Строим систему противодействия угрозам из киберпространства

Андрей Масалович, *советник генерального директора по конкурентной разведке, АО "ДиалогНаука"*

● Хакеры похитили пароли ключевых сотрудников компании и опубликовали фрагменты весьма чувствительной внутренней переписки.
● Злоумышленник организовал в социальных сетях "ссылочный взрыв", и буквально весь Интернет сейчас обсуждает, как на этаже вашей клиники среди бела дня бегает крыса.
● Конкуренты сумели подключиться к внешним серверам обслуживания вашей системы видеонаблюдения – и теперь контролируют каждый ваш шаг.
● Бывший сотрудник уволился нелояльным – и прихватил с собой вашу клиентскую базу.

Что роднит приведенные выше примеры (кстати, взятые из практики)? Во всех случаях места возникновения, развития и преодоления проблем расположены во внешнем киберпространстве, за пределами контролируемой зоны вашей организации. И второе важное отличие – во всех перечисленных случаях служба информационной безопасности, даже если она своевременно обнаружит угрозу (ну, вдруг), не способна ей противостоять – нужны личные усилия руководителей или мобильных штабов корпоративного уровня.

Оборона и разведка

Как обеспечить руководителя современными эффективными средствами раннего предупреждения и противодействия угрозам из киберпространства? Основу таких инструментов (по сути – оборонительного и разведывательного корпоративного кибероружия) составляют системы контроля оперативной обстановки. Пришедшие на смену традиционным службам интернет-мониторинга, такие системы должны обеспечивать руководителю возможность обнаруживать и нейтрализовать различные виды атак из киберпространства.

Современная система контроля

Перечислим основные требования, определяющие облик современной системы контроля оперативной обстановки:

1. Контроль оперативной обстановки в Интернете и социальных сетях.

Система автоматически собирает наиболее важные новости по тематике, определенной руководителем, в том числе факты подготовки и проведения кибератак, уровень собственной защищенности, угрозы бизнесу, репутации и устойчивому развитию компании.

2. Удобный интерфейс руководителя для презентационных экранов, а также планшетов и смартфонов.

Руководитель входит в систему по защищенному каналу из любого места – офиса, автомобиля, в командировке и др. Каждая новость представлена в удобном интерфейсе, с фотографией, заголовком, кратким содержанием, датой и временем появления, ссылкой на первоисточник и текущим количеством дублей в СМИ.

3. Автоматическое определение уровня угроз.

Каждый тематический блок снабжен индикаторами уровня угроз – т.н. "светофорами":
● серый – ничего важного;
● зеленый – были интересные новости, стоит посмотреть;
● желтый – важные новости, их надо прочесть обязательно;
● красный – активная угроза, нужна немедленная реакция.

4. Автоматическое ведение досье на объекты интереса.

Система автоматически ведет досье на различные объекты интереса – людей и компании, а также накапливает данные об аккаунтах в соцсетях, адресах и телефонах, банковских счетах, офисах, автомобилях и т.д. – всего более сорока видов объектов.

5. Выявление связей объектов и первоисточников новостных вбросов.

Система позволяет выявлять разнообразные связи объектов интереса – родственные, деловые, дружеские, активности в соцсетях и другие, в том числе скрытые.

6. "Тепловая карта" враждебной активности в социальных сетях.

Система отслеживает ход распространения информации и строит т.н. "тепловые карты" позитивной и негативной активности обсуждения ключевых новостей.

7. Выявление резонансных тем в социальных сетях и СМИ.

Система позволяет проводить сравнительный анализ упоминаний различных персон и компаний, активности обсуждения целевых новостей в СМИ и социальных группах.

8. Управление работой мобильных штабов.

Система позволяет в самые сжатые сроки организовывать работу мобильных оперативных штабов (в том числе совещаний удаленных подразделений, межведомственных групп и т.д.).

9. Работа с большими данными (Big Data).

Система позволяет проводить сложную аналитическую обработку больших объемов данных и отображать итоговые результаты в удобном графическом виде.

10. Автоматическая генерация дайджестов и отчетов.

Справки, дайджесты и отчеты по заданным темам и активности объектов интереса формируются автоматически.

В мире множатся системы с перечисленными характеристиками, основанные на программах класса Palantir, IBM i2, Watson Analytics и других. В России "первой ласточкой" в новом классе

Смартфон руководителя крупной компании, оснащенный системой "Лавина Пульс"

мобильных центров руководителя можно назвать отечественную систему интернет-мониторинга "Лавина Пульс". Возможности системы по раннему обнаружению и пресечению информационных атак уже оценили более 80 заказчиков. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА" см. стр. 56