BEZPECZEŃSTWO W TELEKOMUNIKACJI I TELEINFORMATYCE Z PUNKTU WIDZENIA OPERATORA TELEKOMUNIKACYJNEGO

Dariusz Kulawik

WYMAGANIA PROCEDURALNE
Obszar publiczny

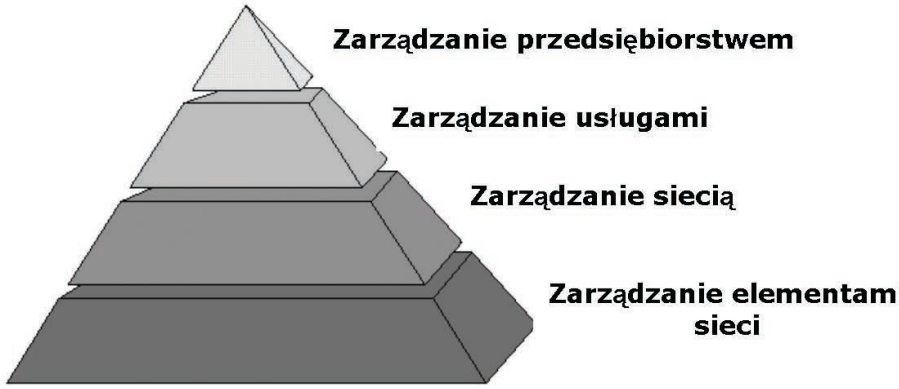
POTRZEBY PRZECIWDZIAŁAŃ
Proceduralne

W artykule opisano warstwy sieci (aktywa telekomunikacyjne i teleinformatyczne) decydujące z punktu widzenia operatora i istotne dla funkcjonowania infrastruktury krytycznej państwa. Omówiono ich znaczenie, istotność oraz praktyczne metody szacowania ryzyka i postępowania z ryzykiem, planowania BCP/DRP oraz pewne aspekty zapewniania bezpieczeństwa przez operatora sieci.

1. CHARAKTERYSTYKA SIECI I PROCESÓW TELEKOMUNIKACYJNYCH

Zgodnie z zaleceniami Międzynarodowej Unii Telekomunikacyjnej (International Telecommunication Unit – Telecommunication ITU-T) architektura systemów zarządzania (sieci zarządzających) operatora telekomunikacyjnego wygląda jak na rys. 1.

Model TMN jest prosty, jednak jego wdrożenie jest bardzo złożone. Istnieje duża liczba norm i standardów ITU-T opisujących interfejsy pomiędzy systemami zarządzania, które zresztą koncentrują się głównie na opisie interfejsów pomiędzy dolnymi warstwami modelu (warstwami elementów sieci, zarządzania elementami sieci oraz zarządzania siecią).



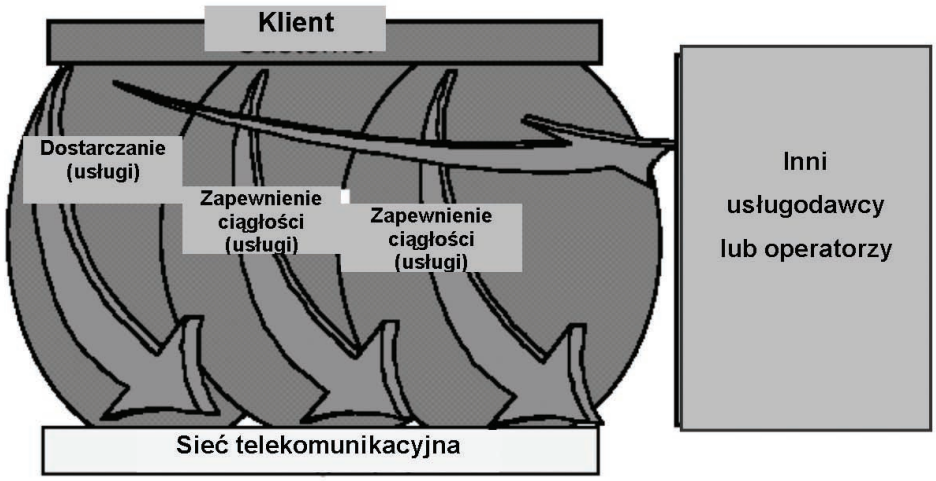
Rys. 1. Podstawowy model TMN (Telecommunication Management Network)

Praktycznie brakuje w tym modelu gotowych norm opisujących interfejsy pomiędzy warstwami zarządzania, zwłaszcza pomiędzy warstwami wyższymi. Brakuje również interfejsów poziomych, wspierających powiązania międzyoperatorskie. Model ten był tworzony metodą „z dołu do góry", głównie przez środowiska techniczne i naukowe, bez przywiązywania wagi do praktyczności wdrożenia, uwzględnienia kosztów, konkurencyjności, potrzeb biznesowych oraz bez podejścia proklienckiego. Nie było też woli ze strony dominujących koncernów telekomunikacyjnych do wdrożenia tych standardów, umożliwiających otwartość rozwiązań i konkurencyjność na rynku, który wymagał coraz większej wyobraźni i umiejętności szybkiego dostosowywania się do tych wymagań. Takie podejście znakomicie zweryfikowało życie, głównie utratą dominującej pozycji na rynku.

Walka konkurencyjna oraz rewolucja IP spowodowały lawinę rozwiązań quasi-TMN z wykorzystaniem prostych protokołów ze świata komputerowego (SNMP, TCP/IP, XML, inne), które może nie były doskonałe, ale działały. Rynek telekomunikacyjny dopuścił rozwiązania komercyjne, systemy „z półki". I chociaż rozwiązania te nie komunikowały się ze sobą za pomocą protokołów zgodnych z interfejsami Q3 (TMN), to działały i były o rzędy wielkości tańsze i lepsze od proponowanych i stosowanych dotąd rozwiązań TMN. W konsekwencji pojawiły się nowe technologie, świat mobilny i IP, konwergencja. Pojawili się też nowi wielcy gracze na rynku.

Z potrzeby chwili powstała międzynarodowa organizacja Tele-Management Forum (TM Forum), zrzeszająca klientów usług telekomunikacyjnych, dostawców usług i sieci telekomunikacyjnych, dostawców systemów zarządzania, dostawców elementów sieci, środowiska non-profit, uczelnie. Organizacja ta, biorąc za podstawę dotychczasowe dokonania i model TMN, opracowała model sieci i procesów w sieci, ukierunkowany na zarządzanie biznesem i usługami telekomunikacyjnymi widzianymi „z góry", czyli od strony użytkowej, przez różne zainteresowane strony, jak klienci, właściciele firm, zarządy. Punktem wyjścia do tych rozważań były trzy główne procesy wyróżniane u każdego dostawcy usług czy operatora: „dostarczaj – utrzymuj – rozliczaj" (ang. *Fulfill, Assure, Bill* – FAB), z uwzględnieniem relacji poziomych pomiędzy operatorami lub operatorami i dostawcami usług, którzy niejednokrotnie współpracują przy dostarczaniu usługi dla jednego klienta (rys. 2).

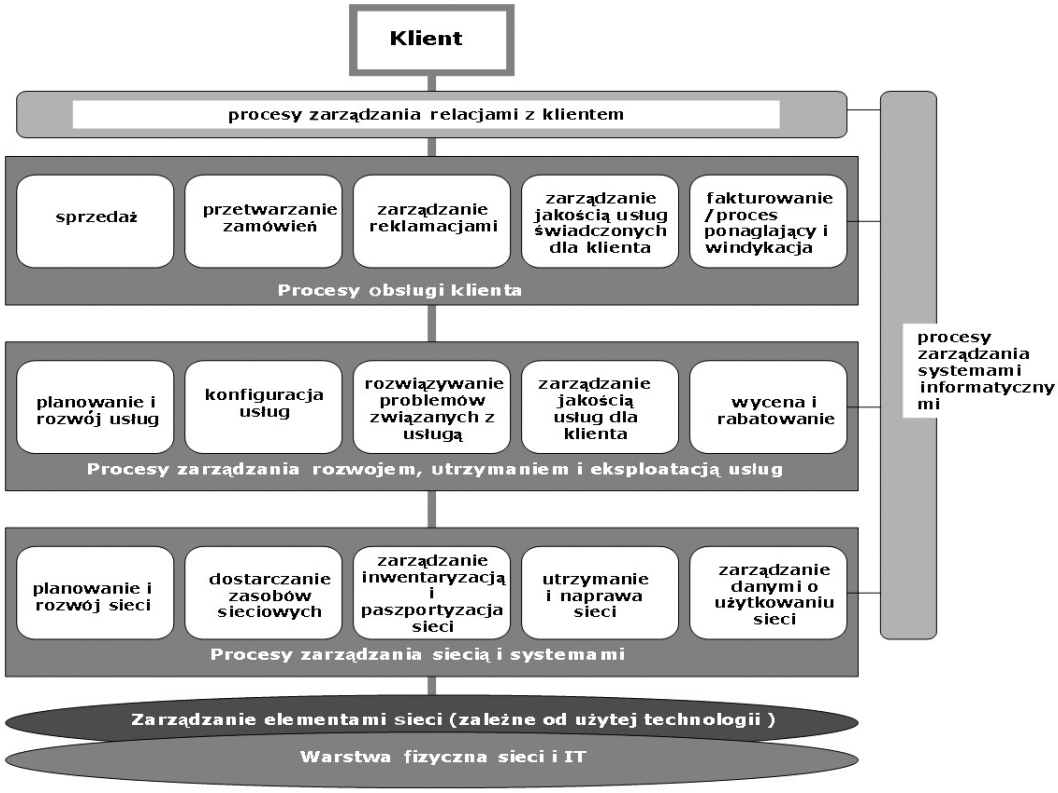
TM Forum opracowało architekturę procesów, które w całości lub części występują u każdego dostawcy usług lub operatora telekomunikacyjnego. W modelu tym (rys. 3) wyróżniamy warstwę sieci (infrastruktury fizycznej i elementów sieci oraz zarządzania elementami sieci), warstwę procesów zarządzania siecią i systemami, warstwę zarządzania usługami,



Rys. 2. Model FAB – ogólny widok procesów w sieci telekomunikacyjnej

warstwę zarządzania relacjami z klientem. W praktyce dodajemy jeszcze warstwę procesów biznesowych, która występuje wyraźnie także w modelu TMN.

