ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо зберігання і використання інформації в сучасному інформаційному суспільстві.

У публікації «Информационная безопасность предприятия: ключевые угрозы и средства защиты» наведено роз'яснення, що таке інформаційна безпека, причини виникнення загроз, методи захисту інформації та вибір інструментів забезпечення безпеки інформації.

У публікації «WannaCry (вирус-вымогатель)» розповідається як він працює, ймовірні розробники, припущення хто винен, приклади атак, використання інших вірусних програм та їх маскування. Як захистити свій комп'ютер.

У публікації «Горячая пора: Пересмотренный стандарт ISO 15489 и будущее управления документами» розповідається про завдання та мету перегляду стандарту ISO 15489, як вони враховані в його новій редакції 2016 року.

У публікації «Штат Новый Южный Уэльс, Австралия: 10 основных цифровых тенденций, влияющих на управление документами, информацией и контентом» розповідається про вплив сучасних цифрових тенденцій на управління документами, інформацією та контентом.

У публікації «Готовящиеся технические отчеты ИСО: Документы в облаке» розповідається про розробку рекомендацій щодо впровадження базової моделі менеджменту питань безпеки, а також правових і технічних проблем, що стосуються документів.

У публікації «Китай: Новые стандарты в области архивного дела и управления документами» розповідається про затвердження в Китаї відразу 12 нових галузевих стандартів. Архівам всіх рівнів наказується забезпечити впровадження цих вимог на практиці.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ: КЛЮЧЕВЫЕ УГРОЗЫ И СРЕДСТВА ЗАЩИТЫ

Источник: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html

Всем известно высказывание «Кто владеет информацией, тот владеет миром». А кто владеет информацией о конкурентах, получает беспрецедентные преимущества в борьбе с ними. Прогресс сделал компании зависимыми от информационных систем, а вместе с этим – уязвимыми к атакам хакеров, компьютерным вирусам, человеческому и государственному фактору в такой степени, что многие владельцы бизнеса уже не могут чувствовать себя в безопасности. Вопрос информационной безопасности становится краеугольным камнем в деятельности организации, но этот же прогресс предлагает решения, способные защитить данные от внешних посягательств.

Что такое информационная безопасность и почему системы ее обеспечения так важны

Так что же такое информационная безопасность? Обычно под ней понимают защищенность информации и всей компании от преднамеренных или случайных действий, приводящих к нанесению ущерба ее владельцам или пользователям. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности.

Любая утечка информации может привести к серьезным проблемам для компании – от значительных финансовых убытков до полной ликвидации. Конечно, проблема утечек появилась не сегодня, промышленный шпионаж и переманивание квалифицированных специалистов существовали еще и до эпохи компьютеризации. Но именно с появлением ПК и интернета возникли новые приемы незаконного получения информации. Если раньше для этого необходимо было украсть и вынести из фирмы целые кипы бумажных документов, то сейчас огромные объемы важных сведений можно запросто слить на флэшку, помещающуюся в портмоне, отправить по сети, прибегнув к использованию семейства руткитов, троянов, бэкдоров, кейлоггеров и ботнетов, либо просто уничтожить посредством вирусов, устроив диверсию.

Чаще всего «утекают» из компаний документы финансового характера, технологические и конструкторские разработки, логины и пароли для входа в сеть других организаций. Но серьезный вред может нанести и утечка персональных данных сотрудников. Особенно это актуально для западных

стран, где судебные иски из-за таких утечек нередко приводят к огромным штрафам, после выплаты которых компании терпят серьезные убытки.

Это интересно

В июле 2017 года произошла одна из крупнейших утечек персональных данных в бюро кредитной истории Equifax в США. В руки злоумышленников попали личные сведения более чем 143 млн потребителей, 209 000 номеров кредитных карт. В результате, по данным на 8 сентября 2017 года, акции бюро упали на 13%[1].

Случается и так, что утечка приносит вред компании через несколько месяцев или лет после того, как она произошла, попав в руки конкурентам или журналистам. Именно поэтому защита должна быть комплексной. Не стоит делить информацию на очень важную и менее важную. Все, что касается деятельности компании и не предназначено для опубликования, должно оставаться внутри компании и быть защищено от угроз.

Актуальные виды угроз информационной безопасности

Аналитический центр InfoWatch опубликовал данные по утечке данных в России за 2016 год. Согласно исследованию, СМИ обнародовали 213 случаев утечек информации из российских госорганов и компаний, что составляет 14% от общемирового количества утечек. Самые частые случаи – это утечка платежной информации и персональных данных – 80%. В 68% случаев виновными оказываются сотрудники организаций, и только в 8% – руководство. По сравнению с 2015 годом количество утечек выросло на 89%. На сегодня Россия занимает второе после США место в списке стран, наиболее сильно страдающих от утечек информации[2].

Но из-за чего чаще всего возникают угрозы информационной безопасности?

1. Невнимательность и халатность сотрудников.

Угрозу информационной безопасности компании, как ни странно, могут представлять вполне лояльные сотрудники и не помышляющие о краже важных данных. Непредумышленный вред конфиденциальным сведениям причиняется по простой халатности или неосведомленности работников. Всегда есть возможность того, что кто-нибудь откроет фишинговое письмо и внедрит вирус с личного ноутбука на сервер компании. Или, например, скопирует файл с конфиденциальными сведениями на планшет, флэшку или КПК для работы в командировке. И ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу. В такой ситуации информация оказывается весьма легкой добычей.

Это интересно

В 2010 году прототип смартфона iPhone 4 был оставлен в баре одним из сотрудников компании Apple Греем Пауэллом. До официальной презентации гаджета оставалось еще несколько месяцев, но нашедший смартфон студент продал его за 5000 долларов журналистам Gizmodo, сделавшим эксклюзивный обзор новинки.

2. Использование пиратского ПО.

Иногда руководители компаний пытаются сэкономить на покупке лицензионного ПО. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного ПО не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности. По данным исследования Microsoft, в 7% изученных нелицензионных программ было найдено специальное программное обеспечение для кражи паролей и персональных данных[3].

3. DDoS-атаки.

Distributed-Denial-of-Service – «распределенный отказ от обслуживания» – это поток ложных запросов от сотен тысяч географически распределенных хостов, которые блокируют выбранный ресурс одним из двух путей. Первый путь – это прямая атака на канал связи, который полностью блокируется огромным количеством бесполезных данных. Второй — атака непосредственно на сервер ресурса. Недоступность или ухудшение качества работы публичных веб-сервисов в результате атак может продолжаться довольно длительное время, от нескольких часов до нескольких дней. Обычно подобные атаки используются в ходе конкурентной борьбы, шантажа компаний или для отвлечения внимания системных администраторов от неких противоправных действий вроде похищения денежных средств со счетов. По мнению специалистов, именно кражи являются основным мотивом DDoS-атак. Мишенью злоумышленников чаще становятся сайты банков, в половине случаев (49%) были затронуты именно они.

На заметку

В 2016 году DDoS-атаки были зафиксированы в каждом четвертом банке (26%). Среди других финансовых структур вредному воздействию подверглось 22% компаний. Усредненный ущерб для кредитных организаций составил 1 172 000 долларов в расчете на банк[4].

4. Вирусы.

Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. По мнению экспертов, это можно объяснить появлением новых каналов проникновения вирусов. На первом месте по-прежнему остается почта, но, как показывает практика, вирусы способны проникать и через программы обмена сообщениями, такие как ICQ и другие. Увеличилось и количество объектов для возможных вирусных атак. Если раньше атакам подвергались в основном серверы стандартных веб-служб, то сегодня вирусы способны воздействовать и на межсетевые экраны, коммутаторы, мобильные устройства, маршрутизаторы. В последнее время особенно активны стали так

называемые вирусы-шифровальщики. Весной и летом этого года миллионы пользователей пострадали от атак вирусов WannaCry, Petya, Misha. Эпидемии показали, что жертвой вирусной атаки можно стать, даже если не открывать подозрительные письма. По информации Intel вирусом WannaCry заразились 530 тысяч компьютеров, а общий ущерб компаний составил более 1 млрд долларов[5].

5. Угрозы со стороны совладельцев бизнеса.

Именно легальные пользователи – одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими, а всех инсайдеров условно делят на несколько групп:

- ***«Нарушители»*** – среднее звено и топ-менеджеры, позволяющие себе небольшие нарушения информационной безопасности — играют в компьютерные игры, делают онлайн-покупки с рабочих компьютеров, пользуются личной почтой. Такая безалаберность способна вызвать инциденты, но чаще всего они являются непредумышленными. Кстати, большинство внешних атак происходят именно через личные почтовые ящики или ICQ сотрудников.

- ***«Преступники»***. Чаще всего инсайдерами являются топ-менеджеры, имеющие доступ к важной информации и злоупотребляющие своими привилегиями. Они самостоятельно устанавливают различные приложения, могут отсылать конфиденциальную информацию заинтересованным в ней третьим лицам и т.д.

- ***«Кроты»*** – сотрудники, которые умышленно крадут важную информацию за материальное вознаграждение от компании-конкурента. Как правило, это весьма опытные пользователи, умело уничтожающие все следы своих преступлений. Поймать их в силу этого бывает очень непросто.

- Еще одна категория – это ***уволенные и обиженные на компанию сотрудники***, которые забирают с собой всю информацию, к которой они имели доступ. Обычно украденная информация используется ими на новом месте работы, целенаправленная продажа данных в России пока не слишком актуальна.

6. Законодательные перипетии.

Государственные органы в России наделены правом конфисковать в ходе проверок оборудование и носители информации. Поскольку большая часть важных данных компании хранится в электронном виде на серверах, то в случае их изъятия компания на какое-то время просто останавливает свою деятельность. Простои при этом никто не компенсирует, а если проверка затягивается, большие убытки могут привести к прекращению деятельности фирмы. Изъятие оборудования – одна из острейших проблем современного бизнеса, при этом поводом для него может послужить все что угодно — от решения следователя до решения суда в рамках какого-либо уголовного дела.

Методы защиты информации

Хотя количество угроз постоянно растет, появляются все новые и новые вирусы, увеличивается интенсивность и частота DDoS-атак, разработчики средств защиты информации тоже не стоят на месте. На

каждую угрозу разрабатывается новое защитное ПО или совершенствуется уже имеющееся. Среди средств информационной защиты можно выделить:

Физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу.

Базовые средства защиты электронной информации. Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.

Анти-DDoS. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик. При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.

Резервное копирование данных. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в случае чрезвычайной ситуации, например, при изъятии сервера органами власти. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке.

План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты после восстановления данных. Сам процесс восстановления следует максимально отработать с учетом всех изменений системы.

Шифрование данных при передаче информации в электронном формате (end-to-end protection). Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования. Итак, защита информации должна осуществляться комплексно, сразу по нескольким направлениям.

Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.

Как выбрать инструменты обеспечения безопасности корпоративной информации

О выборе эффективных инструментов обеспечения информационной безопасности мы поговорили с Олегом Анатольевичем Наскидаевым, директором по развитию бизнеса компании DEAC, специализирующейся на предоставлении услуг по защите информации.

