**WYKAZ**

**PRZEDSIĘWZIĘĆ I PROCEDUR DZIAŁANIA W SPRAWACH BEZPIECZEŃSTWA I ZARZĄDZANIA KRYZYSOWEGO W** **PIERWSZYM STOPNIU ALARMOWYM CRP (ALFA-CRP)**

**MODUŁ ZADANIOWY NR 1 CRP**

Treść zadania:

**Przedsięwzięcia realizowane przez Uniwersytet w Siedlcach w ramach pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)**

Główny wykonawca zadania: Kanclerz

**I. CEL MODUŁU ZADANIOWEGO**

Przygotowanie ***do przeciwdziałania możliwości wystąpienia zagrożenia albo minimalizowania skutków zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych*, którego rodzaj i zakres jest trudny do przewidzenia.**

Wprowadzone regulacje mają na celu zapewnienie bezpiecznego i ciągłego funkcjonowania systemów teleinformatycznych Uniwersytetu oraz bezpieczeństwa osób obsługujących te systemy.

**Wprowadzenie pierwszego stopnia alarmowego CRP (stopnia ALFA-CRP) ma charakter ogólnego ostrzeżenia,** a okoliczności nie uprawniają do uruchomienia przedsięwzięć zawartych w wyższych stopniach alarmowych.

Wszystkie jednostki organizacyjne odpowiedzialne za bezpieczeństwo systemów teleinformatyczny Uniwersytetu powinny być w stanie wprowadzić i utrzymywać przedsięwzięcia tego stanu alarmowego na czas nieograniczony.

**II. WARUNKI OPERACYJNE REALIZACJI ZADANIA**

1. Utrudnienia związane z przerwami w dostawach energii elektrycznej lub łączności.
2. Zakłócenia w przepływie informacji (np. pomiędzy wykonawcami poszczególnych zadań).
3. Absencja pracowników instytucji (np. urlopy, zachorowania).
4. Zaburzenia w funkcjonowaniu firm usługowych, współpracujących.
5. Możliwy chaos organizacyjny (np. fałszywe alarmy, blokada stron internetowych).
6. Inne – których na obecnym etapie nie można zdefiniować.

