

Zalecenia dotyczące bezpieczeństwa systemów teleinformatycznych w Politechnice Łódzkiej.
(na podstawie analizy audytu przeprowadzonego w październiku 2013 r.)
13.01.2014

dokument wyłącznie do użytku wewnętrznego

W systemach teleinformatycznych funkcjonujących w Politechnice Łódzkiej wyodrębniono 10 cech, które należy uznać za krytyczne dla bezpieczeństwa informacji przetwarzanych przez te systemy.

1. **Rozliczalność** (5.2.a) - *właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.* – brak implementacji tej właściwości w systemie jest poważnym zagrożeniem bezpieczeństwa informacji ze względu na brak możliwości przypisania personalnej odpowiedzialności za działania użytkowników w systemie
zalecenie: należy niezwłocznie zapewnić rozliczalność operacji w systemie.
2. **Niezaprzeczalność** (5.2.b) - *brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie* - brak implementacji tej właściwości w systemie jest poważnym zagrożeniem bezpieczeństwa informacji ze względu na możliwość wykonania nieautoryzowanych operacji w systemie (dotyczy to zarówno osób jak i procesów realizowanych w systemie)
zalecenie: należy niezwłocznie zapewnić niezaprzeczalność operacji w systemie.
3. **Aktualność inwentaryzacji** sprzętu i oprogramowania służącego do przetwarzania informacji (5.3.a) – stanowi zagrożenie organizacyjno-prawne polegając na braku możliwości ew. odtworzenia infrastruktury i zasobów po awarii, utrudnia stwierdzenie posiadania wszystkich aktualizacji do oprogramowania lub stanowi zagrożenie prawne związane z nielegalnym korzystaniem z oprogramowania.
zalecenie: należy niezwłocznie wykonać inwentaryzację sprzętu i oprogramowania systemowego oraz sprawdzić legalność i aktualność wersji oprogramowania.
4. **Powierzenie firmie zewnętrznej zarządzania infrastrukturą** teleinformatyczną systemu (5.8.c) lub **utrzymywanie serwisów WWW** (7.8) – może stanowić poważne zagrożenie bezpieczeństwa, jeśli warunki techniczne (SLA) i formalno-prawne tego powierzenia nie zapewniają poufności, integralności i dostępności informacji. (Poufność - *zapewnienie dostępu do informacji tylko osobom upoważnionym*, integralność - *zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania*, dostępność - *zapewnienie, że osoby upoważnione mają dostęp do informacji wtedy i tylko wtedy, gdy jest to potrzebne*.). Jest to szczególnie niedopuszczalne w sytuacji gdy systemy te przetwarzają dane osobowe lub inne dane stanowiące tajemnicę PŁ; w przypadku serwisów WWW może stanowić zagrożenie związane z brakiem dostatecznej kontroli nad systemem, jego dostępnością, poufnością danych, utratą wizerunku.
zalecenie: należy niezwłocznie zanalizować stan formalno-prawny powierzenia i w sytuacji nie zapewnienia poufności, integralności i dostępności informacji albo go uaktualnić albo zaprzestać korzystania z usługi.; w przypadku serwisów WWW: należy niezwłocznie przenieść serwisy WWW na zasoby wewnętrzne Uczelni (własne jednostki lub centralne będące w dyspozycji Centrum Komputerowego PŁ), w okresie przejściowym, np. do czasu wygaśnięcia umowy: zanalizować stan formalno-prawny powierzenia i w sytuacji nie zapewnienia poufności, integralności i dostępności informacji doprowadzić do jego uaktualnienia.
5. **Zdalny dostęp administratora realizowany za pośrednictwem połączenia nieszyfrowanego** (5.10.a) – stanowi szczególne niebezpieczeństwo nieautoryzowanego przejęcia kontroli nad systemem.

zalecenie: należy zaprzestać zdalnego zarządzania systemem za pośrednictwem tej metody.

6. **Administracja systemem realizowana z sieci Internet bez ograniczeń (6.4.a)** – stanowi zagrożenie związane z ryzykiem dostępu do systemu osób niepowołanych (naruszenie poufności)

zalecenie: należy niezwłocznie ograniczyć możliwość zarządzania systemem z nieautoryzowanych adresów sieci Internet poprzez wprowadzenie mechanizmów bezpieczeństwa, np. wprowadzenie list autoryzowanych adresów, dostęp przez VPN, SSH; do czasu wprowadzenia zaleceń należy zaprzestać zdalnej administracji systemem.

7. **Przechowywanie haseł w systemie w postaci niezaszyfrowanej (5.11.b)** – grozi naruszeniem poufności informacji, a tym samym stwarza możliwość jej utraty.

zalecenie: należy niezwłocznie zaimplementować mechanizmy szyfrowania przechowywania haseł lub w przypadku braku możliwości szybkiego wprowadzenia tego mechanizmu bezwzględnie wprowadzić okresową ważność haseł (nie dłuższą niż 30 dni).

8. **Bezpieczne fizyczne rozlokowanie zasobów** systemu teleinformatycznego, redukujące ryzyka wynikające z zagrożeń środowiskowych lub nieautoryzowanego dostępu (5.14) – ulokowanie zasobów systemowych w miejscu, które szczególnie narażone jest na zagrożenia środowiskowe (np. zalanie wodą) lub na dostęp osób niepowołanych naraża system na awarię lub destrukcję.

zalecenie: w przypadku ulokowaniu sprzętu w zagrożonych miejscach należy sprzęt przenieść do miejsca bezpiecznego lub znacząco zmniejszyć ryzyka związane z wymienionymi zagrożeniami (odsunąć od instalacji wodnej, jeśli jest w piwnicy – postawić na wyższych podestach, ograniczyć ruch osób niepowołanych przez zamknięcie stref lub ich dodatkowe zabezpieczenie).

9. **Dedykowany firewall lub zaimplementowanie w systemie mechanizmy typu firewall** pozwalające na eliminację określonego typu pakietów (5.19, 6.3.a) – brak takiej funkcjonalności naraża system na ataki z sieci.

zalecenie: należy niezwłocznie zapewnić dedykowaną dla systemu ochronę firewall.

10. **Wdrożenie mechanizmów podnoszących poziom bezpieczeństwa systemu** – Centrum zapasowe (5.13) – w szczególności dotyczy kopii zapasowej przetwarzanych danych (backup) – jej brak może spowodować całkowitą utratę przetwarzanych w systemie danych; kopia zapasowa powinna być przechowywana w innej geograficznie lokalizacji.

zalecenie: należy zapewnić regularne kopiowanie danych (codzienne, a szczególnych przypadkach rzadziej, jeśli dane w systemie nie zmieniają się – np. serwery WWW) oraz ulokowanie kopii poza umiejscowieniem serwera (w innej serwerowni lub np. na zasobach usługi powszechnej archiwizacji projektu PLATON).

Powyższe zalecenia należy wprowadzić do zarządzanych przez jednostki systemów w terminie:

- 2 tygodni od ich wydania - dotyczy zaleceń: 5, 6, 7;
- 1 miesiąca od ich wydania – dotyczy zaleceń : 1, 2, 3, 4, 10;
- 3 miesięcy od wprowadzenia – dotyczy zaleceń: 8, 9;
- 6 miesięcy od wprowadzenia – dotyczy zalecenia 4 (serwisy WWW).

Pełnomocnik Rektora PŁ
ds. bezpieczeństwa systemów teleinformatycznych
mgr inż. Piotr Szepliński