«Количество и изощренность угроз информационной безопасности ежегодно растет. Несмотря на то, что индустрия услуг по защите информации развивается, злоумышленникам иногда все же удается быть на шаг впереди. И происходит это не потому, что нет эффективных средств защиты или квалифицированных консультантов, способных решить проблему. Скорее, это происходит от того, что руководители компаний не до конца понимают необходимость защиты информационных ресурсов. Недостаточно просто установить антивирусные программы и ограничить доступ к тем или иным данным. Чтобы обеспечить максимальную конфиденциальность информации, придется создать многоуровневую систему ее защиты, и далеко не всегда с этой задачей может справиться собственный IT-отдел фирмы. В таком случае на помощь приходят специализированные компании, профессионально занимающиеся именно защитой информационных ресурсов.

Уже более 15 лет наша компания предлагает комплекс эффективных решений по защите данных. Во-первых, это резервное копирование данных Backup-as-a-Service (BaaS) и их хранение в облаке DEAC на базе одного или нескольких дата-центров. Мы гарантируем полную сохранность информации, а при возникновении у нашего клиента форс-мажорных обстоятельств резервные копии помогут в максимально короткие сроки восстановить жизненно важные для компании данные и избежать убытков.

Во-вторых, высокий уровень защиты данных, расположенных на инфраструктуре DEAC, вне зависимости от их расположения — как в России, так и в Европе — достигается дополнительно при помощи системы защиты от DDoS-атак. Это система, автоматически определяющая и блокирующая все известные виды DDoS-атак. Применение системы гарантирует непрерывность работы сети клиента и обеспечивает быстрое

время отклика на запросы реальных пользователей даже непосредственно во время атаки.

И в-третьих, мы предлагаем разработку плана аварийного восстановления (disaster recovery) ИТ-системы с учетом особенностей бизнеса каждой компании, анализируя риски и определяя важнейшие вопросы безопасности на межгосударственном уровне. План включает не только процедуру резервного копирования, но и комплекс действий для обеспечения непрерывного доступа к бизнес-информации компании».

P.S. Оператор дата-центров DEAC вышел на рынок в 1999 году. На сегодня компания имеет 6 отделений — в Лондоне, Амстердаме, Риге, Франкфурте. В штате DEAC работает более 100 высококвалифицированных экспертов, реализованы проекты более чем в 40 странах мира.

Источники:

1 http://www.tadviser.ru/index.php/Статья:DLP%3A_громкие_утечки_информации

2 http://d-russia.ru/wp-content/uploads/2017/06/InfoWatch_russian_report_2016.pdf

3 http://club.cnews.ru/blogs/entry/ugrozy_ispolzovaniya_piratskogo_rogrammnogo_obespecheniya

4 http://www.tadviser.ru/index.php/Статья:Distributed_Denial-of-Service,_DDoS_(отказ_от_обслуживания)

5 http://www.tadviser.ru/index.php/Статья:Вирус-вымогатель_%28шифровальщик%29

Мнение редакции

Вне всякого сомнения, облачные сервисы, в числе которых услуги резервирования, хранения и обработки данных, обеспечивают самую эффективную защиту информации и бесперебойность доступа к ней в сравнении с иными, локальными средствами информационной безопасности. К этому дата-центры обязывают строгие отраслевые стандарты.

WANNACRY (ВИРУС-ВЫМОГАТЕЛЬ)

Источник: www.tadviser.ru/index.php/Статья:WannaCry_(вирус-вымогатель)

WannaCry (также WannaCrypt или Wana) – вирус-вымогатель, получивший широкое распространение в 2017 году. Он является модифицированной версией вредоносной программы Агентства национальной безопасности США Eternal Blue.

Как работает

WannaCry распространяется через протоколы обмена файлами, установленных на компьютерах компаний и государственных учреждений. Программа-шифровальщик повреждает компьютеры на базе Windows.

Свыше 98% случаев инфицирования вымогательским ПО WannaCry приходятся на компьютеры под управлением Windows 7, причем более 60% заражений затрагивают 64-разрядную версию ОС. Такие данные обнародовали аналитики «Лаборатории Касперского». Согласно статистике, менее 1% зараженных компьютеров работают на базе версий Windows Server 2008 R2 и Windows 10 (0,03%).

После проникновения в папку с документами и другими файлами вирус шифрует их, меняя расширения на .WNCRY. Затем вредоносная программа требует купить специальный ключ, стоимость которого составляет от 300 до 600 долларов, угрожая в противном случае удалить файлы.

В целом WannaCry – это эксплойт, с помощью которого происходит заражение и распространение, плюс шифровальщик, который скачивается на компьютер после того, как заражение произошло.

В этом и состоит важное отличие WannaCry от большинства прочих шифровальщиков. Для того, чтобы заразить свой компьютер, обычным, скажем так, шифровальщиком, пользователь должен совершить некую ошибку – кликнуть на подозрительную ссылку, разрешить исполнять макрос в Word, скачать сомнительное вложение из письма. Заразиться WannaCry можно, вообще ничего не делая[1].

Создатели WannaCry использовали эксплойт для Windows, известный под названием EternalBlue. Он эксплуатирует уязвимость, которую Microsoft закрыла в обновлении безопасности MS17-010 от 14 марта этого года. С помощью этого эксплойта злоумышленники могли получать удаленный доступ к компьютеру и устанавливать на него собственно шифровальщик.

Если у вас установлено обновление и уязвимость закрыта, то удаленно взломать компьютер не получится. Однако исследователи «Лаборатории Касперского» из GReAT отдельно обращают внимание на то, что закрытие уязвимости никак не мешает работать собственно шифровальщику, так что, если вы каким-либо образом запустите его, патч вас не спасет.

После успешного взлома компьютера WannaCry пытается распространяться по локальной сети на другие компьютеры, как червь. Он сканирует другие компьютеры на предмет наличия той самой уязвимости, которую можно эксплуатировать с помощью EternalBlue, и если находит, то атакует и шифрует и их тоже.

Получается, что, попав на один компьютер, WannaCry может заразить всю локальную сеть и зашифровать все компьютеры, в ней присутствующие. Именно поэтому серьезнее всего от WannaCry досталось крупным компаниям – чем больше компьютеров в сети, тем больше ущерб.

По данным «Лаборатории Касперского», к маю 2017 года жертвами WannaCry стали не менее 45 тысяч пользователей из 74 стран. 70% всех

зараженных компьютеров, как утверждают в компании, расположены в России.

Кроме того, вирусом оказались затронуты компьютеры в Великобритании, Испании, Италии, Германии, Португалии, Турции, Украине, Казахстане, Индонезии, Вьетнаме, Японии и Филиппинах.

14 мая 2017 года компания Avast обнаружила 126 тыс. зараженных компьютеров в 104 странах, также выделив Россию среди наиболее пострадавших стран – на нее приходилось 57% заражений.

По состоянию на 14 мая WannaCry собрал более 33 тысяч долларов. Несмотря на то, что многие пользователи заплатили выкуп, не было ни одного сообщения о том, что их файлы были разблокированы. Исследователи обнаружили, что поступление денег на счет вымогателей позволяет отслеживать, какая именно жертва их перевела. У многих вымогателей есть «служба поддержки», которая быстро отвечает жертвам в случае проблем с оплатой. Но не в случае с WannaCry. Более того, эксперты сомневаются, что зашифрованные файлы вообще поддаются дешифровке со стороны вымогателей.

Распространение вируса-вымогателя WannaCrypt удалось приостановить, зарегистрировав домен iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Оказывается, некоторые образцы WannaCry обращались к этому домену и, если не получали положительного ответа, устанавливали шифровальщик и начинали свое черное дело. Если же ответ приходил (то есть домен был зарегистрирован), то зловред сворачивал какую-либо деятельность. Обнаружив отсылку к этому домену в коде трояна, исследователь зарегистрировал его, таким образом приостановив атаку. За остаток дня к домену пришло несколько десятков тысяч обращений, то есть несколько десятков тысяч компьютеров удалось спасти от заражения. Есть версия, что эта функциональность была встроена в WannaCry как рубильник – на случай, если что-то пойдет не так. Другая версия, которой придерживается и сам исследователь: что это способ усложнить анализ поведения зловреда. В исследовательских тестовых средах часто специально делается так, что от любых доменов приходили положительные ответы – и в этом случае в тестовой среде троян бы не делал ничего. К сожалению, в новых версиях трояна злоумышленникам достаточно поменять доменное имя, указанное в «рубильнике», чтобы заражение продолжилось. Так что, вероятно, первый день эпидемии WannaCry не станет последним.

В сети вспыхнула эпидемия вируса-вымогателя

WannaCry как шифровальщик (его еще иногда называет WCrypt, а еще, почему-то, порой зовут WannaCry Decryptor, хотя он, по логике вещей, вовсе даже криптор, а не декриптор) делает все то же самое, что и другие шифровальщики – шифрует файлы на компьютере и требует выкуп за их расшифровку. Больше всего он похож на еще одну разновидность печально известного троянца CryptXXX.

Он шифрует файлы различных типов (полный список можно посмотреть тут[2]), среди которых, конечно же, есть офисные документы, фотографии, фильмы, архивы и другие форматы файлов, в которых может содержаться потенциально важная для пользователя информация. Зашифрованные файлы получают расширение .WCRY (отсюда и название шифровальщика) и становятся полностью нечитаемыми.

После этого он меняет обои рабочего стола, выводя туда уведомление о заражении и список действий, которые якобы надо произвести, чтобы вернуть файлы. Такие же уведомления в виде текстовых файлов WannaCry раскидывает по папкам на компьютере – чтобы пользователь точно не пропустил. Как всегда, все сводится к тому, что надо перевести некую сумму в биткоин-эквиваленте на кошелек злоумышленников – и тогда они якобы расшифруют файлы. Поначалу киберпреступники требовали $300, но потом решили поднять ставки – в последних версиях WannaCry фигурирует цифра в $600.

Вирус работает только на Windows – он использует уязвимость в операционной системе и распространяется вслепую: то есть не выбирает жертв, а заражает тех, кто не защищен. Microsoft закрыл эту уязвимость еще в марте 2017 года: компания выпустила обновление, которое автоматически установилось на компьютеры обычных пользователей. Всем, у кого система обновилась, вирус не угрожает. В некоторых организациях обновления устанавливаются не автоматически, а с одобрения людей, отвечающих за безопасность. Видимо, с проблемами столкнулись те ведомства и компании, в которых обновление не установили.

Microsoft выпустила обновления для операционных систем, которые уже не поддерживаются, чтобы остановить распространение вируса-вымогателя WannaCrypt. Обновление вышло, в том числе для Windows XP, операционной системы 2001 года, хотя она уже три года не поддерживается.

Дягилев Василий, глава представительства компании Check Point Software Technologies в России и СНГ: «Виновником атак, которые начались в конце прошлой недели по всему миру, является версия 2.0 WCry ransomware, также известная как WannaCry или WanaCrypt0r ransomware. Версия 1.0 была обнаружена 10 февраля 2017 года и в ограниченных масштабах использовалась в марте. Версия 2.0 была впервые обнаружена 11 мая, атака возникла внезапно и быстро распространилась в Великобритании, Испании, Германии, Турции, России, Индонезии, Вьетнаме, Японии. Масштаб атаки подтверждает, насколько опасным может быть вымогательское ПО. Организации должны быть готовы к отражению атаки, иметь возможность сканировать, блокировать и отсеивать подозрительные файлы и контент до того, как он попадет в их сеть. Также очень важно проинструктировать персонал о возможной опасности писем от неизвестных источников».

