ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо боротьби з кібернебезпекою та підвищенню надійності систем зберігання електронної інформації у сучасному інформаційному суспільстві.

У публікації «Результаты атаки Petya.A в Украине» розповідається про атаку на Українські компанії кріптовіруса «Petya.A» – нової модифікації вірусу-шифрувальника.

У публікації «По следам недавней атаки» розповідається про результати дослідження вірусів Petya і NotPetya, їх принцип дії та недоліки у захисті інформації.

У публікації «Количество пользователей, столкнувшихся с вирусами-вымогателями, за год выросло на 11,4 %» розповідається, що кіберзлочинці перейшли від атак на рядових користувачів до шкідливих атак на організації.

У публікації «Вредоносные ссылки теперь срабатывают без нажатия на них» розповідається про повідомлення експертів з Trend Micro і Dodge This Security, що кіберзлочинці почали використовувати завантажувач, який встановлює банківський троян навіть без натискання на посилання.

У публікації «Вирус Petya и правильная комплексная защита от него и подобных следующих вирусов» наведені методи, що забезпечують високий рівень захисту від сучасних типів атак, які використовувалися в Petya.

У публікації «А был ли мальчик…?» вказані недоліки які сприяли підвищенню ефективності кібератак. Якщо не будуть прийняті кардинальні рішення, то нас чекають ще більш серйозні потрясіння.

У публікації «Fortinet Security Day - в центре внимания концепция Security Fabric» розповідається про питання кібербезпеки і захисту інформації розглянутих на конференції Fortinet Security Day.

У публікації «Не ставьте бытовые SSD в серверы!» наведені відмінності що визначають серверні SSD від побутових.

У публікації «Серверы и системы хранения Lenovo – краткий обзор решений» наведена лінійка серверів і систем зберігання компанії Lenovo на Українському ринку.

У публікації «F5 Solution Days: в фокусе — доставка приложений и кибербезопасность» розповідається про конференцію F5 Solution Days, вперше проведену у Києві і присвячену доставці додатків і кібербезпеці.

У публікації «Довольный клиент – успешный бизнес» розповідається про питання реалізації проектів в області APM (рішень для моніторингу продуктивності додатків) розглянутих на другий конференції Perform Day Kyiv.

РЕЗУЛЬТАТЫ АТАКИ PETYA.A В УКРАИНЕ

Источник: http://ko.com.ua/rezultaty_ataki_petya_a_v_ukraine_120652

Всего за один день, криптовирус «Petya.A» стал самой масштабной кибер-атакой в истории Украины. Разобраться в его происхождении, последствиях и методах предотвращения взялись специалисты компании Integrity Vision.

В своем прошлогоднем отчете компания McAfee назвала 2016 г. «годом шифровальщиков» («year of ransomware»), но как показывают последние события, прошлый год был разминкой: только за первое полугодие 2017 г., ИТ-инфраструктуры украинских и мировых компаний подверглись кибератакам вирсуов-шифровальщиков: WannaCry, XDATA, а 27 июня — новой версии вымогателя Petya.A

Урон, нанесенный криптовирусом Petya.A, за один день активности в Украине сопоставим и превышает нанесенный WannaCry и XDATA ранее. Из открытых источников известно, что от атаки пострадало более 80 крупнейших Украинских компаний во всех отраслях экономики. Среди которых: НБУ, Ощадбанк, Укргазбанк, ПУМБ, ДТЭК, Укрэнерго, Киевэнерго, Укртелеком, Vodafone, Lifecell, Аэропорт «Борисполь», Укрпочта, «Новая Почта», Укрзализныця и многие другие, также не работали сайты издания Корреспондент, football.ua. Больше всего пострадали банки, государственные ведомства и СМИ, но поскольку не все компании

публикуют данные о последствиях атаки, оценить реальное количество пострадавших предстоит в будущем.

Petya.A – новая модификация одноименного вируса-шифровальщика, который распространялся весной 2016 г. и имел несколько модификаций.

Вектор распространения криптовируса стандартный: таргетированный пользователь получает письмо с вложением или ссылкой на вредоносный файл. Кроме того, согласно данных Microsoft, значительная часть вредоноса была распространена через обновление программного обеспечение для отчетности и документооборота – «M.E.doc.» Распространение по сети – через DoblePulsar и EternalBlue, аналогично методам вируса WannaCry.

Сразу после открытия файла происходит эксплуатации уязвимости CVE-2017-0199 и загружается файл hxxp://84.200.16.242/myguy.xls.

После загрузки запускается powershell-скрипт, который загружает остальной функционал Petya с командного сервера hxxp://coffeinoffice.xyz:80/cup/wish.php.

Загружается файл C:\Windows\perfc.dat с основным функционалом шифровальщика.

Распространение шифровальщика в сети происходит по тому же сценарию, по которому распространялся WannaCry: при эксплуатации уязвимости протокола SMB (MS17-010).

Также производится создание задания отложенной перезагрузки в планировщике и очищаются логи (System, Security, Application).

Шифруется большое количество типов файлов: .3ds, .7z, .accdb, .ai, .asp, .aspx, .avhd, .back, .bak, .c, .cfg, .conf, .cpp, .cs, .ctl, .dbf, .disk, .djvu, .doc, .docx, .dwg, .eml, .fdb, .gz, .h, .hdd, .kdbx, .mail, .mdb, .msg, .nrg, .ora, .ost, .ova, .ovf, .pdf, .php, .pmf, .ppt, .pptx, .pst, .pvi, .py, .pyc, .rar, .rtf, .sln, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls, .xlsx, .xvd, .zip.

