МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТВЕРСКОЙ ОБЛАСТИ
Студенческий пер., д. 28, г. Тверь, 170100
тел.: (4822) 33-30-30
E-mail: digital@tverreg.ru

_____ №_____

На № _____ от _____

Для служебного пользования
Экз. № 1

Руководителям исполнительных органов государственной власти Тверской области

Главам муниципальных районов, городских и муниципальных округов, ЗАТО Тверской области

Об формировании предпосылок к реализации угроз информационной безопасности

Уважаемые коллеги!

Анализ поступающей в Министерство цифрового развития и информационных технологий Тверской области информации свидетельствует о наличии целенаправленных атак профессиональных кибергруппировок на государственные органы власти и органы местного самоуправления через использование фишинговых инструментов, тщательно проработанных под специфику деятельности органа власти (рассылка почтовых сообщений актуальной тематики, рассылка ссылок на сторонние информационные ресурсы в сети Интернет), что влечет за собой формирование предпосылок к реализации угроз информационной безопасности.

Указанные атаки потенциально могут привести к полной компрометации инфраструктуры органа власти, выявлении злоумышленниками инфраструктурных и логических схем информационных ресурсов органов власти, кражи конфиденциальной информации со всех источников: с почтовых серверов, серверов электронного документооборота, файловых серверов общего и ограниченного доступа, рабочих станций руководителей различного уровня. Также следствием атаки может стать полная блокировка инфраструктуры органа власти, вызванная злоумышленниками в необходимый для них момент времени.

Исходя из технических подробностей зафиксированных атак, выделяются две особенности осуществления доступа к инфраструктуре органа власти:

- фишинговые почтовые рассылки вредоносных приложений или ссылок по электронной почте или через популярные мессенджеры (WhatsApp,

Telegram, VK messenger и другие);

- эксплуатация уязвимостей веб-приложений, опубликованных в сети Интернет.

В качестве тем для фишинговых рассылок злоумышленники могут использовать актуальные новости – как внутренние, связанные с непосредственной деятельностью конкретного органа власти, так и общемировые – например, касающиеся эпидемии Covid-19 или геополитической обстановки на границе России или в мире. Такое вредоносное почтовое сообщение имеет вложенное приложение, чаще всего в виде офисного документа со специальным макросом: при открытии такого файла происходит запуск вредоносного ПО и заражение хоста. При этом антифишинговое и антивирусное программное обеспечение как на почтовых серверах, которые обрабатывают соответствующие сообщения, так и установленное непосредственно на автоматизированном рабочем месте сотрудников, зачастую может не распознавать данное приложение как зловредное.

Эксплуатация уязвимостей веб-приложений, как правило, заключается в получении через почтовые сообщения, мессенджеры соответствующих ссылок на внешние ресурсы в сети Интернет, что имеет своей целью осуществить загрузку на АРМ веб-шеллов (вредоносных скриптов, позволяющих управлять сайтами и серверами), через которые в дальнейшем происходит развитие атак. Кроме того, данные ссылки массово размещаются на информационных ресурсах развлекательного характера, а также в социальных сетях, доступ к которым могут осуществлять сотрудники органов власти в рабочее время.

В связи с изложенным выше рекомендуется осуществить следующие организационно-технические мероприятия в органе власти:

1. Ввести в организации полный запрет на открытие почтовых электронных сообщений, полученных от недоверенных адресатов (от неизвестных лиц, либо полученных с неизвестных почтовых адресов, либо не имеющих отношение к рабочей деятельности). Открывать электронные письма и их приложения надлежит только от известных адресатов, либо те, которые ожидает получить пользователь в связи с исполнением должностных обязанностей;

2. Запретить открывать электронные письма, в том числе с доверенных почтовых адресов, содержащие ссылки на сторонние ресурсы в сети Интернет либо имеющие в приложениях к электронному письму подозрительные файлы (приложения, которые не ожидает получить адресат, либо приложения, имеющие подозрительные названия или приложения нерабочего характера);

3. Запретить использовать рабочую электронную почту в личных целях (например, для регистрации на сторонних ресурсах, для размещения в социальных сетях и т.д.);

4. Запретить использование личной электронной почты в рабочем процессе;

5. Запретить предоставление сторонним лицам учетных данных для доступа к рабочему почтовому ящику;

открываемого через интернет-браузер (за исключением корпоративных мессенджеров, включенных в перечень разрешенного ПО исходя из принятой в органе власти политики информационной безопасности);

7. Запретить пересылать по электронной почте или через мессенджеры учетные данные к внутренним ресурсам, за исключением случаев предоставления доступа техническими службами пользователям к информационным ресурсам согласно установленному порядку (регламенту) предоставления доступа;

8. Запретить доступ с автоматизированных рабочих мест к информационно-развлекательным ресурсам в сети Интернет, социальным сетям, если доступ к отдельным подобным ресурсам не предусмотрен служебной необходимостью исходя из должностного регламента работника.

Также прошу в срочном порядке проконтролировать наличие на рабочих местах актуальной версии антивирусного программного обеспечения с обновленными на текущую дату антивирусными базами.

Данную информацию прошу оформить в виде организационно-распорядительного документа организации с последующим ознакомлением сотрудников под роспись, а также довести до руководителей подведомственных учреждений.

Министр цифрового развития и информационных технологий Тверской области **С.В. Снегирев**

Никитин Евгений Олегович
8 (4822) 33-33-00