Авторы

Эксперты компании **Flashpoint** с помощью лингвистического анализа установили национальность хакеров, предположительно создавших и

запустивших вирус WannaCry. Анализ показал, что злоумышленники могут быть из южных областей Китая, Гонконга, Тайваня или Сингапура, так как родным для хакеров был южный диалект китайского языка.

Эксперты проанализировали сообщения с требованием выкупа, которые появлялись на зараженных компьютерах. Все они были переведены на 28 языков, включая русский, норвежский, филиппинский, турецкий и другие[3].

Анализ показал, что практически все сообщения о выкупе были переведены через Google Translate, и только английская и две китайские версии (упрощенная и классическая), вероятно, были написаны носителями языка.

Несмотря на то, что сообщение на английском языке было написано человеком, хорошо владеющим языком, грубая грамматическая ошибка указывает на то, что это не родной язык автора. Flashpoint выяснила, что именно текст на английском стал первоисточником, который впоследствии перевели на остальные языки.

Сообщения о требовании выкупа на китайском языке отличаются от других по содержанию и тону. Кроме того, большое количество уникальных иероглифов свидетельствует о том, что их писал человек, свободно владеющий китайским.

Спустя три месяца после начала атак с использованием вымогательского ПО WannaCry его создатели вывели все имеющиеся в биткойн-кошельках средства – более $142 тыс. Транзакции были замечены ботом издания Quartz. Шифровальщик требовал у своих жертв выкуп в размере $300-$600 в биткойнах. Все полученные деньги распределялись по трем кошелькам. В ночь на 3 августа 2017 года были зафиксированы семь переводов средств, которые были проведены в течение 15 минут. Вероятнее всего, деньги пройдут через цепочку других биткойн-кошельков, чтобы скрыть конечного получателя.

Кто виноват

В.Путин: Спецслужбы США

Президент России Владимир Путин назвал спецслужбы США источником вируса-вымогателя WannaCry, который парализовал компьютеры ведомств в 150 странах.

"Что касается источника этих угроз, то, по-моему, руководство Microsoft об этом прямо заявило. Сказали о том, что первичным источником этого вируса являются спецслужбы Соединенных Штатов, Россия здесь совершенно ни при чем. Мне странно слышать в этих условиях что-то другое", – сказал президент на пресс-конференции по итогам своего визита в Китай.

Глава государства сообщил, что российские учреждения серьезно не пострадали от глобальной кибератаки. "Для нас существенного никакого ущерба не было, для наших учреждений – ни для банковских, ни для системы здравоохранения, ни для других. Но в целом это тревожно, здесь нет ничего хорошего, это вызывает озабоченность", – констатировал Владимир Путин.

Microsoft: Спецслужбы разных стран

Президент корпорации Microsoft Брэд Смит в своем блоге заявил, что ответственность за крупную кибератаку частично несут ответственность спецслужбы разных стран. Он утверждает, что сбор и хранение спецслужбами информации об уязвимостях в программном обеспечении является большой проблемой, поскольку эти данные в итоге попадают в плохие руки.

«Атака представляет собой пример того, что проблема накопления правительствами информации об уязвимостях является таковой, – написал он. – Мы видели, как данные о уязвимостях, которые собирало ЦРУ (Центральное разведывательное управление США), в итоге обнаружились на Wikileaks, а новая уязвимость, которая была украдена у АНБ (Агентство национальной безопасности США), затронула пользователей по всему миру».

Брэд Смит призвал «правительства всего мира» отказаться от накопления таких данных, а также от их эксплуатирования или продажи. Вместо этого спецслужбы должны передавать информацию об уязвимостях разработчикам, считает он.

Microsoft и Британия: Виновата КНДР

В октябре 2017 года президент Microsoft Брэд Смит (Brad Smith) заявил, что к масштабным атакам с использованием вымогательского ПО WannaCry, в мае 2017 года затронувших более 150 стран мира, причастны власти Северной Кореи. Об этом он заявил в эфире телеканала ITV. Ранее эксперты в области кибербезопасности неоднократно высказывали подозрения о связи атак WannaCry с правительством КНДР, но это впервые, когда президент Microsoft заявил об этом публично.

«Полагаю, к этому моменту все осведомленные наблюдатели заключили, что источником WannaCry была КНДР, использовавшая инструменты или кибероружие, похищенные у Агентства национальной безопасности США», – отметил Смит. Он добавил, что за последние полгода атаки, осуществляемые отдельными государствами, участились и стали более серьезными.

В то время, как общество все больше полагается на технологии, риск для наиболее важных сфер жизнедеятельности и функционирования политических институтов растет, полагает глава Microsoft. Он призвал правительства принять больше мер для защиты граждан от подобного ущерба.

Министр по вопросам безопасности министерства внутренних дел Великобритании Бен Уоллес (Ben Wallace) заявил в конце октябре 2017 года в интервью BBC Radio, что правительство Великобритании уверено в причастности КНДР к атакам шифровальщика WannaCry, поразившего в мае нынешнего года серверы Национальной системы здравоохранения Великобритании (NHS). Атака была совершена не простой хакерской группировкой, а иностранным государством, и британские власти в этом твердо убеждены, заявил министр. В Великобритании и ряде других стран

широко распространено мнение о причастности именно КНДР к данным атакам.

США: Виновата КНДР

18 декабря 2017 года США публично обвинили КНДР в атаках с использованием вымогательского ПО WannaCry. О непосредственной причастности Северной Кореи к атакам сообщил советник президента США по вопросам внутренней безопасности Томас Боссерт (Thomas Bossert) в авторской статье в Wall Street Journal.

«Атака без разбору распространялась по всему миру в мае. Оно (вредоносное ПО WannaCry – ред.) шифровало и делало бесполезным сотни тысяч компьютеров в больницах, школах, компаниях и домах. Это было подло, небрежно и причинило большой материальный ущерб. Атака была широко распространенной и стоила миллиарды. Ответственность за нее лежит непосредственно на Северной Корее»,- завил Боссерт[4].

Как пояснил советник, его заявление не является голословным и основывается на полученных в ходе расследования доказательствах. К выводам о причастности КНДР к атакам WannaCry также пришли спецслужбы Великобритании и специалисты ряда частных компаний, отметил Боссерт.

По мере того, как цифровые технологии становятся повсеместными, злоумышленники начинают использовать их в своих целях. Атаки в киберпространстве позволяют им оставаться анонимными и заметать свои следы. С помощью кибератак преступники похищают интеллектуальную собственность и причиняют ущерб в каждом секторе, отметил советник.

Карта распространения и ущерб от вымогателя WannaCry

Американские эксперты оценили ущерб от масштабной хакерской атаки, которая в начале мая 2017 года обрушилась на компьютерные системы госорганов, крупных корпораций и других учреждений в 150 странах мира. Этот ущерб, уверены оценщики KnowBe4, составил $1 млрд. По этим данным, всего WannaCry поразил от 200 тыс. до 300 тыс. компьютеров.

«Предполагаемый ущерб, нанесенный WannaCry за первые четыре дня, превысил $1 млрд, учитывая вызванные этим масштабные простои крупных организаций по всему миру», – заявил глава KnowBe4 Стью Сьюверман. В общую оценку ущерба вошли потеря данных, снижение производительности, простои в работе, судебные издержки, репутационные ущербы и другие факторы.

Данные на 18.05.2017

Атака на LG Electronics

В августе 2017 года вредонос атаковал сервисные центры LG Electronics и вывел из строя их киоски самообслуживания. Компания сообщила об инциденте Корейскому агентству по вопросам интернета и безопасности (KISA), которому удалось взять ситуацию под контроль, поскольку атака находилась на начальном этапе[5].

Как сообщил пресс-секретарь LG Electronics изданию Korea Herald, попытка вымогателя атаковать компанию провалилась. Незамедлительное

отключение сетей сервисных центров позволило избежать шифрования данных и требования выкупа. По данным KISA, киоски были инфицированы WannaCry, однако, каким образом вредонос попал на системы, неизвестно. Возможно, кто-то целенаправленно установил программу на устройства. Не исключено также, что злоумышленники обманным путем заставили кого-то из сотрудников загрузить вредонос.

Атаки на автопроизводителей

21 июня 2017 года Honda Motor сообщила о приостановке производства автомобилей на одном их заводов после атаки вируса-вымогателя WannaCry на компьютерные системы японского производителя.

Речь идет о предприятии Honda, расположенном в городе Саяма (префектура Сайтама, Япония; находится к северо-западу от Токио). Там производятся седан Honda Accord, минивэны Honda Odyssey и Honda Step Wagon. Ежедневный объем выпуска машин на фабрике составляет около 1000 штук.

Как рассказала агентству Reuters представитель Honda, 18 июня 2017 года компания обнаружила, что вредоносная программа WannaCry попала в сети компании в Японии, Северной Америке, Европе, Китае и других регионов, несмотря на предпринятые в середине мая меры по обеспечению безопасности систем.

Система управления производственными линиями на заводе в Саяме была поражена вирусом-шифровальщиком. За разблокировку данных злоумышленники требовали вознаграждение.

В результате предприятие было закрыто на сутки, 20 июня 2017 года его нормальная работа возобновилась. Другие производственные объекты Honda функционировали в штатном режиме.

В результате распространения WannaCry более 200 тыс. компьютеров в 150 странах оказались заблокированными. Помимо Honda, от вируса пострадали другие автопроизводители, включая Renault и Nissan Motor, которые из-за кибератаки вынуждены были временно заморозить производство на заводах в Японии, Великобритании, Франции, Румынии и Индии.

Хотя WannaCry атаковал Windows-компьютеры, у автопроизводителей возникли опасения, что вирус может нарушить работу автомобильной электроники. Тал Бен-Давид, вице-президент компании Karamba Security, которая предлагает ПО безопасности для соединенных с сетями и самоуправляемых автомобилей, считает, что для безопасности машин компании должны устанавливать надежные фабричные настройки без возможности изменения.[6]

Заражение дорожных камер

В июне 2017 года создатели печально-известного вируса-вымогателя WannaCry невольно помогли австралийским водителям избежать штрафов за превышение скорости, сообщает BBC News.[7]

Вредоносное ПО, из-за которого в мае заблокированными оказались сотни тысяч компьютеров под управлением Windows по всему миру, спустя примерно месяц после глобальной атаки поразило более пяти десятков

дорожных камер, преимущественно расположенных в центральной части Мельбурна.

В Австралии полиция отменила 590 штрафов водителям из-за вируса WannaCry

Заражение 55 камер, следящих за соблюдением правил на дорогах Австралии, произошло во время технического обслуживания (NJ) 6 июня. Сотрудник, проводивший ТО, подключил к системе видеонаблюдения инфицированный USB-накопитель и неумышленно загрузил вирус.

WannaCry в системе видеонаблюдения выявили после того, как полицейские заметили, что камеры слишком часто перезагружаются. По данным Bleeping Computer, перезагрузка происходила раз в несколько минут, однако несмотря на это, камеры продолжали работать и фиксировать нарушения.[8]

В результате инцидента полиция австралийского штата Виктория отменила 590 штрафов за превышение скорости и проезды на красный сигнал светофора, хотя правоохранители уверяют, что все штрафы были назначены верно.

