УДК 004.056

ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Петржиковский В. Д.

Российский университет транспорта (МИИТ), Москва, Россия (127994, г. Москва, ул. Образцова, д. 9, стр. 9), e-mail: student.ui.miit@mail.ru

В статье рассмотрены два происшествия в сфере железнодорожного транспорта, показана корреляция между информационной безопасностью и функционированием транспортных систем. Первый инцидент произошел в городе Сакраменто (штат Калифорния) 19 ноября 2017 г. Транспортная компания подверглась атаке, которая уничтожала данные. Это обстоятельство привело к задержкам в движении не только поездов, но и автобусов. Сеть железных дорог в Германии была погружена в хаос, из-за атаки, затронувшей весь мир. Реализация данной кибератаки осуществилась с помощью вредоносной программы WannaCry. В статье представлены методы по пресечению угроз информационной безопасности или по максимальному снижению причиненного вреда в случае успешной реализации атаки. Для корректного функционирования транспорта необходимо, чтобы руководители организаций и служб безопасности уделяли повышенное внимание на соответствие квалификации сотрудников и занимаемых ими должностей. Так как из-за неквалифицированных действий в обеспечение информационной безопасности возможна реализация угроз. Специалистам необходимо следить за последними веяниями и тенденциями в сфере разработки программных продуктов в области информационной безопасности. В статье отмечена важность своевременной установки обновлений для системы безопасности, выпускаемых производителями программного обеспечения.

Ключевые слова: информационная безопасность, уязвимости, угрозы, методы противодействия.

INCIDENTS OF INFORMATION SECURITY IN RAILWAY TRANSPORT

Petrzhikovskiy V. D.

Russian University of Transport (RUT - MIIT), Moscow, Russia

(127994, Moscow, Obrastsova str., 9, bld. 9), e-mail: student.ui.miit@mail.ru

The article considers two incidents in the field of railway transport, shows the correlation between information security and the functioning of transport systems. The first incident occurred in the city of Sacramento (California) on November 19, 2017. The transport company was attacked, which destroyed the data. This circumstance led to delays in the movement of not only trains, but also buses. The railway network in Germany was plunged into chaos, due to the attack that affected the whole world. The implementation of this cyber-attack was carried out using a malicious program WannaCry. The article presents methods to curb threats to information security or to minimize the harm caused in the event of a successful attack. For the correct functioning of transport, it is necessary that the heads of organizations and security services pay special attention to the qualifications of the staff and the positions they occupy. Since, due to unqualified actions in ensuring information security, the realization of threats is possible. Professionals need to follow the latest trends and trends in the development of software products in the field of information security. The article notes the importance of timely installation of security updates produced by software manufacturers.

Keywords: information security, vulnerabilities, information security threats, countermeasures.

Транспортная система — это основа работы экономики в любой стране. Она, как и любые другие утилитарно-инфраструктурные отрасли, дает возможность другим несмежным отраслям нормально функционировать. Поэтому транспортная инфраструктура испытывает колоссальные нагрузки и вопрос безопасности, в том числе и информационной, стоит рассматривать в первую очередь.

Актуальность темы заключается в том, что информатизация и автоматизация все теснее проникают в нашу жизнь, и транспортные системы — не исключение.

Цель работы — проанализировать инциденты на транспорте и показать, насколько велико влияние угроз из сферы информационной безопасности [1] на функционирование транспортной системы в целом.

Инцидент 1. Рассмотрим ситуацию, возникшую в городе Сакраменто, штат Калифорния 19 ноября 2017 г. [6]. Компания *Sacramento Regional Transit* (SacRT) управляет общественным транспортом в Сакраменто, включающим более 60 автобусных маршрутов и систему легкорельсового транспорта. Система Light Rail Sacramento RT состоит из трех железнодорожных линий, 54 станций и 76 транспортных средств, и является одной из самых загруженных в Соединенных Штатах Америки.

Неустановленные злоумышленники совершили атаку на управляющие сервера компании SacRT, уничтожив часть информации, содержащейся на них, и требовали вознаграждения в 1 биткоин (стоит около 8000 долларов), угрожая полностью парализовать работу транспортной системы.

Хакеры объявили о своем присутствии в субботу (18 ноября 2017 г.), когда они взломали главную веб-страницу транспортного агентства Сакраменто, добавив заметку, в которой говорилось: «I’m sorry to modify the home page, i’m good hacker, i I just want to help you fix these vulnerability. This is one of the loopholes, modify the home page ...» («Извините, что изменил домашнюю страницу, я хороший хакер, я просто хочу помочь вам устранить эту уязвимость. Это одна из лазеек, изменение домашней страницы ...»). Данное сообщение оказалось ловушкой. Когда технические специалисты вошли в систему SacRT, чтобы проверить ущерб, хакер реализовал атаку в воскресенье утром, которая уничтожила виртуальные серверы.