Также, вредонос вносит изменения в MBR, после чего происходит перезагрузка.

При перезагрузке система уходит в BSOD, после чего пользователю демонстрируется имитация работы утилиты CHKDSK, но во время так называемой «проверки» на самом деле происходит шифрование данных (кстати данное поведение наблюдалось и в старых версиях Petya). По завершению, ПК перезагружается повторно и в модифицированном boot-скрине выводится текст сообщения шифровальщика:

Сумма выкупа – 300$ в биткоинах.

После оформления перевода пользователю рекомендуется выслать ID кошелька и персональный код на адрес злоумышленника (wowsmith123456@posteo.net) и получить в ответ ключ дешифровки.

На данный момент произведено 42 транзакции и злоумышленники заработали около 10000$ в биткоин-эквиваленте. Интересно, что уже через пару часов после начала атаки стало известно, что ключ расшифровки злоумышленники не высылают даже после оплаты.

Сегодня большинство антивирусных вендоров выпустили сигнатуры для обнаружения угрозы: https://virustotal.com/en/file/027cc450ef5f8c5f653329641ec1fed91f694e0d2...

При всплеске активности предыдущей версии Petya, пользователь под ником leostone смог разработать алгоритм, позволяющий произвести дешифрование данных.

Для этой модификации инструмента дешифрования нет. В отличии от того же WannaCry, для Petya.A также отсутствует killswitch-сайт, который предотвратит дальнейшее шифрование данных. Но для данного шифровальщика можно создать файл C:\Windows\perfc (без расширения) с правами доступа только на чтение, что послужит локальным «выключателем».

Как видим, Petya.A использует самые эффективные инструменты, доступные на данный момент, взяв наиболее удачные, с точки зрения злоумышленника, методики проведения атаки, используемые «классической» версией Petya, XDATA и WannaCry. Что не удивительно: после публикации в открытом доступе инструментария NSA ShadowBrockers, атаки такого типа будут только усиливаться и становиться все более изощренными.

Для защиты от атак нулевого дня такого типа компания CheckPoint предлагает универсальные решения по защите периметра и конечных точек: продукты CheckPoint SandBlast Zero-Day protection. PoC видео, предоставленное пользователем Nick McKerall доступно по ссылке: https://www.youtube.com/watch?v=RBM6k5ADF34

IBM ведет кампанию по мониторингу и противодействию инциденту, так что пользователи которые используют IBM QRadar с подпиской X-Force всегда могут отследить попытки активности вредоноса в своей IT-инфраструктуре с помощью компонентов Threat Intelligence: https://exchange.xforce.ibmcloud.com/collection/Petya-Ransomware-Campaig...

Компания Qualys выпустила сигнатуры обнаружения уязвимостей, которые эксплуатирует вредонос для модуля Vulnerability Manager: https://blog.qualys.com/securitylabs/2017/06/27/petya-ransomware-what-yo...

Напомним, Petya.A атаковал украинские предприятия во вторник. Специалисты выпускают свои рекомендации по предотвращению такого рода атак.

ПО СЛЕДАМ НЕДАВНЕЙ АТАКИ

Источник: http://ko.com.ua/po_sledam_ataki_petya_120724

В настоящее время мы отслеживаем новый вариант ransomware по всему миру, который имеет возможность изменять главную загрузочную запись, аналогичную предыдущей атаке, известной как Petya.

Исследователи ссылаются на него как на Petya, так и на NotPetya, поскольку не определено, является ли это вредоносное ПО вариантом, принадлежащим семье Petya. Новый зловред оказывает влияние на широкий спектр отраслей и организаций, включая критические инфраструктуры, такие как энергетика, банковское дело и транспортные системы.

Это новое поколение вируса-вымогателя имеет несколько векторов атак и включает те же уязвимости, которые были использованы во время недавней атаки Wannacry в мае нынешнего года. Подобно Wannacry, эта атака сочетает в себе вымогательство с поведением червя и относится к новой группе вредоносных программ, называемых ransomworms. Вместо того, чтобы нацеливаться на одну организацию, ransomworms используют широкомасштабный подход, который увеличивает область действия атаки.

Хотя на данном этапе исследование продолжается, мы можем утверждать, что этот вирус-вымогатель демонстрирует поведение, подобное червям (ransomworm) благодаря его активному зонду для SMB-сервера. Мы можем также предположить, что он распространяется через EternalBlue и WMIC. Исследователи изначально полагали, что Petya / NotPetya был передан его первым жертвам через электронные письма, содержащие зараженные документы Microsoft Office, которые использовали CVE-2017-0199. На данный момент мы продолжаем исследования, чтобы подтвердить это. Пока применение соответствующего патча MS Office для вашей системы защитит вас от этого вектора атаки.

Как только уязвимое устройство подверглось заражению, Petya / NotPetya, по-видимому, нарушает главную загрузочную запись (MBR) во время цикла заражения. Затем он посылает пользователю сообщение о выкупе, в котором говорится: «Ваши файлы больше не доступны, потому что они были зашифрованы», и требует выкуп в 300 долларов в цифровой валюте Биткойн. Затем он указывает, что выключение компьютера приведет к полной потере системы.

Это иная тактика, чем обратный отсчет времени или постепенное стирание файлов данных, как в других версиях ransomware. С большинством атак Ransomware единственной потенциальной потерей являются данные. Поскольку Petya изменяет главную загрузочную запись, основной риск - это потеря всей системы. Кроме того, он инициирует перезагрузку системы в течение одного часа, добавив к атаке дополнительный элемент отказа в обслуживании.