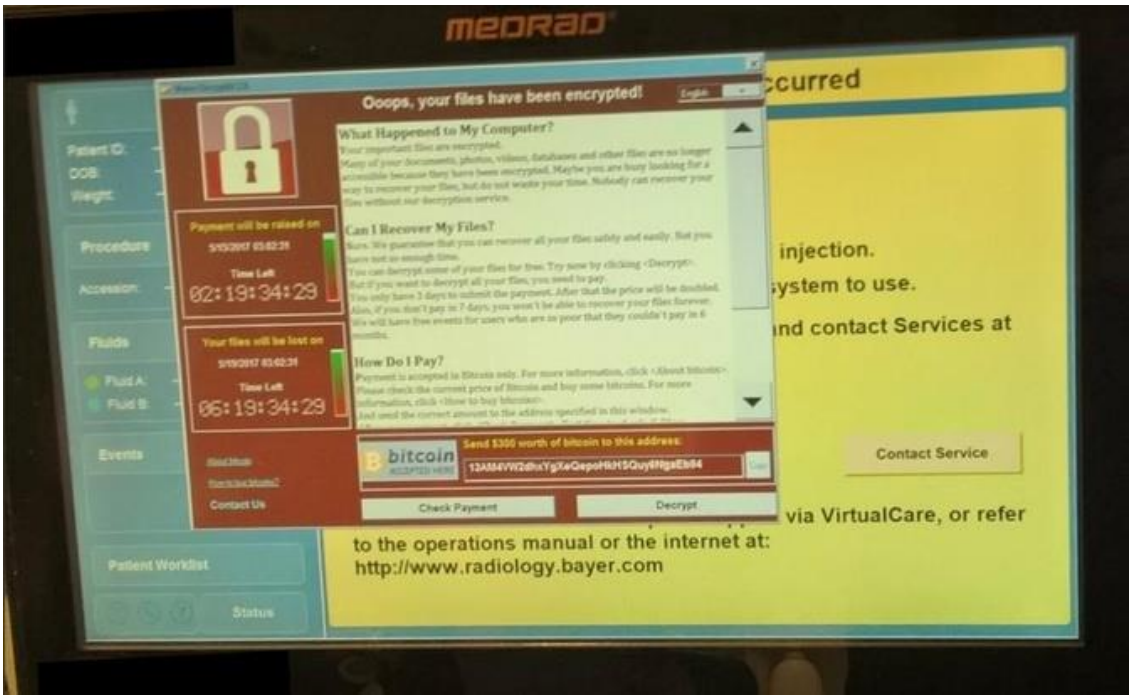
Исполняющий обязанности заместителя комиссара Росс Гюнтер (Ross Guenther) пояснил, что общественность должна быть полностью уверена в правильности работы системы, поэтому в полиции и приняли такое решение.

Хотя основная волна атак WannaCry пришлась на середину мая 2017 года, шифровальщик продолжает причинять беды еще около двух месяцев. Ранее в американской ИБ-компании KnowBe4 подсчитали, что ущерб от WannaCry лишь за первые четыре дня распространения составил более $1 млрд, включая потери в результате утраты данных, снижения производительности, сбоев в работе бизнеса, а также репутационный вред и другие факторы.[9]

Первая атака на медоборудование

WannaCry стал первым вирусом-шифровальщиком, который атаковал не только персональные компьютеры лечебных учреждений, но и непосредственно медицинскую аппаратуру.

17 мая издание Forbes опубликовало снимок экрана устройства Bayer Medrad, зараженного WannaCry, печально известным вирусом-вымогателем, жертвами которого стали более 200 тысяч Windows-компьютеров в 150 странах мира.



Снимок экрана зараженного вирусом WannaCry устройства Bayer Medrad, которе используется при проведении МРТ-обследования

Оборудование Bayer Medrad используется рентгенологами для введения в тело пациента контрастного вещества при проведении магнитно-резонансной томографии, пояснили в издании. В каком именно лечебном учреждении был сделан снимок, не сообщается. Сказано лишь, что фото предоставил источник в системе здравоохранения США, то есть речь о какой-то из американских больниц.

Представитель Bayer подтвердил, что компанию проинформировали о двух случаях заражения оборудования, однако какие именно модели пострадали, не уточняется.

В обоих случаях работа устройств была восстановлена в течение 24 часов. При взломе компьютерной сети медицинского учреждения заражению может подвергнуться и оборудование Bayer под управлением ОС Windows, подключенное к сети, – заявил пресс-секретарь.

Обычно от вредоносного ПО страдают Windows-компьютеры, которыми пользуются в медучреждениях. В частности, WannaCry поразил ПК почти в пяти десятках больниц Великобритании. Инцидент с Bayer Medrad – первый случай, когда жертвой шифровальщика стало само медицинское устройство, подчеркнули в Forbes.

WannaCry смог проникнуть в медоборудование, так как в качестве операционной системы в нем использовалась версия ОС Windows Embedded, поддерживающая уязвимый протокол SMBv1, который и стал начальной точкой заражения.

В тот же день ряд крупнейших производителей медицинских устройств, такие как Smiths Medical, Medtronic и Johnson & Johnson, распространили предупреждения об угрозе заражения, но информации об инцидентах с их оборудованием не поступало.[10]

Касперский призывает ввести государственную сертификацию софта для медицинских учреждений

В ходе недавней выставки CeBIT Australia глава производителя антивирусного ПО KasperskyLab Евгений Касперский поделился некоторыми размышлениями, касающимися вируса-вымогателя WannaCry. От действий последнего пострадали сотни тысяч пользователей из 150 стран, пишет издание ZDNet[11].

Учитывая, что в первую очередь WannaCry поразил сеть медицинских учреждений, их защита является делом первостепенной важности, считает глава антивирусной компании и требует вмешательства государства. «Меня не покидает мысль, что правительствам стоит уделять больше внимания регулированию киберпространства, по крайней мере, это касается критически важной инфраструктуры здравоохранения», – сказал Евгений.

По его мнению, сертификация медицинских учреждений должна включать определённые требования, которые гарантируют защиту ценных данных. Одним из них является получение специальных разрешений, которые удостоверяют, что та или иная клиника обязуется делать резервное копирование данных по графику, а также своевременно производить обновления ОС. Помимо этого государство должно составить перечень обязательных к использованию в секторе здравоохранения систем и приложений (вместе со спецификациями, которые требуются им для безопасного интернет-подключения).

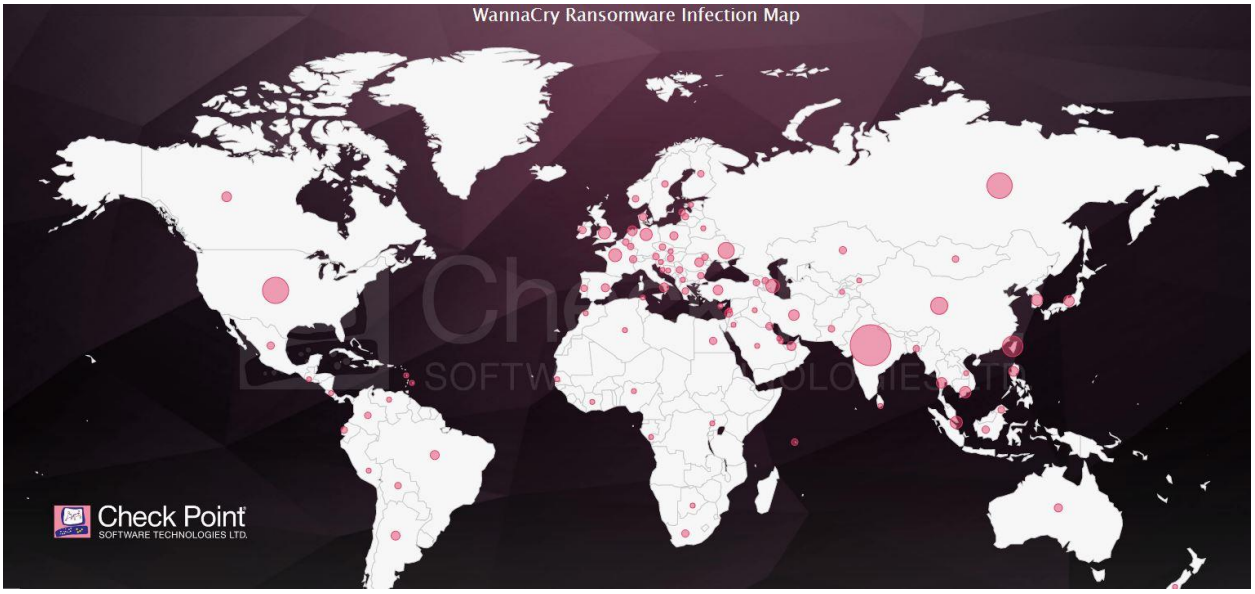
Евгений Касперский считает, что поставляемая производителями медицинского оборудования техника также должна подчиняться требованиям государственных органов. «Производители медтехники выпускают сертифицированную продукцию, которую по условиям контракта нельзя модифицировать. Во многих случаях эти требования не позволяют заменить или обновить ПО в таком оборудовании. Неудивительно, что Windows XP может оставаться непропатченной многие годы, если не навсегда», – говорит эксперт.

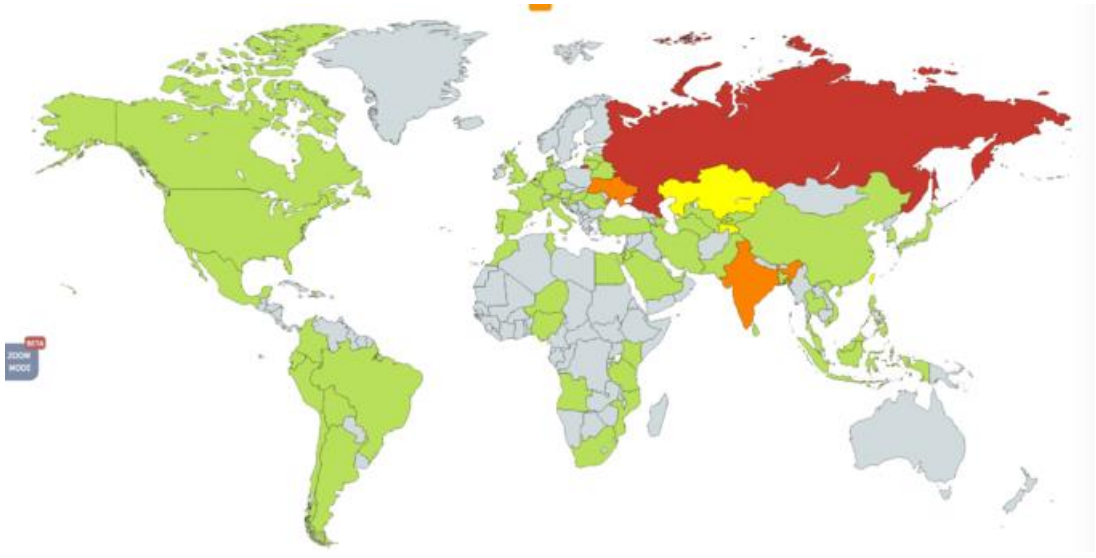
Распространение в России

Россия вошла в тройку стран по распространению вируса

В конце мая 2017 года компания Kryptos Logic, разрабатывающая решения для обеспечения кибербезопасности, опубликовала исследование, которое показало, что Россия вошла в тройку стран с наибольшим количеством хакерских атак с использованием вируса-вымогателя WannaCry.

