Black Energy як загроза об'єктам критичної інфраструктури України

Положенцев Артем[1]
Гнатюк Сергій[2]

1. Кафедра безпеки інформаційних технологій, Національний авіаційний університет, УКРАЇНА, м. Київ, пр-т Комарова 1,
E-mail: artem.polozhencev@gmail.com[1], s.gnatyuk@nau.edu.ua[2]

Abstract: in this paper the concept of "critical infrastructure of the state" and the cyber attack Black Energy, which struck Ukrenergo in some regions of Ukraine, the airport "Borispol" and popular TV channels, are analyzed. The features of cyber attacks planned in advance, which are able to affect the economy of the nation, are highlighted and vulnerabilities of critical elements of infrastructure are shown.

Ключові слова: критична інфраструктура, кібератака, Black Energy

У XXI ст. інформація стає найдорожчим ресурсом, а її захист – невід'ємним елементом сьогодення. Стрімкий розвиток технологій відкрив нову сторінку розвитку і життя людства. Сьогодні ми все більше залежим від інформаційних технологій, які нас скрізь оточують і не тільки допомагають суспільству у повсякденному житті, а й контролюють багато автоматичних процесів, серед яких є і критичні елементи інфраструктури держави.

Актуальність теми полягає в тому, що в мінливій і нестабільній ситуації нашої держави ворог може скористатися неуважністю та неготовністю до активних дій в інформаційному середовищі та завдати значної шкоди як економіці, так і населенню.

Мета дослідження – аналіз терміну «критична інфраструктура держави» та кібератаки вірусом Black Energy, який використовували хакерські угрупування протягом останніх двох років при атаці на критично важливі елементи інфраструктури України.

Після багатьох терористичних актів, які відбулись в кінці 90-х уряди розвинених країн висунули ідею впровадження поняття «критичної інфраструктури держави», порушення роботи таких важливих об'єктів може призвести до колапсу на загальнодержавному, регіональному чи місцевому рівні. За чинним законодавчим актом США, цим терміном називають «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище». Сумісна праця держав ЄС у питанні критичної інфраструктури призвела до визначення під нею сукупності фізичних засобів виробництва, інформаційних технологій, мереж (транспортні, енергетичні і т. п.), служб і інших активів, розлад або руйнування яких мав би серйозні наслідки на здоров'я, охорону, надійність або життєвий рівень громадян або на штатне функціонування урядів в цих державах [1].

Нажаль, на сьогодні, в Україні не має чітко розробленої та описаної системи елементів, які становлять критичну інфраструктуру держави. З Постанов Кабінету Міністрів та інших нормативно-правових документів можна виділити такі об'єкти: підприємства, які мають стратегічне значення для економіки та безпеки держави; об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів; особливо важливі об'єкти електроенергетики та інші схожі підприємства [2].

За статистичними даними спец. служб кількість кібератак в останні роки значно зросла. Однією із таких атак є кібератака за допомогою вірусу Black Energy, якою нещодавно були атаковані українські обленерго. Black Energy вперше був використаний 2007 року. Під атаку попадали державні організації та інфраструктура різних країн. Дане шкідливе намагається отримати повноваження привілейованого користувача операційної системи, а після завершення атаки видаляє завантажувач, що у сукупності призводило до неможливості запуску операційної системи у подальшому. У 2014 році вийшла нова модифікація вірусу, якою саме і були вражені критичні елементи енергетики України.

Кібератака була завчасно спланована та розпочалась 2014 року з моменту, коли хакери почали відправляти електронні листи з нібито небезпечними паролями, які необхідно змінити. До файлу був прикріплений шпигунський модуль, який збирав інформацію про інформаційну систему. Починаючи з червня 2014 і по листопад 2015 року відбувалось активне зараження ресурсів Укренерго таким самим методом. Використовуючи можливості віддаленого доступу до системи, за допомогою даної троянської програми 23 грудня 2015 року близько 15:30 зловмисники провели скоординовану атаку на інформаційну інфраструктуру трьох Укренерго. За віддаленого доступу до адміністративних комп'ютерів, впливаючи на вимикачі на розподільних підстанціях, перекрили подачу електроенергії споживачам, в результаті чого без світла залишились близько 220 тис. людей. Кібератака на одне з обленерго також супроводжувалася масовими дзвінками на номери call-центру, з метою їх перевантаження. За наявною інформацією дзвінки велися з номерів в Російській Федерації.

Щоб запустити атаку зловмисники скористались такими уразливосятми організації: відсутність чітко розроблених посадових інструкцій; недотримання правил політики використання корпоративної пошти; критичні об'єкти інфраструктури на даний момент мають прямий доступ до Інтернету; слабка система протидії шкідливому забезпеченню.

Література

1. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT, 2001). – [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.go; 2. Постанова Кабінету Міністрів України від 23.12.2004 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави».