Правове і наукове забезпечення кібербезпеки України, частина 1

Research · November 2022

DOI: 10.13140/RG.2.2.19543.14243

CITATIONS
0

READS
95

2 authors:

Tetiana Obikhod
Institute for Nuclear Research
240 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Petro Bilenchuk
National Aviation University
26 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Правове і наукове забезпечення кібербезпеки України

У нинішньому році в умовах воєнного стану й дистанційного режиму роботи боротьба з кібератаками повинна залишатися в числі пріоритетних завдань у всіх основних галузях життєдіяльності держави. При тому в першу чергу треба зосередитися на кібербезпеці, нормативно-правовому забезпеченні й зміцненні гарантій безпеки в усіх сферах, що дозволить забезпечити краще розуміння різних деталей безпеки та підвищити інформаційну стійкість.

Петро БІЛЕНЧУК,
професор Європейської академії прав людини

Тетяна ОБІХОД,
кандидат фізико-математичних наук, старший науковий співробітник, доцент Київського університету ринкових відносин

Розбудова Україною власної кібербезпеки, потребує докорінних та невідкладних змін. Така позиція підтверджена атаками на об'єкти критичної інфраструктури, які створили Україні репутацію одного з головних кіберполігонів. Неефективна нормативна база у вигляді Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та серія нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі. Відсутнє й централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні. В той час як інструменти зловмисників трансформуються, зростає й кількість їх жертв. Тож керівники урядових структур та компаній повинні приділяти посилену увагу кібербезпеці, а саме:

1) привести заходи забезпечення безпеки у відповідність із визначеними цілями (наявність антивірусу, брандмауера, IDS, резервних серверів та резервного копіювання, виокремлення основного для безпеки компанії;

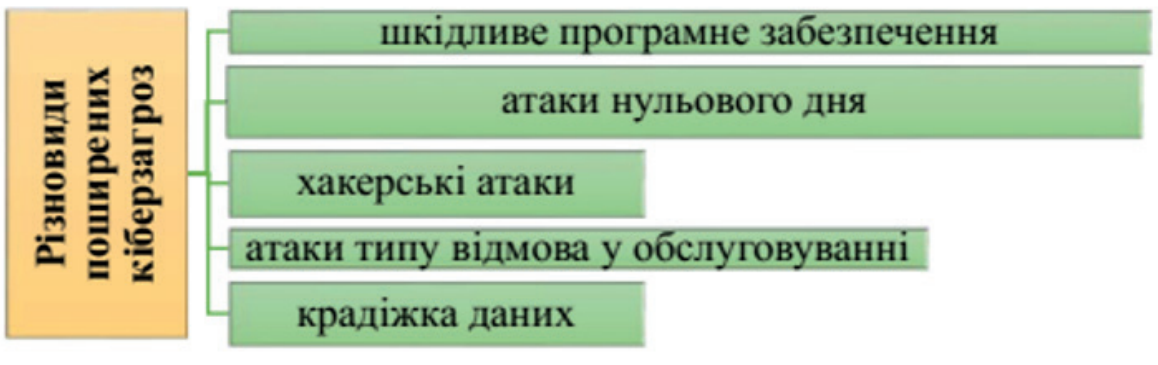
2) дбати про кращі практики управління (підтримувати всю виконану роботу в актуальному стані), як і про поглиблення обізнаності користувачів (управляти змінами, новими стратегіями, процесами і технологіями);

Важливим також є запровадження в Україні на державному рівні практики міжнародної сертифікації по Форензік, кібербезпеці, IT-аудиту, IT-управлінню. Потрібно вибудувати діалог між владою, IT-спеціалістами та бізнесом із питань кібербезпеки. Але для втілення всього цього потрібне розуміння кібербезпеки як системи, — що таке кібератаки, типи зловмисного програмного забезпечення, наслідки кібератаки й сучасні світові ноу-хау забезпечення кібербезпеки. Цим питанням і присвячено дану публікацію.

Кібератака та її небезпечність

Кібератака (англ. cyber-attack) — спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації і/або завдання збитків автоматизованій системі. Аналіз кібератак за 2022 рік дає змогу зробити висновок, що найпоширенішим вектором атак залишається крадіжка облікових даних (19%), потім фішинг (16%), неправильно налаштована хмара (15%) і вразливості стороннього програмного забезпечення (13%). Такі атаки можуть бути небезпечними на всіх рівнях життя держави: економічному, енергетичному, політичному, фінансовому, військовому тощо.

Наприклад, економічні проблеми від зростаючого обсягу шкідливих кібератак можуть бути пов'язаними з перериванням електронної торгівлі та витоком бізнес-даних, порушенням конфіденційності. А ці проблеми спричинять втрату прибутку для корпорацій. Такі виклики призводять до необхідності пильності з боку фахівців з мережевої безпеки організації, обізнаності в нових мережевих загрозах. Різновиди кіберзагроз наведено на діаграмі. 1.



