Uszczegółowienie dyskusji ze spotkania audytorów wewnętrznych w dniu 22 maja 2013 r.

W dyskusjach w ramach panelu I oraz panelu II udział wzięli:
– Pan Sebastian Burgemejster **(SB) – moderator**
– Pani Agnieszka Giebel **(AG)**
– Pan dr Piotr Dzwonkowski **(PD)**
– Pani Sylwia Wystub **(SW)**
– Pan dr inż. Bolesław Szomański **(BSz)**
– Pani Agnieszka Boboli **(AB)**
– Pan Krzysztof Politowski **(KP)**.

DYSKUSJA I

SB: Na co należy zwrócić uwagę, w odniesieniu do omawianych norm, przy budowie systemów zarządzania informatyką? Jakie są punkty wspólne w trakcie budowy, a jakie podczas funkcjonowania tych systemów?

SW: Rozpoczynając budowę systemu zarządzania informatyką, najpierw sprawdzamy, czy zostały określone wymagania dotyczące usług. W następnej kolejności ustalamy aspekty bezpieczeństwa, czyli wymagania bezpieczeństwa, tj. w jaki sposób muszą być chronione informacje powierzane IT, które z tych informacji powinny być bardziej chronione, które mniejszym stopniu, a które informacje są publiczne od momentu powierzenia.

Następnym etapem jest ustalenie wymagań dotyczących ciągłości, np. z jaką częstotliwością mają być robione kopie oraz jakie usługi i na jakim poziomie będą nam potrzebne w przypadku zaistnienia incydentu.

BSz: Należy zwrócić uwagę na dwie rzeczy, które teoretycznie nie wchodzą w skład bezpieczeństwa teleinformatycznego, ale są dla bezpieczeństwa teleinformatycznego krytyczne. Pierwsza z nich to umowy. Jako przykład można podać źle skonstruowaną umowę o zakup klimatyzacji – w przypadku awarii klimatyzacji dochodzi do awarii serwerów (brak chłodzenia). Drugą kwestią jest ochrona fizyczna zasobów. Brak ochrony fizycznej naraża systemy teleinformatyczne na wrogie działania, w tym na kradzież. Szczególną uwagę trzeba zwrócić na grupy wysokiego ryzyka, np. osoby sprzątające, które mają dostęp do zasobów. Następną ważną kwestią jest uświadomienie zarządowi, że bezpieczeństwo informacji obowiązuje wszystkich pracowników, łącznie z zarządem. Jest to dość trudne zadanie. Grupą wysokiego ryzyka są także informatycy, którzy z uwagi na swoje uprawnienia mogą działać (także nieświadomie) na szkodę bezpieczeństwa systemu. Fundamentalnym zabezpieczeniem, które może sprawdzić audytor, jest przechowywanie hasła administratora w bezpiecznym miejscu.

PD: Na początek organizacja powinna nauczyć swój zarząd sposobu zarządzania ryzykiem i bezpieczeństwa informacji.

AB: Najważniejszą rolę pełni kierownik jednostki. Musi on rozumieć, na czym polega kontrola zarządcza i ochrona informacji oraz jaką misję ma kierowana przez niego jednostka.

SB: Proszę o podanie najbardziej znanych/kluczowych incydentów, które mogą się powtórzyć w innych jednostkach.

BSz: Najbardziej znanym incydentem było włamanie przed dwoma laty do bazy SONY. W wyniku tego incydentu na okres 5 tygodni została zamknięta usługa gry na konsolach.

W celu zminimalizowania skutków kolejnych incydentów SONY zaleciło wszystkim swoim dostawcom wdrożenie normy ISO 27001.

