Вымогательское ПО – главный кошмар директоров: 62% готовы платить хакерам

Согласно опросу 1600 директоров по информационной безопасности (CISO («Chief Information Security Officer» или «Главный офицер по информационной безопасности») — это высокопоставленный руководитель, ответственный за разработку, реализацию и управление стратегией безопасности информации в организации.

 CISO отвечает за защиту информации, которая находится в системах и приложениях организации, а также за соблюдение требований в области безопасности данных. В его обязанности входит проведение анализа угроз безопасности, разработка политик безопасности, обеспечение соответствия законодательству, руководство процессом обучения сотрудников в области информационной безопасности и многое другое." data-html="true" data-original-title="CISO" >CISO) по всему миру, более 70% беспокоятся о возможности серьезной кибератаки на их организации в течение года, что на 2% больше, чем годом ранее, и на 22% выше по сравнению с 2022 годом. Более того, 31% уверены, что значительная атака «очень вероятна» (по сравнению с 25% в 2023 году).

Ежегодный отчет Voice of the CISO , подготовленный компанией Proofpoint – это компания, которая занимается защитой от цифровых угроз. Она предлагает ряд решений для защиты корпоративных почтовых систем, включая фильтрацию спама и мошеннических писем, защиту от вредоносного ПО и фишинга, а также контроль доступа к электронной почте и мониторинг компрометации учетных данных. Компания также предоставляет решения для защиты социальных медиа, мобильных устройств и ключевых информационных систем. Она сотрудничает с крупными корпорациями и правительственными организациями по всему миру для обеспечения защиты их цифровой инфраструктуры от различных угроз." data-html="true" data-original-title="Proofpoint" >Proofpoint, основан на данных, собранных фирмой Censuswide в период с 20 января по 2 февраля. В исследовании участвовали CISO из организаций с численностью сотрудников не менее 1000 человек из 16 стран, включая США, Канаду, Великобританию, Францию, Германию, Италию, Испанию, Швецию, Нидерланды, ОАЭ, Саудовскую Аравию, Австралию, Японию, Сингапур, Южную Корею и Бразилию.

Наиболее тревожные ночи проводят специалисты по информационной безопасности в Южной Корее (91%), Канаде (90%) и США (87%). Их волнения связаны с риском разрушительных кибератак, которые могут нанести серьезный ущерб. Однако есть и положительные изменения: 43% опрошенных считают свои организации неподготовленными к атакам, что все же лучше по сравнению с 61% в прошлом году.

Основные угрозы, вызывающие бессонницу у CISO, включают вымогательское ПО (41%), вредоносное ПО (38%), мошенничество по электронной почте (36%),

компрометацию облачных аккаунтов (34%), внутренние угрозы (30%) и DDoS-атаки (30%).

В случае заражения вымогательским ПО, 62% CISA признались, что они, вероятно, заплатят злоумышленникам для восстановления систем и предотвращения утечки данных. Такой показатель остается неизменным по сравнению с прошлым годом, несмотря на доказательства того, что оплата не гарантирует сохранения конфиденциальности информации.

Изучая результаты опроса за 2024 год, невозможно не задаться вопросом: почему кто-то хочет заниматься такой работой? Многие CISO, похоже, тоже так считают. Несмотря на наличие положительных тенденций, таких как увеличение представительства кибербезопасности на уровне совета директоров и более тесное взаимодействие между CISO и членами совета, растет число специалистов, которые жалуются на чрезмерные ожидания. В этом году 66% опрошенных указали на нереалистичные ожидания, по сравнению с 61% в прошлом году, 49% в 2022 году и 21% в 2021 году.

Более 53% респондентов сообщили, что за последние 12 месяцев лично сталкивались с выгоранием или были свидетелями этого явления среди своих коллег. Это можно частично объяснить высокопрофильными юридическими процессами, в которых CISO несут ответственность за утечки данных в компаниях.

Примером может служить обвинение, предъявленное SolarWinds и ее CISO Тиму Брауну за недостаточную подготовку к атаке на цепочку поставок в 2020 году. Такие инциденты заставляют 66% мировых CISO беспокоиться о личной, финансовой и юридической ответственности, что немного выше по сравнению с 62% в прошлом году.