Любопытно, что в дополнение к эксплойтам Microsoft Office Petya / NotPetya использует тот же вектор атаки, что и Wannacry, применяя те же уязвимости Microsoft, которые были обнаружены Shadow Brokers в начале этого года. Однако из-за того, что в этом эксплойте использовались дополнительные векторы атаки, их исправление было бы недостаточным для полного прекращения этого эксплойта, а это значит, что исправление должно сочетаться с хорошими инструментами и практиками безопасности. Клиенты Fortinet, например, были защищены от всех векторов атаки, поскольку они были обнаружены и заблокированы нашими решениями ATP, IPS и NGFW. Кроме того, наша команда AV выпустила новую антивирусную сигнатуру в

течение нескольких часов после выявления атаки, чтобы улучшить первую линию защиты.

Необходимо обратить внимание на два аспекта. Во-первых, несмотря на широкую огласку уязвимостей и исправлений Microsoft и всемирный характер атаки Wannacry, по-прежнему остаются тысячи организаций, в том числе, в области критической инфраструктуры, которые подверглись атаке и не смогли защитить свои системы. Во-вторых, возможно, что эта атака является просто тестом для подготовки будущих атак, нацеленных на недавно обнаруженные уязвимости.

С финансовой точки зрения, атака Wannacry была не очень успешной, так как принесла очень мало дохода своим разработчикам. Частично это объяснялось тем, что исследователи смогли найти возможность обезвредить атаку. Атака Petya намного сложнее, хотя еще и предстоит увидеть, будет ли она более успешной финансово, чем ее предшественница.

На сегодняшний день ясно: 1) слишком многие организации практикуют плохую «гигиену» безопасности. Когда эксплойт нацелен на известную уязвимость, для которой патч доступен в течение нескольких месяцев или лет, жертвы, к сожалению, виноваты сами. Ключевыми элементами этой атаки были уязвимости, для которых исправления были доступны в течение некоторого времени. 2) эти же организации также не располагают достаточными инструментами для обнаружения таких видов эксплойтов.

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ, СТОЛКНУВШИХСЯ С ВИРУСАМИ-ВЫМОГАТЕЛЯМИ, ЗА ГОД ВЫРОСЛО НА 11,4%

Источник:
http://ko.com.ua/kolichestvo_polzovatelej_stolknuvshihsya_s_virusami-vymogatelyami_za_god_vyroslo_na_11_4_120651

«Лаборатория Касперского» выпустила отчет о работе Kaspersky *Security Network касательно активности вирусов-вымогателей с апреля 2016 г.* по март 2017 г.

В начале этого года исследователи «Лаборатории Касперского» обнаружили опасную тенденцию, набирающую обороты: все больше и больше киберпреступников перешли от атак на рядовых пользователей к целевым вредоносным атакам на организации. Целями этих атак стали, прежде всего, финансовые организации по всему миру. Экспертам

«Лаборатории Касперского» встречались случаи, когда вымогатели требовали более полумиллиона долларов.

Общее количество пользователей, столкнувшихся с вирусами-вымогателями в указанный период, выросло на 11,4 % по сравнению с предыдущими 12 месяцами до 2,58 млн пользователей по всему миру.

Доля пользователей, хотя бы один раз столкнувшихся с вирусами-вымогателями, из общего числа пользователей, столкнувшихся со зловредами, уменьшилась почти на 0,8 % до 3,88 %.

Среди тех, кто столкнулся с вирусами-вымогателями, доля тех, кто столкнулся с шифровальщиками, возросла на 13,6 % до 44,6 %.

Количество пользователей, подвергнувшихся атаке шифровальщиков, возросло почти вдвое — от 719 тыс. до 1,15 млн.

Количество пользователей, подвергнувшихся атаке мобильных вирусов-вымогателей, уменьшилось на 4,62 % до 130 тыс.

Территориальная статистика показывает, что атакующие переключились на страны, которые ранее эта проблема не затрагивала. В этих странах пользователи не подготовлены к противостоянию вирусам-вымогателям, а конкуренция между преступниками не так высока.

Также, в рассматриваемый период времени уменьшилось количество пользователей, на которых были совершены мобильные атаки вирусов-вымогателей. Возможно, это является результатом успешного сотрудничества поставщиков защитных решений, правоохранительных органов и прочих организаций. Также, вероятно, на это повлиял рост осведомленности об угрозах и освещение наиболее известных мошеннических кампаний в СМИ.

ВРЕДОНОСНЫЕ ССЫЛКИ ТЕПЕРЬ СРАБАТЫВАЮТ БЕЗ НАЖАТИЯ НА НИХ

Источник: http://ko.com.ua/vredonosnye_ssylki_teper_srabatyvayut_bez_nazhatiya_na_nih_120450

В наши дни существует множество приемов социальной инженерии и прочих ухищрений, к которым прибегают хакеры, чтобы заставить свою жертву нажать на ссылку, инициировав загрузку вредоносного кода. При соблюдении осторожности, воздерживаясь от бездумного нажатия на подозрительные гиперссылки, пользователь мог считать себя в определенной степени защищённым от неприятностей. Теперь ситуация изменилась и не в лучшую сторону.

Эксперты кибербезопасности из Trend Micro и Dodge This Security сообщили, что с недавнего времени преступники начали использовать загрузчик, который устанавливает банковский троян на компьютер жертвы

даже без нажатия на ссылку. Всё что требуется, это поместить указатель мыши над гиперссылкой в файле презентации PowerPoint.

