Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Як протистояти реальним кіберзагрозам об’єктам критичної інфраструктури України

Козюра В.Д.
кандидат технічних наук, доцент
Національна академія Служби безпеки України
Хорошко В.О.
доктор технічних наук, професор
Національний авіаційний університет

Кібератаки, здійснювані проти об'єктів критичної інфраструктури України, до яких відносяться підприємства, установи та організації, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей, носять цілеспрямований характер. Про це свідчать інциденти, пов'язані з енергосистемами західних областей України, спроби вторгнення в інформаційно-телекомунікаційні системи повітряного транспорту, атаки на сайти державних органів, банківські установи і т.п.

Таргетована (цільова) кібератака (від англ. target) є безперервним тривалим процесом несанкціонованої активності кіберзлочинів в умовах конкретного об'єкту критичної інфраструктури, покликаним здолати конкретні механізми забезпечення безпеки і завдати конкретного збитку (фізичного, інформаційного, морального і т.д.). Цей процес видалено керований в реальному часі організованою професійною групою кіберпорушників, озброєних потужними апаратно-програмними засобами.

Інструментарієм таргетованих кібератак є засоби APT (Advanced Persistent Threat – атакуюча безперервна загроза) – комбінація спеціальних утиліт видаленого доступу, шкідливого програмного забезпечення, механізмів використання уразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки.

Таргетована кібератака включає наступні фази:

1. Підготовка – виявлення об’єкту атаки, збір детальної інформації про об'єкт, спираючись на яку виявляються слабкі місця в інфраструктурі, розробка стратегії атаки, моделювання атаки, підбір і розробка інструментів атаки, їх тестування на стендах.

2. Проникнення – активна фаза атаки, що використовує комбіновану техніку соціальної інженерії й уразливостей «нульового дня» для первинного інфікування цілі та проведення внутрішньої розвідки. Після закінчення розвідки і визначення приналежності інфікованого хоста по команді порушника через центр управління може завантажуватися додатковий шкідливий код.

3. Поширення – фаза закріплення усередині об'єкту критичної інфраструктури переважно на ключових комп'ютерах. При необхідності через центри управління вносяться необхідні корективи в шкідливий код на основі зібраної ключової інформації.

4. Досягнення мети – ключова фаза цільової атаки, залежно від вибраної стратегії в ній може застосовуватися внесення змін до технологічних процесів, що призводять до аварій і катастроф, розкрадання закритої інформації, умисне внесення змін до закритої інформації, маніпуляції з бізнес-процесами, розкрадання фінансових ресурсів та ін.

Обов'язкова умова цільової кібератаки – приховання слідів активності на усіх її етапах.

Інструментарієм проникнення на об'єкти критичної інфраструктури є:

- експлойти – шкідливі коди, що використовують уразливості в програмному забезпеченні;
- валідатори – шкідливі коди, вживані в первинному інфікуванні об'єктів атаки з метою збору інформації про хости і передачі її в командний центр для подальшого прийняття рішення про розвиток кібератаки;
- завантажувачі модуля доставки Dropper (використовуються в кібератаках, побудованих на методах соціальної інженерії);
- модуль доставки Dropper – троянська програма, завданням якої є доставка основного вірусу Payload на заражений комп'ютер;
- вірус Payload – основний шкідливий модуль в цільовій атаці, що завантажується на інфікований хост. Складається з декількох модулів, кожен з яких виконує свою функцію (клавіатурного шпигуна, видаленого доступу, поширення усередині інфраструктури, взаємодії з командним центром, шифрування, управління технологічними процесами, очищення слідів активності, самознищення і т.д.).

Що можна протиставити таргетованим кібератакам?

1. Запобігання цільовим атакам – не допустити запуск неконтрольованих процесів в корпоративній мережі. Основні заходи:

а) технічні рішення (захист кінцевих точок, міжмережеві екрани і системи запобігання вторгненням);

б) навчання персоналу (ознайомлення з кіберзагрозами, тренування з кібербезпеці і т.п.).

2. Виявлення слідів атаки, розпізнавання ознак зараження. Для цього використовуються мережеві/поштові сенсори, що дозволяють здійснювати збір інформації з різних контрольних точок, сенсори робочих станцій, що дозволяють збільшити охоплення і деталізацію аналізованої інформації, компоненти динамічного аналізу об'єктів, центри аналізу аномалій, хмарні сервіси – обновлювані в реальному часі бази знань про загрози.

3. Реагування – реакція на інцидент інформаційної безпеки – застосування набору прийнятих процедур, спрямованих на мінімізацію збитку і усунення наслідків атаки. Етапи реагування включають ідентифікацію, заборону, лікування, відновлення, профілактику.

4. Прогнозування – реалізація проактивних заходів, що дозволяють істотно утруднити порушникам підготовку і проведення атаки. Етап прогнозування включає наступний набір послуг: тест на проникнення, оцінка рівня захищеності, своєчасна оцінка уразливостей, аналітичний звіт про загрози інформаційної безпеки.

Необхідно пам'ятати, що відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об’єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах покладається на власників та керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури.

Зарубіжне та вітчизняне трактування терміну «кібербезпека»

Кондратюк М.В.
аспірант кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
Науковий керівник: Грохольський В.Л.
доктор юридичних наук, професор,
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Поняття «безпека» в сучасному світі відіграє чи не найголовнішу роль у всіх життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних і ін. Тому дуже важливо не тільки коректно визначати це поняття і його похідні, а й правильно застосовувати їх за призначенням. На жаль, до теперішнього часу цей вельми бажаний результат не отримано. Однак спроби його досягнення тривають.

Кібербезпека є важливим видом національної безпеки, метою якої є забезпечення основоположних прав, свобод громадян від кіберзагроз, кіберінцидентів та кіберзлочинів. Слід відзначити, що серед науковців, а також на законодавчому рівні відсутнє загальне визначення терміну «кібербезпека». Вважається, що вперше цей термін виник у середині 1990-х років, коли уряд США став досліджувати цю тему. Велика кількість країн прийняли або розробляють стратегії кібербезпеки.

У 2012 р. був введений у дію схвалений світовою спільнотою стандарт кібербезпеки ISO/IEC 27032:2012 “Information technology – Security techniques – Guidelines for cybersecurity”, відповідно до якого кібербезпека (cybersecurity) – сукупність таких її підвидів: мережевої безпеки, безпеки критичних інформаційних інфраструктур, безпеки Інтернету. При цьому під кібербезпекою виходячи з її компонентів розуміється забезпечення конфіденційності, цілісності та доступності інформації в кіберпросторі, а під кіберпростором – складне середовище, яке виникає в результаті взаємодії людей, програмного забезпечення, сервісів, завдяки технологічним пристроям та мережевим зв’язкам [1, с. 70].

Визначення поняття “кібербезпека” також знайшло відображення у фундаментальних правових документах (стратегіях, концепціях) переважної більшості країн світу. 24 квітня 2015 р. за ініціативи Міністерства оборони в США була схвалена оновлена стратегія національної кібербезпеки [2], у положеннях якої визначено основні засади сучасного захисту кіберпростору, функції та завдання публічних адміністрацій у сфері спеціальних інформаційних операцій.