W każdej warstwie istnieje infrastruktura fizyczna i logiczna reprezentująca ją lub wspomagająca jej funkcje. Granice między warstwami nie są i nie muszą być ostre – czasami kilka systemów spełnia jedną funkcję w warstwie lub jeden system wspomaga różne funkcje w wielu warstwach; zwykle systemy w warstwie i między warstwami są zintegrowane ze sobą.



Rys. 3. Statyczny model procesów biznesowych

1.1. WARSTWA SIECI

1.1.1. PODWARSTWA ELEMENTÓW SIECI

Są to zarządzane aktywne elementy sieci (różne domeny, technologie i dostawcy), obiekty budowlane, maszty, kanalizacja, sieci miedziane, światłowodowe i radiowe.

Rozróżniamy następujące domeny telekomunikacyjne: transmisja, komutacja, transmisja danych, IP, systemy dostępowe, zasilanie, klimatyzacja, systemy środowiskowe itp.

Ze względów operacyjno-biznesowych w każdej domenie powinno być kilka technologii oraz kilku dostawców wiodących (co najmniej dwóch różnych dostawców w domenie).

Możemy założyć, że każdy średniej wielkości operator posiada około tysiąca obiektów budowlanych (kilkanaście / kilkadziesiąt obiektów węzłowych (duże centrale telefoniczne i/lub węzły transmisyjne), kilka biurowych, reszta to bezzałogowe obiekty technologiczne), kilka tysięcy kilometrów światłowodów w sieci szkieletowej (w tym także w relacjach międzynarodowych), kilkadziesiąt/kilkaset tysięcy kilometrów sieci dostępowej.

1.1.2. PODWARSTWA ZARZĄDZANIA ELEMENTAMI SIECI

Są to systemy komputerowe, zwykle zależne od domeny lub technologii elementu sieci.

Liczba tych systemów zależy od wielkości i różnorodności technologii użytkowanych przez operatora. Najczęściej jest to kilkanaście systemów, kilku dostawców.

1.2. WARSTWA ZARZĄDZANIA SIECIĄ

Do warstwy tej należą systemy inwentaryzacji sieci, systemy zarządzania sprawnością sieci, systemy zarządzania ruchem, systemy zarządzania awariami, systemy planowania sieci i ruchu, systemy mediacyjne.

Zazwyczaj jest to kilka systemów, kilku dostawców.

1.3. WARSTWA ZARZĄDZANIA USŁUGAMI

Są to systemy inwentaryzacji sieci i usług, systemy monitorowania i alarmowania jakości oraz wspomagania rozwiązywania problemów, systemy prognozowania, symulacji i wspomagania planowania sieci, ruchu i usług, systemy konfiguracji usług.

Zwykle jest to kilka systemów, kilku dostawców.

1.4. WARSTWA ZARZĄDZANIA RELACJAMI Z KLIENTAMI

Do warstwy tej należą, między innymi, systemy zarządzania relacjami z klientem (*Customer Relationship Management* – CRM), systemy bilingowe i rozliczeń operatorskich, systemy zapewniania przychodów (*Revenue Assurance* – RA), systemy kontroli migracji klientów (*Churn Management* – CA).

System CRM wspomaga takie procesy, jak: sprzedaż, obsługa zamówień, udzielanie informacji, obsługa reklamacji i problemów technicznych, zarządzanie jakością obsługi klienta, w tym gwarantowanymi parametrami świadczonych usług na ustalonym poziomie (*Service Level Agrement* – SLA).

Systemy bilingowe odpowiadają za prawidłowe i terminowe sporządzanie rachunków i ich dystrybucję do klientów oraz prawidłowe sporządzanie rozliczeń między operatorami.

Systemy RA odpowiadają za kontrolę i zapewnienie przychodów firmy. Sprawdzają wiarygodność klientów, kontrolują prawidłowość wystawiania rachunków za świadczone usługi, monitorują i wykrywają nadużycia oraz oszustwa telekomunikacyjne (tzw. *Fraud Management* – FM).

System kontroli migracji klientów CM monitoruje poziom zadowolenia klientów, oferty konkurencji i wykrywa wczesne sygnały lub tendencje rezygnacji z usług operatora. Umożliwia podjęcie właściwych działań zapobiegawczych.

1.5 WARSTWA ZARZĄDZANIA BIZNESEM

W tej warstwie występują systemy typu: zarządzania przedsiębiorstwem (*Enterprise Resorce Planning* – ERP), hurtownie danych, systemy analityczne i raportowe, systemy wspomagania podejmowania decyzji, systemy zarządzania bezpieczeństwem itp. Systemy z tej warstwy gromadzą informacje o transakcjach wytworzone przez systemy z warstw niższych w postaci zunifikowanych danych, przetwarzają te dane w sposób inteligentny i wspomagany wiedzą ekspercką, dostarczają właściwym osobom w odpowiednim czasie właściwe informacje, ułatwiające podejmowanie trafnych decyzji. Umożliwiają również dostarczanie obligatoryjnych raportów dla instytucji zewnętrznych, takich jak: Urząd Komunikacji Elektronicznej (UKE), Główny Urząd Statystyczny (GUS), Giełda Papierów Wartościowych (GPW) i inne.

2. WARSTWY SIECI ZARZĄDZANIA, ICH FUNKCJE, ATRYBUTY I PRIORYTETY BEZPIECZEŃSTWA

Bezpieczeństwo operatora telekomunikacyjnego oznacza zapewnienie ciągłości procesów FAB (*Business Continuity Planning* – BCP) we wszystkich warstwach zarządzania, właściwe procedury reagowania kryzysowego i odtwarzania (*Disaster Recovery Planning* – DRP).

W warunkach kryzysowych niewątpliwie priorytetowe jest zachowanie ciągłości działania i utrzymania usług telekomunikacyjnych w ruchu, sprawne odtwarzanie ruchu tam, gdzie jest to niezbędne, według priorytetów narzuconych przez ustawę – Prawo telekomunikacyjne i w stosownych rozporządzeniach uzupełniających.

Poniżej opisano warstwy sieci zarządzającej z punktu widzenia systemów wspomagających procesy każdej z warstw.

2.1. WARSTWA SIECI

2.1.1. PODWARSTWA ELEMENTÓW SIECI

Dla podwarstwy elementów sieci bezwzględnym priorytetem jest zachowanie ciągłości działania. Uzyskuje się to poprzez:

a) budowę i testy odbiorcze sieci zgodnie ze standardami ITU-T i normami krajowymi (np. dla transmisji pomiary stopy błędów, blokowej stopy błędów zgodnie z normą G.703);
b) właściwą synchronizację elementów sieci;
c) nadmiarowe wyposażenie elementów sieci w karty rezerwy gorącej. Wymiarowanie wykonywane przez dostawcę na podstawie wyliczeń statystycznych wynikających z prawa Erlanga i współczynników typu MTBF (*Mean Time Between Failure*), MTR (*Mean Time to Repair*) itp. lub na podstawie parametrów przedstawionych przez operatora;
d) właściwe rozmieszczenie i umieszczenie elementów sieci;
e) właściwe rozmieszczenie części zamiennych;
f) właściwe standardy budowy sieci, właściwe projekty budowy sieci, dokumentację wykonawczą i powykonawczą;
g) właściwe planowanie architektury sieci (budowę zamkniętych pętli transmisyjnych, budowę alternatywnych połączeń logicznych i fizycznych itp.);
h) właściwe wymiarowanie sieci i planowanie jej rozbudowy z wyprzedzeniem, w tym właściwe wymiarowanie punktów styku z innymi operatorami;
i) właściwe procedury utrzymania, w tym prace prewencyjne;
j) właściwe zarządzanie dostępem fizycznym. Dostęp powinien być możliwy tylko i wyłącznie w sposób zdefiniowany i dla osób do tego uprawnionych. Każda operacja dostępu powinna być logowana i nadzorowana, każda operacja zmiany powinna być logowana;
k) właściwe zarządzanie dostępem zdalnym do elementów sieci. Dostęp powinien być możliwy tylko poprzez właściwe systemy zarządzania elementami sieci, tylko i wyłącznie w sposób zdefiniowany i dla osób do tego uprawnionych. Każda operacja dostępu zdalnego powinna być logowana i nadzorowana, każda operacja zmiany powinna być logowana;
l) wszystkie elementy sieci powinny być zdalnie zarządzane;
m) awaria fragmentu sieci lub jej elementów może być awarią nie pilną, pilną, bardzo pilną lub krytyczną, w zależności od kontekstu (wolumenu ruchu, pojemności transmisyjnej, liczby i rodzaju klientów; liczby i rodzaju usług, podpisanych SLA, itp.)
n) właściwe zarządzanie infrastrukturą sieciową/elementami sieci – poprzez systemy warstw wyższych.