По имеющейся информации, данная техника применялась в последних операциях по распространению почтового спама среди организаций и фирм Европы, Ближнего Востока и Африки. «Заряженные» письма e-mail в основном были на финансовые темы и снабжались прикреплённым файлом PowerPoint. Эта презентация имела единственную ссылку по центру, озаглавленную «Loading... please wait». Внедрённый в неё скрипт запускался при наведении на ссылку указателя мыши или тачпада.

В Trend Micro расценивают эти спам-кампании как испытания новой техники заражения и считают, что не пройдёт много времени, как этот метод будет принят на вооружение распространителями действительно опасного вредоносного ПО, такого как ransomware.

ВИРУС PETYA И ПРАВИЛЬНАЯ КОМПЛЕКСНАЯ ЗАЩИТА ОТ НЕГО И ПОДОБНЫХ СЛЕДУЮЩИХ ВИРУСОВ

Источник:
http://ko.com.ua/virus_petya_i_pravilnaya_kompleksnaya_zashhita_ot_nego_i_podobnyh_sleduyushhih_virusov_120648

Посмотрим пошагово, чего же такого пропустили CIO, что могло бы предотвратить эпидемию в украинских компаниях «на корню», что есть в

базовых рекомендациях Defense-in-Depth и реализовать которые не является большой проблемой. Напомню, требования Defense-in-Depth (DiD) достаточно простые и предусматривают реализацию тех или иных сервисов защиты на всех уровнях ИТ-инфраструктуры.

Есть и более «продвинутые» методы защиты, которые обеспечивают высокий уровень защиты от современных типов атак, которые в том числе, использовались и в Petya – Securing Privileged Access.

Итак, начнем с первичного заражения. В данной эпидемии рассматривается 2 основных сценария – проникновение через почтовые сообщения в виде вложения к письму и через систему обновлений MEDoc, так называемую атаку «software supply chain attacks», когда взламывается поставщик ПО. Подробно, кто еще не прочитал – «разбор полетов» можете посмотреть здесь.

При этом в первом сценарии запущенный пользователем из почты исполнимый файл атакует ОС через уязвимости SMBv1 (EternalBlue/EternalRomance) и получает все требуемые права, чтобы выполнить свои процессы – шифрование и распространение.

Какие методы противодействия Defense-in-Depth помогут от подобной атаки:

- Периметр – сервис фильтрации почтовых сообщений (например, в Microsoft Exchange) – просто удаляющий все файлы, кроме разрешенных типов, антивирусная система для электронной почты, если нет чего-то подобного – аренда аналогичных облачных сервисов, например – Exchange Online Protection, «знания» которого не зависят от «расторопности» админов (время внедрения – 30 мин + обновление доменного имени).
- Приложения – антивирусы, которые ловили Petya.A с самого начала эпидемии. Надо обновлять сигнатуры – нет, не слышали?
- Хост – бронирование ОС – накатить готовые политики с рекомендованными настройками безопасности от Microsoft Security Compliance Manager или доточить их под рекомендации – например, отключить SMB v1 как класс и прочие ненужные устаревшие сервисы – плевое дело, управление обновлениями (совсем не сложно, особенно, если Windows не пиратская), с IDS сложнее, но даже тут – всего лишь подписка на Defender Advanced Thread Protection, который, как показала практика, ловит атаки подобного типа на корню.
- ЛПП – обучение не открывать файлы, предупреждение об возможных атаках и наказание – вплоть до увольнения и судебных исков против запустивших вирус (ах, да – страна такая, законы не работают – тогда просто переломайте запустившему вирус ноги).

Так что в данном случае – сам факт заражения существенно снижается...

Уровень	Технологии
Данных	ACL/шифрование/классификация данных с RMS
Приложений	SDL, антивирусы, «бронирование» приложений и сервисов, App/Device Guard
Хостов	«Бронирование» ОС, аутентификация, управление обновлениями, FW, защита от вторжения (IDS), VBS, Device Guard
LAN	Сегментирование и изоляция (VLAN), шифрование (IPSec), защита от вторжения (NIDS)
Периметр	FW, контроль доступа, App FW, NAP
Физическая безопасность	Охрана, ограничение доступа, аппаратный контроль и аудит доступа, отслеживание устройств, камеры наблюдения
Люди, политики, процедуры	Документирование, тренинги, предупреждения и уведомления, наказания…

Сценарий второй — вирус «прилетел» через обновление той или иной LoB-системы и здесь пока почти без шансов – скорее всего компьютер будет заражен, поскольку код выполняется от прав системы.

Но не будем расстраиваться. Мы потеряли один компьютер и далее все зависит исключительно от устойчивости ИТ-инфраструктуры в целом.

Дальнейший сценарий распространения вируса Petya проходит по нескольким направлениям:

- Механизм, использующий уязвимость SMBv1 (EternalBlue/EternalRomance) на находящихся в одной подсети с зараженным ПК компьютерах,
- Или механизм pass-the-hash/pass-the-ticket, используя имеющиеся на зараженном ПК сеансы пользователей.

Первый вариант распространения вируса на соседние ПК блокируется очень просто с Defense-in-Depth:

- LAN – сегментирование и изоляция (VLAN) – совсем просто, особенно учитывая кол-во накупленных в компаниях Cisco и прочего оборудования, надо только сесть и чуть подумать, какой же трафик куда должен ходить между сегментам пользовательских ПК (многочисленных и разнесенных тоже) и серверами приложений (тоже сегментированных между собой по типам приложений и требуемого сетевого доступа). Мы не говорим даже об NDIS – даже без обнаружения вторжения (хотя если Cisco – так чего бы не активировать?) – сегменты сетей стали бы непреодолимым барьером для проникновения вируса вне группы ПК.
- Хост – с его firewall, который, как ни странно, сейчас включается в Windows по умолчанию и только дурацкий ответ на вопрос – «хотите ли вы расшарить свои файлы в сети» – «да, хочу!» – портит всю картину. Ну вот зачем, зачем пользовательскому ПК вообще что-то публиковать в сети? Зачем все админы так любят отключать firewall? Легче работать? А не легче ли написать правила в групповых политиках... И все, даже в рамках одного сегмента сети – такие ПК с firewall будут защищены от посягательств зараженного ПК. А что насчет контроллеров домена и прочих файловых помоек – читай выше, обязательных обновлений и «бронирования» и тут никто не отменял.
- ЛПП – и да, не забываем о персональной ответственности админов и сетевиков за каждый следующий поломаный по сети комп.