Діаграма. 1. Різновиди кіберзагроз.

Віруси, хробаки та троянці — це окремі мережеві атаки, які в більш загальному плані класифікуються як розвідувальні атаки, атаки доступу або атаки типу «відмова в обслуговуванні» (DoS). При DoS-атаці мережа стає непрацездатною й не може реагувати на запити користувачів, тому необхідно впроваджувати інструменти та техніки для нейтралізації зовнішніх і внутрішніх загроз. У цьому аспекті важливу роль у корпоративних мережах відіграють хмарні технології, які дозволяють організаціям використовувати сховище даних або хмарних додатків за межами традиційного периметра мережі, дозволяючи розміщувати ЦОД (центри обробки даних) як всередині, так і ззовні традиційного брандмауера.

Ми живемо в період військової агресії, коли під загрозою перебувають усі критичні сфери життєдіяльності нашої країни за даної ситуації. Особливо важливою постає діяльність об'єктів критичної інфраструктури (ОКІ). Програмне забезпечення й програмні засоби стають найбільш вразливими серед складових інформаційних технологій ОКІ. Системні проблеми відсутності достатньої кількості фахівців з інформаційної безпеки, збільшення кібератак у період військової операції робить завдання вирішення цієї проблеми вкрай актуальним. В історії нашої держави визначено ряд гучних кібератак, наведених у таблиці 1.

Таблиця 1

Перелік реалізованих кібератак на ОКІ у період з 2015–2017 років

№	Найменування атаки	Вражені ОКІ	Дата реалізації
1	Кібератака «BlackEnergy 3»	«Прикарпаттяобленерго»	23 грудня 2015 року
		«Київобленерго»	23 грудня 2015 року
		«Чернівціобленерго»	23 грудня 2015 року
3	Кібератака з використання вірусу Petya	Аеропорт «Бориспіль», «Харків», «Київ»	27 червня 2017 року
		Укренерго, Київенерго, ДТЕК	27 червня 2017 року
		Чорнобильська АЕС	27 червня 2017 року
		Київський метрополітен	27 червня 2017 року
		ЗМІ	27 червня 2017 року
		Укрзалізниця	27 червня 2017 року
		Київводоконал	27 червня 2017 року
		ДП «Антонов»	27 червня 2017 року
		Оператори мобільного зв'язку	27 червня 2017 року

Поетапна реалізація кібератаки «BlackEnergy 3» на системи електропостачання «Прикарпаттяобленерго» наведена нижче:

1) було проведено фішинг-атаку шляхом направлення електронного листа зі шкідливим кодом оператору «Прикарпаттяобленерго» для отримання доступу до мережі системи. Шкідливий код був внесений у вигляді макросу до файлу Microsoft Office;

2) ідентифікація та встановлення у фоновому режимі шкідливого програмного забезпечення «BlackEnergy 3» на робочій станції оператора;

3) викрадення критичних даних для адміністрування з мережі «Прикарпаттяобленерго»;

4) використання віртуальних приватних мереж (VPN) для входу до ICS мереж «Прикарпаттяобленерго»;

5) використання існуючих інструментів для віддаленого доступу та управління в мережі «Прикарпаттяобленерго»;

6) використання модифікованого KillDisk для видалення основних записів завантаження уражених елементів системи, а також цільове видалення деяких журналів подій;

7) управління системи енергопостачання для впливу на підключене навантаження із запланованим відключенням обслуговування;

8) телефонна атака на відмову в обслуговуванні call-центру.

Результатами цієї атаки було вимкнено близько 30 підстанцій, і близько 230 тисяч мешканців залишалися без світла протягом однієї-шести годин.

Зрозуміло, що кібератаки — це не тільки атаки на енергетичні системи, а й на системи управління технологічними процесами, об'єкти інфраструктури, державні фінансові організації. Це ще й кібервійни, кібершпигунство, викрадення особистої інформації. З моменту початку бойових дій це поширилося на системи, пов'язані з урядовою адміністрацією та військовими. Кіберконфлікти надають стороннім особам можливість спостерігати та вимірювати ефективність різних стратегій, методів і технічної зброї. Серед нових комплексних і зухвалих атак, які не піддаються попередній класифікації, належить наступна сумна статистика за 2022 р.:

14 січня 2022 року — внаслідок хакерської атаки деякі урядові сайти та портал «Дія» перестали працювати. Хакери на сайті МЗС України повідомили 3 мовами (українська, російська та ламана польська), що викрали персональну інформацію українців і викладуть її у вільний доступ. Пізніше СБУ повідомила, що сайти відновлені, а витоку даних не було. Злам відбувся через злам October CMS.

