УДК 004.42

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ В ПРОМЫШЛЕННОСТИ

Шакирова А.Ф., студентка гр. ПИб-162, IV курс
Научный руководитель: Славолюбова Я.В., к.ф.-м.н., доцент
Кузбасский государственный технический университет
имени Т. Ф. Горбачева
г. Кемерово

1. Кибербезопасность, информационная безопасность

Кибербезопасность, информационная безопасность (далее ИБ) - действия стратегического характера, направленные на защиту информации и коммуникаций при помощи ряда передовых инструментов, политик и процессов.

Кибербезопасность находится в зоне особого внимания как обычных пользователей, так и разных организаций. По общим данным, безопасность данных в последние семь лет входит в число главных задач IT-подразделений компаний. Современные киберугрозы гораздо сложнее и намного серьезнее, чем мы готовы себе представить. Они атакуют крупные и малые предприятия критической инфраструктуры, энергетического сектора, финансовые организации, транспортные и логистические компании, медицинские и фармакологические фирмы, софтверные компании. Фактически никто от них не защищён.

За последние десять лет мир хакеров трансформировался: если раньше хакеры действовали, как правило, поодиночке, стремясь превзойти конкурентов и показать личное превосходство, то сейчас они объединяются, создают группировки по всем правилам корпоративного менеджмента.

1.1. Профессиональная терминология

APT-угроза, APT-атака - сложная, технологически продвинутая атака, направленная на получение конфиденциальных данных в течение длительного периода.

Резервные копии - копии ваших файлов, которые сохраняются на сервере, жестком диске, компьютере или съемном диске на тот случай, если оригиналы окажутся утеряны.

Облачные вычисления, вычисления в облаке - вычислительные сервисы, предоставляемые с удаленных серверов.

Утечка данных - несанкционированный доступ к данным.

Шифрование - трансформация данных с целью их сокрытия.

Управление рисками предприятия - комплексный подход к защите активов компании путем выявления рисков, принятия контрмер и реагирования на угрозы в режиме реального времени.

Межсетевой экран (файрволл, брандмауэр) - аппаратное или программное решение, направленное на блокирование доступа в сеть для нежелательных пользователей.

Хакер - человек, который со злоумышленными намерениями нарушает правила безопасности для получения доступа к данным.

Система предотвращения вторжений (IPS, intrusion prevention system) - программа, которая распознает и блокирует действия хакеров, направленные на получение доступа к вашему компьютеру или данным.

VPN (виртуальная частная сеть, virtual private network) - более безопасный способ получения доступ к Сети путем маршрутизации вашего соединения через специальный сервер, который скрывает ваше местоположение

2. Классификация вредоносного ПО и методы защиты

Кибератаки доказывают: если задаться целью, можно получить доступ к любой организации. Вопрос только в методах и знаниях. Киберугрозы бывают разными, но цель у них одна– нанести вред системе и пользователям.

Классифицировать их необходимо для того, чтобы эффективно выбрать инструмент для их устранения или предотвращения.

Киберугрозы можно условно разделить на две группы - внешние и внутренние.

Среди многочисленных **внешних** угроз можно выделить такие:

1) Вредоносное ПО: внедряется в систему без разрешения и часто без ведома пользователей, может “сливать” конфиденциальную информацию. В большую семью вредоносных ПО “Лаборатория Касперского” включает трояны, вирусы, черви, программы-шпионы, hoax-программы, майнеры, спам и др.;

2) Вымогатели (они же – шифровальщики, англ. ransomware): разновидность вредоносного ПО. Внедряются в систему, шифруют файлы, а потом выдают сообщение пользователю, что вышлют ключ расшифровки за выкуп. Даже если собрать и перечислить требуемую сумму выкупа, ни расшифровать файлы, ни восстановить систему вам не удастся;

3) Руткиты (англ. Root kit): специальное ПО, скрывающее от пользователя присутствие взломщика в системе или наличие вредоносных программ;

4) Фишинг (англ. Phishing): наиболее простой, но очень эффективный метод кибератаки – рассылка электронных писем или сообщений в мессенджеры, имитирующих сообщения из надежных источников. В результате кибермошенники получают доступ к личным данным пользователя. В случае с частным лицом это может привести к финансовым потерям, при такой атаке на пользователя корпоративной сети злоумышленники получают доступ к системе компании;

5) Социальная инженерия (англ. Social engineering): тактика кибермошенников, эксплуатирующая человеческие качества – доверчивость, страх, лень. Эти атаки могут быть замаскированы под просьбы перечислить деньги на лечение или сделать пожертвование в пользу благотворительного фонда,

либо имитируют официальное обращение с требованием предоставить персональные данные для доступа к ресурсам. Очень часто пользователи пренебрегают проверкой фактов, что играет на руку злоумышленникам;

6) DDoS-атака (аббревиатура от англ. Denial of Service, “отказ в обслуживании”): одновременная множественная отправка интернет-запросов к системе (как правило, ботами), что в итоге блокирует доступ к этой системе добросовестным пользователям;

7) Эксплойт (англ. Exploit): программный продукт, эксплуатирующий уязвимости в ПО для осуществления кибератаки. Может действовать как извне (remote exploit), напрямую из интернета, без предварительного доступа к атакуемой системе, так и изнутри (local exploit), запускаясь в атакованной системе с использованием предварительно полученных прав. Цель атаки, как правило, получение полного контроля над системой (права суперпользователя) или нарушение функционирования системы;

8) Ботнет (англ. Botnet): объединенные в единую сеть компьютеры, инфицированные вредоносами. Обычно является инструментом для скрытого осуществления других хакерских действий – DDoS-атак, фишинга и спам-рассылок и т.д. При этом владельцы таких компьютеров чаще всего не знают, что их машины инфицированы и используются в противоправных целях.