Второй вариант распространения вируса чуть сложнее – Petya использует для атаки на другие ПК в сети наличие открытых пользовательских сеансов/кэшей паролей на зараженном ПК, а учитывая парадигму того, что многие админы на ПК используют один и тот же пароль локального администратора или учетную запись администратора домена для работы на любом ПК компании – здесь для Petya широкое поле деятельности с использованием механизмов атак pth/ptt. Имея на руках администраторские пароли и открытые «всем ветрам» порты соседних ПК – Petya успешно копирует себя через административные шары (Admin$) и запускает удаленно свой код на атакуемой машине.

Но, если обратиться к Defense-in-Depth, то можно обнаружить, что:

- Хост – рекомендовано использование технологий VBS и Device Guard для защиты от кражи идентити подобными способами. Но – VBS есть только в Windows 10 – Ok, но никто не мешает познакомиться с рекомендациями по защите хостов от Pass-the-hash/pass-the-ticket атак для Windows 7 и т.д. – ничего сложного, кроме опять же – использования рекомендованных шаблонов безопасности (их же можно использовать и для Windows 10 без VBS/DG) начиная с отключения кеширования идентити при входе и т.п.
- Хост – простейшая гигиена аутентификации, связанная с использованием уникальных администраторских паролей на каждой рабочей станции/сервере – утилита Local Administrator Password Solution (LAPS) – избавит от головной боли «по запоминанию» каждого пароля, а далее – более сложные процедуры гигиены для администраторов, которые говорят, что для

выполнения определенных действий на ПК должны быть использованы определенные учетные записи, не обладающие полнотой прав на уровне всей сети (а что, никто не в курсе, что с доменным админом ходить по рабочим станциям категорически запрещено?).

- Плюс – уже упомянутые выше механизмы обнаружения вторжения – тот же Defender ATP или Microsoft ATA («заточенный» как раз на обнаружение атак pth/ptt) и, безусловно – firewall и сегментирование сетей для того, чтобы завладевший теми или иными учетными записями вирус не смог подключиться к соседям.
- ЛПП – а здесь уже может «прилететь» и админу компании в целом, если окажется, что его учетная запись «гуляет» почему-то по рабочим местам пользователей или используется на ПК совместно с такими гуляющими админами.

ВСЕ! Было «охренеть как сложно», мы потратили от силы 3 рабочих дня (24 часов и 24×75=1800евро денег высококвалифицированного специалиста) из предоставленных 43 дней с предыдущей атаки для того, чтобы защититься от разрушительного действия вируса типа Petya.

Да, тут некоторые коллеги в комментах дискутировали насчет того, что «нельзя так просто взять и поделить сеть на подсети пользователей и банкоматов – есть моменты администрирования и удобства работы» – но, в любом случае, у CIO было еще минимуму 3-5 дней на подумать, а потом решить, что удобство работы перед угрозой полномасштабной вирусной атаки – отходит на второй план. В общем – даже не думали и не сделали НИЧЕГО.

Наши потери от Petya после принятых общих мер – мы потеряли, скорее всего, все машины, которые заразились путем приезда «обновления от MEDoc» (хотя, при использовании IDS типа Defender ATP – и эти потери могут быть сведены к минимуму), мы потеряли 10 % от тех машин, которые получили «письма счастья», а компания – потеряла работавших на них сотрудников. ВСЕ! Никакой эпидемии, никаких отключившихся касс и банкоматов (!!!), никаких тысяч часов на восстановление ИТ-инфраструктуры. Осталось восстановить требуемые данные из бекапов (или вообще ничего не восстанавливать, кроме ОС на ПК – если ИТ-инфраструктура сделана правильно и все хранится и бекапится централизованно, к тому же – в облако).

Так что это было, добродии?! Почему Petya гулял по украинским сетям, вынося всех и вся (и не надо рассказывать, что «в Европе/России тоже пострадали», «это была спланированная атака на Украину») – как на лень, некомпетентность и пофигизм CIO попавших под раздачу организаций и полный пофигизм Microsoft Ukraine по отношению к наземной угрозе?!

Ах да, Microsoft и «облака наше все»... Сейчас пойдут разговоры о том, что если бы «все было в Azure», то ничего бы не было. Было бы – с тем же результатом – ваши виртуальные машины в Azure были бы в той же ситуации – локальная сеть, открытые порты и т.п. – потому что в гибридной

инфраструктуре облачная часть IaaS по безопасности ну никак не отличается от наземной по необходимости настроек.

Таким же образом, через обновления, Petya успешно бы пролез и на виртуалки в Azure, дальше бы пошел гулять по виртуальным сетям Azure (которые вы бы не поделили на сегменты, не изолировали, не использовали firewall на каждой), а потом и через Site-to-Site VPN залез бы и на наземные ПК пользователей... Или наоборот – с тем же результатом в такой незащищенной от угрозы изнутри «обланой» инфраструктуре.