Włamania na strony www mogą być skutkiem niedostatecznego zabezpieczenia hasłem dostępu (przykład sprzed roku: udane włamanie z uwagi na hasła dostępu „admin" i „admin1"). Przyczyną innych incydentów może być outsourcing usług. Outsourcing usług oznacza utratę kontroli – włamania mają miejsce głównie na strony outsourcowane. Natomiast przetwarzanie w chmurze (operacje są przetwarzane w chmurze, czyli nie wiadomo gdzie) niesie ze sobą ryzyko braku dostępu do danych przez pewien czas. Ostatni taki incydent trwał 8 godzin. Chmura nadzorowana przez np. ministerstwo jest w miarę bezpieczna, natomiast chmura publiczna bez przepisów prawnych nie daje bezpieczeństwa. Znane są też przypadki zawierania umów na przetwarzanie w chmurze przez firmę zewnętrzną, na korzystnych warunkach na czas określony, po upływie którego firma uznaje, że dane w chmurze są jej własnością i żąda kilkukrotnie wyższej opłaty za dalsze świadczenie usługi.

AB: W administracji usługi przetwarzania w chmurze są świadczone w niektórych miejscach, głównie na południu Polski i dotyczą zwłaszcza starostw powiatowych. Centrum Projektów Informatycznych będzie realizowało projekt pod nazwą *Informatyzacja jednostek samorządu terytorialnego z zastosowaniem chmury obliczeniowej*. Jeśli ten projekt zostanie zrealizowany (umowa została podpisana 19 kwietnia), to wtedy takie rozwiązanie pojawi się także w administracji. Przykłady zastosowania chmury obliczeniowej na mniejszą skalę można wskazać już obecnie.

Pytania z sali

Jak standardy norm podchodzą do problemu, gdy dużą część pracy prowadzimy w systemie, który nie jest naszą własnością. Posiadamy tam tylko konta, ale nie możemy zarządzać tym systemem. Co mówią standardy?

BSz: Systemem należy zarządzać. Taki jest cel standardów certyfikowanych przez jednostki certyfikacyjne. Powinniśmy wybierać te firmy, które wdrożyły zarządzanie bezpieczeństwem. Należy zwrócić uwagę, aby usługi świadczone przez zewnętrznych dostawców były odpowiednio nadzorowane i opisane.

SW: Bieżące nadzorowanie i prawo do audytowania powinny być zapisane w umowie z usługodawcą.

AB: Wszystkie prawa i ochronę interesów usługobiorcy powinna regulować umowa (usługobiorca będzie dokonywał audytu, w jaki sposób jego wymagania zostały spełnione).

PD: Audytor zawsze ma możliwość sprawdzenia aktualności listy identyfikatorów (np. czy po odejściu pracownika zaktualizowano listę identyfikatorów).

Jakie wskaźniki zastosować do oceny adekwatności, skuteczności i efektywności systemów bezpieczeństwa informacji?

SW: Odpowiednie mierniki podaje ISO 27004 (20 mierników) lub można zastosować rozwiązanie wskazane w COBIT, który zawiera dużo informacji na temat mierników i pokazuje, jak można takie mierniki wprowadzić. Należy przy tym pamiętać, że nie uzyska się 100% skuteczności danego zabezpieczenia.

PD: Poza tym uniwersalnym i obiektywnym miernikiem dotyczącym ciągłości działania jest miernik *straty czasu na przerwę i odzyskiwanie danych po awarii*. Można nawet dokonywać wyliczeń kosztowych poniesionych strat.

Czy możemy zrobić audyt bezpieczeństwa informacji nie mając norm? Czy jednostka musi zakupić normy?

BSz: Korzystniejsze dla jednostki jest posiadanie norm. Z uwagi na ceny norm najtańszym sposobem ich nabycia jest zakup kilku licencji dla całej instytucji.

SW: Zakup norm nie jest koniecznością, gdyż nie ma obowiązku badania na zgodności z normą. Audyty mogą być prowadzone na podstawie rozporządzenia.

KP: Ważniejsze od posiadania norm są kompetencje pozwalające prowadzić audyt oraz odpowiednie przeszkolenie.

DYSKUSJA II

Pytania z sali

Dlaczego w rozdziale IV § 20 ust. 2 KRI, dotyczącym minimalnych wymagań teleinformatycznych, znalazł się zapis o bezpieczeństwie informacji w całej organizacji?

