Безопасность в опасности

10 признаков того, что ваша КСБ может быть "дырой" в безопасности ИТ-инфраструктуры предприятия

В сфере физической безопасности не принято уделять внимание безопасности цифровой – кибербезопасности. Этот подход ошибочен, ибо современные киберугрозы могут нести больше репутационных, юридических и экономических рисков, чем, например, несанкционированный физический доступ на объект

Глеб Рыбаков
Заместитель генерального директора по информационным технологиям и инновациям ООО "Итриум СПб"

В мае 2024 г. "Лаборатория Касперского" представила отчет "Ландшафт угроз для России и СНГ" за 2023 г. и I квартал 2024 г. Один из его основных выводов гласит: "В последние полтора года угроза хактивизма продолжила набирать обороты. Атакующие обращают внимание на организации со слабой защитой, без привязки к конкретной индустрии, используя любые доступные инструменты в открытой сети".

К аналогичным выводам пришли специалисты "Ростелеком-Солар". По их сведениям, за 2023 г. число событий ИБ в сравнении с 2022 г. выросло на 64%, а с начала 2024-го количество высококритичных атак уже увеличилось более чем в три раза.

При этом в сфере физической безопасности, кажется, по инерции принято не замечать рисков киберугроз. Системы продолжают функционировать годами без обновлений, под управлением старых, неподдерживаемых версий операционных систем, будучи подключенными в общую локальную сеть предприятия, с одной учетной записью admin/12345 на всех АРМ. Выглядит как мина замедленного действия: очень опасно! Почему так?

Почему стоит задуматься?

Современная комплексная система физической безопасности (КСБ) – это сложная информационная система, которая, с одной стороны, обрабатывает большой объем чувствительной информации – сведения о сотрудниках и посетителях, графике их работы, сведения об их местоположении, сведения об охране, состоянии оборудования, а с другой стороны интегрирована с большим числом других ИТ-ресурсов предприятия – кадровой, бухгалтерской, ERP-системами, системами документооборота и др.

Почему КСБ уязвимы?

Программное обеспечение систем физической безопасности ничем принципиально не отличается от других компьютерных программ, использует те же общеупотребимые библиотеки и компоненты, работает под управлением типовых операционных систем, таких как Windows и Linux. Поэтому большая часть средств и способов проникновения, используемых злоумышленниками, применимы и к системе физической безопасности.

Современные КСБ зачастую построены на решениях и продуктах десяти-, а то и двадцатилетней давности, которые были исходно спроектированы для работы в закрытых сетях, без учета современных требований к кибербезопасности, без оглядки на актуальные киберугрозы. В таких решениях не заложены принципы цифровой гигиены: данные передаются по открытым каналам, нет политик управления паролями, работа программного обеспечения в операционной системе осуществляется с полными административными правами.

В результате, с одной стороны, для взлома комплексной системы безопасности злоумышленнику не нужно менять свои сценарии, можно эксплуатировать уже хорошо известные и распространенные уязвимости в программах, библиотеках и ОС. С другой стороны, степень защищенности таких систем очень низкая в силу исторических причин, что делает их предпочтительной целью для кибератаки.

Чтобы понять, несет ли ваша КСБ какие-либо риски в плане кибербезопасности и что можно предпринять в этой связи, для начала нужно иметь представление о том, какие бывают киберугрозы и на что они нацелены.

Обзор актуальных киберугроз

По данным "Ростелеком Солар", в 2024 г. **атаки на "слабые" пароли** остаются самыми популярными (см. рис.). В результате подбора по базам известных, популярных и простых паролей злоумышленник получает доступ к системе от имени и с правами соответствующего пользователя.

Следом идут "кривые руки администраторов" – **уязвимости в контроле доступа и ошибки в конфигурации** программных и технических средств, в результате которых злоумышленник получает доступ к системе, несмотря на наличие средств защиты.

Вообще, **человеческий фактор** исторически является ключевой угрозой. Цифровой взлом – это обычно дорогостоящее деяние, требующее высокой квалификации злоумышленника. В отсутствие должных инструментов ограничения и контроля сотрудник, который уже имеет доступ к системе, может осуществить, например, "слив" (хищение) персональных данных, что обойдется злоумышленнику существенно дешевле взлома, но репутационных и иных издержек для предприятия создаст значительно больше.

Следующим способом взлома является использование **эксплойтов** – известных уязвимостей в коде программ, протоколов и операционных систем, в результате чего злоумышленник получает доступ к системе, а впоследствии и ко всей сети. Эксплуатация уязвимости может произойти при загрузке зараженного веб-сайта в устаревшей версии браузера, открытия в текстовом редакторе непроверенного вложения к электронному письму, использования уязвимой версии протокола для удаленного доступа к ресурсам предприятия.

