Кухаренко Сергій Вікторович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук

СУЧАСНІ ТИПИ КІБЕРЗАГРОЗ

У сучасному суспільстві комп'ютери використовуються практично у всіх областях діяльності. Досить часто виникає необхідність захисту важливої інформації. Великі організації мають в своєму складі фахівців з кібербезпеки (служба захисту інформації) але у організації невеликого або середнього розміру питання безпеки інформації залишають на потім.

На жаль, не існує готових рецептів на всі випадки життя і немає підходів, однаково придатних для всіх організацій, щоб убезпечити себе хоча б від найбільш вірогідних ризиків. Спробуємо виділити основні типи загроз кібербезпеки, на які необхідно звернути особливу увагу. З огляду на те, що захист від атак на мережевий периметр приділяється дуже велика увага і практично будь-який пристрій, яке ви купуєте і встановлюєте у себе в офісі або вдома, наприклад мережевий маршрутизатор або домашній WiFi роутер, вже мають базові засоби захисту.

Спробуємо звернути увагу на ті загрози і методи їх усунення, які виражені не так явно або їх важливість, як правило, недооцінюється.

Виділимо п'ять основних типів кіберзагроз: програми-вимагачі, цільові кібератаки, DDoS-атаки, фішинг і внутрішні загрози, пов'язані з діяльністю інсайдерів і людськими помилками.

Згідно з останнім звітом «Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round» [1] з кіберзлочинності, 86% атак фінансово мотивовані: зловмисники або безпосередньо вимагають гроші у жертви, або виконують сторонній замовлення, наприклад, конкурентів чи інших недоброзичливців.

Найбільшою мірою сьогодні схильні до атак оператори зв'язку, фінансові організації, ритейл-мережі і промисловий сектор. Крім того все більше привертає уваги кіберзлочинців малий і середній бізнес. Це пояснюється тим, що конкуренція в ньому досить висока, а можливості кіберзахисту і оцінки ризиків часто обмежені. Посилює проблему масовий перехід на віддалену роботу, через що периметр мережі організації поширився на будинки співробітників і їх особисті пристрої.

Отже на мій погляд можливо виділити наступні основні типи кіберзагроз на даний час, такі як: програми-вимагачі, цільові кібератаки, DDoS-атаки, інсайдерські загрози та фішинг.

Програми-вимагачі

Віруси-вимагачі шифрують дані на комп'ютері користувача і вимагають викуп за можливість відновити доступ до них. Зазвичай пропонується заплатити викуп криптовалютою. Проникнувши в корпоративну мережу, віруси-вимагачі здатні блокувати відразу велику кількість комп'ютерів.

Найбільш схильні до атак з метою вимагання телекомунікаційні компанії, інтернет-провайдери, освітні установи, урядові і технологічні організації.

У кіберзлочинності спостерігається тенденція до спеціалізації і співпраці. Об'єднуючи зусилля, зломщики успішно справляються з системами захисту великих організацій, розділяючи виручку.

Для повноцінного захисту від вимагачів потрібно не тільки сучасне програмне забезпечення, а й системна профілактика, що включає оцінку ризиків, установку міжмережевих екранів, створення резервних копій, розробку сценаріїв реагування на різноманітні події та інші заходи.

Цільові кібератаки

В останні роки кіберзлочинці перейшли до більш цілеспрямованих атак, зосереджуючись на конкретних галузях з їх характерними уразливими місцями. Зростання частки цілеспрямованих атак зумовлений низкою причин. По-перше, зловмисники жадають не витрачати час на компа-

нії, які не гарантують їм грошову прибуток. По-друге, щорічно з'являються нові групи зловмисників, які спеціалізуються на атаках класу APT (advanced persistent threat – різновид складних кібератак з метою отримання несанкційованого доступу до інформаційних систем жертви та встановлення прихованого доступу до неї з метою використання або контролю в майбутньому).

Цільова атака полягає в тому, що спочатку зловмисники шукають спосіб потрапити в корпоративну мережу: збирають інформацію, шукають уразливості організації (не тільки цифрові, але й фізичні), вивчають розклад, маршрути, слабкості, цікавлять співробітників та інше. Потім здійснюється власне проникнення: зловмисники можуть надіслати на конкретного співробітника фішинговий лист, вкрасти телефон співробітника для вилучення будь-яких корпоративних паролів, втертися в довіру компанії під виглядом підрядника або проникнути в офіс в якості кур'єра. Метою на цьому етапі є прихована установка програмного забезпечення на корпоративній техніці.

На останньому кроці діючи вже зсередини компанії, зловмисники підбираються до інформації, яка їх цікавить і викрадають її в обхід засобів захисту. Потім, як правило, зловмисники замітають сліди, щоб атака не була виявлена.

В цільової атаці можуть використовуватися будь-які інші кіберзлочинні методи – фішинг, вимагання та інше.

Запобігання цільових атак – складне завдання. Однак сучасні засоби захисту при їх правильному і комплексному використанні дозволяють зрозуміти, що відбувається якась неавторизована активність. Кожен користувач повинен спочатку пройти ідентифікацію, тобто довести системі, що це він, а потім авторизацію, тобто отримати строго певні права в системі.

