Jednostka Samorządu Terytorialnego (JST) jest instytucją publiczną, w której dochodzi do codziennych przepływów ogromnej ilości informacji. Jeśli wyobrazimy sobie „przeciętne", 50 tys. miasto to należy zrozumieć, że obsługująca je JST ma w swoich archiwach pokłady danych, dotyczące grubo ponad 50 tys. klientów. Należy też zrozumieć, że statystycznie, co trzeci klient ma powód do kilkukrotnego w ciągu roku, kontaktowania się z JST w celu otwarcia lub kontynuowania sprawy, która również wiąże się z generowaniem obiegu informacji. Doliczając do tego sprawy związane z klientami z sektora małych i średnich przedsiębiorstw ...

Ubiegłoroczne badanie Momentum Research Group pod nazwą NETIMPACT 2004, przeprowadzone po raz pierwszy w Polsce wykazało, że Polska Administracja Publiczna[1] w przerażający sposób odstaje od pozostałych krajów unijnych pod kątem szeroko rozumianego bezpieczeństwa technologii teleinformatycznych.

Ustawa o ochronie informacji niejawnych, ustawa o ochronie danych osobowych, instrukcja kancelaryjna to istotne akty prawne regulujące obowiązek zachowania bezpieczeństwa przechowywania i przesyłania informacji w JST.

Wszechobecne (nie)Bezpieczeństwo

Informatyka w Mieście wiąże się z wieloma zadaniami i obowiązkami JST, do których jest stosowana jako efektywne i nowoczesne narzędzie. Z informatyką nierozerwalnie związana jest informacja, dane, treść, etc.:.
Niezależnie czy rozpatrujemy zagadnienie od strony funkcjonalnej czy technologicznej, bezwzględnie „wymaganym przez ustawodawcę" jest staranność dotycząca bezpieczeństwo informacji.

Przykładowe Funkcjonalności	**Rodzaj Zagrożenia**
Obieg Dokumentów	Podsłuch
Łączność głosowa	Podsłuch
System Informacji Przestrzennej	Kradzież
Monitoring	Paraliż
Archiwum Elektroniczne	Kradzież
Strona Internetowa	Paraliż
Poczta Elektroniczna	Podsłuch
BIP	Paraliż
Centrum Zarządzania Kryzysowego	Paraliż
System Finansowo Księgowy	Paraliż

Poprzez uproszczenie zagrożeń do krótkiej listy, otrzymamy informację o wpływie czynników zewnętrznych oraz ich przełożenie na technologię.

Rodzaj Zagrożenia	**Przyczyna**
Podsłuch	Złodziej działający na zlecenie. Luki w systemie zabezpieczeń zewnętrznych i/lub wewnętrznych. Luki w systemach szyfrujących. Luki w systemach autoryzacji lub autentykacji. Luki w systemach zabezpieczeń pomieszczeń i budynków.
Kradzież	Niezadowolony pracownik. Złodziej działający na zlecenie. Nieskuteczna polityka bezpieczeństwa. Luki w systemie zabezpieczeń zewnętrznych i/lub wewnętrznych. Luki w systemach szyfrujących. Luki w systemach autoryzacji lub autentykacji. Luki w systemach zabezpieczeń pomieszczeń i budynków.
Paraliż	Sabotaż na zlecenie przeciwników politycznych. Infekcja robakiem internetowym. Nieskuteczna polityka bezpieczeństwa. Brak narzędzi automatyzujących ochronę przez zagrożeniem spoza oraz wnętrza organizacji. Brak współpracy pomiędzy stosowanymi systemami zabezpieczeń oraz transmisji danych i głosu.

Poprzez pokazanie zależności: **funkcjonalność < zagrożenie < przyczyna zagrożenia** ;

[1] Badanie zostało przeprowadzone przede wszystkim pośród JST

można postawić tezę, że problem bezpieczeństwa informacji w JST, jest problemem wielowymiarowy. tzn. istnieje wiele źródeł, powodów, grup społecznych, zagadnień technologicznych, które mają bezpośredni wpływ na poziom bezpieczeństwa informacji w JST.

