Komunikat Rektora

Gdańskiej Wyższej Szkoły Humanistycznej w Gdańsku

z dnia 01.06.2024 r.

Szanowni Państwo,

Prezes Rady Ministrów RP podpisał Zarządzenia przedłużające obowiązywanie do 31 sierpnia 2024 r. do godz. 23:59.drugi stopień alarmowy BRAVO i drugi stopień alarmowy BRAVO-CRP na terytorium całego kraju

Drugi stopień BRAVO wprowadza się w sytuacji zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, kiedy jednak konkretny cel ataku nie został zidentyfikowany. Stopień ma charakter prewencyjny.

Drugi stopień BRAVO-CRP dotyczy zagrożenia w cyberprzestrzeni. Stopień alarmowy BRAVO-CRP oznacza, że administracja publiczna jest zobowiązana do prowadzenia wzmożonego monitoringu stanu bezpieczeństwa systemów teleinformatycznych.

Bezpieczeństwo w czasie obowiązywania stopni alarmowych uzależnione jest nie tylko od działania właściwych służb, ale też od czujności nas wszystkich.

Proszę o zwrócenie uwagi na nietypowe zachowania i pojawienie się nieuprawnionych osób na terenie Uczelni, zachowanie szczególnej czujności w stosunku do nietypowego funkcjonowania systemów informatycznych, usług oraz witryny www Uczelni, oraz ostrzeżenie personelu o możliwych zagrożeniach.

Informację o wszelkich niepokojących i nietypowych sytuacjach oraz zagrożeniach proszę kierować do personelu Uczelni lub zgłaszać je na numer alarmowy 112. Sygnały są mało dostrzegalne – jednak zwracanie uwagi na to, co dzieje się w najbliższym otoczeniu, pozwala na odpowiednio wczesne wykrycie zagrożenia.

Przypominam o podstawach bezpieczeństwa w sieci:

- Korzystać z mocnych haseł i stosować unikatowe hasła do różnych systemów.
- Korzystać tylko z zaufanych sieci – nie logować się do serwisów internetowych, korzystając z publicznych i otwartych sieci typu hotspot.
- Stosować oprogramowanie antywirusowe.
- Nie otwierać podejrzanych maili.
- Aktualizować przeglądarkę i system operacyjny.
- Nie klikać w wyskakujące ekrany i podejrzane reklamy.
- Korzystać z dwustopniowej weryfikacji. Podwójna ochrona utrudni uzyskanie dostępu do konta.
- Instalować oprogramowanie tylko ze znanych źródeł.
- Chronić nie tylko komputer, lecz także pozostałe urządzenia – należy zabezpieczyć telefon hasłem lub odciskiem biometrycznym i nie instalować aplikacji niewiadomego pochodzenia.
- Wylogowywać się z serwisów.

Aby chronić dane zalecam:

- Sprawdzić, jakich uprawnień wymaga instalowana aplikacja.
- Nie klikać w linki oraz załączniki. Jeśli otrzymasz podejrzaną wiadomość od znajomego, poświęć chwilę na zweryfikowanie jej.
- Nie podawać w rozmowie (zwłaszcza telefonicznej) poufnych danych.
- Nie wchodzić na stronę banku przez link. Wpisywać adres lub korzystać z tzw. zaufanych zakładek. Stosować podstawowe zasady bezpieczeństwa takie jak używanie złożonych i indywidualnych haseł dla każdej strony i odwiedzanie tylko zaufanych witryn, bez względu na to, za pomocą jakiego urządzenia jest połączenie.
- Uważać na płatności w aplikacjach mobilnych. Używać tylko oficjalnych aplikacji, instalowanych z pewnych źródeł.

REKTOR

prof. dr hab. Zbigniew Machaliński