Внутренние угрозы кибербезопасности – это разнообразные уязвимости в ПО и архитектуре систем и простой человеческий фактор.

Комплексный подход к реализации ИБ заключается в том, что защиту необходимо осуществлять на трех ключевых уровнях – персонал, процессы и технологии.

Персонал компании: пользователи должны знать и четко соблюдать основные меры информационной безопасности: надежные пароли, внимательное отношение к вложениям в электронных письмах, резервное копирование данных, разумное использование внешних интернет-ресурсов с рабочих устройств и др.

Бизнес-процессы и нормативная регламентация: необходимо разработать базовый набор мероприятий по противодействию атакам предпринимаемым и успешно осуществленным. В нем должно объясняться, как определять атаки, защищать системы, выявлять угрозы и противодействовать им, а также восстанавливать работоспособность рабочих систем после осуществленных атак.

Технологии: ключевое звено в системе ИБ. Основные компоненты, которые должны быть защищены, – так называемые конечные устройства: компьютеры, интеллектуальные устройства и маршрутизаторы, сети и облачная среда. Наиболее распространенные технологии для защиты оборудования – брандмауэры, фильтрация DNS, антивирусное ПО, решения для защиты электронной почты.

Одним из элементов системы киберзащиты информационного периметра организации должен быть аудит ИБ. Аудит бывает внешним (проводит независимый подрядчик, как правило, разово) и внутренним (осуществляется

сотрудниками ИБ компании на постоянной основе). В идеале оба вида аудита должны сочетаться и делаться регулярно. Цели аудита:

- Исследование и оценка уровня защищенности информационных систем компании на текущий момент;
- Определение уязвимости, подверженные риску ресурсы, потенциальные киберугрозы;
- Оценить потенциальные убытки, при совершённой кибератаке и цена восстановления;
- Выделить приоритеты внедрения мероприятий по защите систем и информации;
- Минимизировать риски и оценить рентабельность мер кибербезопасности.

3. Самые известные вирусы нанесшие большой урон

MORRIS WORM - «Великий червь», именно так называют первый сетевой червь хакеры всего мира, в 1998 году парализовал 10% всей инфраструктуры ARPANET. Студент MIT Роберт Моррис создал первую компьютерную программу, которая сканировала сеть, копировала себя на компьютеры и пыталась подобрать пароли к системе по словарю из 400 слов.

Чернобыль или CIH - компьютерный вирус, созданный тайваньским студентом Чэнь Ин Хао в июне 1998 года. Работает только на компьютерах под управлением Windows 95/98/ME. Считается одним из самых опасных и разрушительных вирусов, так как после активации он способен повредить данные микросхем BIOS и уничтожить всю информацию с жёстких дисков.

ILOVEYOU - Первый компьютерный вирус, использующий механизмы социальной инженерии позволил его создателям за пару дней заразить около 3 млн компьютеров по всему миру. Если ваш компьютер был заражен, то скрипт, используя вашу почтовую адресную книгу, пересылал себя всем вашим контактам. Пользователи нажимали на интересное вложение, чтобы прочитать, кто же им там признается в любви и происходило заражение системы.

TDL3 - Группу хакеров обвинили в создании ботнета, с помощью которого создатели руткита и владельцы интернет ресурсов накручивали себе посетителей, манипулировали результатами поисковой выдачи, обманывали счетчики рекламы, топили с помощью «черного SEO» конкурентов.

WANNACRY - 12 мая 2017 года около миллиона компьютеров более чем в 200 странах мира подверглись настоящей спланированной и целенаправленной атаке. Большинство крупных коммерческих организаций и правительственных учреждений не смогли включить свои компьютеры. На экране была надпись, предлагающая заплатить выкуп, иначе информация блокировалась и не подлежала восстановлению.

4. Вывод

В век цифровизации нужно вкладывать силы и финансы в развитие кибербезопасности.

Так как большая часть современных производств завязана на цифровом обмене информацией, управлении.

Список литературы:

1. Базовые понятия и термины кибербезопасности [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-basics (дата обращения:7.03.2020).
2. Кибербезопасность организации: защищаем информационный периметр [Электронный ресурс]. – Режим доступа: https://www.sim-networks.com/blog/corporate-cybersecurity-2019 (дата обращения:7.03.2020).
3. САМЫЕ ОПАСНЫЕ И ИЗВЕСТНЫЕ КОМПЬЮТЕРНЫЕ ВИРУСЫ [Электронный ресурс]. – Режим доступа: https://notagram.ru/samye-opasnye-i-izvestnye-kompyuternye-virusy/ (дата обращения:7.03.2020).