Выводы Kryptos Logic основаны на числе запросов к аварийному домену (kill switch), который предотвращает заражение. В период с 12 по 26 мая 2017 года эксперты зафиксировали порядка 14 – 16 млн запросов.





Диаграмма, отражающая страны с наибольшим распространением вируса WannaCry в первые две недели, данные Kryptos Logic

В первые дни массового распространения WannaCry антивирусные компании сообщали, что большая часть (от 50% до 75%) кибернападений при помощи этого вируса пришлась на Россию. Однако, по данным Kryptos Logic,

лидером в этом отношении стал Китай, со стороны которого зафиксировано 6,2 млн запросов к аварийному домену. Показатель по США составил 1,1 млн, по России – 1 млн.

В десятку государств с наибольшей активностью WannaCry также вошли Индия (0,54 млн), Тайвань (0,375 млн), Мексика (0,3 млн), Украина (0,238 млн), Филиппины (0,231 млн), Гонконг (0,192 млн) и Бразилии (0,191 млн).

Тот факт, что в Китае зафиксировано больше всего попыток заражения компьютеров вирусом WannaCry, эксперты объясняют медленным проникновением операционной системы Windows 10. Большая часть ПК в Поднебесной к концу мая 2017 года по-прежнему базируется на Windows 7 или Windows XP.

По данным «Лаборатории Касперского», более 98% пострадавших от WannaCry компьютеров управляются Windows 7. В Kryptos Logic подтвердили, что червь действительно заражает в основном устройства на «семерке», поскольку другие ОС (даже устаревшая Windows XP) гораздо менее уязвимы к этому вирусу и при попытке заражения просто не дают вредоносной программе установиться или отключают компьютер запуском «синего экрана смерти».[12]

Глава Минсвязи: WannaCry не поражал российское ПО

Вирус WannaCry не поражал российское программное обеспечение, а находил слабые места в зарубежном ПО, заявил министр связи и массовых коммуникаций РФ Николай Никифоров в программе "Мнение" "Вести.Экономика" в мае 2017 года.

Он признал, что в некоторых госпредприятиях были проблемы из-за этого вируса. Поэтому информационные технологии, работающие в России, должны быть "наши технологии, российские", подчеркнул Никифоров.

"Более того, у нас есть научно-технический потенциал. Мы одна из немногих стран, которая при некоторых усилиях, организационных, финансовых, технических, способна создать весь стек технологий, позволяющих чувствовать себя уверенно", - заявил министр.

"Вирус не поражал отечественное ПО, вирус поражал зарубежное ПО, которое мы массово используем", - подчеркнул он.

Совбез РФ: WannaCry не нанес серьезного ущерба России

В Совбезе РФ оценили ущерб, который вирус WannaCry нанес объектам инфраструктуры России. Как заявил заместитель секретаря Совбеза РФ Олег Храмов, вирус WannaCry не нанес серьезного ущерба объектам критической информационной инфраструктуры России.

К данным объектам относятся информационные системы в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике и других.

Храмов напомнил, что для надежной защиты собственной критической информационной инфраструктуры в соответствии с указом президента Российской Федерации последовательно создается государственная система

обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

«Благодаря упомянутой государственной системе удалось избежать серьезного ущерба. Критическая информационная инфраструктура оказалась готовой противостоять масштабному распространению этого вируса», — заявил Олег Храмов[13].

При этом заместитель секретаря СБ РФ подчеркнул, что подобные угрозы информационной безопасности становятся все более изощренными и масштабными.

Атака на МВД

12 мая 2017 года стало известно об атаке вируса WannaCry на компьютеры Министерства внутренних дел (МВД) России. Зараженными оказались 1% систем ведомства.

Как сообщило РИА Новости со ссылкой на официального представителя МВД РФ Ирину Волк, Департамент информационных технологий, связи и защиты информации (ДИТСиЗИ) МВД России зафиксировал вирусную атаку на персональные компьютеры ведомства, на которых установлена операционная система Windows.

Благодаря своевременно принятым мерам было блокировано порядка тысячи зараженных компьютеров, что составляет менее 1%. В настоящий момент вирус локализован, проводятся технические работы по его уничтожению и обновлению средств антивирусной защиты, – сообщила Волк 12 мая 2017 года.

Она также отметила, что WannaCry не смог заразить серверные ресурсы МВД, поскольку они используются другие операционные системы и серверы на российских процессорах «Эльбрус». [14]

Ряд персональных компьютеров сотрудников ведомства подвергся заражению WannaCry вследствие нарушения сотрудниками правил пользования информационными системами. Причиной инфицирования стали попытки работников МВД подключить служебные компьютеры к интернету «посредством того или иного механизма». Зараженными оказались исключительно персональные компьютеры сотрудников, внутренняя сеть министерства внутренних дел защищена от внешнего воздействия.

Атака на «большую тройку»

12 мая 2017 года «МегаФон» сообщил о хакерской атаке на свои компьютеры с использованием вируса. Оператор утверждает, что ему удалось избежать серьезных последствий благодаря вовремя предпринятым мерам.

На некоторый срок заблокировалась работа операторов call-центров, они не могли включить свои компьютеры, в точках розничных продаж были проблемы. Поэтому мы были вынуждены внутри нашей сети частично отключать целые сети для того, чтобы вирус не распространялся, – рассказал РИА Новости директор по связям с общественностью компании Петр Лидов.

«МегаФон» отбил атаку благодаря использованию технологий виртуализации (когда файловые ресурсы пользователей размещаются в защищенном «облаке») и реализации технологических мер, ограничивающих распространение вируса. Представитель МТС сообщил ТАСС, что атаки на компьютеры сотрудников оператора были зафиксированы ночью. "Мы их отразили", – добавил он.

«ВымпелКом» также заявил о том, что успешно отразил атаку. В пресс-службе «Ростелекома» сообщили, что в компании фиксировали факт атаки.

После атаки WannaCry «дочка» «Мегафона» ищет новых ИТ-директоров

«Мегафон.Ритейл» – розничная «дочка» сотового оператора «Мегафон» – в мае 2017 года начала поиск новых руководителей и специалистов своего ИТ-подразделения. Такие вакансии размещены «Мегафоном» в базе Headhunter.ru[15].

В Москве ведется поиск кандидатов на позиции «руководитель ИТ» и «директор по информационным технологиям» «Мегафон.Ритейл». Поиск этих вакансий начался в период с 17 по 26 мая 2017 г. Искомые компанией специалисты должны отвечать за эффективную организацию ИТ, организацию бесперебойной работы ИТ-сервисов и инфраструктуры, реализацию федеральных ИТ-проектов и пр.

Издание «Роем.ру» увязывает открытие вакансий ИТ-руководителей «Мегафон.Ритейла» с глобальной атакой вируса-вымогателя WannaCry, начавшейся 12 мая 2017 г.

Атака на Сбербанк

Сбербанк сообщил, что зафиксировал попытки хакерской атаки на свою инфраструктуру, однако все они были отражены. «Системы информационной безопасности своевременно зафиксировали попытки проникновения в инфраструктуру банка. Сеть банка предусматривает защиту от подобных атак. Проникновений вирусов в систему не произошло», – сказано в сообщении Сбербанка, поступившем в РБК. В нем также подчеркивается, что в связи с сообщениями о вирусных атаках службы банка, отвечающие за кибербезопасность, переведены в режим повышенной готовности.

На смену WannaCry

Эксплойт EternalBlue на Windows 10

Специалисты компании RiskSense опубликовали в июне 2017 года пространный доклад о том, как можно заставить работать эксплойт EternalBlue в среде Windows 10, ранее в ней не функционировавший.

EternalBlue – это один из «эксплойтов АНБ», похищенных у кибергруппировки Equation в 2016 г. В середине апреля 2017 г. этот эксплойт, наряду с несколькими другими, распространила группа The Shadow Brokers. Вскоре после этого произошла глобальная эпидемия шифровальщика-вымогателя WannaCry, в котором использовался данный эксплойт[16].

В опубликованном документе исследователи показали, как им удалось обойти инструменты защиты Windows 10 – в частности, придумать новый способ обойти DEP (Data Execution Prevention, функция предотвращения выполнения данных) и ASLR (address space layout randomization – «рандомизация размещения адресного пространства»).

Вирусы Adylkuzz и Uiwix

Специалисты компании Proofpoint обнаружили вирус Adylkuzz, который использует ту же уязвимость в Windows, что и WannaCry. Вирус крадет криптовалюту и уже поразил более 200 тыс. компьютеров. При этом хакеры, создавшие Adylkuzz, заработали уже около 43 000 долларов[17].

Исследователи отмечают, что Adylkuzz начал атаки раньше WannaCry – как минимум 2 мая, а возможно и 24 апреля. Вирус не привлек к себе так много внимания, потому что заметить его гораздо сложнее. Единственные «симптомы», на которые может обратить внимание пострадавший, это замедление работы ПК, так как вирус оттягивает на себя ресурсы системы.

При этом Adylkuzz защитилпострадавших от него пользователей от атак WannaCry, так как закрыл собой брешь в Windows и не позволил другому вирусу ей воспользоваться.

Кроме того, после WannaCry появился еще один шифровальщик – Uiwix, который также использует нашумевшую уязвимость в Windows. Об этом заявили специалисты компании Heimdal Security.

Uiwix, в отличи от многочисленных подражателей WannaCry, действительно шифрует файлы жертв и представляет реальную угрозу. К тому же Uiwix не имеет механизма «аварийного отключения», поэтому невозможно остановить его распространение, зарегистрировав определенный домен.

Данный вирус шифрует данные жертв и требует выкуп в размере 0.11943 биткоина (порядка 215 долларов по текущему курсу).

Попытки наживаться на WannaCry от создателей других вирусов

В июне 2017 года исследователи из компании RiskIQ обнаружили сотни мобильных приложений, выдающих себя за средства защиты от шифровальщика WannaCry, на деле оказываясь в лучшем случае бесполезными, в худшем – вредоносными. Подобные приложения являются частью более масштабной проблемы – фальшивых мобильных антивирусов. Подробнее здесь.

Ошибки в коде WannaCry

Код WannaCry был полон ошибок и имел очень низкое качество. До такой степени низкое, что некоторые жертвы могут восстановить доступ к своим оригинальным файлам даже после того, как те были зашифрованы.

Анализ WannaCry, проведенный исследователями из специализирующейся на безопасности «Лаборатории Касперского», выявил, что большинство ошибок означает, что файлы могут быть восстановлены с помощью общедоступных программных инструментов или даже простых команд[18].

В одном случае ошибка WannaCry в механизме обработки файлов только для чтения означает, что он вообще не может шифровать такие файлы. Вместо этого вымогатель создает зашифрованные копии файлов жертвы. При этом оригинальные файлы остаются неприкосновенными, но помечаются как скрытые. Это означает, что файлы легко вернуть, просто сняв атрибут «скрытый».

Это не единственный пример плохого кодирования WannaCry. Если вымогатель проникает в систему, файлы, которые его разработчики не считают важными, перемещаются во временную папку. В этих файлах содержатся оригинальные данные, которые не перезаписываются, а лишь удаляются с диска. Это означает, что их можно вернуть, используя ПО для восстановления данных. К сожалению, если файлы находятся в «важной» папке, такой как Документы или Рабочий стол, WannaCry запишет поверх оригинальных файлов случайные данные, и в этом случае их восстановление будет невозможным.