2.1.2. PODWARSTWA ZARZĄDZANIA ELEMENTAMI SIECI

Dla podwarstwy zarządzania elementami sieci kluczowe jest zachowanie spójności bazy danych dotyczących rzeczywistej konfiguracji elementów sieci:

a) wszystkie elementy sieci z każdej domeny (technologii) od każdego dostawcy powinny być zarządzane centralnie; do systemów zarządzania elementami sieci zaliczamy również systemy zarządzania obiektami, w tym zarządzania alarmami środowiskowymi oraz systemy kontroli dostępu do obiektów;
b) systemy zarządzania elementami sieci powinny komunikować się z elementami sieci poprzez wyróżnioną sieć zarządzającą, która powinna stanowić wydzielony fizycznie, silnie niezawodny fragment sieci korporacyjnej, z możliwością połączeń alternatywnych na innych segmentach sieci korporacyjnej, np. sieci biurowej lub na sieci VPN (*Virtual Private Network*) MPLS (*Multiprotocol Label Switching*) lub na sieci głosowej komutowanej itp.;
c) systemy zarządzania powinny być dostępne tylko i wyłącznie w sposób zdefiniowany i dla osób do tego uprawnionych. Każda operacja dostępu powinna być logowana i nadzorowana, każda operacja zmiany powinna być logowana;
d) dostęp do systemów powinien być możliwy w sposób lokalny oraz zdalny (tylko i wyłącznie z silną autentyfikacją i kontrolą dostępu). Każda operacja dostępu powinna być logowana i nadzorowana, każda operacja zmiany powinna być logowana;
e) systemy zarządzania powinny zbierać wszelkie informacje dotyczące zdarzeń w elementach sieci na bieżąco, w czasie rzeczywistym. Systemy zarządzania elementami sieci wskutek własnej awarii nie powinny tracić informacji o statusie elementów sieci, a po przywróceniu do ruchu powinny odtworzyć brakującą informację;
f) systemy zarządzania powinny zbierać wszelkie informacje statystyczne dotyczące elementów sieci na bieżąco, w czasie rzeczywistym, aczkolwiek dopuszczalne jest otrzymywanie tej informacji w trybie zwłocznym, np. co 5–15 minut, w zależności od typu elementu sieci. Utrata informacji statystycznej nie jest krytyczna i nie wymaga odzyskania, niemniej jednak systemy zarządzania elementami sieci, po przywróceniu do ruchu po własnej awarii, powinny odtworzyć brakującą informację na podstawie aproksymacji

ze statystyk sprzed i po awarii, według algorytmu uzgodnionego z dostawcą systemu. Uzyskane statystyki służą do monitoringu i zarządzania jakością w pojedynczych elementach sieci, w poszczególnych technologiach czy domenach telekomunikacyjnych w celu inicjowania działań usprawniających (np. rekonfiguracji lub rozbudowy elementów);

g) systemy zarządzania elementami sieci powinny filtrować informacje nieistotne i nadmiarowe;
h) systemy zarządzania elementami sieci służą personelowi technicznemu do uzyskiwania szczegółowych informacji o stanie elementu sieci oraz do dokonywania ich zdalnej rekonfiguracji;
i) systemy powinny być nadmiarowe. Najlepiej, jeśli byłyby umieszczone w oddzielonych fizycznie lokalizacjach (w różnych centrach przetwarzania danych);
j) awaria systemów zarządzania elementami sieci może być awarią pilną lub bardzo pilną (ale niekrytyczną), ponieważ nie wpływa bezpośrednio na ciągłość usług telekomunikacyjnych świadczonych przez operatora. W określonych sytuacjach i dla określonych technologii długotrwała awaria systemów zarządzania elementami sieci może przekształcić się w awarię krytyczną. Operator musi być przygotowany na ewentualność lokalnego monitoringu i ręcznego zarządzania elementami sieci.

2.2. WARSTWA ZARZĄDZANIA SIECIĄ

Dla warstwy zarządzania siecią kluczowe jest zachowanie poufności informacji o architekturze sieci oraz zachowanie spójności między architekturą rzeczywistą i jej obrazem w bazie danych:

a) systemy z tej warstwy powinny być niezależne od technologii sieci. Powinny zbierać i przetwarzać informację w sposób znormalizowany;
b) systemy zarządzania siecią powinny wspomagać następujące funkcje operatora:

- inwentaryzacja i zarządzanie konfiguracją sieci (z wykorzystaniem technologii *Geographical Information Systems* – GIS, tzn. z posadowieniem sieci i jej elementów na mapach cyfrowych),

- filtrowanie i koordynacja zdarzeń. Wizualizacja zdarzeń na ekranie per domena sieci. Wtórna, zależna od kontekstu priorytetyzacja zdarzeń i zarządzanie awariami. Rozdział, koordynacja i zarządzanie pracami, w tym z wykorzystaniem systemów zarządzania pracą mobilną,
- zarządzanie przepustowością sieci,
- zarządzanie ruchem,
- zarządzanie sygnalizacją,
- zarządzanie jakością technologiczną sieci, inicjowanie działań usprawniających,
- planowanie konfiguracji i rozbudowy sieci z uwzględnieniem symulacji awarii krytycznych zasobów sieci;

c) systemy zarządzania siecią powinny komunikować się w ramach sieci zarządzającej, która stanowi wydzielony fizycznie, niezawodny fragment sieci korporacyjnej, z możliwością połączeń alternatywnych na sieci korporacyjnej biurowej lub na sieci VPN MPLS lub na sieci głosowej komutowanej itp.;
d) systemy zarządzania siecią służą personelowi technicznemu do uzyskiwania szczegółowych informacji o stanie sieci oraz do podejmowania właściwych decyzji o pilności i kolejności działań naprawczych oraz planowych pracach prewencyjnych, jak rekonfiguracja ruchu, sygnalizacja, rozbudowa sieci lub prace konserwacyjne na nadprzeciętnie awaryjnych obszarach sieciowych;
e) systemy zarządzania siecią powinny być nadmiarowe, najlepiej rozlokowane w oddzielonych fizycznie lokalizacjach (w różnych centrach przetwarzania danych);
f) powinien być zapewniony bezpieczny dostęp zdalny;
g) awaria systemów zarządzania siecią może być awarią pilną lub bardzo pilną (ale niekrytyczną), ponieważ nie wpływa bezpośrednio na ciągłość usług telekomunikacyjnych świadczonych przez operatora. W określonych sytuacjach i dla określonych funkcji długotrwała awaria systemów zarządzania siecią może przekształcić się w awarię krytyczną. Operator musi być przygotowany na ewentualność suboptymalnego zarządzania siecią, w warunkach częściowego braku informacji o całościowym stanie sieci.

2.3. WARSTWA ZARZĄDZANIA USŁUGAMI

Dla warstwy zarządzania usługami kluczowe jest zachowanie poufności informacji o architekturze usług oraz **spójności** między architekturą rzeczywistą i jej obrazem w bazie danych:

a) systemy z tej warstwy powinny być niezależne od technologii sieci oraz od typu świadczonych usług. Powinny zbierać i przetwarzać informację w sposób znormalizowany;
b) systemy zarządzania usługami powinny wspomagać następujące funkcje operatora:

- inwentaryzacja i zarządzanie konfiguracją usług, mapowanie ich na logicznej i fizycznej reprezentacji sieci operatora (z wykorzystaniem technologii GIS),
- utrzymanie i wprowadzanie nowych usług, zarządzanie taryfami i dyskontami,
- filtrowanie i koordynacja zdarzeń. Wizualizacja zdarzeń sieciowych per usługi. Wtórna, zależna od kontekstu priorytetyzacja zdarzeń i zarządzanie awariami. Rozdział, koordynacja i zarządzanie pracami prewencyjnymi i naprawczymi, w tym z wykorzystaniem systemów zarządzania pracą mobilną,
- zarządzanie przepustowością sieci i usług,
- planowanie konfiguracji i rozbudowy sieci z uwzględnieniem prognoz sprzedaży i zgodnie z harmonogramem promocji oraz wprowadzania nowych usług,
- planowanie premier i promocji,
- zarządzanie jakością poszczególnych usług, inicjowanie działań usprawniających,
- stosowanie obniżek i upustów;

c) systemy zarządzania usługami powinny stanowić wydzielony logicznie fragment sieci korporacyjnej (segment), z możliwością połączeń alternatywnych na sieci korporacyjnej biurowej lub na sieci VPN MPLS, lub na sieci głosowej komutowanej;
d) systemy zarządzania usługami powinny być nadmiarowe, najlepiej rozlokowane w oddzielonych fizycznie lokalizacjach (w różnych centrach przetwarzania danych);

e) awaria systemów zarządzania usługami może być awarią niepilną, pilną lub bardzo pilną (ale niekrytyczną), ponieważ nie wpływa bezpośrednio na ciągłość usług telekomunikacyjnych świadczonych przez operatora. W określonych sytuacjach i dla określonych funkcji długotrwała awaria systemów zarządzania usługami może przekształcić się w awarię krytyczną.

