ACTA UNIVERSITATIS LODZIENSIS
FOLIA OECONOMICA 167, 2003

*Katarzyna Lange-Sadzińska**

COMMON CRITERIA I POLSKIE UNORMOWANIA DOTYCZĄCE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Artykuł traktuje o roli kryteriów CC i innych standardów międzynarodowych w tworzeniu bezpieczeństwa systemów informatycznych i ich wpływie na polskie unormowania prawne.

The paper presents the role of Common Criteria and others international standards to create the security of information systems . The influence of CC on Polish law was discussed.

Wstęp

Standardy dotyczące bezpieczeństwa muszą uwzględniać wiele aspektów problemu (najważniejsze to integralność danych, dostępność danych, poufność danych). Wśród prób podejmowanych w celu stworzenia takich standardów na uwagę zasługują dwie inicjatywy.

Pierwszą jest TCSEC czyli Trusted Computer Security Evaluation (Kryteria oceny wiarygodności oceny systemów komputerowych) zwana też „Orange Book"[1]. TCSEC jest publikacją amerykańskiej organizacji NCSC (National Computer Security Center - Narodowy Ośrodek Bezpieczeństwa Komputerowego USA). Dokument opisuje kryteria oceny poufnych systemów komputerowych. Zdefiniowano w nim metody kontroli dostępu do systemów komputerowych, które mogą wykorzystywać producenci komputerów chcący dostosować swoje wyroby do standardów bezpieczeństwa Departamentu Obrony USA.

TCSEC określa kryteria, które stanowią podstawę oceny wiarygodności danego systemu. W zależności od spełnianych wymagań system otrzymuje klasę

* Zakład Informatyki Ekonomicznej, Uniwersytet Łódzki

[1] TCSEC nazywana jest często „pomarańczową księgą" i stanowi część serii publikacji opatrzonych wspólnym tytułem „tęczowa seria" (Rainbow Series).

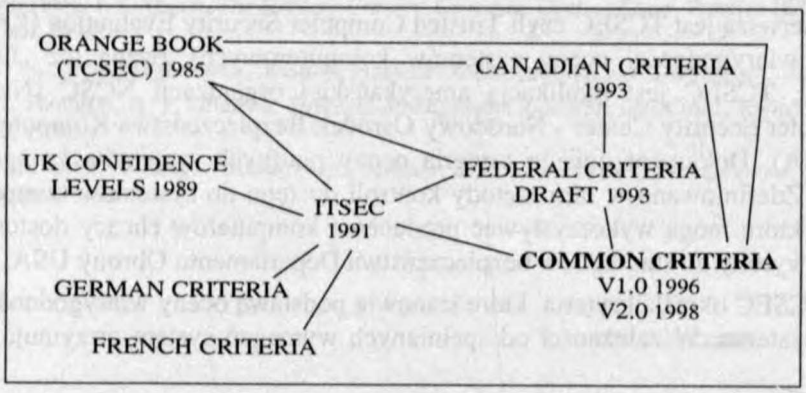
bezpieczeństwa. Istnieją cztery grupy kryteriów oceny wiarygodności określone w standardzie TCSEC:

- polityka bezpieczeństwa (sposób dostępu do informacji),
- możliwość kontroli (mechanizmy identyfikacji, uwierzytelniania, śledzenia, wiarygodnej ścieżki-czyli ew. przechwycenia logu i podszycia się pod system),
- gwarancja działania mechanizmów zabezpieczających (kategorie bezpieczeństwa A, B, C i odpowiednio dla każdej z nich klasy A1, B1, B2, B3, C1, C2),
- wymagana dokumentacja (forma i szczegółowość dokumentacji ocenianego produktu).

Drugim ważnym standardem jest ITSEC (Information Technology Security Evaluation Criteria). ITSEC uznają - Wielka Brytania, Francja, Niemcy, Holandia i Komisja Unii Europejskiej. Ponadto obustronne umowy obowiązujące między Wielką Brytanią, Francją i Niemcami są formalnie uznawane również przez Finlandię, Grecję, Holandię, Szwecję i Szwajcarię.

