6. T. Slonecker, "Visible and Infrared Remote Imaging of Hazardous Waste: A Review" Remote Sens. 2, 2474 (2010).
7. Russ Islam, "Hyperspectral Imaging and its Applications," Introduction to the Physics of Energy 240, Stanford University, Fall 2015.

УДК 004.056

УЯЗВИМОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ТАКСОНОМИЯ СЕТЕВЫХ АТАК

Ахметов Мурат Куанышович, Ню Виктория Владимировна
muratahmetov_1998@mail.ru, nyuvv42@gmail.com
Магистранты 1-го курса специальности
«7М06109 - Администрирование, управления и защита компьютерных сетей на предприятиях»
ЕНУ им Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Сатыбалдина Д.Ж.

Корпоративная ИТ-инфраструктура представляет собой сложную многокомпонентную экосистему, предназначенную для автоматизации бизнес-процессов. Доменная инфраструктура, почтовые сервисы, веб-приложения и бизнес-системы лежат в основе любой корпоративной информационной системы. Хотя размер ИТ-инфраструктуры зависит от масштаба компании и ее численности, большинство компаний имеют общие недостатки информационной безопасности в своих информационных системах. Например, программа-вымогатель WannaCry в 2017 году затронула около 230 000 компьютеров многие, из которых принадлежали правительствам, крупным компаниям и малым предприятиям [1]. Эти инциденты подтвердили, что абсолютно любая компания может пострадать от хакерских атак. В данной статье проводится обзор сетевых уязвимостей корпоративной сети, а также представлена информация о таксономии сетевых атак, которым может быть подвержена корпоративная информационная система.

Прежде всего, определим понятия, которые будут использоваться в работе.

Уязвимость – недостаток защищенности информационной системы, который может быть использован злоумышленником для выполнения несанкционированных действий в системе.

Атака – любое действие злоумышленника, приводящее к нанесению ущерба информационной системе с помощью использования имеющихся уязвимостей [2].

Прямая зависимость между этими двумя понятиям, если отсутствует уязвимость, то и становится невозможна атака, которая может использовать уязвимость.

Первым уровнем возникновения уязвимостей можно считать процесс проектирования информационной системы, примером может быть сервис TELNET, передающий данные о пользователе в открытом виде. Вторым уровнем - возникновение уязвимостей на этапе реализации, к примеру ошибки в настройке стека протоколов TCP/IP, которые могут привести к нарушениям в работе сети. Можно также посчитать и программную реализацию приложений, к примеру, переполняющих буфер. И последним, третьим уровнем, возникновения уязвимости являются последствием ошибок в процессе использования информационной системы, данные уязвимости в основном исходят с пользовательской стороны.

Уязвимости информационной системы условно можно разделить на три группы: объективные, субъективные и случайные.

Объективные уязвимостями считаются те уязвимости, которые основываются на первом уровне, т.е. на особенностях проектирования и реализации информационной системы, на технических характеристиках оборудования и программного обеспечения.

Субъективные уязвимости напрямую зависят от всех пользователей, в том числе и разработчиков, от их действий в сети. Такие уязвимости можно устранить с помощью организационных и программно-аппаратных методов.

Случайные уязвимости зависят от особенностей окружающей среды и каких-либо непредвиденных обстоятельств.

Рассмотрим подверженность компонентов информационной системы каждому из типов уязвимости:

- уязвимости оборудования подвержены всем трем типам уязвимостей;
- уязвимости программного обеспечения также могут подвергаться любой уязвимости.

При этом из-за того, что программное обеспечение делится на системное и прикладное, выделяют различные характеристики уязвимостей для каждой из них. К примеру, в системных возможны уязвимости в микропрограммах, прошивках ПЗУ, ППЗУ, средствах коммуникационного взаимодействия, отсутствие необходимых средств защиты, ошибки в программах, уязвимости в протоколах сетевого взаимодействия. В прикладных: функции и процедуры, не совместимые между собой, фрагменты кода программ, так называемые «дыры», позволяющие обойти систему защиты, отсутствие необходимых средств безопасности, ошибки в программах [3]. Используя каждую из этих уязвимостей, злоумышленник может провести несанкционированную атаку.