А то было бы и хуже – учитывая умение Petya считывать учетные записи админов и зная безалаберность этих админов – Petya.Cloud (с модулем работы в облаке – дописать в код пару строчек) давно бы уже имел административные права на ваши подписки в облаках и делал бы там все, что заблагорассудится, кидая вас еще и на деньги – например – поднимал бы виртуалки для майнинга или ботсетей в вашей облачной подписке, за которые вы бы потом платили по 100К-300К уе/мес.

И даже использование облачного Microsoft Office 365, который вроде как SaaS и его инфраструктура защищается Microsoft – при такой дырявой инфраструктуре на местах – не спасет – с тем же успехом вирус добирается до админского аккаунта O365, используя воровство учетных записей – и дальше подписка O365 уже «не ваша».

Вам об этом не сказали Microsoft, Google, Amazon – все, кто продает «облака»? Так это, им же продать надо, а не решать ваши проблемы – а все проблемы облаков – находятся «на местах», а туда особо уже и не продашь – значит, и инвестировать в наземные части заказчиков не стоит ни копейки – даже тренингами и семинарами...

И всем – приготовиться – это была только очередная волна, ждем следующей, как только ребята найдут другой механизм «заброски» и инфильтрации вируса в корпоративные сети. И этот вирус также не будет обнаруживаться антивирусами по сигнатурам и будет эксплуатировать свежие уязвимости сетей и незакрытые механизмы типа Pass-the-hash/Pass-the-ticket. И вот просто «перенести все в облака» вам не поможет, а подписка на облачные Microsoft ATA/Defender ATP в дополнение к описаным выше мерам – вполне.

А БЫЛ ЛИ МАЛЬЧИК …?

Источник: http://ko.com.ua/a_byl_li_malchik_120669

Аксиома: при целенаправленной (таргетированной) атаке стопроцентный успех обеспечен!

Похоже на то, что эта аксиома никак не укладывается в головах наших государственных «гуру» от кибербезопасности. Очередная атака и все те-же лица в списках пострадавших. Случайность или это тенденция, которая требует переосмысления подходов к вопросам безопасности в киберпространстве? Сложный вопрос.

Не будем анализировать кто, как и с какой целью провел данную атаку.

Обратим внимание только на ключевые моменты этой атаки:

Полная растерянность тех структур, которые отвечают за кибербезопасность в масштабах государства.

Полное отсутствие протоколов оповещения и реагирования на подобные ситуации.

Отсутствие координирующего органа, который смог бы оперативно принимать решения по совместным действиям уполномоченных структур с целью минимизации ущерба от подобного рода атак.

Сразу оговорюсь, создание очередной государственной структуры на старых принципах и подходах ничего не даст. Пора начать понимать, что мир кардинально изменился и войны в киберпространстве будут становиться все эффективней и эффективней.

Необходимо переосмысливать подходы к методам проактивный (упреждающей) защиты и привлекать к разработке этих подходов людей, которые способны мыслить в понятиях существующих угроз современного киберпространства.

Этим подходам не научат ни в учебных вузах полиции, ни СБУ, ни Министерства обороны Украины. У них другие задачи и эти задачи не ориентированы на проактивные подходы в сфере кибербезопасности. Догонять и упреждать, это к сожаление различные подходы и методики. И это надо понимать. Иначе нас ждут еще более плачевные последствия от реализации таргетированных атак на государственном уровне.

По долгу службы мне приходится консультировать структуры различных форм собственности и я, в некотором плане, представляю состояние вопросов кибербезопасности в государственном и частном секторе. Сказать, что там плачевное состояние – это сделать нам самим комплимент. Будем смотреть трезво. Вопрос перезрел и, если в ближайшее время, не будут приняты кардинальные решения, то нас ждут еще более серьезные потрясения.

Выскажу крамольную мысль в какую сторону следовало бы двигаться. Целесообразно рассмотреть вопрос о создании Национального института информационной и кибербезопасности при Кабинете Министров Украины или СНБО Украины, который должен будет заниматься упреждающим анализом киберугроз, разработкой протоколов проактивной защиты и координацией этих вопросов в масштабах государства. Вы скажете, что только что говорил обратное. Все правильно. Но, в силу специфики вопроса, эта структура должна формироваться на принципах комплексных организационных и финансовых составляющих – государственных и частных. Не секрет, что структуры, которые решают «частные» задачи в

киберпространстве существуют и в чьих интересах они работают мы можем только догадываться.

Пора нашим чиновникам начать понимать, что хорошие специалисты в области кибербезопасности стоят дорого, очень дорого! И если мы не сможем обеспечить достойное финансирование, то породим очередной пшик. Что мы и видим в условиях реализации конкретных угроз. Уполномоченных структур полно, а результат достаточно плачевный. Не буду умалять роли тех специалистов, которые там трудятся и делают невозможное. Но через голову они не прыгнут. У них другие задачи и они их должны решать в силу своих служебных обязанностей. На упреждающий анализ угроз у них нет ни сил, ни ресурсов.

