Обеспечение защиты информации РУП «Белтелеком»

В целях организации противодействия угрозам информационной безопасности РУП «Белтелеком» оказываются населению следующие услуги: защита от DDoS атак, фильтрация сетевого трафика, предоставление лицензий на использование антивирусной защиты, повышение осведомленности в сфере информационной безопасности, а также родительский контроль.

Для популяризации информационной безопасности создан Интернет-портал: security.beltelecom.by, посвященный вопросам защиты информации.

В ходе своей деятельности в 2020 году специалисты предприятия РУП «Белтелеком» столкнулись со следующими видами угроз:

1. Увеличилась интенсивность распределенных атак, направленных на отказ в обслуживании информационных систем и сетей.
2. Участилось количество случаев получения работниками предприятия электронных почтовых сообщений, содержащих вредоносное вложение или ссылку на опасный («зараженный») информационный ресурс (фишинг). При этом активно стала использоваться тема пандемии Covid-19.
3. Антивирусным программным обеспечением на сетевом и оконечном оборудовании РУП«Белтелеком» фиксируются случаи наличия вредоносного программного обеспечения (далее - ВПО). Изучение выявленного ВПО показало его ориентированность на похищение банковской информации или шифрование данных. При этом увеличилась и скорость распространения ВПО. Так в сентябре 2020 года было опубликовано исследование уязвимости Zerologon (CVE-2020-1472), а уже в октябре 2020 года специалистами РУП «Белтелеком» зафиксированы подобные атаки на информационные системы предприятия.
4. Увеличились атаки, направленные на оконечное сетевое оборудование абонентов. Используя перебор пароля (брутфорс) модемного оборудования, злоумышленники закрепляются в локальной сети абонента.
5. На оконечных устройствах абонентов (компьютеры, ноутбуки, мобильные устройства и др.) продолжают присутствовать различные уязвимости и ВПО. Указанное связано с использованием устаревшего или нелицензионного программного обеспечения, игнорирование легального приобретения и использования средств защиты информации.

По мнению специалистов предприятия, одним из факторов успешности проведенных атак злоумышленниками является низкий уровень грамотности и осведомленности абонентов в сфере информационной безопасности.

При изучении мировых тенденций в сфере информационной безопасности, из открытых источников (shodan.io, greynoise.io, censys.io и др.) получена информация свидетельствующая, что в национальном сегменте глобальной сети Интернет значительно увеличилось количество попыток «заражения» IoT-устройств.