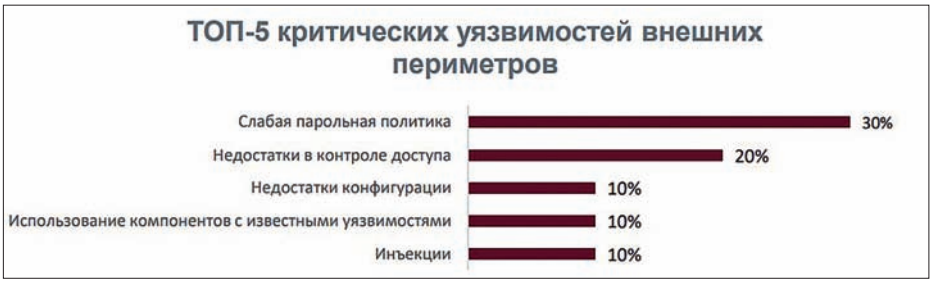
После проникновения в сети предприятия может распространиться **вирус** – компьютерная программа, автоматически или по команде оказывающая негативное воздействие на ИТ-ресурсы. В последнее время наиболее активны **вирусы-шифровальщики** – программы, которые шифруют обнаруженные на компьютере данные, при их помощи шантажируют пользователя, требуя плату за расшифровку. Некоторые вирусы, такие как RuRansom, уничтожают данные безвозвратно в целях нанесения максимального урона. Есть также **майнеры** (используют ресурсы ПК для майнинга криптовалюты), **шпионское ПО** (подслушивает вводимые и передаваемые пользователем данные), **ботнеты** (выполняют массовые действия, такие как DDOS-атаки, по команде злоумышленника) и многие другие.

Вирусы обычно действуют неизбирательно, автоматически поражая системы по воле случая: заранее неизвестно, будет ли запущен на

Нарушение функционирования системы физической безопасности вследствие взлома – это огромные риски для предприятия в целом, его конфиденциальных данных и материальных ценностей, жизни и здоровья сотрудников и посетителей. Кроме того, КСБ может легко стать точкой входа злоумышленника во всю ИТ-систему предприятия, и последствия такого взлома могут быть уже катастрофичными

каком-то компьютере зараженный файл или использована старая уязвимая версия ПО. Если же злоумышленник проникает в сеть конкретного предприятия целенаправленно, он может осуществить **хищение** документов и данных, в том числе персональных, уничтожить или подделать данные. А в случае КСБ широкие возможности **управления** исполнительными устройствами (блокировка дверей, включение автоматики) могут создать прямую угрозу жизни человека и материальным ценностям.

Разберем ключевые факторы возникновения киберугроз для систем комплексной физической безопасности.



Статистика по уязвимостям, по данным "Ростелеком Солар"

В 2024 г. атаки на "слабые" пароли остаются самыми популярными

10 признаков киберугрозы

Отсутствие гибких политик управления паролями

Вычислительная мощность современных компьютеров позволяет подбирать пароли с огромной скоростью. Такие пароли, как qwerty или password1, подбираются за доли секунды. Поэтому, например, современные интернет-сервисы при создании паролей требуют минимум восемь или более символов, обязательно с буквами в разном регистре, цифрами и спецсимволами. Часто обязательной является многофакторная аутентификация.

В это же время ПО систем физической безопасности нередко разрешает использование коротких, простых или даже однобуквенных паролей. И такие пароли используются годами. Зачастую один и тот же простой пароль используется на всех устройствах системы одновременно.

Отсутствие встроенных в ПО политик управления паролями (ограничения их минимальной сложности, требования периодической ротации паролей, отзыва паролей по команде администратора, контроля количества попыток ввода пароля и т.д.) делает атаки через подбор паролей быстрыми и очень эффективными.

Полные права в руках одного пользователя

У отдельно взятого оператора любой критичной информационной системы не должно быть полных прав на управление такой системой и доступа ко всем данным одновременно.

Системный администратор должен иметь доступ к административным функциям – настройкам, управлению системными параметрами, журналам аудита, но не должен иметь доступа к персональным данным или функциям управления охранной сигнализацией. Оператор бюро пропусков не должен иметь возможность выгрузить полный список сотрудников и посетителей со всеми их данными разом или скачать резервную копию базы данных. Система должна предоставлять пользователю только те возможности, которые нужны ему для выполнения непосредственных обязанностей: поиск сотрудника по ФИО, заведение нового пропуска или просмотр журнала системных событий.

В противном случае при взломе или в силу человеческого фактора возможно от лица одного пользователя, например, "слить" все персональные данные из системы или создать нового "администратора" для последующего доступа злоумышленника.

Работа программного обеспечения под учетной записью администратора

Обратите внимание, работает ли ПО системы безопасности в изолированном окружении или с полными правами доступа к операционной системе. Если программа работает под учетной записью администратора, то в случае ее взлома (например, при эксплуатации уязвимости типа Remote Code Execution) злоумышленник получит полный контроль над операционной системой.