Bagatelizowanie problemu bezpieczeństwa nie ma przyszłości, po pierwsze oznacza ignorowanie ustawodawcy, pod drugie oznacza wymierne straty wizerunku i pozycji społecznej oraz pieniędzy, na które możemy przeliczyć czas pracy i wartość zniszczonej/skradzionej informacji. Tym bardziej alarmujące są wnioski płynące z badania NetImpact 2004 w obszarze bezpieczeństwa…

Jak zadbać o bezpieczeństwo informacji w JST ?
Nie ma krótkiej i prostej recepty, propozycją mogą być:

- Analiza problemu w skali makro obok częstego podejścia w skali mikro *typu postawię firewall, zamontuję 10 kamer, uruchomię proxy, aplikacja ma szyfrację*. Podejście mikro gwarantuje nam pozostawienie wielu luk i furtek w globalnym systemie bezpieczeństwa.
- Zlecenie niezależnego audytu. Od poziomu zabezpieczeń budynkowych, poprzez zabezpieczenia infrastruktury fizycznej, jakość i sprawność poszczególnych urządzeń, ich lokalizacja i zasilanie, następnie bezpieczeństwo struktur logicznych do transmisji informacji (dane, głos i obraz), bezpieczeństwo poszczególnych narzędzi aplikacyjnych aż po procedury na poszczególnych stanowiskach pracy.
- Przygotowanie spójnej **polityki bezpieczeństwa**, regulującej funkcjonowanie JST w obszarze poddanym audytowi.
- W większych JST zalecane jest utworzenie dedykowanego stanowiska dla osoby odpowiedzialnej za bezpieczeństwo informacji.
- Analiza potrzeb i kreowanie projektów wykazanych audytem, zgodnych z polityką bezpieczeństwa koordynowanych przez dedykowaną osobę.

Automatyzacja zarządzania bezpieczeństwem.
Z jednej strony nieuchronne uzależnienie od coraz większej porcji informacji przekazywanej drogą elektroniczną. Z drugiej strony coraz szybsze narzędzia i skuteczniejsze metody działania złodziei czy częstsze i gwałtowniejsze ataki robaków, tzw. wirusów internetowych. Sztorm wirusowy zarażający całe instytucje trwa minuty. Kontynenty mogą zostać zainfekowane w ciągu godzin!
Na dzisiejszym etapie rozwoju technologii dotychczasowe metody oparte przede wszystkim na reakcji człowieka są już niewystarczające, o ile człowiek nie posiłkuje się równie skutecznymi i szybkimi narzędziami jak twórcy wirusów czy złodzieje informacji.

Jedna ze strategii budowy polityki bezpieczeństwa zakłada minimalizowanie udziału człowieka w sytuacjach reagowania na próby ataku zarówno z zewnątrz jak i od wewnątrz. Strategia ta prowadzi do przemodelowania ochrony z reaktywnej na **proaktywną**.
W obszarze infrastruktury transmisji informacji, przykładem realizacji podejścia obrony **proaktywnej** jest oparta na mechanizmach **analizy anomalii** koncepcja **Cisco Self-Defending Network**. Na uwagę zasługuje fakt, że ciężar podejmowania decyzji o obronie czy eliminacji zagrożenia został w tym rozwiązaniu zdjęty z człowieka na rzecz zaawansowanych algorytmów.
Cisco Self-Defending Network realizuje automatyzację i proaktywność ochrony danych dzięki aktywnemu wykorzystaniu wspólnego systemu operacyjnego Cisco IOS, stosowanego we wszystkich urządzeniach transmisyjnych Cisco Systems. Elementy Cisco Self-Defending Network potrafią w sposób aktywnych współpracować z narzędziami innych producentów. www.cisco.com/go/security

Podsumowanie
Zgodnie z zasadą: *„Zabezpieczenie systemu jest równe, poziomowi zabezpieczeniu jego najsłabszego ogniwa”*; prowadzenie polityki bezpieczeństwa w skali makro oraz eliminacja czynnika ludzkiego z procesu obrony przed zagrożeniami przekłada się na podniesienie bezpieczeństwa informacji w JST.

Piotr Skirski
Dyrektor ds. Kluczowych Klientów
Cisco Systems Poland