Почему сфера образования становится всё привлекательнее для киберпреступников?

Образовательные учреждения Соединённых Штатов сталкиваются с растущими угрозами киберпреступности. По данным ежегодных отчётов, количество атак на школы увеличивается постоянно. Среди таких атак — вымогательство, фишинг и DDoS.

Федеральная и региональная поддержка, направленная на обновление оборудования и обеспечение безопасности, помогает бороться с этой тенденцией. Однако риски остаются высокими, так как утечка данных учащихся, ущерб репутации учреждений и нарушение учебного процесса могут иметь весьма серьёзные последствия.

Американские школы являются лёгкой добычей для киберпреступников. По данным Агентства по кибербезопасности и безопасности инфраструктуры США (CISA), школы являются наиболее уязвимым типом организаций, которые могут быть интересны вымогателям.

Использование устаревших IT-систем, нехватка бюджета и квалифицированных ИБ-специалистов, а также огромное количество устройств, подключаемых к школьным сетям, создают идеальные условия для атак.

Пандемия COVID-19 только усилила возможные риски для сферы образования. Школы так быстро переходили на дистанционное обучение, что не имели достаточно времени на построение по-настоящему безопасных систем. В результате выросла и уязвимость к кибератакам.

Кроме того, большинство IT-администраторов в школах не имеют полной информации о количестве устройств и серверов, их состоянии и слабостях в защите. Это создаёт повышенную угрозу, так как всего одно незащищённое устройство уже может стать входной точкой для атаки. Даже системы видеонаблюдения представляют опасность, если инфраструктура не защищена должным образом.

Для защиты необходимо улучшить видимость конечных точек в сети, что можно сделать, например, с помощью решений для управления конечными точками. Они позволяют получить полное представление о количестве устройств и их состоянии.

Так, школьный округ Barnaby в Канаде недавно обнаружил в своих сетях на 2000 устройств больше, чем предполагал. Неожиданная находка позволила специалистам увеличить свою осведомлённость и сконфигурировать системы более безопасно.

Высшие учебные заведения также сталкиваются с угрозами вымогательства и

кибератаками, спонсируемыми недружественными государствами. Эти угрозы используют сложные многоступенчатые тактики и уязвимости в системах безопасности. В отличие от корпоративного сектора, безопасность в университетах часто фрагментирована, что усложняет защиту.

Учебные заведения должны уметь выявлять и устранять уязвимости, а также оперативно реагировать на инциденты. План реагирования на инциденты должен включать обнаружение угроз, уведомление страховщиков и властей, сбор доказательств, устранение последствий и восстановление.

Таким образом, сфера образования требует повышенной готовности к киберугрозам, особенно во время летних каникул, так как помимо школьников и студентов на своих рабочих местах зачастую не находится и IT-персонал, способный предпринять хоть какие-то защитные действия в случае кибератаки.

Стоит помнить, что только комбинированные усилия по профилактике и реагированию на инциденты помогут защитить школы и университеты от новых случаев вымогательства и фишинга.