KP: System IT jest usługowym dla całej organizacji. Natomiast kwestii bezpieczeństwa informacji nie można ograniczyć wyłącznie do bezpieczeństwa w systemie teleinformatycznym. W organizacji ok. 80 % incydentów jest generowanych poza systemem informatycznym. Incydenty (ok. 80%) najczęściej generują pracownicy. System teleinformatyczny działa zawsze w otoczeniu – kulturze organizacyjnej, zatem wymaganiami bezpieczeństwa informacji zostało również objęte otoczenie, w którym ten system funkcjonuje. System bezpieczeństwa informacji powinien być zatem kompleksowy.

Jak komórka audytu wewnętrznego ma wywiązać się z przepisu stanowiącego, że audyt bezpieczeństwa informacji przeprowadza nie rzadziej niż na rok?

AG: Zgodnie z upowszechnionym na stronie internetowej stanowiskiem Ministerstwa Finansów oraz Ministerstwa Cyfryzacji i Administracji kierownik jednostki nie powinien automatycznie wskazywać komórki audytu wewnętrznego jako tej, która realizuje audyt bezpieczeństwa informacji.

Co w sytuacji, kiedy nikt w jednostce nie posiada uprawnień/kwalifikacji do przeprowadzania audytu bezpieczeństwa informacji?

AB: W tej sytuacji zadanie należy zlecić na zewnątrz i już w tym momencie wpisać to zadanie do planu finansowego na następny rok.

Dlaczego audyt bezpieczeństwa ma być wykonywany raz do roku?

SB: W normach ISO, jeśli jest obowiązek audytu, audyt musi być przeprowadzany cyklicznie (minimum raz w roku, żeby ocenić funkcjonowanie systemu zarządzania). KRI odnosi się częściowo do norm ISO, więc jeśli funkcjonuje w jednostce audyt jakości, audyt bezpieczeństwa informacji mogą realizować audytorzy z tzw. listy audytorów wewnętrznych jakościowych lub ISO.

BSz: We wszystkich standardach mamy zainteresowane strony. W przypadku bezpieczeństwa informacji również istnieje określona grupa zainteresowanych, tzw. „piąta kolumna". To wszyscy zainteresowani, żeby bezpieczeństwu informacji zaszkodzić. Wynika to ze specyfiki normalnej działalności jednostki – zawsze liczba szkodzących w tej sferze jest duża. Komórki audytu są nieliczne i zwykle mają dużo zadań. Zaletą wszelkich audytów według systemów zarządzania jest to, że są krótkie. Na pierwszym szczeblu audyt może trwać ok. 3 dni. W trakcie pierwszego etapu audytu nie da się doprowadzić do tego, żeby system bezpieczeństwa działał dobrze, natomiast należy ciągle go doskonalić. W bezpieczeństwie

informacji nigdy nie będzie idealnie, natomiast należy dążyć do tego, żeby było bezpieczniej. Inaczej audytuje się systemy zarządzania niż przeprowadza normalny audyt.

SW: Systemy informatyczne i systemy zarządzania regulowane normami są obarczone wysokim ryzykiem. Jeżeli nie były one dawno audytowane, to dobre praktyki mówią, że obszar ten powinien mieć podwyższone ryzyko i być audytowany. Natomiast co roku można audytować te elementy systemu, których podwyższone ryzyko wynika z przeprowadzonej analizy ryzyka.

AG: Należy podkreślić jednak ważną rzecz - nie należy zaczynać od audytu bezpieczeństwa informacji, dopóki nie zostanie zbudowany system bezpieczeństwa informacji. Nie bez przyczyny w prezentacjach była mowa o przywództwie i roli kierownictwa – to nie audytorzy są odpowiedzialni za budowę systemu. Należy zwrócić uwagę, że zgodnie z KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne należy dostosować do wymagań określonych w rozporządzeniu, nie później niż w terminie 3 lat od dnia wejścia w życie rozporządzenia.