По оценке автора, программные средства физической безопасности на рынке часто требуют административных привилегий в ОС для работы, либо для взаимодействия с физическим оборудованием по последовательным интерфейсам, либо потому, что исторически несовместимы с современными политиками безопасности в ОС.

Отсутствие аудита всех действий в системе

Любое действие в системе должно быть зарегистрировано, журнал действий должен быть защищен от подделки, и об этом должно быть известно всем пользователям. Должен быть организован автоматический мониторинг такого журнала и оповещение ответственных лиц о выполнении критичных для системы действий, таких, например, как заведение нового администратора.

Понимание того, что любое действие пользователя гарантированно фиксируется и ассоциируется именно с ним, обычно останавливает сотрудника от нарушения закона и внутренних регламентов предприятия, поскольку ведет к неотвратимому наказанию. А возможность анонимно выполнить деяние, о котором никто никогда не узнает, напротив, способствует случайному или осознанному нарушению правил.

Работа под устаревшими версиями ОС

По оценке автора, большая часть программных средств физической безопасности работает под управлением ОС Windows. В любом программном обеспечении есть ошибки и уязвимости, ОС Windows не исключение. Но, будучи установленным три, пять, а то и 10 лет назад, ПО систем безопасности работает зачастую под управлением устаревших и не поддерживаемых производителем версий ОС. Кроме того, в свете текущей геополитической ситуации в Российскую Федерацию официально актуальные версии ОС и обновления не поставляются. Таким образом, количество уязвимостей в решении становится больше от года к году, и это только вопрос времени, когда очередной вирус ими воспользуется.

Отсутствие регулярных обновлений

По данным "Лаборатории Касперского", самой распространенной в 2023 г. и I квартале 2024 г. стала критическая уязвимость CVE-2021-44228 (Log4Shell) в библиотеке Apache Log4j, которая позволяет удаленно выполнять код. При этом данная уязвимость была обнаружена еще три года назад. Получается, она до сих пор не устранена в огромном количестве программных продуктов.

Не только операционная система требует регулярного обновления и установки патчей безопасности. Программное обеспечение, работающее под управлением ОС, также должно получать обновления на регулярной основе, а производитель должен на регулярной основе выпускать такие обновления, закрывающие выявляемые уязвимости.

Отсутствие налаженного процесса выпуска, распространения и установки обновлений ведет к высокой вероятности эксплуатации не исправленных вовремя уязвимостей.

Некоторые киберугрозы менее существенны для систем физической безопасности. Иные, наоборот, более вероятны: например, в КСБ часто используются сильно устаревшее программное обеспечение и старые операционные системы, с большим количеством известных уязвимостей.

Отключение межсетевого экрана (брандмауэра)

Обратите внимание на то, как настроен межсетевой экран на вычислительной машине с установленным ПО системы физической безопасности. Инструкции по установке многих решений требуют добавить соответствующие программы в исключения брандмауэра (вместо детализированной настройки разрешений для сетевых портов) или выделить большие диапазоны (тысячи портов) для произвольных сетевых подключений в/из этих программ.

Межсетевой экран – основной рубеж защиты компьютера от входящих несанкционированных подключений и исходящих подключений к другим ресурсам сети со стороны потенци-

альных вирусов. Отсутствие грамотно настроенных ограничений для ПО систем безопасности, с одной стороны, открывает возможность несанкционированного подключения к этому ПО для его взлома или эксплуатации уязвимостей в его коде, а с другой стороны делает ИТ-сеть предприятия уязвимой в случае взлома такого ПО.

Использование лишних средств на АРМ операторов системы безопасности

Установка на АРМ средств, которые не требуются для выполнения функций по назначению (игр, мессенджеров, развлекательных сервисов, сторонних программ), повышает риск взлома за счет возможного наличия уязвимостей в таких средствах. Даже если имеется установленный порядок обновления ПО рабочих мест, такие средства вряд ли будут обновлены. На уровне регламентов предприятия должны быть запрещены инсталляция и эксплуатация лишних средств на АРМ, а средствами ОС и настройкой прав пользователей должна быть технически ограничена возможность их установки.

Отсутствие регулярного обслуживания рабочих мест и серверов квалифицированными специалистами

Как упоминалось ранее, существенная доля уязвимостей систем связана с некорректной конфигурацией развернутых средств. Незакрытые сетевые порты, некорректно работающий антивирус, не измененные при установке сетевого оборудования пароли – подобные ошибки в настройке могут очень дорого обойтись предприятию. Более того, новые уязвимости в конфигурации будут появляться и в процессе работы, по мере развития системы.