В результате атакующие уничтожили базу данных, содержащую в себе информацию, отвечающую за работоспособность планировщика маршрутов автобусов и поездов. Так как работа поездов происходила в автоматическом режиме, то произошли задержки в их движении. Также была уничтожена информация о сотрудниках компании.

В прошлом система транспортного агентства страдала от вирусных и вредоносных атак, но никогда не подвергалась атаке, которая уничтожала данные. Руководство агентства

планирует привлечь эксперта для анализа уязвимостей и уменьшения вероятности повторения произошедшего инцидента.

Как этого можно было избежать? Следовало использовать системы обнаружения и предотвращения вторжений, работающих по принципу выявления аномальных состояний системы и на основе анализа поведения пользователя.

Система обнаружения вторжений (IDS) обеспечивает сеть с превентивной защитой от любых подозрительных действий. IDS достигает этой цели с помощью ранних предупреждений, направленных на системных администраторов. Однако в отличие от IPS, она не предназначена для блокировки атак.

Система предотвращения вторжений (IPS) — это устройство, которое контролирует доступ к ИТ-сетям для защиты систем от атак и неправомерного доступа. Она предназначена для анализа данных атаки и принятия соответствующего действия, блокировки атаки на ранних этапах ее реализации, например, создания ряда правил в корпоративном брандмауэре.

Данные системы в настоящее время активно начали использовать искусственный интеллект для снижения вероятности ложных срабатываний.

Инцидент 2. Проведем анализ ситуации, возникшей из-за утечки инструмента, разработанного для внутренних задач агентством национальной безопасности США. Инцидент получил международное внимание средств массовой информации, поскольку экраны информации о пассажирах на вокзалах были заражены вирусом [2]. Сеть железных дорог в Германии была погружена в хаос, из-за атаки, затронувшей весь мир [7]. В мае 2017 г. германская компания Deutsche Bahn AG, являющаяся основным железнодорожный оператором, была атакована с использованием вируса WannaCry. Хакеры размещали текст на экранах информации станций, в которых требовались деньги выкупа.

Злоумышленники, эксплуатируя уязвимость под названием *ETERNALBLUE*, зашифровали данные, на серверах, точках продаж билетов POS (*point of sale*), а также на экранах, показывающих информацию о передвижении поездов.

Инициаторы атаки потребовали 600 долл. США для расшифрования закодированной информации. На устранение последствий атаки у департамента информационных технологий ушло двое суток.

На карте (рис. 1) показаны страны, затронутые в первые несколько часов кибератаки, согласно исследованиям «Лаборатории Касперского», а также Австралии, Швеции и Нью-Йорка [4]. В России были атакованы банки, российские железные дороги (РЖД) и сеть мобильных телефонов. Министерство внутренних дел России заявило, что 1000 его компьютеров были заражены, но вирус был быстро обнаружен и блокирован, и не было

утечки конфиденциальной информации. Автопроизводитель Renault Renault был вынужден прекратить производство на нескольких объектах. Также были атакованы:

– крупные испанские фирмы - такие как телекоммуникационные гиганты Telefonica и коммунальные услуги Iberdrola и Gas Natural;

– университетская компьютерная лаборатория в Италии;

– местный орган власти в Швеции;

– компания доставки FedEx в Великобритании;

– школы в Китае и больницы в Индонезии и Южной Корее и т.д.

