Любые вопросы адресуйте диспетчерам SAMого безопасного в мире аэропорта Softline

Пишите:

Павлу Пучкову,
руководителю направления SAM:
Pavel.Puchkov@softlinegroup.com

Владимиру Нестерову,
менеджеру проектов:
Vladimir.Nesterov@softlinegroup.com

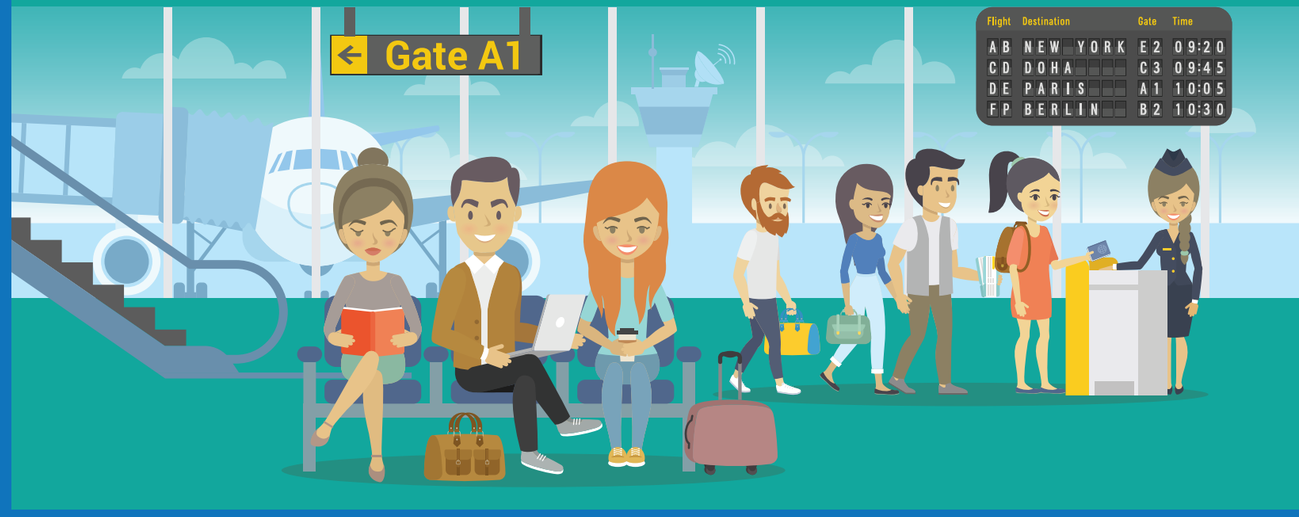
Илье Панкратову,
зам. директора департамента
бизнес-консалтинга:
Ilya.Pankratov@softlinegroup.com

Наш телефон:

+7 (495) 232-00-23

softline®

softline® SAM CyberSecurity



ПРИГЛАШАЕМ В БЕЗОПАСНЫЙ ГЕЙТ!

Мы констатируем факт: каждый год копилка с историями о том, как компании теряют миллионы долларов в год из-за проблем с кибербезопасностью, пополняется. Читая в Сети подборку ИБ-«страшилок», размышляете ли вы о том, как самим не столкнуться с киберугрозами?

Давайте представим, что ИТ-инфраструктура вашей компании — это аэропорт. Для того, чтобы он без перебоев выполнял свою функцию — то есть принимал и отправлял рейсы, правильно организуя большой пассажиропоток, — все его внутренние и внешние системы должны быть отлажены и работали безопасно.

Посторонним вход воспрещен

Аэропорт разделен на несколько зон. В некоторые их них доступ осуществить довольно просто, зайти может каждый. Другие же закрыты для случайных людей. Существуют многочисленные помещения, куда войти могут только единицы — спецсотрудники.

Насколько тщательно разграничены права доступа к ИТ-системам в вашей организации? Вы уверены, что сотрудники работают только в «разрешенных» зонах, а ценные ресурсы надежно защищены от случайных глаз?

Таинственный чемоданчик

Сотрудники аэропорта неслучайно тщательно инспектируют багаж и проверяют пассажиров. Таким образом устраняются многие угрозы авиационной безопасности. Точно также в ИТ-инфраструктуре необходимо проводить проверки на наличие нелицензионного софта.

«Пиратская» программа на пользовательском компьютере запросто может содержать закладку с вирусом. Как потрепанный чемодан — взрывчатку.

Смотри в оба!

Внимательность — «второе имя» бдительных работников аэропорта, где выполнение любого процесса предполагает четкие и быстрые действия. Но представим, что половина сотрудников, включая таможенников и носильщиков багажа, в один прекрасный день… забудут дома очки и перестанут различать, что творится вокруг. Какой же хаос тогда начнется!
Необновленное ПО ненадежно и малоэффективно, как слабовидящий человек, к тому же крайне уязвимо и беззащитно перед злоумышленниками. Его можно сравнить с близорукой стюардессой, способной пустить на борт вооруженного агрессивного пассажира, или перепутать паспорта... Опасная ситуация!

Порядок — основа безопасности

Отсутствие отлаженных процессов SAM — причина возникновения многих угроз корпоративной информационной безопасности.
Если вы не знаете, сколько в компании устаревшего аппаратного и программного обеспечения, вы подвергаете бизнес большому риску.

Безопасность — стратегическое вложение

Специалисты Softline, обладают обширными компетенциями и опытом реализации проектов SAM CyberSecurity. Являясь сертифицированным SAM-партнером Microsoft, Softline реализует полный цикл процедур, направленных на оптимизацию использования программного обеспечения вендора, а также повышение уровня лицензионного соответствия.

Мы поможем вам определиться с подходом к стратегии обеспечения безопасности процессов и технологий. Не только разработаем оценку текущего уровня безопасности, но и дадим рекомендации по повышению зрелости CyberSecurity до более высокого уровня в вашей компании.

SAM CyberSecurity

Проект CyberSecurity SAM. Киберэффективно!

Что это?

Базовый анализ кибербезопасности. Это не масштабный проект с тестами на проникновение в ресурсы. Это именно оценка состояния, рекомендации касательно того, на что ДИТам и сотрудникам службы безопасности следует обратить внимание.

На чем фокусируемся?

На возможных проблемах с установленным софтом, продуктами Microsoft, его использованием и соответствием лицензионным правам.

Что в итоге?

Все скрытые потенциальные опасности обнажаются. Появляется понимание того, каковы угрозы ИБ с точки зрения нелицензионного и необновленного ПО; сколько всего лицензий в компании, какие версии используются. Одним словом, происходит ИБ-оценка надежности IT-инфраструктуры. Мы используем Evidence based-метод: любые подозрения должны быть дополнительно проверены и подтверждены доказательствами.

А что дальше?

SAM CyberSecurity это начало пути к ИБ!
- SAM CyberSecurity – оценка по 20 компетенциям.
- ISO Assessment – оценка по 163 нормам контроля.

Компания Softline предлагает:
- Детальное обследование инфраструктуры.
- Тесты на проникновение (Penetration Testing).
- Оценка готовности персонала.
- Разработка стратегии кибербезопасности.
- Аудит по ISO/IEC 27001.
- Внедрение и поддержка решений для защиты от угроз кибербезопасности.