Практические рекомендации по усилению безопасности ИТ-инфраструктуры

Проведите аудит всей системы и определите основные критичные точки, без защиты которых компания не сможет существовать, а затем — сконцентрируйтесь на них в первую очередь.

01 Проведите ревизию учетных записей (УЗ) вашей сети. Заблокируйте все неиспользуемые УЗ. Для всех используемых административных УЗ поменяйте пароли или убедитесь, что установлен надежный пароль.

- Важно обеспечить сложность пароля. Главные требования к паролям всем известны: длина не менее 8 символов, с обязательным использованием букв разного регистра, цифр и специальных символов.
- Архиважно: пароль должен быть уникальным. Ни в коем случае он не должен был использоваться где-либо ранее: на сторонних сайтах или сервисах. Пользователи склонны использовать устоявшиеся пароли, но при этом не отслеживают своевременно все возможные утечки баз данных с паролями. Больше того, об этих утечках не всегда известно. А они происходят регулярно. Любой вполне надежный пароль, установленный пользователем на стороннем сервисе несколько месяцев назад, вполне может оказаться в одной из свежих украденных баз данных, что позволит злоумышленникам получить удаленный доступ. Вывод прост: лучше забыть и восстановить пароль, нежели подвергнуть компрометации всю сеть предприятия.
- Также может быть полезно использовать сервисы вроде Have I Been Pwned, если это не противоречит политике безопасности компании. Применение таких сервисов позволит выявлять случаи утечек паролей пользователей.

02

Проверьте степень защищенности доступа по протоколу RDP (Remote Desktop Protocol, протокола удалённого рабочего стола) или другого программного обеспечения для удаленного доступа (если оно используется).

На сегодня, при наличии установленного и работающего в системе антивируса, случаи шифрования файлов практически не встречаются. Самая распространенная схема — компрометация удаленного доступа, получение повышенных привилегий в системе, удаление антивируса или его отключение, за которыми следует запуск вспомогательных утилит и шифровальщика. То есть, речь идет о комплексных атаках с использованием различных техник.

Если в вашей организации используется RDP, то он должно быть надежно защищен. Все учетные записи, которые используются для подключения, должны быть под контролем. В обязательном порядке они должны иметь длинный, уникальный и сложный пароль, который невозможно подобрать ни простым перебором, ни перебором по словарям. Все неактуальные учетные записи должны быть отключены.

Если это возможно, дополнительно RDP (а равно VNC и прочие способы удаленного подключения) канал стоит скрыть за VPN. Если это невозможно, то на внешнем оборудовании - роутере или шлюзе - необходимо настроить ограничение на удаленное подключение, оставив возможность подключаться удаленно только с определенных IP или подсетей. Также стоит рассмотреть лучшие практики по защите средств удаленного доступа от несанкционированного подключения. Включение и просмотр аудита удаленных подключений, ограничение числа подключений при неудачном вводе пароля более определенного числа раз и замена стандартного порта заметно осложнят злоумышленникам процесс и заметно снизят вероятность успешного входа.

Нужно осознавать: при компрометации удаленного доступа система практически обречена. И ни один антивирус уже не сможет полноценно защитить систему и сеть предприятия от последствий. При инцидентах такого рода злоумышленники чаще всего удаляют антивирус или выводят его из строя. Но иногда хакеры могут не использовать никаких вредоносных утилит, чтобы похитить и затем зашифровать данные. В этом случае им не придется удалять антивирус, так как невозможно будет отличить злонамеренные действия от действий легитимного администратора. Нередки случаи, когда при подобных инцидентах файлы либо упаковываются в обычные архивы с длинным неизвестным паролем, либо скачиваются на внешние серверы, а оригиналы из системы полностью удаляются. Также для шифрования могут использоваться системные средства, такие, как Windows Bitlocker.

В последнем случае никаких вредоносных действий относительно системы и антивируса не выполняется в принципе, только стандартные пользовательские или административные операции. Еще один вывод : к обеспечению информационной безопасности компании необходимо подходить комплексно.

03 Проверьте настройку удаленного доступа к серверам Linux и выполните основные рекомендации по настройкам SSHD:

- Запретите использование входа по паролю - применяйте только SSH ключи, сами ключи при этом защищайте паролем (В принципе, ключ можно сохранить без пароля и подключаться по нему далее без пароля. Но мы не рекомендуем этот способ). Сами ключи лучше хранить на внешнем носителе информации и подключать к компьютеру по необходимости.
- Запретите возможность непосредственного входа по SSH под учетной записью root. При необходимости повышения привилегий в пользовательской сесии используйте sudo.
- Ограничьте перечень пользователей, имеющих право подключения по SSH.
- На уровне системного межсетевого экрана установите - по умолчанию - для всех подключений политику на отклонение входящих подключений. Избранные порты должны быть открыты для подключений только в случае необходимости. Разрешить для подключений из общей сети только публичные сервисы (например, http/https, smtp). Чувствительные сервисы (например, SSH) нужно ограничивать подключениями через VPN.
- Для любых сервисов типа СУБД (mysql, postresql, redis, mongodb и т.п.) исключите возможность подключения с внешних адресов. Эти подключения должны осуществляться строго с доверенных адресов (локальная сеть или VPN).
- Избегайте настроек сервисов, открывающих входящие подключения на интерфейсе 0.0.0.0. Это допустимо только для публичных сервисов, для всех иных должен использоваться не публичный интерфейс (локальная сеть или VPN).
- Включите аудит действий пользователей (auditd) и настроите уведомление об активности root или sudo - например, через отправку на электронную почту.
- Рассмотрите возможность использования дополнительных методов аутентификации по SSH, таких, как Google Authenticator или аналоги. Любой 2FA метод многократно снизит риск несанкционированного подключения.