2.4. WARSTWA ZARZĄDZANIA RELACJAMI Z KLIENTEM

Dla warstwy zarządzania relacjami z klientem kluczowe jest zachowanie poufności danych osobowych i danych telekomunikacyjnych:

a) systemy z tej warstwy powinny być niezależne od typu świadczonych usług oraz od segmentu klienta. Powinny zbierać i przetwarzać informację w sposób znormalizowany;
b) systemy zarządzania relacjami powinny wspomagać następujące funkcje operatora:

- inwentaryzacja i zarządzanie konfiguracją klientów i świadczonych im usług, w tym zapewnienie możliwości mapowania usług na logiczne i fizyczne zasoby sieciowe,
- utrzymanie i wprowadzanie nowych abonentów,
- filtrowanie i koordynacja zdarzeń. Wizualizacja zdarzeń sieciowych per klienci (w celu identyfikacji klientów objętych np. awarią masową). Wtórna, zależna od kontekstu priorytetyzacja zdarzeń i zarządzanie awariami z dodaniem kontekstu poziomu obsługi klienta (SLA). Rozdział, koordynacja i zarządzanie pracami, w tym z wykorzystaniem systemów zarządzania pracą mobilną,
- udzielanie informacji o usługach, techniczne wsparcie klienta, udzielanie informacji o numerach (książka telefoniczna),
- przyjmowanie zleceń, przyjmowanie informacji o awarii,
- naliczanie płatności za usługi według właściwych taryf, drukowanie i dystrybucja rachunków, udzielanie informacji o rachunkach i płatnościach, obsługa reklamacji, udzielanie rabatów,
- marketing, promocje, sprzedaż, telesprzedaż,
- zapewnianie przychodów: sprawdzanie wiarygodności klientów (*credit checking*), wykrywanie i zarządzanie fraudem telekomunikacyjnym, zarządzanie poprawnością bilingu (*end-to-end*

billing reconciliation), zarządzanie poprawnością opłat między operatorami (*end-to-end interconnect reconciliation*), windykacja, zarządzanie odejściami (migracją) klientów,
- zarządzanie jakością obsługi klienta, stosownie do wymagań i gwarantowanego SLA, inicjowanie działań doskonalących,
- wspomaganie zadań samoobsługowych;

c) systemy zarządzania relacjami z klientem powinny stanowić wydzielony logicznie fragment sieci korporacyjnej (segment), z możliwością połączeń alternatywnych na sieci korporacyjnej biurowej lub na sieci VPN MPLS, lub na sieci komutowanej itp.
d) systemy zarządzania relacjami z klientem powinny być nadmiarowe, najlepiej rozlokowane w oddzielonych fizycznie lokalizacjach (w różnych centrach przetwarzania danych);
e) awaria systemów zarządzania relacjami z klientem może być awarią niepilną, pilną lub bardzo pilną (ale niekrytyczną), ponieważ nie wpływa bezpośrednio na ciągłość usług telekomunikacyjnych świadczonych przez operatora. W określonych sytuacjach i dla określonych funkcji długotrwała awaria systemów zarządzania relacjami z klientem może przekształcić się w awarię krytyczną. Operator musi być przygotowany na wystąpienie awarii systemów wspomagających, gdy nie ma dostępu do informacji szczegółowej dotyczącej klienta i zachodzi konieczność pracy ręcznej, np. w arkuszach Excel lub na kartkach papieru. Sprawdzonym modelem obsługi klienta jest rozproszenie telefonicznego centrum obsługi klienta (TCOK) w kilku lokalizacjach, z pełnym bilansem i przelewem ruchu, z możliwością pełnej obsługi, niezależnie od lokalizacji klienta i TCOK.

2.5. WARSTWA ZARZĄDZANIA BIZNESEM

Dla warstwy zarządzania biznesem krytyczne są dane zapewniające przewagę biznesową oraz raporty giełdowe chronione prawnie. Wiarygodność danych jest bezwzględnie wymagana, czas dostępu ma tu znaczenie wtórne:

a) systemy zarządzania biznesem powinny wspomagać następujące funkcje operatora

- inwentaryzacja środków trwałych i ich amortyzacja, księgowość, kontroling, sprawozdawczość,
- hurtownia danych, raportowanie i systemy wspomagania podejmowania decyzji,
- zarządzanie jakością we wszystkich warstwach modelu zarządzania, utrzymanie certyfikatu jakości ISO 9000 i innych uzyskanych certyfikatów, inicjowanie działań doskonalących,
- zarządzanie relacjami z mediami,
- zarządzanie relacjami z inwestorami,
- zarządzanie bezpieczeństwem (szacowanie ryzyka i postępowanie z ryzykiem, systemy zapobiegania włamaniom odporne na tzw. ataki dnia pierwszego (*Intruder Detection/Prevention Systems* – IDS/IPS), systemy zarządzania siecią korporacyjną, systemy wykrywania nadużyć wewnętrznych, systemy zarządzania tożsamością, systemy zarządzania dostępem, systemy zbierania i monitorowania informacji zewnętrznych, systemy monitorowania, filtrowania i korelowania wszystkich zdarzeń bezpieczeństwa, badania trendów i anomalii, klasyfikacji zachowań, badania ich zgodności z rolami biznesowymi, badania akuratności dostępów rzeczywistych z przydzielonymi itd.);

b) systemy zarządzania biznesem powinny stanowić wydzielone logicznie fragmenty sieci korporacyjnej (segmenty), z możliwością połączeń alternatywnych na sieci korporacyjnej biurowej lub na sieci VPN MPLS lub na sieci głosowej komutowanej itp.;
c) systemy zarządzania biznesem powinny być nadmiarowe, najlepiej rozlokowane w oddzielonych fizycznie lokalizacjach (w różnych centrach przetwarzania danych);
d) awaria systemów zarządzania biznesem może być awarią niepilną, pilną, bardzo pilną lub krytyczną, chociaż nie musi wpływać bezpośrednio na ciągłość usług telekomunikacyjnych świadczonych przez operatora, ale może wpłynąć na biznes i postrzeganie marki w sposób krytyczny dla działalności przedsiębiorcy. W określonych sytuacjach i dla określonych funkcji długotrwała niekrytyczna awaria systemów zarządzania biznesem może przekształcić się w awarię krytyczną. Operator musi być przygotowany na ewentualność awarii systemów wspomagających, w razie braku dostępu do informacji szczegółowej dotyczącej wyników finansowych, na wypadek błędnie wyliczonych danych biznesowych lub tym podobnych sytuacji.

W tabeli 1 przedstawiono schematyczny obraz wartości atrybutów bezpieczeństwa informacji w poszczególnych warstwach zarządzania procesami operatora/dostawcy usług. Wartości te ilustrują poglądy autora i nie muszą się pokrywać ze zmierzonym stanem bezpieczeństwa u operatora.

Tabela 1. Wartości atrybutów bezpieczeństwa informacji w poszczególnych warstwach zarządzania (ocena w skali od 1 do 4, 1 = min, 4 = max)

Warstwa	*Poufność*	*Integralność*	*Dostępność*	*Rozliczalność*
Elementów sieci	*2*	*2*	*3*	*3*
Zarządzania elementami sieci	*2*	*3*	*2*	*3*
Zarządzania siecią	*3*	*3*	*1*	*3*
Zarządzania usługami	*2*	*2*	*2*	*2*
Zarządzania relacjami z klientem	*3*	*3*	*2*	*2*
Zarządzania biznesem	*3*	*3*	*1*	*2*

Poufność – *ochrona przed ujawnieniem informacji nieuprawnionemu odbiorcy.*

Integralność – *ochrona przed modyfikacją, zniekształceniem lub zniszczeniem informacji przez osobę nieuprawnioną.*

Dostępność – *gwarancja uprawnionego dostępu do informacji zawsze, gdy jest to niezbędne.*

Rozliczalność – *możliwość określenia i weryfikacji odpowiedzialności za działania, usługi i realizowane funkcje.*

W rzeczywistości w każdej warstwie mogą wystąpić informacje jawne lub poufne. O ich klasyfikacji decyduje właściciel informacji.

Dla atrybutu „dostępność" wartości najniższe nie oznaczają, że dana informacja może być niedostępna w ogóle, lecz jedynie to, że czas dostępu do niej nie jest krytyczny i może wynosić np. kilka godzin lub kilka dni bez istotnego wpływu na straty lub ciągłość działania operatora.

Wnioski:

- Im niższa warstwa w modelu zarządzania, tym wyższe wymagania odnośnie do dostępności (niezawodności) i rozliczalności. Ogólnie, systemy transakcyjne (operacyjne) muszą pracować w sposób ciągły, każda operacja dostępu i zmiany powinna być rejestrowana. Operator telekomunikacyjny **musi** świadczyć usługi telekomunikacyjne, nawet jeśli chwilowo nie jest w stanie ich taryfikować. Intuicyjnie, dla centrali telefonicznej jedna sekunda przerwy w ruchu jest krytyczna, zaś jeden bit przekłamany nie ma praktycznego znaczenia.
- Im wyższa warstwa, tym większą wagę przywiązuje się do ochrony poufności i integralności informacji. Dla systemów zarządzania relacjami biznesowymi i biznesem (systemów analitycznych, taktycznych lub strategicznych) kilkugodzinna przerwa w działaniu procesów nie ma znaczenia, zaś wyciek lub przekłamanie informacji mogą być krytyczne.
- Z przyczyn praktycznych i ekonomicznych metody, techniki i technologie ochrony sieci i systemów są identyczne niezależnie od warstwy, natomiast podczas analizy zdarzeniom i incydentom nadaje się różną wagę , różne priorytety oraz przypisuje im różne instrukcje postępowania, co pozwala na reagowanie adekwatne do bodźca i potencjału zagrożenia.