Migracja standardów do wspólnego rozwiązania czyli CC (Common Criteria)

Standardy dotyczące bezpieczeństwa obowiązujące w USA i krajach Europy zachowują wzajemną odpowiedniość, która pozwoliła stworzyć wspólny standard. Poniżej przedstawiono schemat dotyczący rozwoju standardu Common Criteria.



Rys. 1 Rozwój standardu Common Criteria
Źródło: Common Criteria... The Standard for Information Security, *Origins of the Common Criteria,* http://www.commoncriteria.org/docs/origins.html

Standard Common Criteria Version 2.1 ratyfikowano przez ISO jako standard ISO 15408.

Ze względów historycznych i dla podkreślenia kontynuacji prac używa się terminu **Common Criteria**, przy oficjalnej nazwie ISO "Evaluation Criteria for Information Technology Security"(ECITS). W literaturze spotkać można również określenie „Common Criteria for Information Technology Security Evaluation" (CCITSE).

Korzyści dla grup użytkowników

Poniżej scharakteryzowano standard Common Criteria z punktu widzenia grup użytkowników tego standardu.

Tabela 1 Wykorzystanie CC przez grupy użytkowników.
Na podstawie http://www.redium.ncsc.mil/tpep/library/ccitse

Użytkownicy	Standard Common Criteria
Konsumenci	Common Criteria dostarcza potencjalnym klientom podstawowe informacje i wskazówki przed zakupem produktu technologii informatycznej (IT). Pomaga stwierdzić, czy produkt, który mają zakupić spełnia wymogi bezpieczeństwa zgodnie ze standardem. Standard pozwala uświadomić konsumentom konieczność spełniania wymagań bezpieczeństwa przez produkty IT.
Programiści	Common Criteria służy jako zbiór wymagań bezpieczeństwa, które mają być wybrane i uwzględnione w produktach IT. Standard CC wskazuje sposób projektowania i tworzenia produktów, który pozwoli sprawdzić, czy produkt spełnia wymagania bezpieczeństwa.
Oceniający produkt	Standard CC pozwala rozstrzygać czy produkt odpowiada wymaganiom bezpieczeństwa.

Standard ISO/IEC 17799

Standard ISO/IEC[2] 17799 ustanowiony przez połączony komitet powołany przez ISO i IEC jest pierwszym standardem na forum międzynarodowym prezentującym całościowe podejście do zarządzania zabezpieczeniami. Norma

[2]IEC - International Electrotechnical Commission

ISO/IEC 17799 „Praktyczne zasady zarządzania bezpieczeństwem informacji" określa sposoby postępowania z informacją w firmie, zwracając uwagę na poufność, dostępność i spójność danych. Jest to szczególnie ważne w organizacjach przetwarzających dane poufne, prowadzących produkcję specjalną oraz obawiających się nieuczciwych działań konkurencji. Norma wskazuje podstawowe zagadnienia i określa metody i środki konieczne dla zabezpieczenia informacji.

Polskie akty prawne

Standard ISO/IEC 17799, który powstał na podstawie zaleceń i standardów narodowych dotyczących zarządzania zabezpieczeniami duże znaczenie dla naszych uregulowań w tym względzie.

Polski Komitet Normalizacyjny zaadaptował normę ISO/IEC 17799 jako Polską Normę ISO/IEC 17799 zatytułowaną „Praktyczne zasady zarządzania bezpieczeństwem informacji". Dokument stanowi pierwszą część cyklu, zawierającą zalecenia o charakterze ogólnym.

Zgodnie z planami Polskiego Komitetu Normalizacyjnego norma ta będzie obowiązywać w Polsce od połowy 2003 roku.

Norma ISO/IEC 17799 dotyczy w głównej mierze zarządzania, mniejszy nacisk kładąc na zagadnienia techniczne i informatyczne. Norma wskazuje procesy, które powinny być nadzorowane w celu zmniejszenia ryzyka utraty ochrony danych. Została napisana przystępnie i zawiera wiele przykładów wdrażania zalecanych procedur.

