Додаток

РЕКОМЕНДАЦІЇ
з посилення заходів на об'єктах кіберзахисту
напередодні Дня захисників і захисниць України
в період з 30 вересня по 2 жовтня 2023 року

Для попередження та зменшення можливих наслідків від кіберінцидентів/кібератак спрямованих на державні інформаційні ресурси, електронні комунікаційні та інформаційні-комунікаційні системи органів державної влади та місцевого самоврядування, об'єктів критичної інфраструктури, організацій та підприємств державної і приватної форми власності, а також постачальників електронних комунікаційних мереж та послуг рекомендуємо вжити наступні заходи:

1. Тимчасово заблокувати доступ до мережі Інтернет систем, функціонування яких не є критичним або які не будуть використовуватися у визначений період.

2. Провести з усіма співробітниками, що мають у період свят доступ до інформаційних систем, інструктаж щодо дотримання внутрішніх політик інформаційної безпеки та правил кібергігієни (https://cert.gov.ua/recommendation/31), приділити увагу питанням безпечного використання Інтернет-ресурсів, електронної пошти, роз'яснити потенційні сценарії соціальної інженерії, фішингу тощо з урахуванням святкової тематики (святкові повідомлення, привітання тощо).

3. Забезпечити у визначений період чергування на критично важливих системах (сервісах), об'єктах системних адміністраторів та адміністраторів безпеки.

4. Обмежити коло осіб, що мають віддалений доступ до інформаційних систем. У разі необхідності забезпечення віддаленого доступу, такий доступ надавати за рішенням керівника згідно з рекомендаціями Держспецзв'язку (https://cert.gov.ua/recommendation/11388).

5. Забезпечити логування подій та збереження їх на окремому дисковому сховищі, а також постійний моніторинг співробітниками, що визначені у пункті 3.

6. Організувати та забезпечити встановлення оновлень операційних систем та програмного забезпечення, особливу увагу приділити оновленням антивірусного програмного забезпечення (АВПЗ), системи управління подіями інформаційної безпеки (SIEM), системи виявлення вторгнень (IDS), системи попередження вторгнень (IPS), інших та актуальність сигнатур шкідливого програмного забезпечення (ШПЗ) в АВПЗ.

7. Забезпечити наявність актуальних резервних копій критично важливих систем (сервісів) та даних, передбачити наявність ресурсів для резервного копіювання.

8. В разі виявлення підозрілої активності для швидкого реагування на можливі кіберінциденти та кібератаки НЕГАЙНО інформувати відповідно до визначеного пунктом 4 розділу II «Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки»:

Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA на електронну адресу: cert@cert.gov.ua; за номерами телефонів: (044)-281-88-05/(044)-281-88-25, або за допомогою форми на сайті https://cert.gov.ua/contact-us.

Департамент кіберполіції Національної поліції України на електронну адресу: incident@cyberpolice.gov.ua.

Ситуаційний центр забезпечення кібербезпеки Служби безпеки України на електронну адресу: incident@dis.gov.ua та за номером телефоном: (093)-348-23-34.

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України на електронну адресу: report@ncscc.gov.ua

Начальник Головного управління радіоелектронної та кіберборотьби Генерального штабу Збройних Сил України полковник Іван ПАВЛЕНКО