15 лютого цього року — DDoS-атака на 15 банківських сайтів, сайтів зо доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин. За даними Ради національної безпеки США, кібератака була влаштована ГРУ Росії. Пізніше, 23 лютого, перед початком російського вторгнення в Україну було повторно атаковано низку державних сайтів та банківських сайтів. Компанія ESET виявила на зламаних сайтах шкідливі програмні засоби HermeticWiper, скомпільовані ще 28 грудня 2021 року.

Останні світові дані про кібератаки

Щодо останніх світових даних про кібератаки (2022 р.), то найбільш вражаючими є наступні з них:

1. З криптовалютою. Ринок компаній або інструментів для зберігання, конвертації та іншого керування криптоактивами процвітає. Таке швидке розширення мало й свої недоліки, якими швидко скористалися хакери. Наприкінці березня північнокорейська Lazarus Group вкрала стейблкоїн Ethereum і USDC на 540 мільйонів доларів із популярного «мосту» блокчейну Ronin.

2. Блокчейн-міст. Блокчейн-міст — це програма, яка дозволяє користувачам переміщувати криптовалюту з одного блокчейну в інший. Неможливо здійснити транзакцію в блокчейні біткойн за допомогою, наприклад, Dogecoin. Це робить мостові додатки життєво важливими, а дехто навіть скаже, що вони є «відсутньою ланкою» для того, аби зробити криптовалюту мейнстрімом. У лютому було викрадено варіант Wormhole Ethereum на суму 321 мільйон доларів, а в квітні зловмисники змогли використати протокол стейблкойна «Beanstalk», щоб отримати криптовалюту на суму 182 мільйони доларів на той час.

3. Промисловість. Двадцять сьомого червня дві іранські металургійні компанії Mobarakeh Steel Company та Khuzestan Steel Industries зазнали нападу. Відповідальність за це взяла на себе хактивістська група під назвою Predatory Sparrow. Одна атака, спрямована на фабрику в Хузестані, призвела до несправності машини, вивергання вогню та розплавленої сталі на фабрику. Атака могла завдати набагато більшої шкоди, але в Ірані є енергетичні обмеження.

4. Вторгнення за допомогою дронів. Використання дронів для здійснення кібервторгнень також було темою розмов протягом деякого часу. Дослідник безпеки Грег Лінарес сам стикався з трьома такими спробами за минулі два роки. Останній стосується неназваної фінансової компанії, яка помітила незвичайну активність у своїй внутрішній мережі злиття. Пізніше було виявлено, що в їхній мережі Wi-Fi є шахрайський пристрій. За допомогою сигнальних трекерів їх вивели на дах будівлі та виявили два дрони. Один із них, модифікований DJI Phantom, перевозив Wi-Fi-ананас, інший, потужніший та з більшою вантажопідйомністю, DJI Matrice 600, перевозив Raspberry Pi, міні-ноутбук (!), 4G-модем, пристрій Wi-Fi та акумулятори. Видається ймовірним, що якась початкова атака підробки Wi-Fi могла отримати внутрішні облікові дані для доступу до внутрішньої мережі.

Тенденції на 2022 рік ще аналізуються, хоча здається, що багато звичайних груп підозрюваних так само активні. Тож на сьогодні програми-вимагачі все ще є серйозною та жахливою загрозою для багатьох компаній. Проведені опитування, такі як IBM Security Cost of Data Breaches 2022, продовжують висвітлювати, що більшість компаній могли б досягти набагато кращих результатів, використовуючи лише базові передові методи безпеки. Основними векторами атак залишаються крадіжки облікових даних і фішингові електронні листи, тому життєво важливо продовжувати підвищувати обізнаність за допомогою корпоративного навчання та публічних рекламних

кампаній. Ну й нарешті, агресія рф проти України свідчить, наскільки ефективною може бути кіберзброя для зриву задумів командування та управління під час війни.

Головні загрози кібербезпеці

Хоча загрози кібербезпеці постійно змінюються, наведемо деякі з найвідоміших і найпоширеніших їх типів, на які варто звернути увагу на поточному ринку.

Фішинг. Ці загрози, які колись здебільшого обмежувалися погано написаними фішинговими електронними листами, набули популярності та витонченості, а атаки соціальної інженерії здійснюються на настільних комп'ютерах і мобільних пристроях за допомогою голосових дзвінків, текстових повідомлень та соціальних мереж. Ці атаки досягають усе більшого рівня успіху. Так, Федеральна торгова комісія (США) стверджує, що в 2020 році було подано 4,8 мільйона звітів про крадіжки особистих даних і шахрайства, що на 45% більше, ніж у 2019-му, при цьому фішинг становить 44% всіх кібератак. Різноманітні атаки, як-от фішинг, під час якого зловмисники переслідують цілі високого рівня, також зростають.

