PISA
Platforma pentru Inițiative de Securitate și Apărare

DCAF Geneva Centre for Security Sector Governance

Sweden
Sverige

Молдова и кибербезопасность: участившиеся атаки на фоне войны ставят под пристальный контроль политики по обеспечению надежной цифровой экосистемы

МАТЕРИАЛ РАЗРАБОТАН В КОНТЕКСТЕ ПРОЕКТА "ИНФОРМАЦИОННАЯ КАМПАНИЯ ПО ЗАДАЧАМ ПОЛИТИК В ОБЛАСТИ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ МОЛДОВА", РЕАЛИЗУЕМОГО ПЛАТФОРМОЙ ПО ИНИЦИАТИВАМ В ОБЛАСТИ БЕЗОПАСНОСТИ И ОБОРОНЫ (ПИСА) И ПОДДЕРЖИВАЕМОГО ЖЕНЕВСКИМ ЦЕНТРОМ ПО УПРАВЛЕНИЮ СЕКТОРОМ БЕЗОПАСНОСТИ (DCAF), В РАМКАХ ПРОЕКТА "УКРЕПЛЕНИЕ УПРАВЛЕНИЯ СЕКТОРОМ БЕЗОПАСНОСТИ В МОЛДОВЕ", ФИНАНСИРУЕМОГО ШВЕЦИЕЙ.

В 2023 году в Республике Молдова было зарегистрировано более 1000 крупных киберинцидентов. Это наибольшее количество на сегодняшний день, и наибольший рост приходится на фишинговые атаки. В целом, по данным Службы информации и безопасности, Молдова сталкивается с четырьмя основными типами киберугроз: DDoS-атаки, фишинг через государственные электронные письма, атаки методом грубой силы для получения доступа к государственным информационным системам и захват официальных веб-страниц. Самыми опасными считаются DDoS-атаки (распределённые атаки на отказ в обслуживании), которые означают наводнение сервера или сети чрезмерным трафиком, чтобы сделать их недоступными. Эти атаки постоянно увеличивались в размере и сложности, но 2023 год ускорил рост этой тенденции непредсказуемыми темпами. Геополитика является ключевым фактором, объясняющим их беспрецедентную частоту, как в странах США, России, Украины, Израиля, Германии, Франции, Польши и Объединённых Арабских Эмиратах. Большое количество кибератак, которые проводятся одновременно и координируются государственными и негосударственными акторами, в настоящее время представляет собой серьёзную угрозу для глобальной безопасности.

В этих условиях Республика Молдова приняла меры для обеспечения надёжной цифровой экосистемы. В феврале 2024 года, например, было создано Национальное агентство по кибербезопасности. Его цель - защищать критическую инфраструктуру государства и общества от кибератак и обеспечивать высокий уровень безопасности для сетей и IT-систем государственных и частных учреждений. Институциональная структура для обеспечения кибербезопасности в настоящее время разделена между следующими учреждениями: Министерство экономики, Служба информационных технологий и кибербезопасности (STISC), Группа реагирования на компьютерные чрезвычайные ситуации в рамках STISC (CERT-GOV-MD), Агентство электронного управления, Министерство обороны, Министерство внутренних дел, Служба информации и безопасности, Генеральная прокуратура, Государственная канцелярия и Комиссия по национальной безопасности, обороне и общественному порядку Парламента Республики Молдова.

В стремлении к гармонизации с протоколами ЕС, правительство постоянно вводило меры регулирования и политики в области кибербезопасности. Однако их внедрение и создание возможностей не поспевали за развитием политик. Таким образом, можно констатировать, что Республика Молдова сегодня имеет фрагментированную систему кибербезопасности, недостаток специалистов в этой области и пробелы в технических возможностях правительства. Выделение финансовых и человеческих ресурсов также не соответствует растущим и меняющимся потребностям в области кибербезопасности. Государственная группа реагирования на компьютерные чрезвычайные ситуации (CERT) невелика, но она служит связующим звеном для всех коммуникаций и отчетов о киберинцидентах.

Первоочередной рекомендацией является необходимость усиления киберустойчивости (способности противостоять и быстро восстанавливаться после кибератак), а также острая необходимость защиты критической инфраструктуры, такой как энергетические сети, финансовые системы и коммуникации. Многие из этих инфраструктур используют старые технологии, уязвимые для атак, и нуждаются во внедрении строгих протоколов безопасности и эффективных систем резервного копирования. Постоянный аудит безопасности и принятие лучших международных практик необходимы для укрепления безопасности этих инфраструктур. Способность к быстрому и эффективному реагированию на кибератаки необходима для минимизации их воздействия путем укрепления национальных CERT-групп, обеспечения их ресурсами и передовыми технологиями, а также проведения регулярных учений и симуляций. Международные партнёрства с организациями, такими как ENISA и НАТО, предоставляют доступ к важной информации и ресурсам для предотвращения и борьбы с кибератаками, в то время как обмен информацией с другими государствами помогает справляться с общими угрозами. Обучение общественности по вопросам защиты граждан от кибератак становится важным. Следовательно, необходимо начать национальные кампании по повышению осведомлённости о важности кибербезопасности, создать доступные руководства и ресурсы для граждан и малого бизнеса, а также ввести кибербезопасность в школьные и университетские программы. Программы непрерывного обучения для IT-специалистов и широкой общественности, наряду с инвестициями в стартапы и сотрудничеством с частным сектором, существенно способствовали бы развитию экосистемы кибербезопасности в Молдове.

Узнайте больше об этом в полном обзоре: bit.ly/3XOgdgl