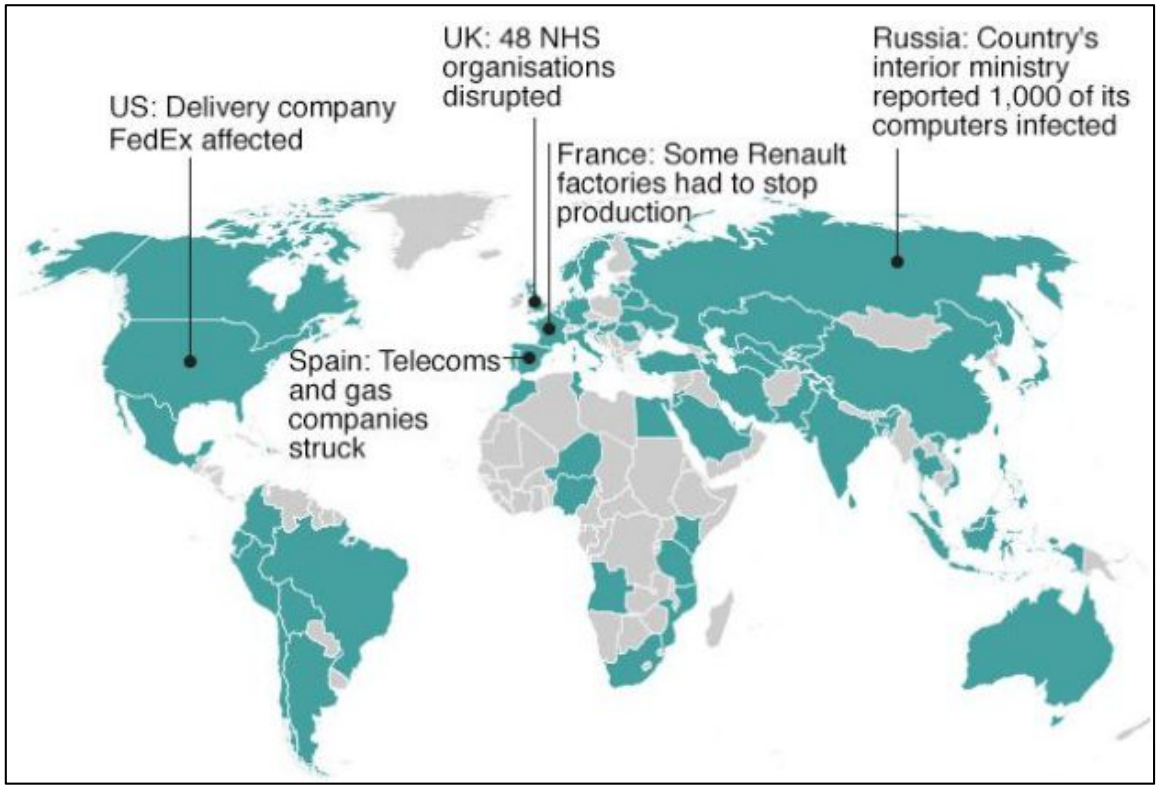

Рис. 1. Страны, в которых были совершены атаки с помощью вредоносной программы *WannaCry* в первые часы инцидента

На основе уроков, извлеченных из инцидента с вирусом WannaCry, в рамках Deutsche Bahn, был разработан план, в котором была усилена безопасность, разработаны меры по противодействию потенциальным будущим кибератакам. Безопасность стала одним из самых важных приоритетов для руководства компании, была расширена команда по кибербезопасности, в которой по-прежнему остается множество открытых вакансий.

Как этого можно было избежать? Данной уязвимости подвержен протокол SMB V1. Поскольку атакующие использовали уязвимость нулевого дня, то классические антивирусные программы, использующие сигнатурный принцип определения вторжений, не

имели возможность отразить атаку. Корпорация Microsoft выпустила патч [5], закрывающий уязвимость в Microsoft Windows 14 марта — за несколько месяцев до произведенной атаки.

Анализируя график (рис. 2), где по оси абсцисс отмечена версия операционной системы, по оси ординат число успешно атакованных устройств, можно заметить, что более всего пострадали электронные вычислительные машины (ЭВМ) под управлением Microsoft Windows Server 2008 R2, основная поддержка которой закончился 13 января 2015 г. (табл. 1) [3].