Тем не менее, множество ошибок в коде дает надежду пострадавшим, поскольку любительский характер вымогателя предоставляет широкие возможности для восстановления, по крайней мере, файлов.

«Если вы были заражены вымогателем WannaCry, велика вероятность, что вы сможете восстановить многие файлы на своем пострадавшем компьютере. Мы рекомендуем частным лицам и организациям использовать утилиты восстановления файлов на пострадавших машинах в своей сети», — сказал Антон Иванов, исследователь безопасности из «Лаборатории Касперского».

Уже не первый раз WannaCry характеризуется как некая любительская форма вымогателя. А тот факт, что за три недели после атаки лишь мизерная доля зараженных жертв выплатила в общей сложности 120 тыс. долл. в биткоинах в виде выкупа, позволяет утверждать, что вымогатель, хотя и вызвал массовый переполох, не сумел получить больших денег, что является конечной целью программ-вымогателей.

Инструмент для удаления WannaCry

Windows XP является одной из уязвимых операционных систем, пораженных вымогательским ПО WannaCry. Несмотря на выход исправляющих уязвимость обновлений, огромное количество компьютеров стали жертвами вредоноса. К счастью, французский исследователь безопасности Адриан Гине (Adrien Guinet) разработал инструмент, позволяющий удалить WannaCry с системы без уплаты выкупа.

Стоит отметить, инструмент работает только в случае, если после заражения системы компьютер не был перезагружен. Если система была перезапущена, и WannaCry зашифровал файлы, программа Гине будет бесполезна.

Разработанный исследователем инструмент ищет ключ для дешифровки в памяти самого компьютера и способен восстановить простые числа закрытого RSA-ключа, используемого WannaCry при шифровании

файлов жертвы. Как пояснил Гине, его инструмент ищет числа в процессе wcry.exe, генерирующем закрытый RSA-ключ.

После зашифровки закрытого ключа его незашифрованная версия удаляется из памяти инфицированного компьютера с помощью функции CryptReleaseContext. Тем не менее, как пояснил исследователь, CryptDestroyKey и CryptReleaseContext стирают только указывающий на ключ маркер, но не числа, благодаря чему закрытый ключ можно извлечь из памяти.

Программа работает только на Windows XP и не тестировалась на других версиях ОС. Скачать инструмент можно с репозитория GitHub.

Как обезопасить свой компьютер от заражения?

- Установите все обновления Microsoft Windows.
- Убедитесь, что все узлы сети защищены комплексным антивирусным ПО. Рекомендуем технологии на базе эвристики, которые позволяют детектировать новые угрозы и обеспечить защиту от так называемых атак нулевого дня. Это повышает безопасность в случае, если в систему проникает ранее неизвестная вредоносная программа.
- Откажитесь от использования ОС Microsoft Windows, которые не поддерживаются производителем. До замены устаревших операционных систем используйте обновление, выпущенное Microsoft для Windows XP, Windows 8 и Windows Server 2003.
- Используйте сервисы для доступа к информации о новейших угрозах.
- При подозрении на заражение отключите инфицированные рабочие станции от корпоративной сети и обратитесь в службу технической поддержки вашего поставщика антивирусных решений за дальнейшими рекомендациями.

ГОРЯЧАЯ ПОРА: ПЕРЕСМОТРЕННЫЙ СТАНДАРТ ISO 15489 И БУДУЩЕЕ УПРАВЛЕНИЯ ДОКУМЕНТАМИ

Источник: http://rusrim.blogspot.com/2018/03/iso-15489-1.html
Автор: Наташа Храмцовская

Статья известного австралийского специалиста Касси Финдлей была опубликована 12 марта 2018 года на её блоге CassieFindlay.com. Данная статья подготовлена ею для публикации в журнале «Архивные документы и манускрипты» (Archives and Manuscripts), том 46, вып.2, июль 2018 года.

В мае 2012 года в Берлине была сформирована новая рабочая группа Международной организации по стандартизации (ИСО), которой было поручено проанализировать и провести пересмотр международного стандарта ИСО 15489 по управлению документами. К тому времени прошло уже двенадцать лет с момента выхода в свет первой редакции стандарта. За этот период было предпринято несколько попыток организовать его пересмотр, которые провалились – возможно, под тяжестью ожиданий.

Действительно, мне, как руководителю этого проекта в рамках рабочей группы, на этом заседании пришлось выслушать ряд довольно острых высказываний об огромной важности нашей работы и о том, что, соответственно, каждый шаг будет бдительно контролироваться.

Без сомнения, ставки были высоки. ISO 15489 занимал центральное место среди стандартов и технических отчетов по вопросам управления документами, которые были подготовлены вслед за публикацией ISO 15489-1:2001 и ISO/TR 15489-2:2001. Он был официально адаптирован более чем 50 странами и переведен на 15 языков (*в России стандарт адаптирован усилиями ВНИИДАД как ГОСТ Р ИСО 15489-1-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования» - Н.Х.*). В моей собственной работе международный стандарт ISO 15489 и ее австралийский прародитель AS 4390 обеспечили основу практически для всего, что я делала в качестве консультанта по вопросам управления документами, педагога и разработчика политик. Методология «Проектирования информационных систем и систем управления документами» (Designing Information and Recordkeeping Systems, DIRKS – *в первой редакции ISO 15489 именно она легла в основу его второй части - технического отчета ISO/TR 15489-2:2001 – Н.Х.*), которую любят, ненавидят и часто понимают абсолютно неправильно, осталась для меня и многих других коллег краеугольным камнем нашей практики (*точности ради, следует отметить, что подавляющее большинство ценителей DIRKS – это австралийцы. В целом методология – в ИСО она известна под слегка измененным названием Design and Implementation of Records Systems, DIRS – содержит немало полезного и даже сегодня с ней имеет смысл познакомиться, однако она уже сильно морально устарела, поскольку была создана ещё в конце прошлого века с расчётом на мощные централизованные корпоративные системы управления документами. В те времена не было ни облаков, ни мобильных вычислений, ни таких огромных объёмов документации в деловых системах и в системах электронной почты… – Н.Х.*).

Координатор (convenor) нашей рабочей группы Ханс Хофман (Hans Hofman), я и другие члены Редакционной группы [1] разделяли мнение о том, что данный процесс пересмотра открывает значительные возможности для нашей профессии и одновременно является чем-то вроде спасательного круга перед лицом неопределенное будущего.

Действительно, в настоящем журнале в 2014 году мы с моими коллегами по австралийской дискуссионной группе по вопросам управления

документами и архивного дела (Recordkeeping Roundtable) представили аргументы, говорящие о том, что наши профессиональные методы не справляются с масштабами и сложностью современных проблем управления документами, и что мы рискуем потерять четкое представление о том, что отличает нашу работу от деятельности представителей родственных профессий [2].

Мы осознали, что наш опыт и знания [*как специалистов по управлению документами – Н.Х.*] имеют критически-важное значение во взаимосвязанном и насыщенном информацией мире, и ключевыми элементами нашего вклада является документационный анализ (appraisal – *см. пояснения Кассии Финдлей здесь:* https://rusrim.blogspot.ru/2017/06/iso-15489-2.html – *Н.Х.*) и обеспечение доступа. Однако в 2012 году эта мысль и чувство неотложности реформ разделялись не всеми нашими коллегами, многие из которых предлагали вариант минимальных изменений, которые не вызовут слишком много последствий в их юрисдикциях – или же в тех юрисдикциях, которые только-только начинают всерьёз применять принципы, заложенные в первой редакции ISO 15489: 2001.

Редакционная группа в 2012 году также осознавала необходимость разработать документ, который проживёт достаточно долго. Мы понимали, что если взять в качестве ориентира предыдущий промежуток времени между редакциями, то новая редакция потенциально может оставаться в силе вплоть до 2030 года. Это была отрезвляющая мысль, учитывая экспоненциальные темпы технологических инноваций, которые мы сейчас наблюдаем.

В отчете за 2015 год Всемирного экономического форума (World Economic Forum) перечислены шесть «мега-тенденций», которые с тех пор стали лишь ещё более очевидными в повседневной жизни людей, живущих в странах с развитой экономикой [3]. Люди и вещи постоянно соединены с Интернетом и друг с другом. Для всех доступны вычислительные мощности и почти неограниченная емкость систем хранения. Машинное обучение и искусственный интеллект используют огромные объемы данных для самообучения, позволяющего компьютерным системам взять на себя работу и принятие решений, которые раньше были привилегией людей и организаций. Децентрализованные протоколы и технологии вводят модели доверия, основанные на вычислениях, устраняя необходимость в авторитетных органах, осуществляющих аутентификацию транзакций между сторонами. Сложные инструменты и роботы, ранее доступные только для высокотехнологичных отраслей и государственных структур, теперь доступны людям на дому.

Как в эту картину вписывается управление документами? Что будет представлять собой специалист по управлению документами будущего? В 2012 году мы попытались начать работу по пересмотру стандарта с ответа на подобные вопросы. Мы обратили внимание на то, что когда выполняемая нами работа подпитывается данными и детально документируется, то детальные и легко модифицируемые правила доступа приходится

реализовывать сложными способами. Мы отметили, что информация и документы более не ограничиваются организационными, географическими или физическими границами – что новые модели ведения деловой деятельности распространяют обязанности по управлению документами за рамки традиционных границ организаций и юрисдикций. Выросли ожидания общественности, клиентов, пользователей услуг, лиц, информация о которых содержится в документах и иных сторон, заинтересованных в создании, захвате и управлении документами, в отношении прозрачности принятия решений как государственными органами, так и коммерческими организациями. Ожидания в плане обеспечения информационной безопасности и неприкосновенности частной жизни также становятся все более значимыми для заинтересованных сторон - как внутри, так вне периметра организации.

Принимая всё это во внимание, мы согласились с тем, что при разработке новой редакции стандарта нам необходимо было создать документ на перспективу, стараясь избежать многочисленных ловушек бумажного мышления. В этот момент ключевым для нас было подтверждение нашего понимания документов как фактора, поддерживающего и способствующего деловой деятельности, а не как «вещей».

Часто на протяжении всего процесса разработки мы делали паузы, чтобы ещё раз напомнить себе о необходимости рассматривать документы как данные, будь то структурированные или неструктурированные, сопровождающиеся обеспечивающими контекст метаданными, которые также служат инструментом управления во времени; а также чтобы напомнить себе о том, что такие данные и метаданные могут быть представлены в любом количестве форм и в виде групп или агрегаций различных типов.

В этом мире жизненно важны аналитические навыки понимания контекста и принятия решений о том, каким образом мы изначально собираемся создавать документы, как мы будем принимать решения об управлении ими в таких критических точках, как миграция системы. Часть членов Редакционной группы также активно выступала за то, чтобы стандарт основывался на [*австралийской, малопопулярной за пределами это континента – Н.Х.*] идее континуума документов, согласно которой управление документами представляет собой непрерывную деятельность - по целому ряду причин и с учетом интересов множества пользователей, которые следует учесть помимо ограничений времени, места и ответственного хранения.