3. ZASADY BEZPIECZEŃSTWA

Zawsze u każdego operatora telekomunikacyjnego występują dwa obszary informacji poufnych oraz zwykle dwie organizacje zajmujące się bezpieczeństwem i ochroną informacji w tych obszarach:

a) informacje niejawne (w sensie ustawy o ochronie informacji niejawnych) oraz współpraca z uprawnionymi organami państwa, wynikająca z obowiązków wymienionych w ustawie – Prawo telekomunikacyjne;

b) informacje korporacyjne (firmowe) – dane osobowe (w sensie ustawy o ochronie danych osobowych), dane teletransmisyjne (w sensie ustawy – Prawo telekomunikacyjne), tajemnica przedsiębiorstwa (w sensie ustawy o ochronie przed nieuczciwą konkurencją), inne.

3.1. INFORMACJE NIEJAWNE

W obszarze informacji niejawnych odpowiedzialność spoczywa na kierowniku jednostki organizacyjnej (zykle jest to prezes firmy), który jest bezpośrednio wspomagany przez pełnomocnika zarządu do spraw ochrony informacji niejawnych i jego jednostkę organizacyjną. W ramach tej struktury operator musi posiadać certyfikowaną kancelarię tajną oraz pracowników certyfikowanych przez uprawnione organy państwa do dostępu do informacji niejawnych. Wymagania dla kancelarii tajnej są dobrze opisane w obowiązujących przepisach. Każdy operator musi spełniać te wymagania.

Analogiczne do rozważań dla modelu warstwowego da się przypisać wartości atrybutów bezpieczeństwa dla obszaru informacji niejawnych.

Tabela 2. Wartości atrybutów bezpieczeństwa informacji dla obszaru informacji niejawnych (skala od 1 do 4)

Warstwa	*Poufność*	*Integralność*	*Dostępność*	*Rozliczalność*
Kancelaria tajna	*4*	*4*	*4*	*4*

3.2. INFORMACJE KORPORACYJNE

W obszarze informacji korporacyjnych obowiązują zasady opisane w polityce bezpieczeństwa firmy. Dokument ten nie powinien być zbyt długi, wystarczy kilka zdań deklaratywnych, mówiących o wadze, jaką firma przywiązuje do bezpieczeństwa i ciągłości działania, do jakości swoich usług, produktów i rozwiązań. Operatorzy publiczni są organizacjami rynkowymi i ich głównym celem długoterminowym jest przetrwanie i odniesienie sukcesu (cokolwiek by to znaczyło dla różnych grup interesów) dzięki świad-

czeniu **bezpiecznych usług** telekomunikacyjnych (dla klientów z różnych segmentów lub branż pojęcie to ma rożne znaczenie, różną wartość i cenę), a nie świadczeniu stricte usług bezpieczeństwa. Dlatego też w promowaniu usług i postrzeganiu ich przez klienta musi być pełna harmonia. Klient nie „kupi" bezpieczeństwa, jeśli nie widzi w tym sensu biznesowego. Produkty i usługi zawsze trzeba dobrze opakować i właściwie przedstawić, eksponując zyski. Dla klientów mających specyficzne i silne wymagania bezpieczeństwa mają sens projekty wdrożeniowe z udziałem personelu klienta oraz uprawnionego, certyfikowanego personelu operatora.

Szczegółowe zasady obowiązujące w firmie powinny być opisane w dokumentach niższego rzędu, np. regulaminach, procedurach i instrukcjach dotyczących bezpieczeństwa informacji, ochrony fizycznej i bezpieczeństwa osób i mienia, szacowania ryzyka, zarządzania kryzysowego, planowania ciągłości biznesowej i działań odtworzeniowych, monitoringu, audytowania i prowadzenia działań doskonalących. Najważniejsze zasady powinny być opisane w sposób popularny (językiem prostym, powszechnie zrozumiałym) w regulaminie bezpieczeństwa, który powinien obowiązywać wszystkich pracowników i współpracowników operatora oraz osoby przebywające na jego terenie.

Wszystkie zasady bezpieczeństwa są jednakowo ważne, stanowią jednolity łańcuch obronny, który jest tak mocny, jak mocne jest jego najsłabsze ogniwo.

3.2.1. BEZPIECZEŃSTWO FIZYCZNE

Podstawą każdego systemu bezpieczeństwa jest bezpieczeństwo fizyczne. Problemem każdego operatora telekomunikacyjnego jest rozległość i rozproszenie obiektów oraz sieci.

Dlatego też każdy obiekt budowlany, każde pomieszczenie musi mieć przydzielonego administratora i właściciela (głównego użytkownika), który osobiście odpowiada za wszystko, co się dzieje w nadzorowanych przez niego pomieszczeniach.

Każdy obiekt węzłowy (a pamiętamy, że u operatora średniej wielkości jest ich kilka/kilkadziesiąt, u dużego operatora – nawet kilkaset) powinien posiadać ochronę fizyczną i być strzeżony w reżimie 24/7/365 przez

certyfikowane firmy ochroniarskie. Dodatkowo powinny być zagwarantowane inne usługi bezpieczeństwa na żądanie, jak reakcja zespołów interwencyjnych, asysta, konwojowanie. Obiekty centrali muszą być wyposażone w podwójne linie zasilające z dwóch różnych stacji transformatorowych 15 kV, w systemy zasilania awaryjnego UPS (*Unit Power System*) pozwalające na kilkadziesiąt godzin pracy niezależnej, w generatory prądu zmiennego zaopatrzone w paliwo na co najmniej 72 godziny pracy, w systemy przeciwpożarowe (w tym detekcji i monitoringu, wczesnego wykrywania dymu, systemy aktywnego gaszenia, np. gazem FM200 – gdy przepisy prawne, analiza ryzyka lub klienci tego wymagają), systemy nadzoru alarmów środowiskowych i kontroli dostępu, systemy telewizji dozorowej CCTV (*Closed-Circuit Television*). Wszystkie systemy powinny być centralnie monitorowane i zarządzane w trybie 24/7/365 przez centrum zarządzania siecią (CZS), właściwie konserwowane i unowocześniane. Obiekty te są także podzielone na strefy dostępu, z wyraźnym wydzieleniem pomieszczeń technologicznych.

Każdy obiekt bezzałogowy (około tysiąca u operatora średniej wielkości, nawet kilkunaście tysięcy (!) u dużego operatora) powinien być wyposażony w homogeniczne systemy zdalnego monitorowania alarmów i kontroli dostępu. Wszystkie obiekty powinny być monitorowane i zarządzane zdalnie z CZS. Obiekty bezzałogowe powinny być również wyposażone w systemy UPS, umożliwiające kilkugodzinną autonomiczną pracę w wypadku zaniku zasilania, aż do czasu powrotu napięcia lub przybycia załogi interwencyjnej, wyposażonej w przewoźne lub przenośne generatory prądu zmiennego.

Obecnie występuje tendencja wyposażania wszystkich obiektów w system centralnie nadzorowanych kamer internetowych, tak aby dać operatorom CZS możliwość właściwego oglądu sytuacji w wypadku wystąpienia jakiegoś niepokojącego zdarzenia czy alarmu i podjęcia optymalnej decyzji. W obiektach technologicznych rezygnuje się z ciągłej obecności pracowników ochrony fizycznej dozorujących obiekt. Zamiast tego, wzmacnia się nadzór elektroniczny i wykorzystuje się sprawnie i profesjonalnie działające mobilne zespoły interwencyjne, z gwarantowanym minimalnym czasem dojazdu. Jest to rozwiązanie skuteczniejsze i tańsze.

Dostęp do obiektów powinien być przydzielany dla każdego wejścia (wyjścia) indywidualnie każdemu pracownikowi, współpracownikowi lub

klientowi, w ramach typowych profili dostępu, zależnych od funkcji i roli biznesowej każdego użytkownika. Dostęp do obiektów powinien być przydzielany za pomocą systemu kontroli tożsamości i dostępu, z zachowaniem reguł biznesowych i aktualnej polityki bezpieczeństwa.

Sieci dostępowe kablowe są instalowane w kanalizacji kablowej. Dostęp do sieci jest możliwy na przełącznicy głównej (zawsze znajduje się ona w chronionym obiekcie budowlanym), w studzienkach i szafkach kablowych oraz na terenie lub w pomieszczeniach klienta. Studzienki kablowe mogą być chronione podwójną pokrywą. Pokrywy wewnętrzne, szafki kablowe, obiekty bezzałogowe powinny być zamykane certyfikowanym zamkiem w systemie „klucza – matki" (*Master Key System* – MKS). Dodatkowo ciągi kablowe mogą być chronione elektronicznym systemem sygnalizacji otwarcia, adresowalnym do każdej studzienki lub szafki indywidualnie. Za ochronę części sieci dostępowej zlokalizowanej na terenie lub w pomieszczeniach klienta zwykle odpowiada klient. Są też możliwe inne aranżacje techniczno-organizacyjne, w zależności od wzajemnych ustaleń i konkretnych potrzeb lub możliwości. Za fragmenty sieci dostępowej dzierżawione od innego operatora zwykle odpowiada inny operator, chyba że inaczej ustalono warunki techniczno-organizacyjne w umowie o wzajemnej współpracy.