Ustawodawca założył, że jest czas na stworzenie systemu, który będzie można audytować. Błędnym zatem jest przekonanie, że trzeba audytować system, który nie istnieje lub dopiero się tworzy.

KP: Odnosząc się do kwestii zapewnienia audytu wewnętrznego nie rzadziej niż raz w roku – działanie to powinno bazować na analizie ryzyka. Nie jest wymagane, żeby co roku dokonywać całościowego przeglądu systemu zarządzania bezpieczeństwem informacji. Taki pierwszy audyt powinien być dokonany całościowo i może być zlecony na zewnątrz (outsourcing), by ustalić co funkcjonuje w jednostce. Kolejny audyt może skupiać się na tym, co się wiąże się z wydanymi rekomendacjami.

Czy możliwe byłoby ustalenie zakresu czasowego oraz minimalnych czasowych punktów kontroli w zakresie przeprowadzania audytu bezpieczeństwa informacji (np. całościowy przegląd co 3 lata)?

AB: Nie można ustalić arbitralnie, że audyt przeprowadza się np. co 3 lata, bo wynika to ze specyfiki jednostki i analizy ryzyka. Natomiast należy podkreślić, że komórki audytu wewnętrznego same nie udźwignią tego obowiązku. Trwają zatem obecnie prace związane z nowelizacją ustawy i wydaje się, że zostaną również podjęte prace nad zmianą rozporządzenia.

KP: Należy zwrócić uwagę, że zagrożenia dla bezpieczeństwa informacji narastają i nie unikniemy kwestii audytowania tego obszaru, czy w sektorze publicznym, czy np. bankowym. Kwestie bezpieczeństwa teleinformatycznego są bardzo istotne. W świetle tego wymagane będzie bardziej precyzyjne dookreślenie, jak dokonywać tego audytu.

BSz: Nie jest prawdą, że w jednostkach nie ma systemu bezpieczeństwa informacji – zawsze są jego elementy. Większość tych elementów jest nieopisana. Sama budowa świadomości, do której przyczynia się audyt, poprawia bezpieczeństwo. 3-letni cykl audytu wynika z systemu certyfikacji. Audyt certyfikacyjny, a potem audyty nadzoru, które zajmują 1/3 czasu są wpisane w przepisach dotyczących norm. Co roku nie trzeba wykonywać całościowego audytu. Trzeba pamiętać, że zawsze sprawdzamy co jest zgodne z normą, a co jest zrobione, nawet jeśli nie jest udokumentowane.

PD: Jeżeli komórki audytu są przeciążone zadaniami to znaczy, że kierujący jednostką nie ma świadomości zagrożeń związanych z bezpieczeństwem informacji. Cały proces należy zacząć od inwentaryzacji zagrożeń związanych z bezpieczeństwem informacji. Lista takich ryzyk byłaby przydatna dla kierownika jednostki.

Dlaczego w przepisach nie zostało wpisane explicite, że podmiot realizujący zadania publiczne ma wdrożyć system oparty o normę ISO 27001?

KP: Z punktu widzenia prawnego było to niemożliwe. Normy są dobrowolnego stosowania i nie można w polskim systemie prawnym zobowiązać podmiotów do ich stosowania. W § 20 ust. 2 KRI zostały ujęte obszary, które powinny być ujęte w systemie zarządzania bezpieczeństwem informacji. Oprócz norm dopuszczalne jest stosowanie innych metod, o ile zostaną objęte obszary wymienione w § 20 ust. 2 KRI.

Czy Departament DA mógłby wydać dobre praktyki lub przewodnik, który byłby pomocny do przeprowadzenia audytu bezpieczeństwa informacji?

KP: Przeprowadzanie audytu zarządzania bezpieczeństwem informacji wymaga 10 % wiedzy z zakresu teleinformatyki, a reszta to wiedza z zakresu zarządzania jednostką. Jeśli plan audytu wymaga specyficznych działań, np. dokonania testów penetracyjnych, to nie ma sensu utrzymywania specjalistów wykonujących takie prace na etacie w jednostce.