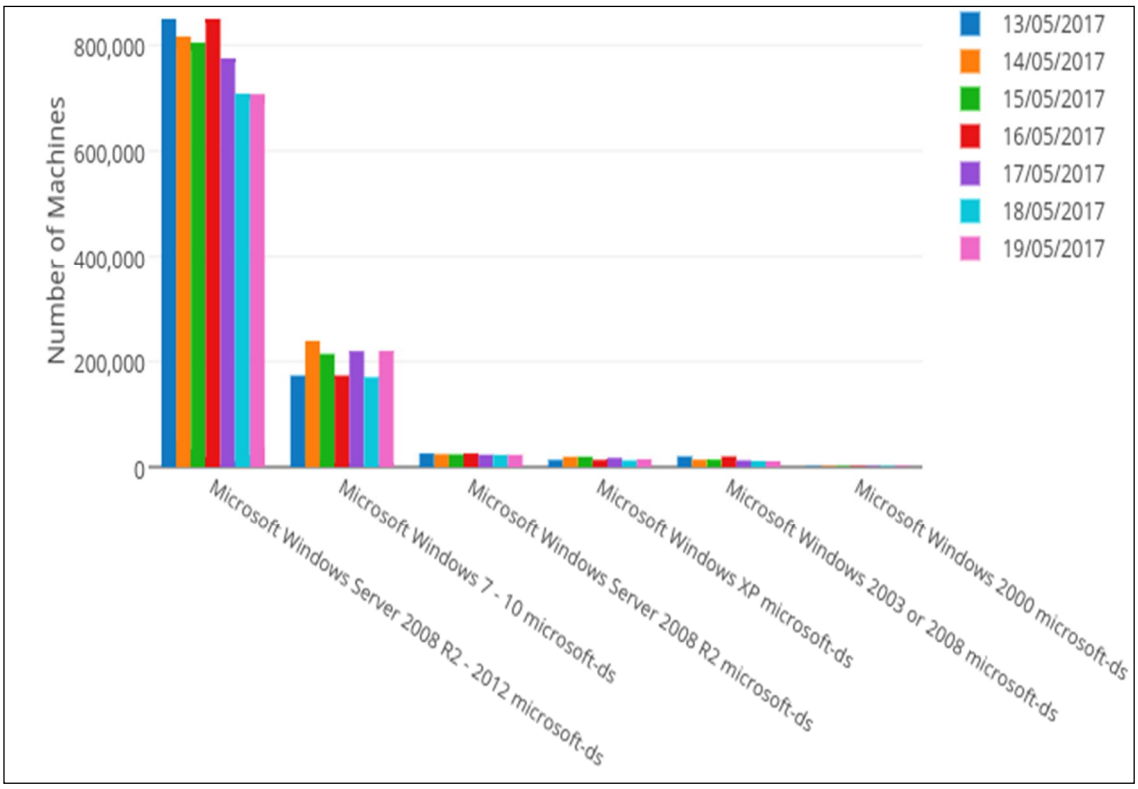

Рис. 2. Результаты атаки с помощью вредоносной программы *WannaCry*

Табл.1. Основные продукты, для которых осуществляется переход от основной фазы поддержки к расширенной

Продукты	Дата прекращения поддержки
Windows 7 Корпоративная Windows 7 Корпоративная N Windows 7 Домашняя Windows 7 Домашняя расширенная Windows 7 Профессиональная Windows 7 Профессиональная N Windows 7 Начальная	Основная фаза поддержки завершается 13.01.15 г.

Windows 7 Начальная N Windows 7 Максимальная Windows 7 Максимальная N	
Windows Server 2008 Datacenter Windows Server 2008 Datacenter без Hyper-V Windows Server 2008 Enterprise Windows Server 2008 Enterprise без Hyper-V Windows Server 2008 for Itanium-Based Systems Windows Server 2008 Foundation Windows Server 2008 R2 Datacenter Windows Server 2008 R2 Enterprise Windows Server 2008 R2 for Itanium-Based Systems Windows Server 2008 R2 Standard Windows Server 2008 Standard Windows Server 2008 Standard без Hyper-V	Основная фаза поддержки завершается 13.01.15 г.
Windows Storage Server 2008 Basic Windows Storage Server 2008 Basic (32-разрядная версия) Windows Storage Server 2008 Basic Embedded Windows Storage Server 2008 Basic Embedded (32-разрядная версия) Windows Storage Server 2008 Enterprise Windows Storage Server 2008 Enterprise Embedded Windows Storage Server 2008 R2 Windows Storage Server 2008 R2 Essentials Windows Storage Server 2008 Standard Windows Storage Server 2008 Standard Embedded Windows Storage Server 2008 Workgroup Windows Storage Server 2008 Workgroup Embedded	Основная фаза поддержки завершается 13.01.15 г.

Экономия на обновлении версий программного обеспечения нецелесообразна ввиду репутационных потерь и снижения доступности услуг компании потребителям и как следствие финансовые потери. Данная атака было реализована из-за некорректной конфигурации систем защиты информационной сети предприятия.

Рассмотрим шаги, предотвратившие или снизившие время на восстановление работоспособности информационной системы.

1. Правильно сконфигурированная система обновлений исключила бы возможность эксплуатирования уязвимости в протоколе SMB V1, закрытой задолго до начала атаки.

2. Система обнаружения вторжений (IDS), обнаружив не характерную активность ввода-вывода в дисковой подсистеме, уведомила бы системного администратора о начале атаки.

3. Правильная конфигурация маршрутизирующего устройства вкупе с использованием Firewall исключила бы использование данного протокола неавторизованным лицом извне локальной вычислительной сети (ЛВС).

4. Грамотное использование мандатного управления доступа предотвратило бы повреждение большей части информации.