Sieci dostępowe radiowe są chronione skutecznie na poziomie kodowania sygnału radiowego. W systemach dostępu radiowego nie ma łatwej możliwości nieautoryzowanego podsłuchu lub ingerencji w sygnał radiowy, a zwykle jest to wręcz niemożliwe.

Wszystkie osoby mające dostęp do obiektów operatora muszą przestrzegać zasad zawartych w regulaminach bezpieczeństwa. Dla pracowników lub współpracowników operatora powinny być organizowane cykliczne, rutynowe szkolenia z dziedziny bezpieczeństwa. Dodatkowo muszą być organizowane szkolenia specjalistyczne lub na żądanie określonych grup pracowniczych, odgrywających specyficzne role biznesowe.

3.2.2. BEZPIECZEŃSTWO INFORMACJI

Kolejnym istotnym obszarem jest bezpieczeństwo informacji. Właścicielem informacji zawsze jest prezes zarządu. Wszystkie informacje w firmie powinny być podzielone na grupy informacji (np. finansowe,

kadrowe, komercyjne i klienckie, technologiczne, itp.). Każda grupa informacji musi mieć przydzielonego właściciela (z reguły na poziomie członka zarządu), który jednoosobowo odpowiada za bezpieczeństwo informacji z jego grupy. Informacje w grupie powinny być podzielone na typy informacji, do których jest przypisana klauzula poufności (np. jawne, do użytku wewnętrznego, zastrzeżone – tajemnica przedsiębiorstwa). Informacje są przetwarzane w systemach. Systemy są chronione adekwatnie do klauzuli poufności przetwarzanych informacji. Za każdy system odpowiada jednoznacznie wyznaczony administrator systemu. Dodatkowo nad przestrzeganiem zasad bezpieczeństwa informacji powinien czuwać pion kontrolny, który wspiera i kontroluje działania właścicieli informacji i administratorów systemów. Działania pionu kontrolnego są koordynowane przez dział bezpieczeństwa. Pracownicy różnych działów wykonują pewne funkcje kontrolne w uzupełnieniu do swojej zwykłej roli biznesowej w firmie.

Wszystkie systemy bezpieczeństwa fizycznego, bezpieczeństwa informacji (w tym systemy zapewniające odporność na tzw. ataki dnia pierwszego), serwery aplikacji, poczty elektronicznej, Proxy, serwery produkcyjne (CRM, biling...), systemy bezpieczeństwa (IDS/IPS...) i inne, powinny być podpięte pod system monitoringu zdarzeń, który non-stop przez cały rok analizuje miliardy zdarzeń zapamiętanych w zunifikowanej postaci. System ten powinien filtrować zdarzenia nadmiarowe oraz korelować zdarzenia pochodzące z wielu niezależnych systemów i aplikacji (w tym pochodzące ze źródeł zewnętrznych, np. białego wywiadu), agregować informację i tworzyć zdarzenia złożone, wtórne, w kategorii takich obiektów, jak człowiek-użytkownik, grupa ludzi, obiekt budowlany, przejście kontrolowane, grupa e-mailowa, system, aplikacja i tym podobne. Dla każdego obiektu i na podstawie długotrwałych obserwacji statystycznych system powinien tworzyć profile zachowań indywidualnych, typowe zachowania klasyfikować w grupy, śledzić zachowania odbiegające od normy, roli biznesowej, wykrywać zmiany zachowań, trendy i tendencje zmian wraz z podaniem przyczyn dominujących. System powinien zapewniać również zadawanie skomplikowanych zapytań, w tym również w technologii *fingerprinting* oraz powinien mieć bogate możliwości graficzne wizualizacji i analizy wyników. Powinien tworzyć alarmy i raporty oraz rozsyłać je do odpowiedzialnego personelu, np. operatorów CZS, specjalistów bądź administratorów IT, do działu bezpieczeństwa, do działu relacji z mediami itp. System powinien gwarantować, że żadne z milionów zdarzeń dziennie nie będzie zignorowane lub przeszacowane. Powinien wcześnie wyłowić negatywne tendencje,

przydzielić priorytety, wskazać dominujące przyczyny negatywnych trendów i zapewnić możliwość wczesnego reagowania na zagrożenia. Wdrożenie takiego systemu znakomicie zastępuje pracę kilkudziesięciu ludzi, którzy i tak percepcję mieliby ograniczoną do analizy i korelacji bardzo skończonej liczby zdarzeń.

Istotnym elementem bezpieczeństwa informacji jest również właściwa architektura systemów, właściwa polityka zarządzania wersjami oprogramowania (w tym wgrywanie poprawek systemowych i aplikacyjnych we właściwym czasie, testy laboratoryjne w warunkach zbliżonych do naturalnych dla nowych wersji sprzętu i oprogramowania), właściwe zarządzanie konfiguracją oprogramowania oraz właściwe procedury tworzenia kopii baz danych i oprogramowania, a także właściwe i testowane procedury odtworzeniowe.

3.2.3. BEZPIECZEŃSTWO OSOBOWE

Kolejnym obszarem jest bezpieczeństwo osobowe. Przez bezpieczeństwo osobowe rozumie się wszelkie działania zabezpieczające instytucję przed zaskakującymi działaniami od wewnątrz, czyli ze strony własnego personelu. Przede wszystkim to ludzie są nośnikami informacji, to ludzie obsługują systemy i popełniają błędy, to ludzie są narażeni na pokusy lub celowe działania zewnętrzne.

Ataki z zewnątrz z reguły są przypadkowe i mogą spowodować problem, ataki wewnętrzne są precyzyjnie wymierzone w słabe punkty firmy i mogą ją zniszczyć. Statystycznie ponad ¾ poważnych problemów wynika z wewnętrznych incydentów bezpieczeństwa.

Bezpieczeństwo osobowe to wiedza, czy ludzie robią to, co powinni robić. To również samokontrola każdego pracownika. Popełnić błąd może każdy, ale ten sam błąd najwyżej raz. Zawsze trzeba mówić to, co się chce powiedzieć, a nie mówić to, co się wie.

Bezpieczeństwo osobowe to przede wszystkim:

a) tworzenie odpowiedniej i stabilnej kultury korporacyjnej przedsiębiorstwa;
b) właściwa komunikacja;

c) zarządzanie kadrami i zasady rekrutacji (szczegółowa weryfikacja pracowników na istotne stanowiska pracy, właściwe umowy o pracę, regulaminy pracy, regulaminy bezpieczeństwa, umowy o przestrzeganiu poufności informacji);
d) zarządzanie tożsamością i uprawnieniami dostępu do informacji;
e) zarządzanie obowiązkami, uprawnieniami i odpowiedzialnością;
f) współpraca i zaufanie, ale brak tolerancji na krytyczne błędy, celowe lub wynikające z postaw rażąco lekceważących;
g) organizacja warsztatów, ćwiczeń i szkoleń;
h) monitorowanie zdarzeń, zachowań i ich trendów, w tym z wykorzystaniem technik białego wywiadu i firm detektywistycznych; reagowanie na nietypowe sytuacje bądź zachowania;
i) audyty i badania poziomu kultury korporacyjnej;
j) korygowanie zachowań niepożądanych oraz wyciąganie konsekwencji służbowych i prawnych;
k) szkolenia, szkolenia, szkolenia...

Kulturę organizacji buduje się długo, zniszczyć ją można w jednej chwili. I dlatego bardzo ważna jest stabilność oraz ciągłość historyczna kultury korporacyjnej, która musi być niezależna od chwilowych zmian wynikających z przeobrażeń organizacyjnych, osobowych, trendów i mody, czy nawet ze zmiany strategii firmy.

Człowiek jest zwykle najsłabszym ogniwem w łańcuchu bezpieczeństwa. Cała sztuka polega na tym, aby uczynić z niego element najsilniejszy, ewentualne zaś podatności na błędy lub skutki jego błędów neutralizować metodami technicznymi, proceduralnymi i (lub) organizacyjnymi.

3.2.4. ZARZĄDZANIE KRYZYSOWE

Kolejnym zagadnieniem z obszaru bezpieczeństwa jest zarządzanie kryzysowe, zwłaszcza w kontekście kryzysów rozległych, powstałych z przyczyn niezależnych od operatora, jak np. katastrofy naturalne, epidemie, strajki, sabotaż lub dywersja, zmiany na rynku, zmiany prawa, zmiany na giełdzie, zmiany kursów walut itp. W ramach prac nad zapewnieniem ciągłości biznesowej należy wyróżnić procesy i zasoby krytyczne operatora (zwykle nie więcej niż cztery lub pięć), będące przedmiotem priorytetowej ochrony i odtwarzania, wdrożyć organizację kryzysową, opracować i uzgodnić procedury i plany zachowania ciągłości biznesowej. Procedury i plany muszą być

cyklicznie weryfikowane pod kątem aktualności, biorąc pod uwagę zmiany zewnętrzne i wewnętrzne w firmie, podlegają też testom i ćwiczeniom praktycznym w celu weryfikacji poprawności, efektywności oraz zupełności. Muszą być też uzgadniane z organami państwa (plan ogólny a także szesnaście planów rejonowych). Konieczne są ciągłe prace doskonalące, w tym inwestycyjne, w celu optymalizacji czasu przywrócenia ciągłości działania i odtworzenia na wypadek powstania sytuacji katastroficznych, niezależnie od ich przyczyny.