AG: Obszar bezpieczeństwa informacji tak czy inaczej jest obszarem wysokiego ryzyka i nie można go wyłączać z analizy ryzyka sprawdzonej w ramach audytu wewnętrznego. Jeśli chodzi o pomoc Ministerstwa Finansów – musielibyśmy skorzystać z wiedzy specjalistów. Jeśli zdołamy zebrać grupę specjalistów, to możemy podjąć się tego zadania.

W § 1 pkt 2 KRI jest mowa o minimalnych wymaganiach dla rejestrów publicznych i wymiany informacji w postaci elektronicznej. Co w przypadku, gdy system informatyczny nie jest rejestrem publicznym i nie wymienia informacji np. system kasy zapomogowo-pożyczkowej?

BSz: Norma 13335 sugerująca, że dla każdego systemu należy budować politykę bezpieczeństwa, została wykreślona. Natomiast w przypadku zarządzania bezpieczeństwem informacji - dla wszystkich systemów ustala się podstawowe zabezpieczenia w oparciu o analizę ryzyka. Dla najważniejszych systemów ustala się poważne zabezpieczenia. Audyt bezpieczeństwa informacji sprowadza się do poziomych sprawdzeń wszystkich systemów jednocześnie. Przy nowoczesnym podejściu najważniejsze jest wykazanie ryzyka dotyczącego wszystkich systemów. Rolą audytora jest wskazanie rzeczywistego ryzyka, a resztę mogą zrobić specjaliści (informatycy).

Jestem z małej gminy, mamy 7 jednostek podległych. Czy jeżeli każda z tych jednostek odrębnie zawrze w procedurach kontrolnych zapis, że ten obszar jest uregulowany w oparciu o normę ISO (nie certyfikujemy się, bo nas na to nie stać), czy to wystarczy?

AB: Na razie wystarczy.

Każda jednostka organizacyjna samorządu ma swojego kierownika. W KRI jest zapis, że to kierownik jednostki ma zapewnić coroczny audyt bezpieczeństwa informacji. Czy dotyczy to także jednostek organizacyjnych samorządu takich jak np. biblioteka, basen? Czy w każdej z tych jednostek oraz w jednostkach pozarządowych, realizujących zadania publiczne trzeba przeprowadzić audyt bezpieczeństwa informacji?

AB: Tak. Jak wspominano wcześniej, komórki audytu wewnętrznego mogą nie podołać temu zadaniu. Dlatego trzeba teraz planować zasoby na ten cel na 2014 r.

AG: Pytanie jest o zakres podmiotowy rozporządzenia w sprawie KRI. Katalog jednostek prowadzących audyt wewnętrzny jest zamknięty. Jest również szereg jednostek, które zostały wymienione w pytaniu, które nie prowadzą audytu wewnętrznego na podstawie ustawy o finansach publicznych, a są objęte obowiązkiem prowadzenia audytu bezpieczeństwa informacji.

SB: W przypadku małych systemów informatycznych, np. w bibliotece, głównym aktywem są dane osobowe i w związku z tym głównym zagrożeniem jest wyciek danych osobowych lub utrata integralności tych danych. Zakładamy, że te aktywa są sklasyfikowane jako osobowe i będą one w odpowiedni sposób audytowane.

Większość audytorów nie posiada wiedzy specjalistycznej z zakresu audytu informatycznego. Przygotowanie ram takiego audytu byłoby dla nich pomocne do przeprowadzenia tego audytu. Czy takie ramy można byłoby opracować?

BSz: Norma ISO 27001 zawiera załącznik normatywny A, w którym jest lista 134 zabezpieczeń (m.in. polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie systemami i sieciami). Ponadto norma ISO 27006 zawiera załącznik D, opisujący jak je audytować. Mogą to być wskazówki dla audytorów.