VPN должен быть безопасным

Сделать белый список адресов кому можно обращаться. Или хотя бы черный. При подключении по http сразу редирект на https, в случае отказа сбрасвать соединении. Проверка оператора SIM. Проверка номера телефона по звонку

SSH доступ по ключу RSA. Или по паролю длина которого не менее 12 символов, что соответсвует международному стандарту ISO.

Использование FTPS вместо FTP.

Доступ к хранилищу Backup копий с помощи 2 аутентификации с минимальными правами. Повышение привилегий только определенным сотрудникам.

Администрирование RDP только по 443 порту с поддержкой TLS + аутентификация.

При валидации pin кода изначально послать запрос по HTTP не отпарвляя пин код. Затем получив ответ от сервера перейти на HTTPS в противном случае сбросить соединение.

При аналитике сделать аутентификацию с минимальными правами на минимальное время. При администрировании сделать аутентификацию и сделать запрос на повышение привилегий.

Личный кабинет для интранета и SMS-шлюз использовать только защищенное соединение, а так же постоянно обновлять версию веб сервера и антивирусное ПО.

При использовании LDAP протокола фильтровать данные и блокировать LDAP инъекции.

Перенести sms центр в Inside. А затем отправлять code и ip по защищенному соединению.

Доступ к базе данных с пинкодами с минимальными правами для чтения и записи, удаления и обновления. Запуск сервиса без доступа root. Запуск всех сервисов без root. Фильтрация данных при сохранении в БД и дроп запросов с инъекцией. Объединение всех БД в один сегмент, чтобы не приходилось искать уязвимости в нескольких местах. Доступ к данным пользователя только при его аутентификации. Доступ сотрудника к данным только при необходимости с минимальными правами.То же самое с тестовым хранилищем данных