Таксономией атак называют классификационную схему, которая структурирует знания о предметной области атак на компьютерные системы и определяет отношения между элементами знаний.

Таксономия атак, основанная на параметрах (dimensions).

Первым оцениваемым параметром является вектор. Вектор атаки, или метод атаки, представляет собой путь, который позволяет получить несанкционированный доступ к информационной системе. Это одно из ключевых понятий, с помощью которых можно описать кибератаку. Среди них можно выделить, например, шелл-шок, переполнение буфера, состояние гонки, подделку межсайтовых запросов, внедрение кода, вирусы и черви.

Шелл-шок (англ. Shellshock) – это ошибка безопасности в оболочке Unix Bash, впервые обнаруженная 24 сентября 2014 года. Эта уязвимость может эксплуатировать различные системы и запускаться либо удаленно, либо с локальной машины. Сервисы, работающие с клиентами, могут использовать Bash для обработки определенных запросов. Это может позволить злоумышленнику получить права суперпользователя или администратора.

Переполнение буфера – это состояние, когда программа пытается записать данные за пределами предварительно выделенных буферов фиксированной длины. Это происходит, когда фрагмент кода не проверяет правильную длину ввода, а значение не соответствует размеру, ожидаемому программой [5]. Эта уязвимость может быть использована злоумышленником, который получил права суперпользователя или администратора. Состояние гонки возникает, когда несколько процессов одновременно обращаются к одним и тем же данным. Это также позволяет злоумышленнику получить локальное повышение привилегий с обходом SMEP.

Подделка межсайтовых запросов, или CSRF, (в англ. также используется термин session riding) – это тип атаки на веб-сайт, когда несанкционированные команды передаются от пользователя, которому веб-сайт доверяет. Для этого используются недостатки протокола HTTP.

Внедрение кода – это «введение» кода злоумышленником в уязвимую программу, что изменяет процесс выполнения. Например, доступ к приложению баз данных можно получить с помощью операторов SQL для структурной модификации и манипулирования контентом [6]. Злоумышленники могут использовать SQL-инъекцию и изменять информацию других клиентов.

Вирус – это самореплицирующаяся программа, которая может распространяться через некоторые типы зараженных файлов и внедряться в другую программу [4].

Червь – это самореплицирующаяся программа, которая может распространяться без использования зараженных файлов. Черви обычно распространяются через сетевые службы на компьютерах или через электронную почту.

Кроме того, есть понятие вектора физической атак, которая может исходить от человека, датчика, оборудования и т.д. Это может быть, как социальная инженерия, так и, например, аппаратная закладка.

Социальная инженерия – это процесс использования социальных взаимодействий для получения информации о жертве или информационной системе. Он часто вовлекает человека в нарушение правил безопасности. Например, сотруднику может быть предложено открыть носитель с вредоносным содержимым.

Аппаратная закладка (троян) – это устройство в схеме, которое может вносить изменения в его работу. Это может способствовать выходу системы из строя или утечке данных. Аппаратные трояны также могут отключать, нарушать или уничтожать весь чип [7] или его сегменты.

Второй параметр – это воздействие атаки – характеризует степень последствий от вторжения. Он также важен для понимания последствий атак. Например, злоумышленник использует вектор переполнение буфера, чтобы получить рут. Это влечет компрометацию привилегий.

Кибервлияние показывает воздействие на цифровые платформы, такие как веб-приложение, программа, операционная система, файлы и т. д. Оно включает компрометацию привилегий, компрометацию пользователей, компрометацию файлов, отказ в обслуживании и установку вредоносных программ.

Компрометация привилегий: с помощью векторов, таких как переполнение буфера, состояние гонки, атакующий может получить привилегии суперпользователя. Компрометация пользователя: злоумышленник получает несанкционированное использование другой учетной записи пользователя или привилегий на хосте, веб-приложении или базе данных, может осуществляться через CSRF.

