Załącznik nr 12 do zarządzenia nr 5/2015 – „Procedura ochrony przed złośliwym oprogramowaniem”

PROCEDURA OCHRONY PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

§ 1.

1. „Procedura ochrony przed złośliwym oprogramowaniem”, zwana w dalszej części „Procedurą”, określa rodzaje i działanie złośliwego oprogramowania, działania profilaktyczne i ochronne przed złośliwym oprogramowaniem oraz osoby odpowiedzialne za ich stosowanie w Przedszkolu nr 13 w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Przedszkola nr 13 w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Przedszkola nr 13 w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Przedszkolu – należy przez to rozumieć Przedszkole nr 13 w Rybniku.

§ 2.

Do złośliwego oprogramowania zalicza się w szczególności:

1) wirus – program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika,
2) robak – złośliwe oprogramowanie rozmnażające się tylko przez sieć Internet, zwłaszcza przez pocztę elektroniczną, nie potrzebuje programu „żywiciela”,
3) wabbit – program rezydentny nie powielający się przez sieć Internet, wynikiem jego działania jest jedna określona operacja, np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera,
4) trojan – ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku, zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak włamywacza (hakera),
5) backdoor – przejmuje kontrolę nad zainfekowanym komputerem, umożliwiając wykonanie na nim czynności administracyjnych, łącznie z usuwaniem i zapisem danych. Podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia włamywaczowi administrowaniem systemem operacyjnym przez sieć Internet i wykonywanie zadań wbrew wiedzy i woli użytkownika,
6) program szpiegujący – oprogramowanie zbierające informacje o użytkowniku bez jego zgody, np. informacje o odwiedzanych witrynach, hasła dostępu. Występuje często jako dodatkowy i ukryty komponent większego programu, odporny na usuwanie i ingerencję użytkownika. Może wykonywać działania bez wiedzy użytkownika, np. zmieniać wpisy do

rejestru systemu operacyjnego i ustawienia użytkownika. Może pobierać i uruchamiać pliki z sieci Internet,

7) rootkit – maskuje obecności pewnych uruchomionych programów lub procesów systemowych, które z reguły służą włamywaczowi (hakerowi) do administrowania zaatakowanym systemem. Rootkit zostaje wkompilowany lub wstrzyknięty w istotne procedury systemowe, jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja,
8) keylogger – odczytuje i zapisuje wszystkie naciśnięcia klawiszy przez użytkownika. Dzięki temu adresy, kody, cenne informacje mogą odstać się w niepowołane ręce.

§ 3.

1. Profilaktyka i ochrona przed złośliwym oprogramowaniem obejmuje w szczególności:
   1) instalację, stosowanie i regularne uaktualnienia oprogramowania antywirusowego (wykrywającego i naprawczego),
   2) uświadamianie pracowników w zakresie bezpieczeństwa informacji oraz właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami,
   3) stałe monitorowanie komunikatów pochodzących z zainstalowanego oprogramowania antywirusowego,
   4) zakaz korzystania z nieautoryzowanego oprogramowania,
   5) zakaz korzystania z sieci Internet bez aktywnej ochrony oprogramowaniem antywirusowym,
   6) sprawdzanie (skanowanie) oprogramowaniem antywirusowym komputerów i nośników służących do przetwarzania informacji, w tym tych otrzymywanych spoza Przedszkola oraz wiadomości elektronicznych,
   7) korzystanie z list dyskusyjnych i sprawdzanie stron internetowych zamieszczających informacje o złośliwym oprogramowaniu,
   8) tworzenie kopii zapasowych.
2. Za stosowanie elementów profilaktyki i ochrony przed złośliwym oprogramowaniem, o których mowa w ust. 1 pkt 1, 6, 7 i 8 odpowiada informatyk, za stosowanie elementu, o którym mowa w ust. 1 pkt 2 odpowiada Dyrektor, a za stosowanie elementu, o którym mowa w ust. 1 pkt 3, 4 i 5 odpowiadają wszyscy pracownicy Przedszkola.

§ 4.

W przypadku, gdy ochrona przed złośliwym oprogramowaniem, o której mowa w § 3 ust. 1 jest niewystarczająca, użytkownik zawiadamia o tym fakcie informatyka.

§ 5.

Szczególną uwagę należy zwracać na ochronę przed wprowadzeniem złośliwego oprogramowania w trakcie konserwacji lub wykonywania procedur awaryjnych, kiedy

możliwe jest obejście normalnych mechanizmów ochrony przed złośliwym oprogramowaniem.

§ 6.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.