После долгого и порой болезненного процесса разработки, к 2016 году была подготовлена пересмотренная редакция стандарта, которая была одобрена нашими коллегами и опубликована Международной организацией по стандартизации (ИСО). Стандарт, который был официально представлен общественности в мае того же года в Веллингтоне, Новая Зеландия – ISO 15489:2016 «Управление документами – Понятия и принципы» – уходит

от сохранившихся обычаев и практик, связанных с бумажным делопроизводством, и предлагает набор «готовых для использования в электронной среде» принципов, лежащих в основе управления документами, а также описания ключевых методов, инструментов и процессов создания, захвата и управления документами во всех формах.

В стандарте описываются базовые виды работ, поддерживающих создание и управление документами таким образом, чтобы удовлетворялись законодательно-нормативные и деловые требования, а также ожидания общественности. Он объясняет, как эффективно и подотчетным образом реагировать на происходящие со временем изменения в этих требованиях. ISO 15489-1:2016 также перечисляет ключевые процессы и инструменты контроля и управления, необходимые в управлении документами, с акцентом на гибкие варианты реализации в различных деловых условиях. Подчеркивается важность метаданные и их ключевая роль. По тесту стандарта подходы к разработке и внедрению процессов работы с метаданными согласованы с существующими рекомендациями в стандарте ISO 23081 [4], тем самым поддерживая все аспекты создания и управления документами.

В обновлённом стандарте особое внимание уделяется документационному анализу как наиболее важному инструменту, обеспечивающему надлежащее и эффективное управление документами. В ходе обсуждений в рабочей группе данный вопрос был одним из самых спорных. В пересмотренном ИСО 15489:2016 понятие документационного анализа (appraisal – *традиционно это термин толкуется как «экспертиза ценности» - Н.Х.*) используется в австралийском смысле и трактуется куда более широко, чем это привычно в ряде юрисдикций. В этой связи было и остается необходимым явным образом напомнить пользователям стандарта о том, что данное понятие, не ограничиваясь отбором документов на постоянное архивное хранение, расширено таким образом, чтобы охватывать анализ деловой деятельности [*с точки зрения управления документами – Н.Х.*], требований и рисков, помогая принимать решения по широкому кругу связанных с документами вопросов.

Как мы это знаем в Австралии, данные, собираемые в рамках такого, регулярного проводимого документационного анализа, необходимы для правильно функционирующей программы создания и управления документами – в любой среде. Такой стратегический подход «на упреждение» особенно ценен для установления приоритетности работ по проектированию систем и сервисов, где присутствуют требования по управлению документами, а также для того, чтобы справляться с объемами и сложностью электронных документов. Была сформирована новая рабочая группа ИСО для описания того, как проводить документационный анализ в интересах управления документами, – с тем, чтобы продолжить продвижение этой новой точки зрения среди международной аудитории.

В пересмотренном стандарте мы намеренно избегали определенных вопросов ради того, чтобы наилучшим образом достичь те цели, которые мы

поставили перед собой в самом начале работы. Объясняя роль документационного анализа как необходимого элемента при принятии любых решений, касающихся управления документами, мы по сути дела охватили ранние этапы методологии DIRKS, впервые описанной в австралийском стандарте AS 4390 1990-х годов (предшественнике стандарта ISO 15489:2001). Мы решили не специфицировать дополнительно методологию проектирования и внедрения систем в новой редакции стандарта, с тем, чтобы этот вопрос мог решаться в соответствии с местными или отраслевыми предпочтениями. Мы изучим возможность дать дополнительные рекомендации в других стандартах и технических отчетах ИСО по вопросам управления документами [5].

Стандарт не определяет свою целевую аудиторию. Такое решение было принято отчасти для того, чтобы не складывалось впечатление, что стандарт имеет отношение только к профессионалам, работающим с документами в определенных условиях – специалистам по управлению документами, архивистам и т.д. – тем самым помогая нам реализовать свои устремления в отношении этого документа, проистекающие из идеи документационного континуума.

Стандарт не является сертификационным и не содержит требований, которые могли бы быть проверены в ходе аудита. Мы предпочли подготовить нормативное утверждение о том, что такое управление документами, и оставить вопросы проверки качества или соответствия законодательно-нормативным требованиям на усмотрение национальных или отраслевых органов по стандартизации. Мы считаем, что это был наиболее уместный подход для выполнения работы, которая, как мы знаем, вызывает много споров; а также для обеспечения того, чтобы не ограничивались возможности для применения инновационных подходов.

С момента выпуска новой редакции в 2016 году я заметила, что реакция на стандарт была интересной смесью любопытства, позитивности и, иногда, непонимания. В некоторых странах переход к ведению деловой деятельности в электронной форме всё ещё находится на ранних стадиях, и в таких случаях необходимо заверить коллег в том, что, хотя новый стандарт ориентирован на электронную среду, он по-прежнему в полной мере применим в бумажной или гибридной среде.

В некоторых странах наше использование термина «appraisal» требует дополнительных объяснений и «продажи» преимуществ той работы, которую мы описываем.

Мой комментарий: *Авторы новой редакции не захотели пойти по самому простому пути, избавлявшему от всех этих терминологических неурядиц, – что, однако, требовало от австралийцев и их соратников поступиться «своим» термином. Достаточно было вместо навязывания нового определения традиционного и по-прежнему востребованного термина ввести новый! Собственно, уже после публикации стандарта по этому пути пошли испанские специалисты, чей вариант терминологии («документационный анализ») я и позаимствовала.*

Как я подчеркиваю в своих докладах о новом стандарте, незнакомство с некоторыми из представленных нами идей и опасения по поводу того, что «за бортом» останутся некоторые из наших старых методов, могут представлять собой проблему. В то же время для специалистов по управлению документами как профессии сейчас наступает горячее, решающее время. Без восприятия инноваций и сосредоточения внимания на особом вкладе, который мы вносим в подотчетность и эффективность деловой деятельности, прямо сейчас и в долгосрочной перспективе, мы рискуем постепенно стать ненужными.

Специалисты по управлению документами располагают уникальными и невероятно ценными знаниями и навыками, но наши стремления заявить об этом часто оказывались неудачными ввиду чрезмерно регламентирующих или не помогающих в работе, зацикленных на разных контрольных списках попыток донести эти знания. Нам следует использовать более незашоренные подходы к людям, с которыми нам нужно работать (в частности, к ИТ-специалистам), чтобы создавать инновационные решения для задач управления документами, а также обеспечивать деловую отдачу своим работодателям и сообществам посредством наших усилий по осознанию меняющихся потребностей в области управления документами. Пересмотренный международный стандарт ISO 15489:2016 «Информация и документация. Управление документами - Понятия и принципы» как раз и был разработан, чтобы помочь нам всё это сделать.

Примечания:

[1] В рамках ИСО рабочая группа и ещё более компактная Редакционная группа формируются путем голосования в головном комитете (в нашем случае, это был технический подкомитет ISO/TC46/SC11 «Управление документами», см. https://www.iso.org/committee/48856.html). В нашей рабочей группе WG13 редакционная группа включала представителей Австралии, Голландии, Франции, Швеции, Соединённых Штатов, Канады и Эстонии, и на протяжении её существования её численность колебалась от 7 до 9 человек.

Мой комментарий: *Редакционная группа была, я бы сказала, необходимым злом. С одной стороны, её члены достаточно эффективно блокировали попытки остальных членов технического комитета и рабочей группы повлиять на текст стандарта, упорно продвигая собственные, порой довольно спорные взгляды. С другой стороны, учитывая очень большую разницу мнений практически по всем существенным вопросам, без такой группы документ вообще сложно было бы подготовить. В результате новая редакция стандарта ISO 15489 оказалась сильно перекошена в пользу специфической австралийской точки зрения на управление документами – а хорошо это или плохо, покажет время.*

[2] Кейт Камминг (Kate Cumming), Касси Финдей (Cassie Findlay), Анн Пико (Anne Picot) и Барбара Рид (Barbara Reed) «Пересмотр архивных методов» (Reinventing Archival Methods). Статья также доступна в виде препринта по адресу Also available as a preprint at:

https://rkroundtable.org/2014/08/01/introduction/ (*на эту тему см. также* https://rusrim.blogspot.ru/2012/12/i.html - *Н.Х.*)

[3] Всемирный экономический форум (World Economic Forum) «Глубокий сдвиг: Обзорный отчет о трансформационных технологических изменениях и их социальных последствиях», (Deep Shift: Technology Tipping Points and Societal Impact Survey Report), сентябрь 2015 года, см.: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[4] См. ISO 23081-1:2006 «Информация и документация – Процессы управления документами – Метаданные документов – Часть 1: Принципы» (Information and documentation - Records management processes - Metadata for records - Part 1: Principles). - *адаптирован в России как ГОСТ Р ИСО 23081-1-2008, см.* http://protect.gost.ru/v.aspx?control=8&baseC=6&id=166090 – *Н.Х.*

[5] На момент написания этой статьи, работа в техническом подкомитете ИСО ТС46/SC11 по тематике проектированию и внедрению систем проходила в форме пересмотра стандарта ISO 16175 «Информация и документация – Принципы и функциональные требования к документам в электронной офисной среде» (Information and documentation - Principles and functional requirements for records in electronic office environments) в 3-х частях.

ШТАТ НОВЫЙ ЮЖНЫЙ УЭЛЬС, АВСТРАЛИЯ: 10 ОСНОВНЫХ ЦИФРОВЫХ ТЕНДЕНЦИЙ, ВЛИЯЮЩИХ НА УПРАВЛЕНИЕ ДОКУМЕНТАМИ, ИНФОРМАЦИЕЙ И КОНТЕНТОМ

Источник: http://rusrim.blogspot.com/2018/03/10.html

Данная заметка Ирене Чимин (Irene Chymyn) была опубликована 12 марта 2018 года на сайте Управления государственных документов австралийского штата Новый Южный Уэльс, посвящённом инициативе «Выдержать проверку временем – защитить наше электронное будущее» (Future Proof – Protecting our digital future).

Недавно мы посетили выставку, на которой была представлена общая картина современных цифровых тенденций, и мы увидели, как эти тенденции связаны с развитием решений в области управления документами, информацией и контентом.

Некоторые из обсуждавшихся тенденций касались **пользователей и того, как они используют и требуют технологии:**

- Пользователи меняют способ применения информационных технологий (ИТ) – они требуют, чтобы эти технологии всегда были

включены, подключены к сетям и предоставляли информацию в режиме реального времени;

- Пользователи также меняют модели проведения закупок. Теперь программные приложения предлагаются в Интернете, при этом используются модели на основе подписки, не требующие какой-либо помощи и поддержки от ИТ-службы. С точки зрения управления документами, государственным органам следует оценить свои деловые потребности, ценность и конфиденциальность своей деловой деятельности, а также создаваемых в её рамках документов, прежде чем закупать и внедрять какие-либо веб-приложения;
- доступность через мобильные устройства.

Модель развертывания систем для управления документами, информации или контентом смещается с локальных решений на собственной площадке к гибридным или же к чисто облачным. Этот сдвиг потенциально обещает сделать интеграцию документных систем с предоставляемым как услуга программным обеспечением менее сложной. Тем не менее, прежде чем переносить свои документные системы в облако, убедитесь, что Вы выполнили условия, установленные в Типовых правилах перемещения документов за пределы штата Новый Южный Уэльс GA35 (Transferring records out of NSW for storage with and maintenance by service providers based outside of the State, https://www.records.nsw.gov.au/node/649).