- Ограничьте возможность выполнения скриптов в /tmp и других временных каталогов через параметры монтирования noexec, nosuid, nodev – однако следует помнить, что такие ограничения могут оказать влияние на легитимные процессы (например, установщики прикладного ПО), поэтому нужно быть внимательным при применении данной рекомендации.
- Разнесите системные каталоги по разным разделам (/var, /home, /tmp) для ограничения последствий при их переполнении.
- Удалите все неиспользуемые сервисы, установленные из шаблона ОС (telnet, ftp, rsh, nfs и т.д.). Ненужные службы, которые не удалены, отключите (systemctl disable или иным аналогичным способом).
- Ограничьте использование sudo только разрешенными пользователями (настройкой sudoers).

04 Проверьте саму систему и критичное ПО на известные уязвимости. По возможности используйте наиболее актуальные сборки операционной системы (ОС) и прикладного ПО. Установите все последние обновления к ним.

Эксплойты операционной системы и широко распространенного софта могут являться лазейкой для получения доступа к системе в обход любых методов защиты. Чем старее парк используемых ОС, тем выше риск компрометации. Для современных ОС, в первую очередь, всегда должно быть включено автоматическое обновление. Но главное : это обновление должно на деле проводиться. Это касается любого критичного софта, как, например, различных СУБД, почтовых серверов и клиентов, ПО для проектирования, моделирования, или любого другого. Обновления должны быть плановыми и систематическими, чтобы выход очередной 0-day уязвимости не застал пользователей врасплох и не стал причиной компрометации всей сети в обход любого антивирусного ПО.

05 Защитите антивирус от удаления и обновите его до актуальной версии. Антивирусное ПО должно быть установлено на всех машинах сети.

Сегодня практически не встречаются случаи, когда при установлении антивируса вместе с ним в систему был успешно занесен и запущен троянец шифровальщик.

Первое, что делают злоумышленники при удаленном проникновении в систему — пытаются отключить, удалить или иначе вывести из строя любое антивирусное ПО.

Везде, где это возможно, необходимо установить запрет на удаление антивируса локально (если используется наша версия антивируса с централизованным управлением), запрет на отключение самозащиты (также если используется наша версия антивируса с централизованным управлением) и пароль для доступа к его настройкам. В случае компрометации удаленного подключения такие ограничения повышают шансы успешно защититься и осложняют задачу злоумышленникам, давая администраторам время среагировать на атаку.

Любая рабочая станция без антивируса или с антивирусом, в котором не обновляются компоненты и базы, создает опасность для всей остальной сети. Особенно, если эта машина доступна из внешней сети.

При использовании централизованных версий антивируса Dr.Web под Windows так же рекомендуется рассмотреть возможность использования Контроля приложений, входящего в состав центра управления Dr.Web и антивирусных агентов, начиная с 12 версии. При корректной настройке, в системе в принципе невозможен будет запуск любых действий не авторизованных администратором.

06 Регламентируйте проведение процедуры регулярного резервного копирования (бэкапа). Это — наиважнейший принцип защиты.

Правильно организованная система резервного копирования является основным средством защиты как от шифровальщиков, так и от других проблем, связанных с повреждением данных и выходом оборудования из строя. Серьезная ошибка, которую допускают многие администраторы в реальных инцидентах - хранение резервных копий в той же сети или системе, в которой эти копии создаются. Недостаточно просто сделать резервную копию одной системы на некоем соседнем сервере, без дополнительных манипуляций. При киберинциденте, и, в частности, при шифровании данных, с высокой степенью вероятностью эти резервные копии окажутся зашифрованными наряду со всеми остальными данными в системе. Именно такое течение инцидентов мы и видим на практике в обращениях пользователей, которые до нас доходят. При шифровании данных, бэкапы в сети - одна из первых целей злоумышленников.

Резервное копирование ценной информации должно выполняться на носители, которые недоступны для записи из основных систем, где хранятся оригиналы. Ни с одной рабочей станции в сети не должно быть одновременного доступа к записи и чтению всех существующих бэкапов. В любой момент времени должно существовать хотя бы две, а лучше три резервные копии корпоративных данных, без которых предприятие не сможет функционировать. Как минимум одна из этих копий должна быть полностью изолирована от остальной сети. В план резервного копирования обязательно нужно добавлять периодическую проверку восстановления из резервной копии. То есть, резервная копия не только должна просто существовать, но должна быть целостной, а администраторы должны иметь возможность и практический навык по быстрому восстановлению работоспособности сети из данного бэкапа. При применении такого протокола, во-первых, в критической ситуации персонал будет иметь натренированный опыт данной операции, что заметно сократит период восстановления, а, во-вторых, позволит избежать ситуации, когда ввиду некорректной настройки параметров данные из резервной копии невозможно восстановить.

07 Разработайте план аварийного восстановления, и периодически устраивайте учения.

Персонал должен иметь инструкции на случай возникновения недопустимых последствий, а руководитель должен быть уверен в том, что этот план жизнеспособен.

Из практики нам известно, что организация полноценной автоматизированной системы резервного копирования может быть сопряжена с рядом трудностей. Однако, нельзя полностью игнорировать эту процедуру, так как добиться результата можно и с использованием минимальных средств. Даже банальное ручное копирование бухгалтерской 1С базы и ряда важных документов на usb-накопитель, пусть даже раз в неделю, многократно снизит возможные финансовые, правовые и репутационные последствия от потери всей совокупности данных.

www.drweb.ru
pr@drweb.com