Отдельные принципы, заложенные в архитектуру системы безопасности на этапе ее проектирования много лет назад, делают конечное решение исходно "дырявым"

Технические и программные средства должны быть развернуты и регулярно обслуживаться только квалифицированными специалистами, а такие специалисты в своей работе должны руководствоваться надежными регламентами и в том числе требованиями по информационной безопасности. Если ваши компьютеры настраивает вчерашний выпускник филфака, то вероятность взлома многократно возрастает.

Подключение оборудования по последовательному порту

Большая часть производителей средств систем безопасности продолжает эксплуатировать устаревшее оборудование, подключаемое к компьютеру по последовательным портам. Такое подключение вместо, например, сетевого обусловлено чаще всего низкой производительностью оборудования и невозможностью программного обеспечения последнего реализовывать высокоуровневые защищенные протоколы коммуникации. Таким образом, протоколы информационного обмена с оборудованием оказываются либо полностью открытыми, либо защищенными чисто формально – так, что взлом такой защиты является элементарным.

В результате при получении доступа к соответствующему компьютеру злоумышленник также получает возможность выполнять команды управления над подключенным оборудованием – разрешать доступ, снимать помещения с охраны и др. Он может действовать хитрее, например добавить свою карту в базу данных оборудования и впоследствии пройти на охраняемую территорию без ограничений.

Как с этим жить?

Ваша система работает в защищенной среде, пользователям выданы ограниченные права и сложные пароли, а коммуникация в сети осуществляется строго по mutual TLS? Поздравляем, вряд ли ваша система будет "дырой" в безопасности!

Но если нет, то что делать?

Обновление операционной системы

Если программные средства системы физической безопасности работают под управлением устаревших или уязвимых версий операционных систем, следует оперативно обновить такие ОС. Предпочтительно осуществить миграцию на актуальную версию какой-либо российской операционной системы для получения регулярных обновлений и патчей безопасности. К сожалению, большая часть средств безопасности может работать только под управлением не поддерживаемых в РФ ОС семейства Microsoft Windows, а российские ОС относятся к семейству Linux. В таком случае возможна только замена программных средств на поддерживающие Linux и российские ОС.

Настройка наложенных средств

При наличии сетевых угроз можно выделить КСБ в отдельную защищенную подсеть. Но это не всегда возможно на физическом уровне, так как коммуникации уже смонтированы на этапе строительства. В таком случае автор рекомендует установку наложенных средств, таких как VPN, для защиты сетевого обмена, а также грамотную настройку межсетевых экранов и сетевого оборудования.

Следует также установить/обновить антивирусное программное обеспечение и средства ИБ-мониторинга, использовать актуальные базы сигнатур вирусов и угроз.

Подключение ко внешней системе учетных записей

В случае если ПО системы безопасности не поддерживает гибкие политики управления паролями и аутентификацией в целом, но поддерживает интеграцию со средствами вроде OpenLDAP или Keycloak, то рекомендуем настроить такую интеграцию и делегировать контроль аутентификационных данных специализированной системе.

Внедрение регламента эксплуатации КСБ

При невозможности закрыть уязвимости техническими мерами можно прибегнуть к организационным – разработать корпоративный регламент эксплуатации системы физической безопасности, предотвращающий создание типовых уязвимостей: делегировать выдачу паролей только доверенным администраторам, которые будут контролировать их сложность и время жизни; с заданной периодичностью проводить аудит безопасности, устанавливать соответствующие обновления; периодически просматривать системные журналы на предмет нетиповой активности.

Основной минус такого подхода – человеческий фактор. Регламент будут выполнять люди, а всем людям свойственно ошибаться.

Модернизация программных средств

К сожалению, не все уязвимости можно закрыть наложенными средствами и организационными мерами. Отдельные принципы, заложенные в архитектуру системы безопасности на этапе ее проектирования много лет назад, делают конечное решение исходно "дырявым".

К таким принципам относятся ориентированность на работу в изолированном сегменте сети, отсутствие защиты протоколов коммуникации с оборудованием или работа в операционной системе только с административными правами.

Устранить угрозы, возникающие вследствие таких фундаментальных особенностей, можно только при помощи качественной модернизации, выбора надежной продукции иного производителя – средств, которые исходно спроектированы с учетом актуальных киберугроз.

Заключение

Цифровые технологии существенно изменили мир. Цифровизация делает нашу жизнь проще и эффективнее, но и несет с собой новые риски – киберугрозы.

Количество кибератак неуклонно растет, а современные системы физической безопасности подвержены им даже в большей степени, чем другие информационные системы

На рынке почти нет решений, которые исходно спроектированы и реализованы в соответствии с актуальными требованиями кибербезопасности. Киберугрозы можно частично купировать наложенными средствами и организационными мероприятиями, но полноценно закрыть "дыру" в безопасности можно, лишь выбрав современный, полностью киберзащищенный продукт. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru