Научная статья
Original article
УДК 004.424

КИБЕРАТАКИ АНАЛИЗ И РИСКИ

CYBER ATTACKS ANALYSIS AND RISKS

Кодацкий Никита Максимович, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), nickitadatsky@gmail.com
Мотуз Александр Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), alexandrmotuz14@gmail.com

Kodatsky Nikita Maksimovich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), nickitadatsky@gmail.com
Motuz Alexander Sergeevich Bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), alexandrmotuz14@gmail.com

Аннотация: Кибератака - это набор действий, выполняемых злоумышленниками, которые пытаются получить несанкционированный доступ, украсть данные или нанести ущерб компьютерам, компьютерным сетям или другим вычислительным системам. Кибератака может быть запущена из любого места. Атака может быть осуществлена отдельным лицом или группой с использованием одной или нескольких тактик, приемов и процедур.

Annotation: A cyberattack is a set of actions performed by cybercriminals who are trying to gain unauthorized access, steal data, or damage computers, computer networks, or other computing systems. A cyberattack can be launched from anywhere. An attack can be carried out by an individual or a group using one or more tactics, techniques and procedures.

Ключевые слова: кибератака, киберпреступники, угрозы

Keywords: cyberattack, cybercriminals, threats

Лица , которые запускают кибератаки обычно называют киберпреступников, угрозы актеров, плохих актеров, или хакеров. Они могут работать в одиночку, в сотрудничестве с другими злоумышленниками или в составе организованной преступной группы. Они пытаются определить уязвимости - проблемы или слабые места в компьютерных системах - и используют их для достижения своих целей.

Киберпреступники могут иметь различные мотивы при проведении кибератак. Некоторые совершают нападения ради личной или финансовой выгоды. Другие - « хактивисты », действующие во имя социальных или политических целей. Некоторые атаки являются частью операций кибервойны, проводимых национальными государствами против своих противников или действующих в составе известных террористических групп.

Статистика кибератак

Каковы затраты и влияние кибератак для бизнеса?

Ожидается, что глобальная стоимость кибератак будет расти на 15% в год и достигнет более 10 триллионов долларов. Растущую часть этих затрат составляют атаки программ-вымогателей, которые в настоящее время обходятся предприятиям в 20 миллиардов долларов США в год.

Средняя цена утечки данных в США составляет 3,8 миллиона долларов. Еще одна тревожная статистика заключается в том, что публичные компании теряют в среднем 8% стоимости своих акций после успешного взлома.

Насколько хорошо организации подготовлены к кибератакам?

В недавнем опросе 78% респондентов заявили, что они считают, что меры кибербезопасности их компании нуждаются в улучшении. 43% малых предприятий не имеют средств киберзащиты. В то же время организации любого размера сталкиваются с глобальной нехваткой навыков в области кибербезопасности: почти 3,5 миллиона открытых рабочих мест по всему миру, 500 000 из них только в США.

Примеры кибератак

Вот несколько недавних примеров кибератак, оказавших глобальное влияние.

Атака программ-вымогателей Kaseya

Компания Kaseya, американский поставщик программного обеспечения для удаленного управления, подверглась атаке на цепочку поставок, которая была обнародована 2 июля 2021 года. Компания объявила, что злоумышленники могут использовать ее продукт VSA для заражения компьютеров клиентов программами-вымогателями.

Сообщается, что атака является очень сложной и объединяет несколько новых уязвимостей, обнаруженных в продукте Kaseya: CVE-2021-30116 (утечка учетных данных и ошибка бизнес-логики), CVE-2021-30119 (XSS) и CVE-2021-30120 (ошибка двухфакторной аутентификации). Вредоносная программа, использующая эти уязвимости, была доставлена клиентам с помощью поддельного обновления программного обеспечения с надписью «Kaseya VSA Agent Hot Fix».

Атаку осуществила российская киберпреступная группа REvil. Касея сказал, что от взлома пострадали менее 0,1% их клиентов, однако некоторые из них были поставщиками управляемых услуг (MSP), которые использовали программное обеспечение Kaseya, и атака затронула их клиентов. Вскоре после атаки в прессе сообщалось, что 800-1500 малых и средних компаний были заражены вымогателем REvil в результате атаки.

Атака на цепочку поставок SolarWinds

Это была масштабная инновационная атака на цепочку поставок, обнаруженная в декабре 2020 года и названная в честь своей жертвы, управляющей ИТ-компании SolarWinds из Остина. Его провела APT 29, организованная киберпреступная группа, связанная с правительством России.

В результате атаки было скомпрометировано обновление, предназначенное для программной платформы SolarWinds, Orion. Во время атаки злоумышленники внедрили вредоносное ПО, известное как Sunburst или Solorigate, в обновления Orion. Затем обновления были распространены среди клиентов SolarWinds.

Атака SolarWinds считается одной из самых серьезных кибершпионажных атак на Соединенные Штаты, поскольку она успешно нанесла удар по вооруженным силам США, многим федеральным агентствам США, включая агентства, отвечающие за ядерное оружие, критически важные инфраструктурные услуги и большинство компаний из списка Fortune 500. организации.

Атака Amazon DDoS

В феврале 2020 года Amazon Web Services (AWS) стал целью крупномасштабной распределенной атаки типа «отказ в обслуживании» (DDoS). Компания испытала и предотвратила DDoS-атаку со скоростью 2,3 Тбит / с (терабит в секунду), при которой скорость пересылки пакетов составила 293,1 млн пакетов в секунду, а скорость запросов в секунду (об / с) - 694201. Считается одной из крупнейших DDoS-атак в истории.

Атака удаленного выполнения кода Microsoft Exchange

В марте 2021 года была проведена масштабная кибератака на популярный корпоративный почтовый сервер Microsoft Exchange. Он использовал четыре отдельных уязвимости нулевого дня, обнаруженные на серверах Microsoft Exchange.

Эти уязвимости позволяют злоумышленникам подделывать ненадежные URL-адреса, использовать их для доступа к системе Exchange Server и обеспечивать прямой путь к хранилищу на стороне сервера для вредоносных

программ. Это атака с удаленным выполнением кода (RCE), которая позволяет злоумышленникам полностью скомпрометировать сервер и получить доступ ко всем его данным. На пораженных серверах злоумышленники украли конфиденциальную информацию, внедрили программы-вымогатели и развернули бэкдоры практически не отслеживаемым способом.

Только в Соединенных Штатах от атак пострадали девять государственных учреждений и более 60 000 частных предприятий.

Атака знаменитостей Twitter

В июле 2020 года Twitter был взломан группой из трех злоумышленников, которые захватили популярные аккаунты Twitter. Они использовали атаки социальной инженерии для кражи учетных данных сотрудников и получения доступа к внутренним системам управления компании, что позже было идентифицировано Twitter как вишинг (телефонный фишинг).

Были взломаны десятки известных аккаунтов, в том числе Барака Обамы, Джеффа Безоса и Илона Маска. Злоумышленники использовали украденные аккаунты для публикации мошенничества с биткойнами и заработали более 100000 долларов. Через две недели после событий Министерство юстиции США предъявило обвинение трем подозреваемым, одному из которых на тот момент было 17 лет.

Другие известные атаки

2018 г.

- Starwood Hotels компании Marriott объявила об утечке личных данных более 500 миллионов гостей.
- Бренд MyFitnessPal от UnderArmor утек в утечку адресов электронной почты и информации для входа в 150 миллионов учетных записей пользователей.

2017 г.

- Атака программы-вымогателя WannaCry затронула более 300 000 компьютеров в 150 странах, причинив ущерб на миллиарды долларов.

- Equifax столкнулся с уязвимостью с открытым исходным кодом в неустановленном программном компоненте, в результате чего произошла утечка личной информации 145 миллионов человек.

2016 г.

- Атака NotPetya поразила цели по всему миру, несколько волн продолжались более года, а ущерб был нанесен более чем в 10 миллиардов долларов.
- В результате атаки на сайт знакомств для взрослых FriendFinder были скомпрометированы данные 412 миллионов пользователей.
- В результате инцидента с утечкой данных Yahoo были скомпрометированы учетные записи 1 миллиарда пользователей, вскоре после того, как предыдущая атака раскрыла личную информацию, содержащуюся в 500 миллионах учетных записей пользователей.

Литература

1. Толковый словарь по вычислительной технике. – М.: Издательский отдел "Русская редакция" ТОО "Channel trading Ltd", 2005.
2. Материалы сайта "Сервер информационных технологий". WEB: www.citforum.ru.
3. Хомоненко А. Базы данных: Учеб. Для вузов. – 2-е изд. – СПб., 2000.
4. Фёдорова А., Елманова Н. Базы данных для всех. –М.: Компьютер пресс , 2001.
5. Глушаков С.В., Ломотько. Базы данных (2001 год издания). – М.: АСТ, 2001.
6. Карпова Т. Базы данных: модели, разработка, реализация, 2001.
7. Когаловский М.Р. Энциклопедия технологий баз данных. –М.: Финансы и статистика, 2002.
8. Конноли Т., Бегг Л., Страчан А. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 2-е изд. – Вильямс, 2000.
9. Ханенко В.Н. Информационные системы. – СПб.: Питер, 2001

10. Корнеев В.В., Гареев А.Ф. и др. Базы данных. Интеллектуальная обработка информации. М.: Изд. С.В. Молгачева, 2001.
11. Ребекка М. Райордан Основы реляционных баз данных, 2001.

References

1. Explanatory dictionary of computer technology. - M.: Publishing department "Russian edition" LLP "Channel trading Ltd", 2005.
2. Materials of the site "Information Technology Server". WEB: www.citforum.ru
3. Homonenko A. Databases: Proc. For universities. - 2nd ed. - St. Petersburg, 2000.
4. Fedorova A., Elmanova N. Databases for everyone. –M.: Computer press, 2001.
5. Glushakov S.V., Lomotko. Databases (2001 edition). – M.: AST, 2001.
6. Karpova T. Databases: models, development, implementation, 2001.
7. Kogalovsky M.R. Database Technology Encyclopedia. –M.: Finance and statistics, 2002.
8. Connolly T., Begg L., Strachan A. Databases. Design, implementation and support. Theory and practice. - 2nd ed. - Williams, 2000.
9. Khanenko V.N. Information Systems. - St. Petersburg: Peter, 2001
10. Korneev V.V., Gareev A.F. and other databases. Intelligent information processing. M.: Ed. S.V. Molgacheva, 2001.
11. Rebecca M. Riordan Fundamentals of Relational Databases, 2001.

© Кодацкий Н.М., Мотуз А.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Кодацкий Н.М., Мотуз А.С. КИБЕРАТАКИ АНАЛИЗ И РИСКИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.