Jako polska norma obowiązuje również standard ISO/IEC 15408 (część 1 i 3) czyli opisane wcześniej Common Criteria.

Dotychczas obowiązywały inne dokumenty traktujące o zarządzaniu zabezpieczeniami:

- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz. U. Nr 11, poz. 95.
- Rozporządzenie Prezesa RM z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych. Dz. U. Nr 18 poz. 162.
- Zalecenia Urzędu Ochrony Państwa dotyczące bezpieczeństwa teleinformatycznego, wersja 1.1, sierpień 2000 r.

Powyższe akty nie obejmowały jednak wszystkich aspektów bezpieczeństwa.

Podsumowanie

Zabezpieczenie informacji jest coraz ważniejszym warunkiem prowadzenia biznesu i jednocześnie coraz trudniejszym zadaniem do wykonania. Od prawidłowości działania systemu bezpieczeństwa może zależeć nie tylko działanie i wiarygodność, ale także losy całej firmy.

Wynika to z faktu, że wcześniej firmy udostępniały swoje zasoby i dane w ograniczonym stopniu. Obecnie dostępność Internetu powoduje narażenie słabo chronionych zasobów informacji firmy na zamierzony lub przypadkowy atak.

Sytuacja ta wymusza na kierownictwie firm dołożenie wszelkich starań w celu zastosowania dobrych zabezpieczeń danych, co sprowadza się do wdrożenia obowiązujących norm. Jednocześnie firmy oczekują od ustawodawcy proponowania norm, które przy danym stanie wiedzy zapewnią podstawową gwarancję bezpieczeństwa.

Źródła

1. E. Andrukiewicz, *Polska Norma ISO/IEC 17799 – jak tworzyć bezpieczeństwo systemów informatycznych w przedsiębiorstwie*, Materiały Konferencji ENIGMA, Warszawa 2001.
2. J. Cendrowski, R. Kośla, *Rola Kryteriów Oceny Zabezpieczeń w realizacji polityki bezpieczeństwa teleinformatycznego*, Materiały Konferencji ENIGMA, Warszawa 2001.
3. J. Cendrowski, *Projekt Polskiej Normy PR ISO/IEC 17799. Praktyczne zasady zarządzania zabezpieczeniami informacji*, Seminarium: Techniczne Aspekty Przestępczości Teleinformatycznej, Optimus Warszawa, 2001.
4. J. Cendrowski, *Ochrona informacji niejawnych cz. 5*, Szkolenia specjalistyczne administratorów systemów i pracowników pionów ochrony, „IT Secury Magazine", kwiecień 2000, nr 4(8).
5. P. Krawczyk, *Dla audytorów bezpieczeństwa, Ochrona danych i bezpieczeństwo sieci*, Ipsec.pl, 2002.
6. A. Niemiec, *Zarządzanie bezpieczeństwem informacji w świetle norm ISO*, Referaty i artykuły związane z zarządzaniem, Wrocław 2000.
7. D. Comer, *Sieci komputerowe i intersieci*, WNT, Warszawa 2000.
8. T. Sheldon, *Wielka encyklopedia sieci komputerowych*, ROBOMATIC, 1999.
9. *Common Criteria for Information Technology Security Evaluation*, Part 1:Introduction and general model, August 1999 Version 2.1, CCIMB – 99-031
10. *Common Criteria for Information Technology Security Evaluation*, Part 2: Security functional requirements, August 1999 Version 2.1, CCIMB – 99-032
11. *Common Criteria for Information Technology Security Evaluation*, Part 3: Security assurance requirements, August 1999 Version 2.1, CCIMB – 99-033
12. Common Criteria... The Standard for Information Security, *Origins of the Common Criteria*, http://www.commoncriteria.org/docs/origins.html
13. http://www.redium.ncsc.mil/tpep/library/ccitse
14. http://csrc.nist.gov/cc/ccv20/ccv2list.htm
15. http://csrc.nist.gov/cc/cem/cemlist.htm
16. raport CESG http://www.cesg.gov.uk