Очень большое внимание уделяется **программному обеспечению для аналитики данных** и тому, как развиваются такого рода приложения. В число этих приложений входят, в частности, те, которые

- Предоставляют функциональные возможности для визуализации данных, и в которых можно создавать графики, карты и информационные панели и манипулировать ими;
- Позволяют коллективно использовать идеи и знания для целей принятия решений и сотрудничества;
- Поддерживают доставку аналитики / отчетов в любом формате на любое устройство.

Автоматизация работы с метаданными и классификации в рамках управления документами

Мы внимательно следим за этой тенденцией, поскольку она потенциально способна изменить управление документами, каким мы его знаем. Идея заключается в том, что новые технологии способны автоматически и последовательно снабжать документы и информацию метаданными, помогающими вести поиск и проводить просмотр материалов, сгруппированных по заданным критериям (faceted browsing).

Использование технологий машинного позволит систематически и последовательно выполнять классификация документов, с установлением им сроков хранения, отсчитываемых от наступления событий-триггеров. Следует отметить, что архивно-документационная служба штата на прошлогоднем Форуме специалистов по управлению документами (Records Managers Forum) представила результаты собственного пилотного проекта по

применению технологий машинного обучения (см. https://futureproof.records.nsw.gov.au/podcast/episode-76/ , *см. также пост на моём блоге* http://rusrim.blogspot.ru/2018/01/2017.html - *H.X*.).

Что это значит для нас и для Вас?

Попросту говоря, нам необходимо освоить новые знания и навыки; а с учётом того, насколько быстро развиваются технологии – каждому, по-видимому, необходимо стать специалистом по работе с данными, бизнес-аналитиком, специалистом по эргономике или же разработчиком программного обеспечения; и, конечно же, экспертом по правовым вопросам, способным интерпретировать положения и условия, связанные с закупкой программных приложений.

Ирене Чимин (Irene Chymyn)

ГОТОВЯЩИЕСЯ ТЕХНИЧЕСКИЕ ОТЧЕТЫ ИСО: ДОКУМЕНТЫ В ОБЛАКЕ

Источник: сайт технического подкомитета ISO/TC 46/SC 11: https://committee.iso.org/sites/tc46sc11/home/projects/ongoing/records-in-the-cloud.html

Данная заметка была опубликована на сайте подкомитета Международной организации по стандартизации (ИСО) TC46/SC11 «Управление документами» в разделе «Текущие проекты».

В настоящее время продолжается работа над техническим отчетом **ISO/DTR 22428 «Информация и документация – Управление документами в облаке: Вопросы и проблемы»** (Information and documentation - Records management in the cloud: Issues and concerns, см. также https://www.iso.org/standard/73173.html). Он будет содержать рекомендации по внедрению базовой модели менеджмента вопросов безопасности, а также правовых и технических проблем, касающихся документов.

Основные элементы информационной безопасности описаны во многих стандартах и руководствах – *таких, как ISO/IEC 27001 «Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования» (Information technology – Security techniques – Information security management systems – Requirements),* – которые охватывают оборудование, программное обеспечение и т.д., а также некоторые новые схемы соглашений об уровне обслуживания между клиентами и поставщиками (например, документы Альянса облачной безопасности, Cloud Security Alliance), но очень мало пока что затронута тема хранящихся в облаке электронных активов.

В число ключевых аспектов модели, разрабатываемой подкомитетом ТС46/SC11, также входят правовые вопросы и вопросы нормативного регулирования, с учетом того, что эта модель должна обеспечивать понимание хорошей практики для большинства стран, законодательно-нормативная база которых определит пути её практической реализации.

В техническом отчете будут описаны:

- Процессы управления жизненным циклом (на основе стандартов ISO1 5489, ISO 30301, ISO 17068 и др.);
- Эталонные архитектуры (reference architectures) управления электронными документами;
- Как оценивать основные факторы риска для облачных сервисов (с точки зрения как заинтересованных сторон, так и поставщиков облачных услуг).

Работа над этим документом включает описание вариантов применения, помогающих объяснить основные проблемы, возникающие в нетехнической среде, в том числе:

- Вопросы безопасности в отношении электронных документов;
- Законодательно-нормативные требования и требования стандартов;
- Оценка риска для документов в любом облачном контексте;
- Необходимость принять во внимание возможность сбоев и неудач при резервном копировании и обеспечении долговременной сохранности.

Цель работы заключается в том, чтобы подготовить практичный и понятный инструмент как для технической, так и для деловой облачной среды, предложив варианты применения и примеры основных используемых в мировой практике схем.

В настоящее время идёт голосование по очередной версии 30-страничного документа, которое завершится в апреле 2018 года.

Содержание документа следующее:

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Общие требования

- 4.1. Процесс управления жизненным циклом электронного документа в облаке
- 4.2. Метаданные при управлении документами на основе облачных сервисов.
- 4.3. Облачная эталонная архитектура для управления аутентичными электронными документами

5. Модель заинтересованных в облачных услугах сторон

- 5.1. Действующие лица
- 5.2. Пользователь электронных документов

- 5.3. Аудитор
- 5.4. Агент-специалист по управлению документами в облаке (RM agency)
- 5.5. Поставщики облачных услуг

6. Варианты использования облачных электронных документов
- 6.1. Коллективно используемые клиентами SaaS-приложения
- 6.2. Разработанные клиентами SaaS-приложения
- 6.3. Использование клиентом только инфраструктуры как услуги (IaaS)
- 6.4. Использование клиентом нескольких IaaS-услуг
- 6.5. Облачный сервис депозитарного доверенного хранения (escrow)
- 6.6. Варианты с участием агента-специалиста по управлению документами в облаке

7. Факторы риска для электронных документов в облаке
- 7.1. Риски облачных сервисов
- 7.2. Факторы риска для заинтересованных сторон
- 7.3. Риски облачных систем

8. Социальные и правовые риски, связанные с документами в облаке
- 8.1. Правовые факторы риска
- 8.2. Социальные риски

В описании области применения отмечается:

В настоящем техническом отчете описываются все риски и проблемные вопросы, которые могут возникнуть при управлении документами с использованием облачных сервисов. Технический отчет охватывает вопросы и проблемы, относящиеся к облакам всех типов – публичным, частным и гибридным. В нём также описываются риски, связанные с многоуровневой архитектурой облачных сервисов.

Из-за существующих серьезных технических, деловых и социально-правовых рисков стороны, заинтересованные в управлении документами с использованием облачных сервисов, должны заблаговременно выявлять эти риски и принимать меры по их смягчению. Настоящий технический отчет также содержит общие требования и указывает заинтересованные стороны и риски, связанные с управлением документами в облаке.

Целевая аудитория настоящего технического отчета включает архивистов и специалистов по управлению документами, которые используют облачные сервисы для управления документами; разработчиков развертываемого в облаке программного обеспечения для управления документами и поставщиков облачных услуг для управления документами.

КИТАЙ: НОВЫЕ СТАНДАРТЫ В ОБЛАСТИ АРХИВНОГО ДЕЛА И УПРАВЛЕНИЯ ДОКУМЕНТАМИ

Источник: http://rusrim.blogspot.com/

14 декабря 2017 года Государственное архивное управление Китая (国家档案局, далее Госархив) сообщило на своём сайте (см. http://www.saac.gov.cn/news/2017-12/14/content_214080.htm) об утверждении сразу 12 новых отраслевых стандартов и об их предстоящей официальной публикации и вступлении в силу начиная с 1 января 2018 года.

В их число вошли (на английском языке даны китайские самоназвания):

- **DA/T 31-2017 «Требования к оцифровке бумажных документов»** (档案数字化规范, Specification for digitization of paper-based records), взамен DA/T 31-2005, см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c0e4801.pdf
- **DA/T 35-2017 «Предотвращение и борьба с насекомыми и плесенью в архивах – Общие правила»** (档案虫霉防治一般, General rules for control of insect pests and moulds in archives), взамен DA/T 35-2007, см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c111f02.pdf
- **DA/T 59-2017 «Требования к сбору устных исторических материалов и управлению ими»** (口述史料采集与管理规范, Specification for the collection and management of oral history materials), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c18d404.pdf
- **DA/T 60-2017 «Технические требования к вакуумной и заполненной азотом герметичной упаковке бумажных архивных документов»** (档案真空充氮密封包装技术要求, Technical requirements of vacuum and nitrogen-filled sealed packaging for paper archives) см. также http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c18ea05.pdf
- **DA/T 61-2017 «Классификация и описание повреждений бумажных документов эпохи династий Мин и Цин»** (明清质档案病害分类与图示, Classification and legends of the diseases of the Ming and Qing paper archives), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c1f4f10.pdf
- **DA/T 62-2017 «Требования к оцифровке архивных видеозаписей»** (音录像档案数字化规范, Specification for digitization of audio-visual records), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c192107.pdf

- **DA/T 63-2017 «Стандарт метаданных для электронных архивных аудио- и аудиовизуальных документов»** (音录像电子档案元数据方案, Metadata standard for digital audio and audio-visual records, см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c193a08.pdf
- **DA/T 64-2017 «Требования к консервации и реставрации бумажных архивных документов»** (纸质档案抢救与修复规范, Specifications for rescue and restoration of paper archives), в 3-х частях:
  - **DA/T 64.1-2017 «Часть 1: Классификация уровней ущерба»** (破损等级的划分, The grading of damage), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c198009.pdf
  - **DA/T 64.2-2017 «Часть 2: Порядок определения состояния сохранности архивных документов»** (档案保存状况的查方法, Survey methods of preservation conditions), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c19940a.pdf
  - **DA/T 64.3-2017 «Часть 3: Требования к качеству реставрации»** (修质量要求, Quality requirements for restoration), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c19b70b.pdf
- **DA/T 65-2017 «Технические требования к смарт-системе мобильных архивных стеллажей»** (档案密集架智能管理系统技术要求, Technical requirements for archive intelligent mobile shelving system), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c19d30c.pdf
- **DA/T 66-2017 «Требования к архивации и правила архивной классификации инженерной документации городского железно-дорожного транспорта»** (城市轨道交通工程文件归档要求与档案分规范, Filing requirements and archives classification rules of urban rail transit engineering document), см. http://www.saac.gov.cn/xxgk/site2/20171214/64006a6bf3e51b9c1f8111.pdf
- **DA/T 67-2017 «Требования к аутсорсингу услуг по управлению документами»** (档案保管外包服务管理规范, Requirement on the outsource service of records keeping) http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c1a020e.pdf
- **DA/T 68-2017 «Требования к аутсорсингу архивных услуг»** (档案服务外包工作规范, Specifications on the work of archives service outsourcing), см. http://www.saac.gov.cn/news/site2/20171214/64006a6bf3e51b9c1a150f.pdf

Кроме того, 11 января 2018 года Госархив опубликовал на своём сайте ещё один документ – **«Требования к базовым функциональным возможностям систем управления электронными документами»** (子档案管理系统基本功能规定), см. http://www.saac.gov.cn/news/2018-01/11/content_217821.htm.

Архивам всех уровней предписывается обеспечить внедрение этих требований на практике.

Мой комментарий: Хочу обратить внимание на то, что китайские архивисты не только переводят и адаптируют все основные международные стандарты ИСО, но и продолжают разработку собственных национальных стандартов – таких стран сейчас почти так же мало, как и стран, владеющих ядерным оружием или космическими технологиями.

Источник: сайт Государственного архивного управления Китая http://www.saac.gov.cn/

ЗМІСТ