уникнути цього, користувачі можуть або закрити порт 11211 за допомогою фаєрвола, або настроїти memcached-сервер, щоб він міг використовуватися тільки з локального хоста.

Список бібліографічних посилань

1. Виды взломов сайтов и их предотвращение // Captcha.Ru. URL: http://captcha.ru/articles/antihack/ (дата звернення: 10.10.2018).

2. Виды хакерских атак // Хакерские Атаки URL: https://sites.google.com/site/hakerskieataki/home/vidyhakerskih-atak (дата звернення: 10.10.2018).

Одержано 30.10.2018

УДК 343.9

Дмитро Юрійович УЗЛОВ,
кандидат технічних наук,
начальник Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області;
ORCID: https://orcid.org/0000-0003-3308-424X;
Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент
завідуючий кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0003-4722-3159;
Олексій В'ячеславович ВЛАСОВ,
заступник начальника Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ЗЛОЧИННОСТІ

Інформаційний злочин – це навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. Інформаційні злочини включають до себе досить широкий спектр протиправної діяльності:

– шахрайство;

– незаконне копіювання;

– поширення шкідливих вірусів;

– злом паролів;

– крадіжка номерів банківських карт і інших банківських реквізитів;

– фішинг;

– поширення протиправної інформації (наклепу, матеріалів порнографічного характеру, матеріалів, що збуджують міжнаціональну та міжрелігійну ворожнечу і т.п.);

– зміна комп'ютерних даних;

– комп'ютерний саботаж або шкідливе втручання через комп'ютерні мережі в роботу різних систем;

– несанкціонований доступ, перехоплення даних та багато інших.

У 2005 році була створена та запроваджена серія міжнародних стандартів інформаційної безпеки, що опубліковані спільно Міжнародною Організацією зі стандартизації (ISO) та Міжнародною електротехнічною Комісією (IEC). Центральне місце в цій серій полягає ISO/IEC 27001 – міжнародний стандарт в галузі IT, який встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті будь-якої організації. Вимоги, викладені в ISO / IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру. Згідно цих нормативів, ефективна протидія інформаційним злочинам полягає в наступних діях:

– організація захисту від впливу вірусного програмного забезпечення;

– організація захисту від апаратного перешкоджання роботі пристроїв;

– відновлення працездатності програмно-апаратних комплексів після шкідливого втручання або збоїв в роботі обладнання;

– виявлення, моніторинг та попередження шкідливого втручання;

– захист програмного забезпечення на стороні клієнта, сервера або проміжних шарів;

– захисті мереж та протоколів обміну даних;

– розробка та впровадження політик безпеки внутрішніх та зовнішніх мереж;

– контроль доступу, ідентифікації та автентифікації.

Типовими підходами до реалізації програм протидії злочинам в інформаційній сфері є:

– виявлення загроз та їх класифікація;

– аналіз та вивчення досвіду інцидентів порушення безпеки;

– розробка технологій моніторингу та попередження атак;

– розробка технологій протидії атакам у момент скоєння;

– розробка технологій прогнозування атак.

Ідеологія цього стандарту побудована за необхідності глибинного вивчення та аналізу існуючих обставин та виявленні актуальних загроз інформаційній безпеці. Це все стає можливим лише після опрацювання значних масивів накопичених даних різноманітного характеру, що відтворюють або документують наслідки шкідливого впливу на інформаційні системи. Найбільш придатними для цього виявились технології добування даних (або Data Mining / інтелектуальний аналіз даних), які здійснюються шляхом виявлення прихованих (нетривіальних, раніше невідомих та потенційно корисних) закономірностей або взаємозв'язків між об’єктами, подіями та процесами у великих масивах даних. Інтелектуальний аналіз даних здійснюється автоматично шляхом застосування методів математичної

статистики, штучних нейронних мереж, розпізнавання образів, теорії нечітких множин або генетичних алгоритмів.