Priorytetem w zarządzaniu kryzysowym jest szacowanie ryzyka i planowanie działań w kierunku zmniejszenia prawdopodobieństwa zdarzenia, zwiększenia odporności systemu lub przeniesienie ryzyka na inne strony (np. przez podwykonawstwo, ubezpieczenia), tak aby poziom ryzyka resztkowego był akceptowalny.

Niemniej jednak podczas planowania BCP należy założyć, że mimo działań prewencyjnych doszło do najgorszego, czyli całkowitego zniszczenia obiektu (np. centrali), niezależnie od przyczyny. I dla takiego przypadku należy pisać scenariusze i planować działania zachowania ciągłości i działania odtworzeniowe.

Na takie sytuacje rozsądnie jest zaplanować użycie wstępnie wyekwipowanych obiektów kontenerowych oraz przygotować scenariusze przerzucenia ruchu i usług na pozostałe, jeszcze sprawne obiekty technologiczne. Celem dnia pierwszego jest utrzymanie lub odtworzenie ruchu na obiektach i dla klientów priorytetowych, następnie odtworzenie transmisji i przerzucenie całego ruchu według przygotowanych scenariuszy dla obiektów współpracujących w czasie najkrótszym z możliwych, a potem spokojne przystąpienie do odtworzenia zniszczonego obiektu i przywrócenie stanu sprzed katastrofy.

Plany awaryjne muszą być testowane na żywo lub w warunkach symulowanych, gdy to pierwsze jest zbyt ryzykowne lub kosztowne. Zauważone braki muszą być usuwane, a nieskuteczne działania usprawniane.

3.2.5. ZARZĄDZANIE RYZYKIEM

Celem zarządzania ryzykiem jest to, aby reakcja na ryzyko była adekwatna do skutków, zaś koszty postępowania z ryzykiem niższe od ewentualnych strat.

Jedną z prostych i skutecznych metod szacowania ryzyka, praktycznie do zastosowania w każdej dziedzinie biznesowej, jest metoda oparta na tabeli wyliczeniowej. Z trzech czynników zmiennych (wskaźnik wartości strat, wskaźnik prawdopodobieństwa ryzyka oraz wskaźnik odporności systemu na to ryzyko) jest wyliczana wartość rzeczywista ryzyka (pomijalne, małe, średnie i duże).

Tabela 3. Możliwe wartości wskaźnika ryzyka

Prawdopodobieństwo wystąpienia zdarzenia dla wskazanego aktywu	Skala wartości dla ryzyka	0			1			2		
	Skala wartości dla podatności	0	1	2	0	1	2	0	1	2
Skutki	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	1	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**
	2	**0**	**2**	**4**	**2**	**4**	**6**	**4**	**6**	**8**
	3	**0**	**3**	**6**	**3**	**6**	**9**	**6**	**9**	**12**
	4	**0**	**4**	**8**	**4**	**8**	**12**	**8**	**12**	**16**

*Wskaźnik ryzyka = skutki * (wartość ryzyka + wartość podatności).*

- *Ryzyko jest pomijalne, gdy wskaźnik ryzyka = 0, 1, 2.*
- *Ryzyko jest małe, gdy wskaźnik ryzyka = 3, 4, 6.*
- *Ryzyko jest średnie, gdy wskaźnik ryzyka = 8, 9, 12.*
- *Ryzyko jest duże, gdy wskaźnik ryzyka = 16.*

Tabela 4. Możliwe wartości wskaźnika ryzyka

Wartość (strat lub zysków)	*Wartość (strat lub zysków)*
Pomijalna (0)	Skutki finansowe dla firmy nie przekroczą zapewne x0 zł. Nie mają żadnego wpływu na strategię i działalność operacyjną firmy. Są niezauważalne dla uczestników.
Mała (1)	Skutki finansowe dla firmy wyniosą zapewne między x0 a x1 zł. Nie mają wpływu na strategię i działalność operacyjną firmy. Są mało zauważalne dla uczestników.
Średnia (2)	Skutki finansowe dla firmy wyniosą zapewne między x1 a x2 zł. Mają mały wpływ na strategię i działalność operacyjną firmy.
Duża (3)	Skutki finansowe dla firmy wyniosą zapewne między x2 a x3 zł. Mają umiarkowany wpływ na strategię i działalność operacyjną firmy. Wzbudzają umiarkowane zaniepokojenie uczestników.
Bardzo duża (4)	Skutki finansowe dla firmy przekroczą zapewne x3 zł. Mają duży wpływ na strategię i działalność operacyjną firmy. Wzbudzają duże zaniepokojenie uczestników.

Tabela 5. Skala wartości wskaźnika ryzyka

Stopień prawdopodobieństwa	*Opis*	*Wskaźniki*
Niskie (0) – mało prawdopodobne	Raczej nie zdarzy się w ciągu 10 lat bądź prawdopodobieństwo jest mniejsze od 2%	Nie zdarzyło się nigdy. Raczej się nie zdarzy.
Średnie (1) – możliwe	Raczej zdarzy się w ciągu 10 lat bądź prawdopodobieństwo wynosi poniżej 25%	Mogło się zdarzyć więcej niż raz w analizowanym okresie (np. 10 lat). Może być trudne do kontrolowania, np. wskutek pewnych okoliczności zewnętrznych. Czy zdarzyło się do tej pory?
Wysokie (2) - prawdopodobne	Raczej zdarzy się w ciągu roku bądź prawdopodobieństwo wynosi powyżej 25%	Zdarzyło się kilka razy w analizowanym okresie (np. 10 lat). Zdarzyło się niedawno.

Tabela 6. Skala wartości dla podatności

Stopień podatności	*Opis*	*Wskaźniki*
Niski (0) – aktyw bardzo odporny na ryzyko	Wpływ ryzyka na aktyw jest pomijalny (np. <5%). W ostatnim okresie (np. 10 lat) mimo zarejestrowania wystąpienia przypadków ryzyka nie zaobserwowano żadnego wpływu ryzyka na aktyw lub wpływ ten był pomijalny (mniejszy od 5%).	Rodzaj ryzyka nieadekwatny dla aktywu. Zastosowano niezbędne akcje zapobiegawcze i (lub) naprawcze redukujące wpływ ryzyka lub prawdopodobieństwo jego wystąpienia do minimum (<2%). Organizacja nie jest gotowa do wykorzystania wystąpienia ryzyka. Przypadki wystąpienia ryzyka powinny być rejestrowane.

Stopień podatności	*Opis*	*Wskaźniki*
Średni (1) – aktyw średnio odporny na ryzyko	Wpływ ryzyka na aktyw nie jest pomijalny (ale <25%). W ostatnim okresie (np. 10 lat) zarejestrowano wystąpienia przypadków ryzyka oraz zaobserwowano nieregularny wpływ na aktyw (w granicach do 25%).	Stwierdzono pewną korelację i wpływ występowania ryzyka na aktyw. Nie zastosowano jeszcze akcji zapobiegawczych i (lub) naprawczych całkowicie eliminujących wpływ ryzyka na aktyw lub całkowicie eliminujących prawdopodobieństwo jego wystąpienia (do poziomu <2%), lub akcje takie nie są planowane. Przy aktualnej organizacji istnieje szansa wykorzystania ryzyka. Przypadki wystąpienia ryzyka i jego wpływ na aktyw powinny być rejestrowane.
Wysoki (2) – aktyw nieodporny na ryzyko	Wpływ ryzyka na aktyw jest duży (>25%). W ostatnim okresie (np. 10 lat) zarejestrowano przypadki wystąpienia ryzyka oraz zaobserwowano regularny wpływ na aktyw (w granicach powyżej 25%).	Stwierdzono powtarzalną korelację i wpływ występowania ryzyka na aktyw. Nie zastosowano jeszcze akcji zapobiegawczych i (lub) naprawczych, redukujących wpływ ryzyka na aktyw przynajmniej do poziomu średniego lub redukujących prawdopodobieństwo jego wystąpienia (przynajmniej do poziomu <25%). Przy istniejącej organizacji z dużą pewnością można wykorzystać szansę. Przypadki wystąpienia ryzyka i jego wpływ na aktyw muszą być rejestrowane.

Dla każdej wartości ryzyka są przewidziane typy działań prewencyjno-usprawniających (np. nic nie rób, obserwuj/monitoruj, zmień procedurę, otwórz projekt, przenieś ryzyko na stronę drugą lub trzecią, wyłącz natychmiast system, przerwij pracę lub proces). Chodzi o to, aby reakcja była proporcjonalna do wartości zagrożenia (skutków).