**III. PRZEDSIĘWZIĘCIA DO WYKONANIA W RAMACH MODUŁU**

**ZADANIOWEGO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Po wprowadzeniu pierwszego stopnia alarmowego CRP (stopnia ALFA-CRP)**  **należy niezwłocznie wykonać następujące zadania (czynności):** | | | | |
| **Lp.** | **Zadanie** | **Czynności do wykonania w ramach zadania** | **Wykonawca** | **Uwagi** |
| **1** | **2** | **3** | **4** | **5** |
| 1 | Poinformować stan osobowy o wprowadzeniu pierwszego stopnia alarmowego CRP (stopnia ALFA-CRP). | Zredagować Ogłoszenie Rektora i przedstawić do podpisania. | Kanclerz,  Specjalista ds. obronnych i sytuacji kryzysowych,  Specjalista ds. SZBI |  |
| Rozesłać Ogłoszenie na skrzynki e-mail kierowników podstawowych jednostek organizacyjnych oraz umieścić na stronie internetowej Uniwersytetu. | Kanclerz  Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych |
| 2 | Wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych Uniwersytetu. | Monitorowanie i weryfikacja, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej.  Monitorowanie bezpiecznej eksploatacji systemów informatycznych. | Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni, Inspektor Ochrony Danych Osobowych (IODO) |  |
| Sprawdzanie dostępności usług elektronicznych.  Prowadzenie działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemów teleinformatycznych UPH przed niepowołanym dostępem. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni, Inspektor ODO |
| Dokonywać, w razie potrzeby, zmian w dostępie do systemów.  Weryfikacja osób dopuszczonych do przetwarzania informacji. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni, Inspektor ODO. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| 3 | Poinformować personel Uniwersytetu o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personel odpowiedzialny za bezpieczeństwo systemów teleinformatycznych. | Zwołać posiedzenie Kolegium rektorskiego, na którym omówić procedury i zadania związane z wprowadzonym stopniem alarmowym CRP. | Sekretarz rektora,  Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, |  |
| Poinformować użytkowników systemów informatycznych o zagrożeniach związanych z zaistniałą sytuacją. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni. |
| Aktualizacja, w miarę możliwości, użytkowanych systemów operacyjnych, oprogramowania wspierającego działanie serwerów, oprogramowania antywirusowego i zapór sieciowych w celu wyeliminowania ewentualnych błędów i luk umożliwiających naruszenie bezpieczeństwa teleinformatycznego. | Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych,, Administrator CKDM, Administrator CZSK, Administratorzy lokalni, IODO. |
| Monitorowanie logów i raportów serwerów WWW pod kątem wykrycia zdarzeń mających na celu nieuprawnioną modyfikację treści serwisu WWW. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni. |
| Instalowanie i konfiguracja, w miarę możliwości, dodatkowych narzędzi zwiększających bezpieczeństwo. | Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni. |
| 4 | Dokonać weryfikacji posiadanych kopii zapasowych systemów teleinformatycznych. | Dokonać sprawdzenia systemów kluczowych dla funkcjonowania Uniwersytetu. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych,, Administrator CKDM, Administrator CZSK, Administratorzy lokalni. |  |
| Dokonać weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemów Uniwersytetu. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych, Administrator CKDM, Administrator CZSK, Administratorzy lokalni. |
| **1** | **2** | **3** | **4** | **5** |
| 5 | Sprawdzać działanie środków łączności wykorzystywanych w celach zapewnienia bezpieczeństwa z poszczególnymi obiektami oraz zewnętrznymi podmiotami biorącymi udział w reagowaniu kryzysowym. | Sprawdzać działanie łączności telefonicznej przewodowej i bezprzewodowej oraz stan sprawności akumulatorów zapasowych do zasilania awaryjnego. | Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych,, Specjalista OZSK |  |
| Sprawdzenie łączności z Wydziałem Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Miasta Siedlce, w tym skrzynki e-mail. | Specjalista ds. obronnych i sytuacji kryzysowych |
| Sprawdzenie łączności z Zespołem ds. Obronnych i Zarządzania Kryzysowego MEiN, w tym skrzynki e-mail. | Specjalista ds. obronnych i sytuacji kryzysowych |
| 6 | Sprawdzać aktualny stan bezpieczeństwa systemów teleinformatycznych. | Oceniać wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji. | Zespół ds. wdrażania SZBI |  |
| Podejmowanie działań korygujących w celu ograniczenia ryzyka wystąpienia incydentów bezpieczeństwa informacji. | Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych,, Administrator CKDM, Administrator CZSK, Administratorzy |
| Działanie w procesie obsługi incydentów bezpieczeństwa informacji. | Specjalista ds. SZBI, Kierownik Działu Informatyki, w tym Sekcji Aplikacji i Systemów Informatycznych,, Administrator CKDM, Administrator CZSK. |
| 7 | Informować na bieżąco o efektach przeprowadzanych działań oraz reagowania na zaistniałe incydenty bezpieczeństwa teleinformatycznego. | Składanie dobowych raportów do MEiN o stanie realizacji zadań wynikających z wprowadzonego stopnia alarmowego. | Specjalista ds. obronnych i sytuacji kryzysowych. |  |
| Przekazywanie informacji Kanclerzowi o istotnych incydentach naruszenia bezpieczeństwa informacji. | Specjalista ds. SZBI |
| Zgłaszanie incydentów które mogą spowodować obniżenie jakości lub przerwanie realizacji zadania przez Uczelnię do właściwego CSIRT NASK lub CSIRT GOV. | Specjalista ds. SZBI |

**IV. ORGANIZACJA KIEROWANIA**

1. Zadania po wprowadzeniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP), kanclerz realizuje poprzez ww. wykonawców.

2. Wprowadzenie któregokolwiek ze stopni alarmowych powinno wiązać się ze zwołaniem posiedzenia Kolegium rektorskiego.

**V. POTRZEBY W PRZYPADKU PRZEDŁUŻAJĄCYCH SIĘ DZIAŁAŃ**

W przypadku przedłużania się okresu, na który wprowadzono pierwszy stopień alarmowy CRP (stopień ALFA-CRP), nie przewiduje się potrzeb odnośnie wsparcia prowadzonych działań.

**VI. BUDŻET ZADANIA**

Realizacja w ramach budżetu własnego.