Інтелектуальний аналіз даних застосовується до таких проблем, як:

– виявлення вторгнень і аудит безпеки, аналіз веб-логів, а також аналіз даних аудиту (ґрунтуючись на результатах аналізу даних, можна потім визначити, чи відбулися якісь спроби несанкціоновані вторгнення та/або були здійснені будь-які несанкціоновані запити);

– аналіз зв'язків може бути використаний для відстеження шкідливого коду, що поширюється самостійно по відношенню до його авторів;

– групування за визначеними критеріями та без чітко визначених ознак може бути використано для виявлення різних груп кібер-атак, з подальшим використанням отриманих моделей для протидії атакам в момент, коли вони безпосередньо відбуваються;

– прогнозування може бути використано для визначення потенційних атак у майбутньому;

– отримання інформації про зловмисників за допомогою електронної пошти та телефонних розмов;

– підтримка прийняття рішень і збереження конфіденційності інформації.

Інтелектуальний аналіз даних в межах систем виявлення вторгнень застосовується для трьох цілей:

– зниження кількості хибнопозитивних спрацювань системи;

– виявлення аномалій;

– виявлення шаблонів атак.

Основні напрямки використання інтелектуального аналізу даних в сфері веб-безпеки:

– виявлення атак шляхом пошуку аномалій в логах веб-сервера або веб-проксі;

– виявлення шкідливих інтернет-сторінок;

– зниження хибнопозитивних спрацьовувань при скануванні вразливостей веб-сайту;

– виявлення фішингових веб-сайтів.

Основні напрямки застосування інтелектуального аналізу даних при аутентифікації:

– виявлення аномалій в процесі аутентифікації;

– біометрична аутентифікація;

– автоматична кореляція подій інформаційній безпеки.

Основні напрямки застосування інтелектуального аналізу даних при побудові систем автоматичної кореляції подій інформаційній безпеки:

– зниження кількості хибнопозитивних подій інформаційній безпеки перед кореляцією;

– кореляція на основі угруповання подій, за допомогою дерева рішень, навчаючись на вже наявних події і їх атрибутах;

– кореляція на основі групування подій інформаційній безпеки без чітко визначеного критерію на основі помилок відновлення за допомогою нейронних мереж;

– кореляція на основі навчання моделі і побудови шаблонів помилкових і істинних подій, заснованих на помічених системним оператором даних.

Список бібліографічних посилань

1. Узлов Д. Ю. Використання методів і моделей інтелектуальної обробки неструктурованої криміналістичної інформації // Інтелектуальні системи та прикладна лінгвістика : матеріали III Всеукраїнської науково-практичної конференції. Харків : НТУ «ХПІ», 2014. С. 13-15.

2. Manning C. D., Raghavan P., Schütze H. Introduction to Information Retrieval. Cambridge : Cambridge University Press, 2008. 544 p.

3. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies. New York : CRC Press Taylor & Francis Group, 2009. 440 p.

Одержано 02.11.2018

УДК 343.98

Станіслав Олександрович ФІЛІППОВ,
кандидат психологічних наук, доцент, докторант
Національної академії Державної прикордонної служби України;
ORCID: https://orcid.org/0000-0001-6700-4194

ЗНАЧЕННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОТИДІЇ ТРАНСКОРДОННІЙ ЗЛОЧИННОСТІ

Своєчасна та повна необхідна інформація про осіб, що перетинають державний кордон, забезпечує функціонування системи протидії транскордонній злочинності саме у той спосіб, що відповідає характеристикам оптимальності та ефективності. Беззаперечним чинником, що детермінує дієвість системи прикордонної безпеки, є наявність умов, за яких застосування персональних даних і документів для вчинення транскордонних кримінальних правопорушень або взагалі є неможливим, або створює можливості для їх подальшого припинення. На посилення цієї дієвості працює впровадження біометричних технологій у виготовлення документів для виїзду за кордон (далі – проїзних документів). Це дозволяє не тільки підняти рівень їх захисту, а також забезпечує можливість ідентифікації за таким набором персональних даних, що виключає помилку. У свою чергу, це значно посилює можливості як запобігання злочинності, так і припинення окремих злочинів.

І. Підроблені документи під час перетину державного кордону використовуються у вчиненні таких кримінальних правопорушень як торгівля людьми або інша незаконна угода щодо передачі людини; контрабанда; виготовлення, зберігання, придбання, перевезення,