Секция « Экономика и право»

УДК 002:004

ПРОТИВОДЕЙСТВИЕ ИНСАЙДУ: ТЕХНИЧЕСКИЕ РЕШЕНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ

Бахматова Е.И.
Белорусский национальный технический университет

Инсайдеры – актуальная современная угроза информационной безопасности компании. Чем масштабнее деятельность организации, тем сложнее обеспечивать эффективный контроль действий сотрудников при использовании корпоративных информационных ресурсов. Инсайдер – текущий или бывший сотрудник, подрядчик, аутсорсер или доверенный бизнес-партнер организации, в отношении которого одновременно выполняются следующие условия: (1) наличие на текущий момент или в прошлом санкционированного доступа к информационным активам организации; (2) намеренное превышение и использование имеющихся полномочий способом, оказавшим отрицательное влияние на конфиденциальность, целостность и/или доступностьинформации и/или информационной системы организации. Технические способы защиты от инсайда требуют наличия не только программно-технических решений (например, DLP-система, SecurityInformationandEventManagement, Honeypotи др.), но и специалистов, осуществляющих их эксплуатацию и обслуживание. Комплекс организационно-технических мероприятий противодействия инсайду включает: оценку благонадежности кандидатов при приеме на работу; закрепление наставников за новичками; повышение лояльности персонала; физическое отключение или программное блокирование всех интерфейсов (USB-портов и т.д.);блокирование всего исходящего трафика; запрет на использование средств Instantmessenger; блокирование всех сайтов, за исключением необходимых для работы;мониторинг HTTP-трафика; учет всех вносимых/выносимых предметов; использование камер наблюдения и др. Наибольшей эффективностью с точки зрения соотношения «затраты ресурсов – эффект» характеризуются мероприятия, связанные с управлением персоналом (при приеме на работу, наставничество, повышение лояльности). Неоспоримое преимущество данных мероприятий также заключается в отсутствии негативного влияния на качество информационно-знаниевого обмена внутри компании.

Литература

1. Scott, J. In 2017, The Insider Threat Epidemic Begins / James Scott, Drew Spaniel // Institute for Critical Infrastructure Technology [Electronic resource]. – Washington D.C, February, 2017. Mode of access: http://icitech.org/wp-

content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf. – Date of access: 09.02.2017