Мандатное управление доступом (MAC) — это тип контроля доступа, который жестко закодирован в операционную систему, как правило, на уровне ядра. MAC может применяться к любому объекту или запущенному процессу в операционной системе, также MAC позволяет сохранять высокий уровень контроля над объектами и процессами операционной системы. Мандатное управление доступом может применяться к каждому объекту и может управлять доступом процессов, приложений и пользователей к нему (рис 3).

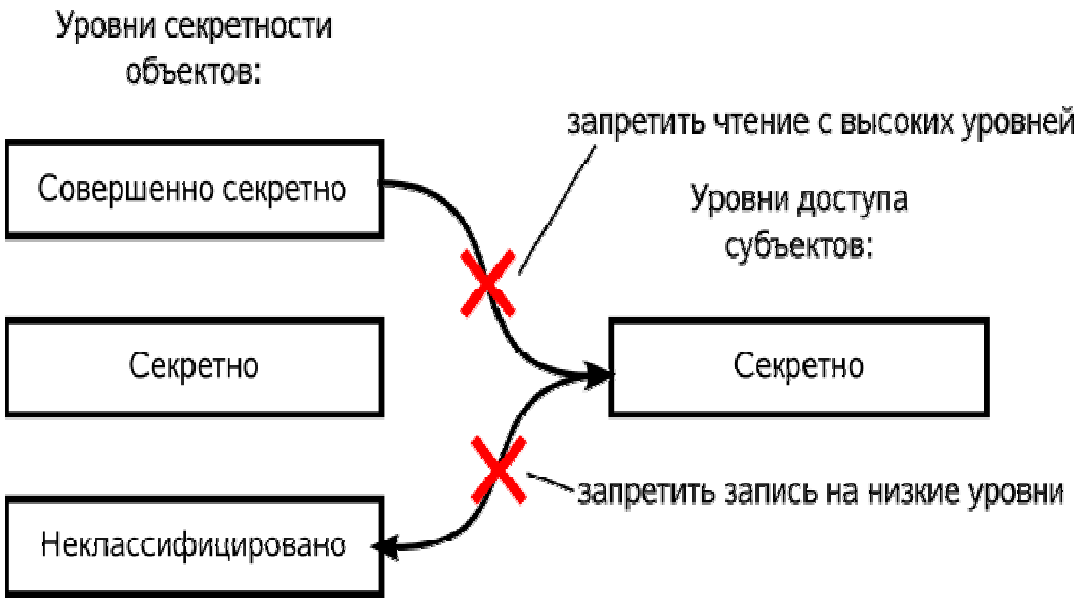

Рис. 3. Мандатное управление доступом

Критерии MAC определяются системным администратором, строго соблюдаются операционной системой (ОС) или ядром безопасности и не могут быть изменены конечными пользователями.

Механизм принудительного контроля доступа (MAC) ограничивает способность субъекта (пользователей или процессов) получать доступ или выполнять какую-либо операцию над объектами (файлы, каталоги, порты TCP/UDP и т.д.). Объекты и субъекты имеют набор атрибутов безопасности. Всякий раз, когда субъект пытается получить доступ к объекту, правило авторизации, выполняемое ядром операционной системы, проверяет данные атрибуты безопасности и решает, может ли доступ субъект получить доступ.

Литература

1. Груздева Л. М. Основы информационной безопасности: учеб. пособие/ Л.М. Груздева. - М.: Юридический институт МИИТа, 2018. - 101 с.
2. Монахов, Ю.М. Вредоносные программы в компьютерных сетях: учеб. пособие / Ю.М. Монахов, Л.М. Груздева, М.Ю. Монахов; Владим. гос. ун-т. - Владимир: Изд-во Владим. гос. ун-та, 2010. – 72 с.
3. Продукты, поддержка которых прекращается во второй половине 2014 г. [Электронный ресурс] // support.microsoft.com: сайт. – URL: https://support.microsoft.com/en-us/gp/support-reaching-end-2nd/ru (дата обращения: 27.11.2018).
4. Cyber-attack: Europol says it was unprecedented in scale [Электронный ресурс] // bbc.com: сайт. – URL: https://www.bbc.com/news/world-europe-39907965 (дата обращения: 27.11.2018).
5. Microsoft Security Bulletin MS17-010 – Critical [Электронный ресурс] // docs.microsoft.com: сайт. – URL: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010 (дата обращения: 27.11.2018).
6. Hackers attack Sacramento transit system and demand $8,000 ransom [Электронный ресурс] // sacbee.com: сайт. – URL: http://www.sacbee.com/news/local/article185669953.html (дата обращения: 27.11.2018).
7. WannaCry virus was ‘wake-up call’ for railway industry [Электронный ресурс] // railtech.com: сайт. – URL: https://www.railtech.com/all/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/ (дата обращения: 27.11.2018).