Корпоративная защита от внутренних угроз информационной безопасности

В наши дни одним из наиболее актуальных вопросов защиты корпоративной информации – обеспечение безопасности от внутренних утечек по техническим каналам связи. Одна из главных угроз корпоративной информационной безопасности – неправомерными действиями сотрудников (т.н. инсайдеров), приводящие к потере конфиденциальных данных, совершенные как целенаправленно, так и из-за халатности, невнимательности или незнания элементарных правил безопасности предприятия. Именно «на их совести» большинство громких краж данных, зафиксированных по всему миру в последние годы. Причиной утечек также могут быть действия посторонних лиц, находящихся на территории предприятия и имеющих доступ к вычислительносетевой инфраструктуре (клиенты, поставщики и т.п.). Утечки информации могут породить целый ряд проблем:

1. Утечка персональных данных. Может повлечь за собой как санкции со стороны контролирующих органов, так и отток клиентов, связанный с утратой доверия к компании.
2. Утечка коммерческой тайны и ноу-хау. Утечка информации об инвестиционных планах, маркетинговых программах, инновациях, данных клиентской базы способна привести к срыву важных и прибыльных проектов.
3. Утечка служебной переписки. Служебная переписка может дать конкурентам много информации о ситуации в компании. Copyright
4. Утечки в прессу. Могут повлечь за собой разглашение коммерческой тайны организации.
5. Утечка информации о системе безопасности. Открывает широкие возможности для деятельности криминальных структур.
6. Утечка сведений, составляющих государственную тайну и т.д. Необходимость защиты от внутренних и внешних угроз информационной безопасности не только доказана на практике, но и упомянута в ключевых международных стандартах по организации и менеджменту информационной безопасности (например, в ISO/IEC 27001).

Технологии корпоративной защиты от внутренних угроз информационной безопасности, относящиеся к классу Data Leak Prevention (DLP) позволяют выявлять и предотвращать утечки конфиденциальной информации и персональных данных, защищать компании от мошенничества, воровства и коррупции, детектировать неправомерные действия сотрудников и нецелевое использование корпоративных ресурсов. Системы корпоративной безопасности позволяют однозначно выявлять инциденты и дают весь необходимый набор инструментов для проведения внутренних расследований и дальнейшей правовой защиты корпоративных интересов. Специалисты по корпоративной безопасности должны обладать теоретическими знаниями по обеспечению корпоративной защиты от внутренних угроз, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов, в совершенстве владеть системами и технологиями для достижения целей защиты. Неотъемлемой частью работ по обеспечению корпоративной безопасности от внутренних утечек является проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его. Для этого специалисты должны уметь проводить весь цикл работ по установке, развёртыванию, настройке, использованию DLP-систем, включая разработку политик информационной безопасности, классификацию объектов защиты, применение технологий фильтрации различных видов трафика, фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.

Важным направлением обеспечения безопасности корпоративной информации – реализация прозрачного доступа к территориальнораспределенным информационным ресурсам компании через сети связи общего пользования, в том числе Интернет. Для защиты передаваемых данных используется технологии виртуальной частной сети (Virtual Private Network, VPN) и межсетевого экранирования, включая:

- защиту информации, передаваемой по каналам связи;
- защиту сети в целом, ее сегментов от несанкционированного доступа, как из внешних, так и из внутренних сетей;
- контроль трафика между узлами VPN-сети, включая фильтрацию трафика; • использование в качестве транспортной среды передачи данных каналы сетей связи общего пользования;
- возможность модернизации, модульного наращивания VPN-сети;
- централизованное управление VPN-сетью. Для предотвращения и минимизации последствий атак на корпоративную инфраструктуру и объекты защиты, необходимо их своевременное выявление и правильная классификация с использованием технологий класса IDS (Intrusion Detection System).

Помимо перечисленного, специалист по корпоративной безопасности должен уметь подготовить отчёты о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой) менеджменту организации, которую защищает, а также правильно оценить угрозы и риски информационной безопасности

2.Сфера деятельности

Информационно-коммуникационные технологии

3. Перечень программ по компетенции

1.Дополнительная профессиональная программа профессиональной переподготовки «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных VPN технологий (с учётом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»

2Дополнительная профессиональная программа повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учётом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»