Почему институт? Да потому что это, по моему субъективному мнению, форма структуры, которая комплексно сможет заниматься исследованиями, мониторингом угроз, разработкой протоколов взаимодействия, обучения и хозяйственной деятельностью. Да-да, хозяйственной деятельностью. Это необходимое условие для обеспечения комплексных возможностей мониторинга, получения дополнительного финансирования для исследований и разработки отрасле-ориентированных проактивных подходов, привлечения высококвалифицированных специалистов, оснащения структуры современными цифровыми средствами и программным обеспечением и так далее. Никакое государственное финансирование не обеспечит гибкость и высокие стандарты в силу непрогнозируемой динамики изменения угроз в современном киберпространстве. Организационная форма института позволяет быть гибкими и меняться в соответствии с возникающими угрозами. А вхождение в него на ассоциативных или иных правах наших учебных вузов, которые проводят обучение в областях информационной и кибербезопасности, и уполномоченных государственных структур позволит обеспечить рафинированный отбор кадров для работы в области проактивной защиты государства от киберугроз, а также эффективное взаимодействие с различными государственными и частными структурами по противодействию актуальным угрозам. Если грамотно подойти к этим вопросам, то можно еще обеспечить и экономическую выгоду от взаимодействия ассоциативных структур в масштабах государства.

Статус национального института даст возможность взаимодействия с государственными и международными структурами в области кибербезопасности, что важно в силу глобальности существующих угроз.

Важно, чтобы для разработки концепции создания такой структуры были привлечены действительно специалисты в области кибербезопасности, а не «теоретики». Также важна прозрачность самой такой структуры в силу ее двойного назначения, а здесь без общественного контроля не обойтись.

Это не простой вопрос, и я не претендую на полноту освещения подхода к построению такой координирующей структуры, но то, что она нужна это уже очевидно.

FORTINET SECURITY DAY - В ЦЕНТРЕ ВНИМАНИЯ КОНЦЕПЦИЯ SECURITY FABRIC

Источник: http://ko.com.ua/taxonomy/term/5173
Автор – Леонид Бараш

Чем глубже проникают ИТ в нашу жизнь, бизнес и производство, тем острее становятся вопросы кибербезопасности и защиты информации. Решения компании Fortinet в этом ИТ-сегменте были темой конференции Fortinet Security Day.

Компанию Fortinet представила региональный старший директор Дерья Аксой (Derya Aksoy).

Эта американская мультинациональная компания была основана в 2000 г. в Саннивейле, Калифорния. Она разрабатывает и поставляет на рынок ПО, устройства и сервисы в области кибербезопасности, такие как брандмауэры, антивирусы, IPS, средства защиты для конечных точек. В компании работают свыше 4,7 тыс. сотрудников, она имеет более 100 представительств по всему миру. Fortinet является одной из самых быстрорастущий компаний и по величине дохода, который превышает 1 млрд. долл., занимает четвертое место в мире в сегменте кибербезопасности. Инновационность ее решений подтверждена 380 патентами и еще 200 находится в стадии рассмотрения. По данным IDC, Fortinet является наибольшей в мире компанией-производителем устройств в области ИТ-безопасности. Ее решения обеспечивают сквозную безопасность для всех типов организаций, Среди ее заказчиков – крупнейшие телекоммуникационные компании, финансовые учреждения, аэрокосмические компании, департаменты Министерства обороны.

На конференции речь пойдет о концепции Fortinet Security Fabric, которую компания предложила год назад, продолжила г-жа Аксой. Она (концепция) предусматривает широкую мощную автоматизированную защиту всей ИТ-инфраструктуры, включая публичные и частные облака, ЦОД, сети, филиалы, конечные точки и т. д.

В заключение выступающая отметила важность украинского рынка для Fortinet и намерение компании увеличить инвестиции в его развитие. Компания также планирует увеличить свою долю на рынке кибербезопасности Украины.

О новом архитектурном подходе к построению системы безопасности, называемом Security Fabric, рассказал менеджер по работе с ключевыми заказчиками Мирослав Мищенко.

Новые тенденции цифровой эры, такие как IoT, SDN, облачные услуги, мобильные вычисления, машинное обучение и в целом цифровизация бизнеса, изменяют ландшафт кибербезопасности, увеличивая возможности

для атак. Построению надежной защиты ИТ-ресурсов препятствуют разнообразие решений и отсутствие взаимодействия и интеграции между ними.

Но что, если данные и элементы безопасности во всех различных средах организации могут быть хорошо интегрированы, связаны и согласованы, как бесшовная ткань? Такой подход позволит компаниям видеть, контролировать, интегрировать и управлять безопасностью своих данных по всей своей организации, даже в облаке, обеспечивая безопасную цифровую бизнес-модель. Он также позволит безопасности динамически расширяться и адаптироваться по мере того как все больше и больше рабочих нагрузок и данных добавляются и в то же время легко отслеживать и защищать данные, пользователей и приложения при их перемещении между IoT, интеллектуальными устройствами и облачными средами.

Компания Fortinet предлагает новый архитектурный подход к построению системы безопасности, называемый Security Fabric, который впервые позволяет предприятиям объединить все свои дискретные решения по безопасности в единое целое.

Этот подход основан на трех ключевых атрибутах. Первый – широта. Она заключается в охвате защитой всей поверхности возможных атак. Решения безопасности, развернутые по всей сети, не могут оставаться изолированными объектами. Чтобы обеспечить безопасность сегодняшних сетей, администраторы должны обладать видимостью во всей среде, включая конечные точки, точки доступа, сетевые устройства, ЦОД, облако и даже приложения и сами данные. Фабрика также обеспечивает гибкую и открытую интеграцию с решениями других компаний-партнеров в области безопасности.

Всесторонняя видимость распределенного предприятия связывает вместе данные, приложения, устройства и рабочие процессы, чтобы обеспечить уровень информированности и реагирования, управляемые через единую консоль, который никогда ранее не был доступен. Информированность о каждом элементе сети, включая решения других поставщиков, а также о том, как передаются данные между ними, позволяет администраторам находить и реагировать даже на самые сложные угрозы.