Для запобігання цільових атак потрібне строгий і чіткий розподіл прав доступу всередині компанії і дотримання принципу мінімальної достатності: тобто виконуються лише ті дії, які потрібні для необхідних процесів.

DDoS-атаки

DDoS-атака – це атака на будь-яку обчислювальну систему (наприклад, сервер) з метою вичерпати її апаратний ресурс шляхом величезної кількості одночасних звернень до неї. Коли система не справляється з обробкою цих звернень, відбувається відмова в обслуговуванні (Denial of Service) і система виходить з ладу.

DDoS-атаки становлять небезпеку в першу чергу для компаній, діяльність яких безпосередньо пов'язана з інтернетом (електронна комерція), а також для операторів зв'язку.

Останнім часом зловмисники використовують для своїх ботів пристрої інтернету речей (IoT), тобто, наприклад, побутові прилади з підключенням до інтернету: принтери, розумні колонки, кондиціонери, системи освітлення в розумному будинку та інше. Виробники IoT-пристроїв, як і користувачі цих пристроїв, найчастіше не приділяють уваги їх безпеки, тому заразити IoT-пристрій відносно просто.

Для боротьби з DDoS-атаками застосовують DDoS-фільтри, що дозволяють вибірково відсікати зайві звернення до сервера, що йдуть від ботів. Профілактика DDoS-атак включає розумну мінімізацію контактів системи з іншими пристроями: доступ до системи повинен бути закритий для портів, протоколів і додатків, взаємодія з якими не передбачено.

Інсайдерські загрози

Велика група загроз, джерелом яких є власні співробітники. Поширена в організаціях, де відсутній контроль за наданням прав доступу високого рівня, а також відсутні розмежування з прав доступу до інформаційних ресурсів.

Інсайдерські загрози можуть бути пов'язані як зі злим умислом, так і з випадковими діями, з людською помилкою.

Для боротьби необхідно реалізовувати принцип мінімальної достатності: працівнику треба давати тільки ті права, які йому потрібні для виконання робочих обов'язків. Крім того, також допоможуть системи і методи, які аналізують поведінку користувачів. Вони побудовані на технологіях штучного

інтелекту і здатні до навчання на основі статистики, постійно моніторять активність співробітників на робочих місцях. Якщо ті відхиляються від заздалегідь заданих сценаріїв діяльності, то формуються оповіщення для служби безпеки, яка може заблокувати ту чи іншу дію.

В останні роки зловмисники все частіше використовують передові технології, такі як штучний інтелект, і застосовують методи соціальної інженерії, тобто експлуатують уразливість людської психології.

Фішинг

Це вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних. Найчастіше приманкою є електронний лист, здатний зацікавити одержувача, а гачком – закладений в цей лист шкідливий виконуваний файл або гіперпосилання на нього.

На даний час, це може бути посилання на свіжу статистику по темі, що стосується Covid, або якусь іншу актуальну інформацію, яка цікава багатьом користувачам [2].

Небезпека фішингу в тому, що головний елемент в ньому не технічний, а психологічний. Зловмисники знають, що людину обдурити легше, ніж машину. Сучасні засоби захисту дозволяють в автоматичному режимі у всіх файлах, які передаються поштою або через інтернет, аналізувати посилання в процесі відкриття і переривати цей процес, якщо фіксують запуск виконуваних файлів.

Висновки

Ці фактори, серед інших, говорять про те, що базове розуміння кіберзагроз необхідно перемістити з професійної області ІТ-фахівців в область загального знання. Кожен співробітник повинен мати певне уявлення про сучасні загрози, а тим більше керівник, який ставить завдання фахівцям з кібербезпеки.

Список використаних джерел:

1. Отчет Verizon Business 2020 о расследовании утечек данных (DBIR2020) [Електронний ресурс]. – Режим доступу:

https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-go-round

2. Global Threat Landscape Report [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/Threat-Report-H1–2020.pdf

Ключові слова: Кібербезпека, кіберзлочинність, кібератака, порушення даних.

Ключевые слова: кибербезопасность, киберпреступность, кибератака, нарушение данных.

Keywords: cybersecurity, cybercrime, cyberattack, data breach

Онацький Олексій Віталійович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки та інформаційних технологій,
кандидат технічних наук, доцент

Красношлик Олександр Юрійович
Національний університет «Одеська юридична академія»,
студент 3 курсу спеціальності 125 – Кібербезпека

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ НА ОСНОВІ АСИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ

Автентифікація – це процедура перевірки автентичності суб'єкта котрий входить в систему та пред'являє свій ідентифікатор. Основним міжнародним стандартом з криптографічних протоколів автентифікації є стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії ISO/IEC9798 – Information technology – Security techniques – Entity authentication, що складається з шести частин [1]:

– ISO/IEC9798–1:2010 Part 1: General;

– ISO/IEC9798–2:2019 Part 2: Mechanisms using authenticated encryption;

– ISO/IEC9798–3:2019 Part 3: Mechanisms using digital signature techniques;