Компрометация файлов: злоумышленник вносит изменения с помощью переупаковки, внедрения кода.

Отказ в обслуживании (DoS). Злоумышленник может провести атаку типа «отказ в обслуживании», которая делает подключенный компьютер, такой как база данных или вычислительный ресурс, недоступным для предполагаемых клиентов.

Установка вредоносного ПО. Атака может быть запущена с помощью установленного пользователем вредоносного программного обеспечения. Установленное вредоносное ПО может позволить злоумышленнику получить полный контроль над скомпрометированными системами, что может привести к раскрытию конфиденциальной информации или удаленному управлению хостом.

Физическое воздействие

Компрометация оборудования. Атаки социальной инженерии могут привести к неисправности оборудования, например, жесткого диска.

Компрометация поставщика: аппаратный троян (закладка) от поставщика ставит под угрозу целостность источника.

Нарушение конфиденциальности: подслушивание даже на уровне физического провайдера может привести к нарушениям конфиденциальности.

Третий параметр – цель атаки.

Операционная система. Атака может быть специфична для уязвимостей в конкретной операционной системе. Операционная система в системе с устаревшим оборудованием обычно не имеет обновленных мер безопасности, поэтому очень уязвима для атак.

Сеть, сама сеть или ее протоколы, также могут быть целью злоумышленников, например, ping-флуд [4].

Облако: ресурсами облачной службы могут быть программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS).

Также может быть и физическая цель, как датчики, позволяющие контролировать производственную систему, приводы и даже люди.

Четвертый параметр – это последствия атаки.

Кража интеллектуальной собственности при производстве может обходится в миллиарды долларов и потерю рабочих мест. Контрафактные продукты и украденные образцы могут нанести ущерб интересам или репутации клиентов и производителей.

Утечка конфиденциальных данных: утечка частной информации от клиентов в базе данных может влиять на репутацию и вести к разрыву договорных отношений. Финансовое мошенничество. Утечка финансовой информации клиента, такой как данные кредитной карты, во время покупки, адрес для выставления счета, может привести к финансовому мошенничеству.

Отказ в обслуживании (DoS): отказ в обслуживании может быть как воздействием, так и следствием. Примером является DoS сервера (воздействие), вызывающее DoS системы онлайн-биллинга клиента (следствие).

Физические последствия могут включать в себя потерю доступности системы, например, станка с ЧПУ, что может быть критическим, повышение энергопотребления, нарушение работы машины, замедленная работы и непредвиденный выход из строя. Аварии, как взрыв электростанции/прекращение работы могут привести не только к материальному ущербу, но и к человеческим жертвам и даже экологической катастрофе.

Список использованных источников

1. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
2. M. Abomhara G.M. Kien "Cyber Security and the Internet of Things: Vulnerabilities Threats Intruders and Attacks" J. Cyber Secur. Mobil vol. 4 no. 1 2014.
3. Hou Y., Ren X., Hao Y., Mo T., Li W. (2018) A Security Vulnerability Threat Classification Method. In: Barolli L., Xhafa F., Conesa J. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 12. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-69811-3_38
4. Kaynar, K. (2016). A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, 29, 27–56. doi:10.1016/j.jisa.2016.02.001
5. Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q. AVOIDIT: A cyberattack taxonomy. In: 9th Annu Symp Inf Assur, 2014.
6. Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 66, 214–235. doi:10.1016/j.jnca.2016.03.005
7. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity. doi:10.1093/cybsec/tyy006

УДК 681.5

СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ПРИТОЧНО-ВЫТЯЖНОЙ ВЕНТИЛЯЦИЕЙ

Байтханова Айжан Дәулетқызы
baitkhanova.a@mail.ru
магистрант кафедры САУ ЕНУ им.Л.Н.Гумилева
Научный руководитель – С.К.Сагнаева

Введение

Автоматическое управление вентиляционными системами оптимизирует их работу. Особенное значение автоматика для вентиляции имеет при возведении больших зданий. Здесь