АРЕСБАНК

О ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ

Уважаемые клиенты - юридические лица, индивидуальные предприниматели и физические лица, занимающиеся в установленном порядке частной практикой!

Напоминаем, что в соответствии с Договором ЭДО[1] Банк не несёт ответственности за ущерб, возникший, в том числе, в следующих случаях:

- **воздействия на программно-аппаратные комплексы вредоносных программ;**
- **неправомерного доступа к программно-аппаратным комплексам Системы, в том числе, по причине неисполнения Клиентом требований, предусмотренных Правилами «AUTHORITY»;**
- **вследствие неправомочного использования Сертифицированных Сертификатов/ Сертификатов, ключей электронной подписи, Логинов – Паролей, Разовых секретных паролей, Номеров мобильного телефона, Мобильного приложения, Мобильных устройств Клиента.**

В РАМКАХ ВОЗРАСТАЮЩИХ АТАК ЗЛОУМЫШЛЕННИКОВ, УВЕДОМЛЯЕМ О НЕОБХОДИМОСТИ

Проведения мероприятий, направленных на соблюдение требований по информационной безопасности, включающих:

- использование и своевременное обновление антивирусных средств защиты;
- использование антифишинг-систем, в том числе автоматического анализа ссылок (вложений);
- регулярное обучение персонала по противодействию социальной инженерии и фишингу;
- ограничение бесконтрольного доступа работников в сеть «Интернет»;
- использование для работы в Интернет-банк выделенных рабочих персональных компьютеров работникам бухгалтерии, финансовых подразделений, осуществляющих проведение платежей со счетов юридического лица.

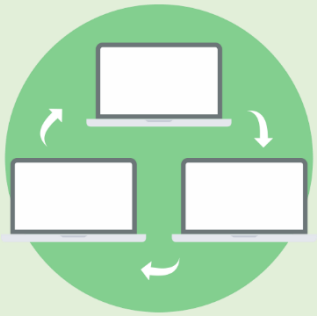
[1] п. 8.2 Договора присоединения Клиентов ООО КБ «АРЕСБАНК» - юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном порядке частной практикой, к электронному документообороту

Информационный буклет #1.07 «О проведении мероприятий, направленных на повышение уровня защищенности объектов инфраструктуры клиентов – юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном порядке частной практикой»

Проведения мероприятий, направленных на повышение уровня защищенности объектов вашей инфраструктуры, включающих:

- не допускать использования работниками организации рабочих устройств для личного использования, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах;
- с учетом перехвата вредоносным программным обеспечением SMS- сообщений, сменить второй фактор подтверждения операции на PUSH-уведомления, использовать аппаратный ключ (токен) с учетом требований безопасности при его эксплуатации, производить его извлечение из USB-порта сразу после подписания платежных поручений;
- использование решений для мониторинга и выявления киберугроз и оперативного реагирования на инциденты (MDR-решений);
- с помощью аппаратных или программных средств сетевой защиты (Firewall, корпоративные прокси-серверы) ограничить доступ в сеть «Интернет». Маршрутизировать трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами.

Проведения мероприятий, при выявлении инцидента информационной безопасности рекомендуется:



- не перезагружать компьютер, не запускать антивирусные решения, извлечь токены доступа и съемные носители информации;
- отключить устройство от локальной сети и сети Интернет;
- выполнить процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения (например, «FTK Imager») для дальнейшего проведения расследования;
- сохранить образец вредоносного программного обеспечения для проведения анализа и последующей передачи его в Банк (в рамках анализа компьютерного инцидента);
- в случае заражения мобильного устройства, необходимо включить авиа-режим и извлечь SIM-карту. Если в устройстве используется электронная сим-карта, допустимо выключить устройство. Сбрасывать устройство до заводских настроек не рекомендуется, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.