BI.ZONE

Шпаргалка безопасника:

несколько шагов к устойчивой инфраструктуре

Киберпреступники рассчитывают на человеческий фактор. К миллионным потерям может привести простая ошибка: необновленное ПО, случайно предоставленные полномочия, выключенный антивирус.

Со всеми новыми векторами и вредоносами важно не забывать о базовых правилах и процедурах, которые составляют фундамент кибербезопасности. Мы подотовили несколько чек-листов, которые вы можете использовать как шпаргалку. Регулярно сверяйтесь с ней, чтобы оградить свою инфраструктуру от большинства киберугроз.

68%

специалистов по продажам открыли вредоносные письма при проведении учебных атак

BI.ZONE

Чек-лист: АРМ бухгалтера

Путь к деньгам компании можно проложить через бухгалтерию — и злоумышленники пользуются этим. Пройдитесь по чек-листу и проверьте, безопасно ли АРМ вашего бухгалтера.

- [ ] Бухгалтер работает под учетной записью пользователя с ограниченными правами
- [ ] Используются только поддерживаемые версии Windows
  Windows 10
- [ ] Windows обновляется регулярно
  Служба Windows Update включена
- [ ] Прикладное ПО обновляется регулярно и своевременно
  Особое внимание Microsoft Office
- [ ] На АРМ работает антивирусное ПО, учитывающее региональную специфику
  Например, Kaspersky, ESET, Dr.Web
- [ ] Данные ДБО и прочих систем хранятся исключительно в менеджере паролей
  Например, KeePass или 1Password
- [ ] Используются сильные пароли (длина не менее 15 символов, включает буквы и цифры)
  Рекомендуем использовать генератор в менеджере паролей
- [ ] Установлен максимальный уровень User Account Control (UAC)
- [ ] Запуск исполняемых файлов из директорий `«Загрузки»` (`Downloads`), `«Документы»` (`Documents`) и `%TEMP%` заблокирован с помощью локальных политик безопасности
  - `secpol.msc`
  - `Software Restriction Policy`
- [ ] Запуск браузера Internet Explorer заблокирован
  Если его использование все же необходимо, заблокируйте в IE посещение любых сайтов, кроме используемых для систем ДБО
- [ ] Отключены плагины и расширения веб-браузеров
- [ ] Заблокирован запуск макросов в ПО Microsoft Office
  Для этого откройте в меню Office `Центр управления безопасностью` > `Отключить все макросы без уведомления`
- [ ] Регулярно проводится инвентаризация ПО
  Особое внимание к программам для удаленного управления системой: TeamViewer, Ammyy Admin, Lite Manager и Другие
- [ ] Заблокированы удаленные подключения по RDP
  Исключение можно сделать только для доступа по VPN — с сертификатом или токеном
- [ ] Токен для работы с системами ДБО подключается только при проведении платежных операций

BI.ZONE

Чек-лист: противодействие фишингу.

Электронная почта — критическая точка входа в инфраструктуру компании. Одно несторожно открытое письмо способно привести к компрометации ваших систем. Чек-лист поможет контролировать безопасность почтового клиента и офисных приложений.

- [ ] Microsoft Office регулярно и своевременно обновляется
  Включена служба Windows Update
- [ ] Макросы VBA в программах Microsoft Office заблокированы групповыми политиками
  Либо разрешены только в документах из надежных расположений (Trusted Locations)
- [ ] Разрешены только макросы, подписанные цифровыми сертификатами надежных издателей
- [ ] Исполнение ActiveX в документах Microsoft Office заблокировано политиками безопасности
- [ ] Включена проверка на соответствие расширения формату файла в Microsoft Excel (Force file extension to match file type)
- [ ] Включена проверка корректности формата файла Microsoft Office (Office File Validation)
- [ ] Включен защищенный просмотр (Protected View) для документов, полученных через Microsoft Outlook и скачанных из интернета
- [ ] Функция доверенных документов (Trusted Documents) отключена
- [ ] Запуск исполняемых файлов из директорий «Загрузки» (Downloads), «Мои документы» (Documents) и %TEMP% запрещен с помощью политик безопасности

BI.ZONE

Чек-лист: настройка политик аудита Windows

Настройки по умолчанию лишают компанию важной информации об инциденте, которая помогла бы при расследовании. Часто ненастроенный журнал событий хранит данные лишь за один-два дня — при таком подходе очень сложно восстановить хронологию кибератаки.

Этот чек-лист разбит на две части: первая посвящена общим принципам настройки аудита Windows, вторая — рекомендуемым событиям для учета. С его помощью вы упростите жизнь себе и форензикам в случае инцидента.

Общие принципы

- [ ] Расширенное логирование событий безопасности

  Советуем привести его к Windows Security Baselines или вариантам из раздела «Рекомендуемые события для учета»

- [ ] Увеличенный объем журналов безопасности

  Не меньше 1024 Мб

- [ ] Централизованное хранение журналов безопасности

  Лучше собирать их из различных систем на выделенном сервере при помощи Windows Event Forwarding

- [ ] Передача событий журналов безопасности в средства SIEM

Чек-лист: рекомендуемые события для учета

Чтобы журнал событий безопасности Windows был достаточно подробным, мы рекомендуем включить в учет следующие пункты:

Вход учетной записи

- [ ] Аудит проверки учетных данных
  Успех/отказ

Управление учетными записями

- [ ] Аудит управления учетными записями компьютеров
  Успех/отказ
- [ ] Аудит других событий управления учетными записями
  Успех/отказ
- [ ] Аудит управления группами безопасности
  Успех/отказ
- [ ] Управление учетными записями пользователей
  Успех/отказ

Доступ к службе каталогов (на контроллерах домена)

- [ ] Аудит доступа к службе каталогов
  Успех/отказ
- [ ] Аудит изменения службы каталогов
  Успех/отказ

Вход/выход

- [ ] Аудит блокировки учетных записей
  Успех
- [ ] Аудит выхода из системы
  Успех
- [ ] Аудит входа в систему
  Успех/отказ
- [ ] Аудит специального входа
  Успех/отказ

Изменение политики

- [ ] Аудит изменения политики аудита
  Успех/отказ
- [ ] Аудит изменения политики авторизации
  Успех/отказ

Подробное отслеживание

- [ ] Аудит создания процессов
  Успех

Система

- [ ] Аудит других системных событий
  Успех/отказ
- [ ] Аудит изменения состояния безопасности
  Успех/отказ
- [ ] Аудит целостности системы
  Успех/отказ

BI.ZONE

Чек-лист: обеспечение безопасности устройств под управлением ОС Android

Считается, что устройства на Android проще взломать за счет открытости этой операционной системы. Однако при грамотном подходе к ее настройке можно существенно повысить уровень защищенности от киберугроз. Наш чек-лист поможет в этом.

- [ ] Установка приложения из недоверенных источников запрещена
- [ ] Режим разработчика отключен
- [ ] Отключение Google Play Protect запрещено
- [ ] Получение прав суперпользователя (root) запрещено
- [ ] Модификация загрузчика мобильного устройства запрещена
- [ ] Установка недоверенных сертификатов запрещена
- [ ] Приложениям не предоставляются права администратора устройства без необходимости
- [ ] Приложениям не предоставляются права на запуск AccessibilityService без необходимости
- [ ] Приложениям не предоставляются права на смену приложения по умолчанию для работы с СМС
- [ ] Для разблокировки устройства используются сложные пароли и графические ключи
  Пароль состоит минимум из 15 символов, включает буквы и цифры
- [ ] Для учетной записи Google установлена двухфакторная аутентификация
- [ ] На устройстве используется шифрование данных