Передовые практики и методы обеспечения безопасности

Предлагаемые рекомендации и общие для всех проблемы в связи с обеспечением безопасности актуальны в современном мире, где используется множество подключенных устройств. Осознание угрозы – это лишь первый шаг. Необходим следующий шаг: использование передовых практик и методов для подключенных устройств. Воспользуйтесь этим списком в качестве руководства к действию.

1. Нельзя откладывать

Планирование внедряемых технологий. Выработка методов их защиты.

2. Защита данных

Использование зашифрованных и проверенных соединений, где это возможно.

3. Контроль услуг

Рассмотрите возможности отказа от технологических услуг, которыми вы не планируете пользоваться.

4. Изменение паролей

Использование паролей по умолчанию упрощает хакерам доступ к устройствам. **Активация паролей пользовательского интерфейса.**

5. Дистанционное управление

Используйте надёжно защищённую систему дистанционного управления, при помощи которой вы сможете быстро вносить изменения в настройки. Чем дольше устройства, решения и системы используют устаревшие настройки, тем легче хакерам взломать их защиту.

6. Контроль регистрации действий

Использование журналов учёта деятельности и регистрации, что позволяет обнаруживать ненадлежащую активность в сети.

7. Доступ для тех, для кого это необходимо

Графики и планы обновления защиты должны быть доступны только тем сотрудникам, которым это необходимо. Если слишком много сотрудников имеют доступ к планам обновления защиты, риски нарушения безопасности возрастают.

8. Мониторинг устройств, с которыми отсутствует связь

Необходимо разработать метод постоянного мониторинга системы для учёта устройств, с которыми нет связи. Если возникают подозрения, что устройство было изъято из эксплуатации, удалите регистрацию такого устройства, пока не будет подтверждено его место нахождения.

9. Доступность обновления

Необходимо выбирать для использования такие устройства, которые будут обновляться в течение всего срока эксплуатации, что позволит обеспечивать соответствие новым стандартам. При этом системы обновления должны предотвращать возможности изменения файлов обновления.

10. Изъятие устройств из эксплуатации

Необходимы планы по изъятию устройств из эксплуатации, учитывающие удаление корпоративных настроек, учётных записей и регистрационных данных пользователей, чтобы исключить вход в существующую систему предприятия с изъятого из эксплуатации устройства.

11. Целостность, конфиденциальность и доступность

На всех этапах использования устройства в организации должны обеспечиваться целостность, конфиденциальность и и доступность устройства.

12. Непрекращающееся планирование мер

Обновление средств защиты должно быть постоянным приоритетом. Планирование мер безопасности не должно носить характер разового мероприятия.

Знаете ли вы, что ...

360000 долл. США

Шифрование минимизирует расходы в связи с кибератаками в среднем на **360000 долл. США**, делая этот метод наиболее эффективным в борьбе с хакерами.[1]

81%

На долю украденных или плохо защищённых паролей приходится **81%** случаев нарушения защиты данных хакерами.[2]

1,2 миллиона долл. США

Компании, которые имеют в штате группы специалистов и планы для реагирования в случае нарушения защиты данных, сокращают расходы по причине нарушения безопасности данных более чем на **1,2 млн долл. США.**[3]

38%

38% фирм сообщили о случаях нарушения защиты с участием устройств промышленного класса.[4]

40%

40% опрошенных отмечают, что кибератаки являются фактором, который повышает важность защиты мобильных устройств.

197 дней

Организации в среднем требуется 197 дней, чтобы обнаружить взлом системы безопасности.[5]

[1] Отчёт «Стоимость нарушения безопасности данных» 2019 г., IBM Security • [2] 2017 «Расследование нарушений безопасности данных», Verizon, IBM Security • [3] Отчёт «Стоимость нарушения безопасности данных» 2019 г. • [4] «Отчёт о реагировании на угрозы», Carbon Black, ноябрь 2018 г. • [5] «Стоимость нарушения безопасности данных», Ponemon Institute, 2018/2019 г.