Рекомендации по повышению защищенности ИТ-инфраструктуры

Базовые рекомендации ИБ

1. В кратчайшие сроки завершить все переходные процессы в ИТ-инфраструктуре. Минимизировать обновления, глобальные настройки.

2. Постараться достигнуть состояния максимальной стабильности инфраструктуры, необходимого уровня отказоустойчивости.

3. Перенести данные и сервисы из иностранных облачных систем на локальные вычислительные ресурсы.

4. Сформировать ЗИП или заключить сервисный контракт для минимизации рисков простоя сервисов в случае выхода из строя оборудования, выбрав партнера с большим складом оборудования и запчастей.

5. При отсутствии технической поддержки со стороны производителя услугу может оказать сервисный партнер. Без производителя очевидны некоторые ограничения, тем не менее такой подход позволит минимизировать риски до

приемлемого уровня, как минимум, на период миграции на другого производителя.

6. Провести аудиты правил безопасности. Максимально ограничить доступ в/из сети Интернет. Закрыть доступ всем западным решениям из вашей сети к серверам обновлений и лицензирования там, где это приемлемо, а также рассмотреть временное отключение обновлений софта до стабилизации ситуации. Рассмотреть вариант дополнительной установки отечественных МСЭ на границе с интернетом (эшелонированная защита).

7. Провести аудит настроек ИБ: проверить, на всех ли компонентах (как средствах защиты информации, так и системного и прикладного ПО) включены доступные меры защиты (управление доступом, логирование, аутентификация, антивирусная защита и т.д.) и их настройки в соответствии с потребностями бизнес-процессов и рекомендациями производителей, а также стандартами безопасности (hardening guide).

8. Провести сканирование инфраструктуры на наличие открытых нелегитимных и уязвимых сервисов. Для объективного представления уровня защищенности важно дополнительно провести сканирование и из сети Интернет.

9. Сменить пароли на оборудовании. Использовать только сложные пароли, не менее 12 знаков (с цифрами, буквами, верхним/нижним регистром).

10. С особым вниманием отнестись к защите удаленных пользователей, особенно администраторов: использовать двухфакторную аутентификацию, усилить защиту протоколов удаленного доступа включая RDP, но не ограничиваясь.

11. Провести резервирование данных и конфигураций для обеспечения возможности оперативного восстановления. Резервные копии безопаснее хранить в изолированной среде, недоступной из сети Интернет, и/или на съемных носителях.

12. По возможности ограничить использование внешних ресурсов, API, загружаемых виджетов, сервисов, которые разработаны и хостятся иностранными организациями (например, Google Analytics).

13. Внедрить сегментацию и микросегментацию для гранулярного контроля трафика, прежде всего ограничить доступ (в том числе для внутренних пользователей) к инфраструктурным сервисам (AD, SCCM, DNS и т.д.).

14. Защитить ключевые сервисы соответствующими решениями. Например, в части защиты web-приложений и серверов можно обеспечить фильтрацию трафика с помощью Web Application Firewall (WAF).

15. Сохранить на локальные ресурсы используемые программные модули, библиотеки и иные ресурсы, расположенные в иностранных репозиториях (GitHub).

Дополнительные рекомендации

1. Подготовиться к возможным DDOS-атакам, так как из-за ухода крупнейших поставщиков релевантных решений некоторые организации остались без защиты. Ограничить количество подключений (rate-limit) и попыток открытия новых сессий с одного ip-адреса и полуоткрытых (embryonic), внедрить географические ограничения.

2. Внедрить мониторинг инцидентов ИБ в вашей инфраструктуре, как минимум, в части самых критичных сервисов и приложений.

3. Усилить защиту электронной почты.

4. Проработать и протестировать планы на случай внештатных ситуаций (DRP), включая утерю данных и отключение ключевого оборудования.

5. Провести актуализацию моделей угроз/оценки рисков ИБ с целью переоценки вероятности угроз ИБ, связанных с рисками цепочек поставок, страновыми рисками и нарушением доступности и работоспособности. Пересмотреть и актуализировать меры, направленные на управление данными рисками.

6. Заблокировать трафик из других стран, если это уместно. Например, если ваши покупатели и целевая аудитория находятся исключительно в РФ.

7. Заблокировать трафик из сети TOR.

8. Внедрить практику контроля действий администраторов (особенно важно) и пользователей. Рассмотреть возможность внедрения систем класса PAM.

9. Ограничить средствами прокси-сервера или контентной фильтрации доступ пользователей к информационным ресурсам сети Интернет (ввести белый список ресурсов и сервисов).

10. Провести инструктажи с пользователями по тематике ИБ для повышения осведомленности об актуальных атаках и приемах нарушителей.

Рекомендации по продуктам Microsoft

1. Почтовая система на базе Microsoft Exchange

- Настроить контентную фильтрацию для блокировки сообщений, содержащих потенциально опасные вложения с расширениями CMD, BAT, EXE, PS1, VBS, SCR, HTA.
- Активировать механизмы проверки подлинности домена-отправителя (DKIM, DMARC, SPF).
- Проверить актуальность баз антивирусных сигнатур Microsoft Exchange и обновить их при необходимости.
- Убедиться в отсутствии доступа к Exchange Admin Center (/ecp) из внешней и внутренней сети. Организовать возможность доступа администраторов системы только с IP-адресов внутренней сети.
- Произвести уведомление пользователей о правилах информационной безопасности при работе с внешними почтовыми сообщениями.
- Рассмотреть возможность внедрения механизма Data Loss Prevention, встроенного в Microsoft Exchange.

2. Сервер автоматических обновлений Windows Server Update Services (WSUS)

- В случае использования сервера обновлений WSUS выполнить блокировку загрузки любых обновлений ОС Windows и сопутствующих продуктов, выпущенных после 23.02.2022.
-

3. Active Directory Domain Services

- Разработать и применить групповую политику по отключению службы «Центр обновления Windows» для всех серверов, клиентских ПК и ноутбуков, использующих ОС Windows.
- Убедиться и реализовать возможность использования доверенных российских вышестоящих DNS-серверов.

4. Провести аудит лицензий Microsoft на предмет использования облачных версий. Разработать и внедрить политику отказа от использования облачных версий продуктов Microsoft. Осуществить переход на полностью локальные инсталляции версий продуктов Microsoft.

5. Проверить корректность выполнения заданий резервного копирования всех основных информационно-управляющих систем и сервисов и убедиться в их актуальности.