykhi@pjwstk.edu.pl
Data: 14 czerwca 2013, 17:13
Temat: Re: Pytanie macierze dyskowe - projekt Szpital ZMI
Odpowiedź:
Witam,
Dyski w serwerach zawierają dane systemu hosta (VMware), macierze zawierają dyski z danymi maszyn wirtualnych i są podpięte do serwera za pośrednictwem switcha przez iSCSI.
Z poważaniem
Tomasz Witkowski
