Załącznik Nr 8 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Klasyfikacja incydentów bezpieczeństwa teleinformatycznego w Urzędzie Miasta Szczecin.

§ 1. Katalog zgłoszeń związanych z zagrożeniem bezpieczeństwa teleinformatycznego Urzędu.

Lp.	opis incydentu	adresat zgłoszenia i forma zgłoszenia	procedura / opis działania
1	Wykrycie (gdziekolwiek w zarządzanej infrastrukturze IT Urzędu) plików bez praw autorskich tj. stanowiących wykroczenie przeciwko ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.	Zgłoszenie do ASI poprzez pocztę elektroniczną lub telefonicznie	Usunięcie plików przez ASI w porozumieniu z pracownikiem lub bez porozumienia. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń. ASI który usuwa pliki lub odnotowuje pliki w rejestrze, jeżeli jest to zasób legalny powstanie wynikowy rejestr plików, do których Urząd posiada prawa autorskie. ASI zarządzający infrastrukturą sprawdza czy pliki zostały zapisane w kopiach zapasowych sieciowych, w przypadku potwierdzenia kieruje stanowiący zabezpieczenie zasób do czyszczenia zawartości
2	Wykrycie złośliwego oprogramowania w kategoriach: wirusy, robaki, trojany, spyware lub inne.	Zgłoszenie do ASI	ASI prowadzi akcję naprawczą poprzez zdalny dostęp, po jej zakończeniu, potwierdza usunięcie zagrożenia w HD, (zawsze potwierdzamy fakt usunięcia). Zalecenie: Akcja naprawczo musi być skuteczna, jeżeli system nie daje się odwirusować, to komputer kierowany jest do reinstalacji systemu w serwisie WInf. Usunięcie zagrożenia przez Serwis WInf, który dodatkowo skanuje stację, jeżeli nieskuteczne to stacja podlega reinstalacji systemu. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń.
3	Wykrycie złośliwego oprogramowania stanowiącego najwyższe zagrożenie, jak rootkit, keylogger, dialer.	Zgłoszenie do ASI	ASI prowadzi akcję naprawczą poprzez zdalny dostęp, po jej zakończeniu, potwierdza usunięcie zagrożenia w rejestrze zdarzeń. (Zawsze potwierdzany jest fakt usunięcia). Zalecenie: Akcja naprawcza musi być skuteczna, jeżeli system nie daje się odwirusować, to komputer kierowany jest do reinstalacji systemu w serwisie WInf. Usunięcie zagrożenia przez serwis WInf, który dodatkowo skanuje stację, jeżeli nieskuteczne to stacja podlega reinstalacji systemu. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń.
4	Wykrycie faktu podłączenia urządzenia z technologią komputerową do sieci LAN Urzędu, którego Urząd nie jest właścicielem.	Zgłoszenie do ASI i do kierownika.	Następuje odłączenie urządzenia przez ASI, przywrócenie stanu właściwego i potwierdzenie o odłączeniu w HD. ASI lub pracownik podmiotu zewnętrznego przywracają stan właściwy. Obowiązek rejestracji zdarzenia w poprzez rejestrze zdarzeń
5	Wykrycie faktu podłączenia urzędowego komputera, który nie przeszedł autoryzacji w domenie Urzędu do sieci LAN Urzędu	Zgłoszenie do ASI	Przeprowadzenie autoryzacji przez ASI. ASI lub pracownik podmiotu zewnętrznego przywracają stan właściwy. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń
6	Wykrycie komputera, który jednocześnie połączono do sieci LAN Urzędu i do innej sieci komputerowej	Zgłoszenie do ASI	Odłączenie komputera przez ASI, tj, przywrócenie stanu właściwego i potwierdzenie do ASI. Postępowanie dwutorowe. 1. Jeżeli sprzęt jest własnością Urzędu to ASI poucza pracownika i kończy procedurę, 2. Jeżeli sprzęt jest obcy to ASI składa doniesienie do przełożonych, w przypadku stwierdzenia szkody zabezpiecza dowody.

			Dyrektor WInf informuje Sekretarza Miasta ASI lub pracownik podmiotu zewnętrznego przywracają stan właściwy. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń.
7	Stwierdzenie nieprzestrzegania polityki haseł Urzędu	Zgłoszenie do ASI lub/i ASU	ASI poucza pracownika, informuje jego kierownika i zleca procedurę zmiany hasła. ASI weryfikuje prawidłowość zmiany hasła. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń.
8	Zgłoszenie niewłaściwego zabezpieczenia fizycznych zasobów IT Urzędu lub faktu ich przełamania (drzwi, zamki, alarmy, karty dostępu, klimatyzacja, energetyka)	Zgłoszenia do kierownika, ASI, ABI, Biura Obsługi Urzędu i MJOG.	Pracownicy ww. podejmują akcje zabezpieczające zależne od poleceń przełożonych. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń
9	Wykrycie / zgłoszenie niewłaściwej realizacji procedur wewnętrznych obowiązujących w WInf np. brak backupu, brak hasła lub ujawnienie hasła	Zgłoszenie do dyrektora WInf.	Działania zależne od decyzji dyrektora WInf. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń
10	Inne zdarzenia, które mogą wpływać na bezpieczeństwo fizycznych zasobów informatycznych w Urzędzie	Każdy pracownik poprzez zgłoszenie do kierownika, ASI, ASU lub ABI	Działania zależne od decyzji dyrektora WInf. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń
11	Wykrycie i zgłoszenie niedozwolonych prawem czynności dotyczących podpisu elektronicznego	Zgłoszenie do kierownika, ASI, ASU lub ABI	Działania zależne od decyzji dyrektora WInf. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń
12	Wykrycie i zgłoszenie działania skierowanego przeciwko zasobom teleinformatycznym Urzędu, np. maile noszące znamiona wykroczenia lub przestępstwa, skanowanie zasobów, nieuprawniona ingerencja w zasoby, ataki DOS i DDOS, kradzież, wandalizm, manipulacja socjotechniczna	Zgłoszenie do kierownika, dyrektora WInf,ASI, ASU lub ABI	Działania zależne od decyzji dyrektora WInf. Obowiązek rejestracji zdarzenia w rejestrze zdarzeń

§ 2. Procedury rejestracyjne dotyczące powyższych zgłoszeń prowadzi WInf przy pomocy odpowiedniego oprogramowania.

§ 3. Zdarzenie odnotowane ponownie, dla tego samego użytkownika skutkuje przekazaniem informacji kierownikowi i Sekretarzowi Miasta.