Програмне забезпечення-вимагач. Під час атаки програмного забезпечення-вимагача кіберзлочинець встановлює частину зловмисного програмного забезпечення на комп'ютер або сервер (зазвичай цільовий бізнес), яке шифрує конфіденційну інформацію, яку знаходить. Потім зловмисник вимагає викуп, щоб розшифрувати дані, як правило, у формі платежів у біткойнах, які неможливо відстежити. У 2019 році в усьому світі хакери вимагали близько 25 мільярдів доларів викупу, а загальні витрати на відновлення та збитки наближалися до 170 мільярдів доларів. Екстремальні атаки програм-вимагачів можуть вивести з ладу ланцюжок поставок, виробничі можливості або здатність компанії працювати.

Атаки ботнетів. Історично ботнети використовувалися для запуску атак типу «відмова в обслуговуванні» (DoS) або розподілених атак «відмова в обслуговуванні» (DDoS), а також для прихованого захоплення обчислювальних ресурсів підприємства, як правило, для майнінгу криптовалют. NetScout повідомляє, що минулого року загальна кількість DDoS-атак вперше перевищила 10 мільйонів. Підприємства піддаються ризику не лише через те, що вони стають об'єктами атак ботнетів, але й через те, що в їхніх власних мережах встановлено шкідливе програмне забезпечення для ботів.

Хмарні експлойти. Спроби використання хмарних ресурсів нині зростають, оскільки організації продовжують переносити служби в хмару та розширювати таку інфраструктуру. Як і в інших експлойтах, хакери часто мають намір використовувати заражені корпоративні хмарні ресурси для викрадення даних або видобутку криптовалюти. Популярність хмарних атак у 2020 році зросла на 250%.

Атаки, пов'язані з роботою з дому. Обмеження, пов'язані з пандемією COVID-19, змушують мільйони корпоративних працівників працювати вдома рік або й більше. Оскільки гігієна домашньої безпеки користувачів зазвичай не така ретельна, як на рівні підприємства, це відкриває двері для атак, спрямованих на незахищені мережі Wi-Fi, паролі, які легко зламати, і навіть фізичну крадіжку таких пристроїв, як ноутбуки та смартфони.

Атаки на національну державу. Вважається, що резонансна атака SolarWinds, яка сталася в 2020 році, була ініційована російською розвідкою. Під час атаки кіберзлочинці впровадили бекдори в мережі десятків міжнародних компаній і державних установ, які надали їм постійний доступ протягом майже року, перш ніж їх виявили. Це актуалізувало необхідність стратегій проактивної протидії цим складним операціям кібершпигунства. Наведемо різновиди операцій кібершпигунства по роках, діаграма 2.

Слід наголосити, що сучасні загрози кібербезпеки істотно еволюціонували. Оскільки за останній рік загрози кібербезпеці різко зросли, вони також стають дедалі складнішими та цілеспрямованішими. Кіберзлочинці зазвичай використовують загальнодоступну інформацію, таку як дані соціальних мереж, особисті дані та паролі. Завдяки цим даним, які зазвичай доступні на чорному ринку, хакерам легше, ніж будь-коли, заповнити прогалини в інформації про потенційну ціль. Тим часом технологія, доступна для здійснення цих атак, стає все більш поширеною. Зловмисники можуть використовувати ті ж типи ресурсів, що й будь-яке підприємство, включаючи хмарні обчислення, штучний інтелект (AI) і розподілені обчислювальні ресурси, щоб збільшити ймовірність успішної атаки.

Цілі кібератаки

Як правило, це **гроші.** Кінцевою метою більшості атак, прямо чи опосередковано, є фінансова вигода. Цього можна досягти шляхом крадіжки банківських облікових даних, номерів кредитних карток, ширшої крадіжки особистих даних або прямої крадіжки грошових ресурсів, таких як криптовалюта.

Дані. Це включає в себе крадіжку особистої інформації (такої як номери соціального страхування, записи про медичне страхування тощо) або корпоративних даних (включаючи інтелектуальну власність, вихідний код, записи клієнтів тощо). Основна мета зловмисника щодо цих даних полягає в тому, щоб або використати їх для здійснення нових атак, або продати.

Обчислювальні ресурси. Кіберзловмисники часто прагнуть використати доступну обчислювальну потужність підприємства для здійснення додаткових атак або через традиційний центр обробки даних, або через хмару. Ці ресурси зазвичай використовуються для видобутку цінних криптовалют або запуску ботнетів, які запускають зловмисне програмне забезпечення або інший шкідливий код для запуску DDoS-атак.

Загальний хаос. Хоча й менш поширені, деякі атаки все ж здійснюються, щоб створити хаос і завдати шкоди жертвам. До цієї категорії належать атаки на системи водопостачання, електромережі та іншу критичну інфраструктуру.

(Далі – буде)

Діаграма 2