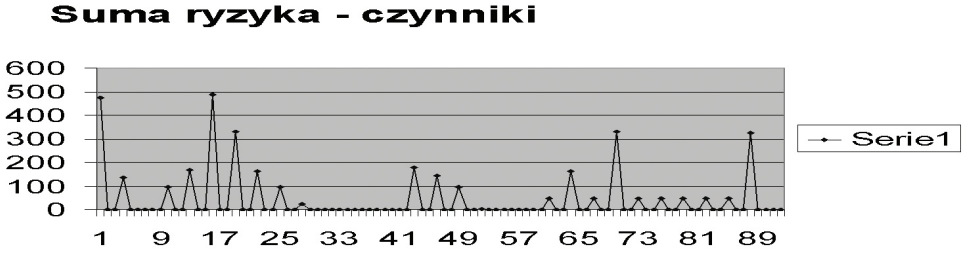
Tabela 7. Wartość ryzyka i zalecane działania

Wartość ryzyka	*Czynności i ich skala czasowa*
Pomijalne	Nie jest wymagana żadna akcja. Żadne specjalne zapisy nie muszą być też przechowywane. Tolerujemy ryzyko.
Małe	Ryzyko jest zachowane. Możliwe jest wdrożenie nowego rozwiązania lub usprawnienia pod warunkiem, że nie spowodują one żadnych dodatkowych kosztów. Wskazany jest monitoring w celu zapewnienia kontroli nad kosztami oraz sprawdzanie, czy zagrożenie również nie zmienia wartości w czasie.
Średnie	Wskazane jest zmniejszenie wartości ryzyka, ale koszty akcji prewencyjnej muszą być starannie kontrolowane i ograniczone. Redukcja wartości ryzyka musi nastąpić w z góry założonym czasie. W celu zredukowania wartości ryzyka do działań powinny być przypisane właściwe i wystarczające zasoby. W wypadku, gdy sprawa dotyczy pracy w toku, akcja prewencyjna musi być podjęta w trybie pilnym.
Duże	Praca nie powinna być kontynuowana (dotyczy również pracy w toku), dopóki wartość ryzyka nie będzie zredukowana do akceptowalnego poziomu. Gdy wartość ryzyka nie może być zmniejszona nawet z użyciem nieograniczonych zasobów, to w takim wypadku należy rozpatrzyć rezygnację z danego działania (procesu).

Szacowanie wartości ryzyka i podejmowanie działań usprawniających jest składnikiem nierozłącznym każdego działania w obszarze zarządzania przedsiębiorstwem. Szacowanie ryzyka jest procesem powtarzalnym dla tego samego typu obiektów. I dlatego jest konieczne przechowywanie historycznych wartości wskaźników; dodatkową jakością poznawczą jest porównywanie wartości ryzyka w czasie (wartości wszystkich wskaźników mogą być zmienne w czasie), a także wartości ryzyka dla obiektów tej samej klasy, w celu identyfikacji działań globalnie optymalnych i najpilniejszych.

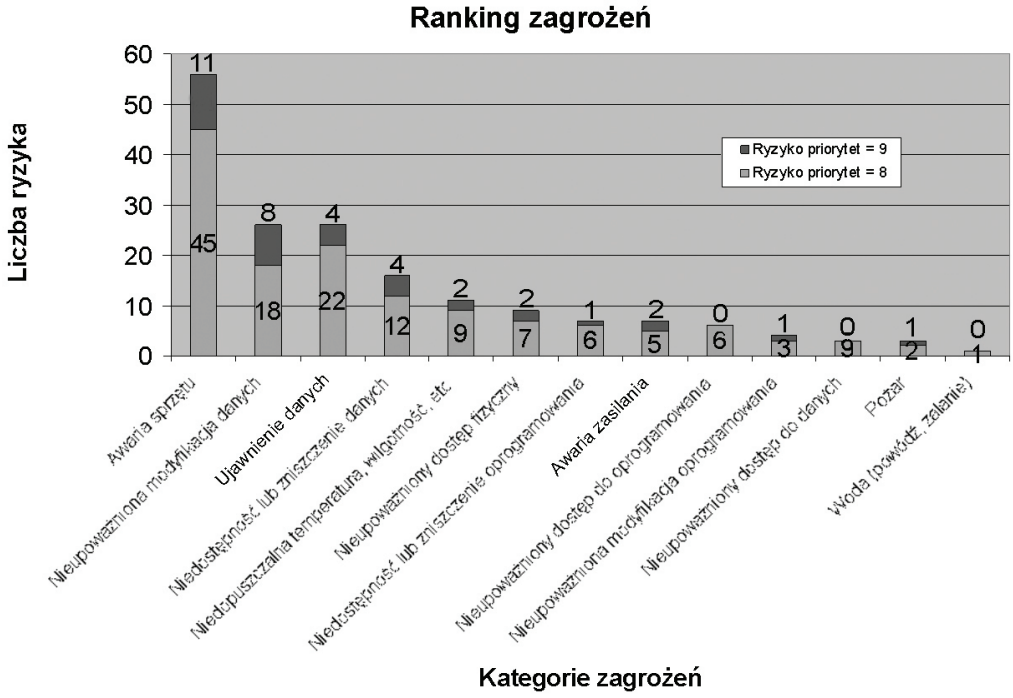
Rys. 4. Przykład analizy zbiorczej: na osi odciętych są czynniki ryzyka, na osi rzędnych jest suma wyników szacowania ryzyka dla 100 analizowanych obiektów

Z rysunku 4 wynika, że w pierwszej kolejności należałoby się zająć ryzykiem nr 1, 17, następnie nr 20, 70 i 89.



Rys. 5. Przykład analizy zbiorczej: na osi odciętych są obiekty poddane analizie ryzyka, na osi rzędnych jest suma wyników szacowania ryzyka dla wszystkich czynników ryzyka

Jak wynika z rysunku 5, w pierwszej kolejności należałoby zająć się obiektami nr 1, 7, 15, 21, 23, 33, 37, 41 itp.



Rys. 6. Przykłady analizy zbiorczej: ranking zagrożeń (czynników ryzyka) dla 100 analizowanych obiektów i dwóch najwyższych wyników (8 i 9 w skali 0-16)

Z rysunku 6 wynika, że dla rodzaju ryzyka „awaria sprzętu" w jedenastu obiektach wartość wskaźnika ryzyka wyniosła 9 (ryzyko średnie, musimy coś zrobić) oraz w czterdziestu pięciu obiektach wartość ta wynosi 8 (ryzyko małe, powinniśmy coś zrobić lub zaplanować działanie w przyszłości, na razie musimy bezwzględnie monitorować awarie, reagować na nie, ale przede wszystkim kontrolować statystyki, czy proces nie ulega zmianie, np. czy prawdopodobieństwo zdarzenia stale i niepokojąco rośnie).

Opisana metoda szacowania ryzyka nie musi być jedyną używaną w firmie. Wszędzie tam, gdzie istnieją bardziej precyzyjne metody wyliczania ryzyka, metody branżowe lub narzucone normami, to należy je stosować, a wyniki zapisywać, analizować i wykorzystywać w sposób podobny do podanego.

4. PODSUMOWANIE

Tak długo, jak operatorzy i ich aktywa są bezpieczni w sensie opisanym powyżej, tak długo są gotowi świadczyć swoje usługi w sposób nieprzerwany. Operatorzy w Polsce już dzisiaj są gotowi świadczyć usługi telekomunikacyjne na wysokim poziomie niezawodności i bezpieczeństwa.

Spełnianie wymagań specjalnych jest kwestią otwartą i indywidualnie do rozwiązania w ramach projektów specjalnych, realizowanych przez operatorów wspólnie z klientem. Oprócz bezpiecznych nowoczesnych usług zaawansowanych technologicznie operatorzy mogą świadczyć usługi standardowe, jak np. kolokacja, dzierżawa ciemnych światłowodów, dzierżawa kabli, dzierżawa kanalizacji, szyfrowanie transmisji i innych, według zapotrzebowania.

Postęp technologiczny, mobilność, konwergencja technologii i usług, standaryzacja, prostota i otwartość interfejsów oprócz niewątpliwych dobrodziejstw przyniosły nowe zagrożenia i podatność na ataki, typowe dla świata IP. Zagrożenia te nie zawsze są sterowalne przez operatorów, bo wynikają z technologii dostawców i ich podatności na zagrożenia oraz z natury działania Internetu, jak np. ataki powodujące natłok i blokadę usług i sieci (*Denial of Service* – DoS lub *Distributed Denial of Service* – DDoS), co zresztą ostatnio miało miejsce w Estonii, gdzie dostęp do wielu publicznych i rządowych serwerów i usług internetowych został zablokowany poprzez atak DDoS z terenu obcych państw, a awaria serwera ukraińskich służb celnych skutecznie zablokowała na wiele dni towarowy ruch graniczny.

Dlatego też, z punktu widzenia bezpieczeństwa narodowego, dobrze jest zapewnić dywersyfikację i nadmiarowość świadczenia usług dla podmiotów specjalnych. Infrastrukturę krytyczną należy budować, używając sieci i za-

sobów zarówno państwowych, jak i operatorów prywatnych, będących na liście przedsiębiorstw o strategicznym znaczeniu dla gospodarki i obronności państwa.

Wszędzie tam, gdzie jest przesyłana informacja niejawna, zaleca się, aby nadawca i odbiorca informacji zadbał o jej właściwe utajnienie, operator zaś powinien skoncentrować się na tym, co potrafi robić najlepiej, czyli świadczeniu usług, np. polegających na dostarczaniu niezawodnego i szybkiego medium transmisyjnego, tak aby operacja szyfrowania i deszyfrowania nie wpływała na nietolerowalne opóźnienia transmisji sygnału.