Что такое кибербезопасность?

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

- **Безопасность сетей**– действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.
- **Безопасность приложений**– защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- **Безопасность информации**– обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- **Операционная безопасность**– обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
- **Аварийное восстановление и непрерывность бизнеса** – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.
- **Повышение осведомленности**– обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Виды киберугроз

Кибербезопасность борется с тремя видами угроз.

1. **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
3. **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы – ниже мы приводим самые распространенные.

Вредоносное ПО

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы–** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
- **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
- **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
- **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

SQL-инъекция

Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

Фишинг

Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

Атаки Man-in-the-Middle («человек посередине»)

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не

подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

DoS-атаки (атаки типа «отказ в обслуживании»)

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Новейшие киберугрозы

С какими из новейших киберугроз сталкиваются пользователи и организации? Рассмотрим некоторые из тех, что попали в отчеты правительств Великобритании, США и Австралии.

Троянец Dridex

В декабре 2019 года Министерство юстиции США обвинило лидера группы киберпреступников в участии в атаке с использованием зловреда Dridex. Эта кампания затронула общественные, правительственные и деловые структуры по всему миру.

Dridex – банковский троянец с широким набором возможностей, который появился в 2014 году. Он проникает на компьютеры жертв с помощью фишинговых писем и вредоносных программ. Dridex может красть пароли, данные банковских карт и личную информацию пользователей, которые затем используют мошенники. Размер причиненного им финансового ущерба исчисляется сотнями миллионов.

1. **Обновите программное обеспечение и операционную систему.** Используя новое ПО, вы получаете свежие исправления безопасности.
2. **Используйте антивирусные программы.** Защитные решения, такие как Kaspersky Total Security, помогут выявить и устранить угрозы. Для максимальной безопасности регулярно обновляйте программное обеспечение.
3. **Используйте надежные пароли.** Не применяйте комбинации, которые легко подобрать или угадать.
4. **Не открывайте почтовые вложения от неизвестных отправителей –** они могут быть заражены вредоносным ПО.
5. **Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов –** это один из стандартных путей распространения вредоносного ПО.
6. **Избегайте незащищенных сетей Wi-Fi в общественных местах –** в них вы уязвимы для атак Man-in-the-Middle.

Больше информации по теме:

- Что такое киберпреступность: риски и противодействие
- Как не стать жертвой распространенных киберпреступлений
- Угрозы безопасности для интернета вещей
- Что такое спам и фишинг

Продукты и решения:

- Кибербезопасность домашних устройств
- Защитные решения для малого бизнеса
- Endpoint Security для бизнеса Расширенный
- Службы корпоративной кибербезопасности
- Осведомленность о безопасности: тренинги для сотрудников
- Кибербезопасность промышленного предприятия