В сочетании с динамической сегментацией сети, которая логически разделяет данные и ресурсы, Security Fabric может заглянуть внутрь сети, чтобы обнаруживать угрозы при переходе из одной зоны сети в другую. Такое широкое развертывание и глубокая видимость помогает контролировать внутренний трафик и устройства, предотвращает несанкционированный доступ к данным и ресурсам и контролирует распространение вредоносных программ.

Василий Лымар: «Проблема производительности устройств Fortinet решается с помощью нескольких типов специализированных процессоров»

Второй атрибут – это эффективность. Вследствие требований к производительности, предъявляемым к современным сетям, безопасность

должна быть не только распространенной, но и чрезвычайно эффективной. Сегодняшний цифровой бизнес не может позволить себе жертвовать защитой ради производительности в любом сегменте сети. Он также не может оставить незащищенным даже одного пользователя или приложение.

Решения по безопасности Fortinet основаны на самых быстрых в отрасли специально разработанных процессорах безопасности SPU (Security Processing Unit), которые снижают нагрузку на инфраструктуру, а также на высоко оптимизированных версиях ПО, что позволяет организациям построить надежную систему защиты без ущерба для производительности.

Завершает перечень атрибутов автоматизация. Fortinet Security Fabric позволяет всем элементам быстро обмениваться информацией об угрозах и координировать действия. Но поскольку атака может скомпрометировать сеть за считанные минуты, видимости недостаточно. Сеть также должна иметь возможность реагировать на скорость атаки. Таким образом, решения по обеспечению безопасности не только должны иметь возможность сопоставлять информацию об угрозах для определения уровня риска, им также необходимо автоматически синхронизировать скоординированный ответ. Решениям безопасности необходимо динамически адаптироваться к изменениям сетевых конфигураций, а также устанавливать и применять новые политики по мере того как защищаемая среда адаптируется к изменениям бизнес-потребностей. Меры и контрмеры безопасности должны обеспечиваться автоматически, поскольку новые устройства, рабочие нагрузки и службы развертываются в любом месте, от удаленных устройств до облаков. Security Fabric может динамически изолировать затронутые устройства, части сегментов сети, обновить правила, развернуть новые политики и удалять вредоносное ПО.

Реализация предложенной архитектуры системы безопасности может выполняться поэтапно, начиная с защиты самых критичных ресурсов и понижения высоких рисков.

Фундаментом Fortinet Security Fabric является FortiGate с операционной системой FortiOS. Их установка является первым шагом при разворачивании Security Fabric. Возможности этого альянса представил системный инженер Fortinet Василий Лымар.

Для защиты сети возможностей классического брандмауэра сегодня недостаточно. Нужно защищать приложения, фильтровать веб-контент, защищаться от вредоносного кода, предотвращать утечку данных, попытки вторжений и многое другое. Устройства, выполняющие столь широкий набор функций защиты, называются UTM (Unified Threat Management). По словам выступающего, именно Fortinet была пионером в этой отрасли. Согласно магическому квадранту Gartner, решения компании уже несколько лет занимают первую позицию в правом верхнем квадранте.

Александр Чемерис: «В FortiMail совмещены три технологии: защита от спама, антивирусная защита и интеграция с «песочницей» FortiSandbox для проверки кода, для которого еще нет сигнатур»

Кроме функций защиты, FortiGate предоставляет ряд дополнительных возможностей, таких как динамическая маршрутизация, L2-коммутация, VPN, управление беспроводными контроллерами и рядом других.

При реализации столь большого набора функций в одном устройстве возникает вопрос, как быстро оно может работать? Проблема производительности решается с помощью нескольких типов специализированных процессоров, основными из которых является Network Processor, занимающийся ускорением выполнения функций брандмауэра и шифрования IPsec, и Content Processor, который выполняет сигнатурный анализ. В моделях начального уровня используется комбинированный ASIC System-on-the-Chip. За счет этой архитектуры обработка трафика существенно ускоряется.

Затем докладчик сделал обзор модельного ряда устройств FortiGate. Он включает устройства начального, среднего и высокого уровня, а также модульное устройство, предназначенное для телекомоператоров и ЦОД. Для виртуальных сред компания предлагает использовать виртуальные версии FortiGate, которые поддерживают все основные гипервизоры. Есть также подписка на облачные сервисы FortiGate. Для интеграции с продуктами других производителей имеется API.

Согласно данным компании Verizon, первые две позиции в списке угроз 2016 занимают электронная почта и веб-ресурсы. О решениях Fortinet для их защиты рассказал менеджер по работе с ключевыми заказчиками Александр Чемерис.

Для защиты электронной почты компания предлагает лучший, по словам А. Чемериса, продукт в своем классе FortiMail. В нем совмещены три технологии: защита от спама, антивирусная защита и интеграция с «песочницей» FortiSandbox для проверки подозрительного кода, для которого еще нет сигнатур.

Обычно FortiMail устанавливается рядом с почтовым сервером. Если же у компании нет почтового сервера, но планируется его приобретение, то FortiMail может также выполнять его функции. Продукт имеет экспертное заключение ГСССЗИ СБУ и может использоваться госорганами Украины. Еще один привлекательный аспект – нет лицензирования по количеству пользователей и почтовых ящиков. Однако для обновления сигнатур нужна ежегодная подписка. FortiMail может работать также как виртуальная машина на ресурсах компании или в облаке Azure или AWS.

По мере расширения использования Интернета бизнесом увеличивается спрос на брандмауэр для веб-приложений. FortiWeb обеспечивает защиту на всех уровнях, к примеру, анализирует поведение, верифицирует протоколы, анализирует сигнатуры, защищает от DDoS-атак и т. д. В FortiWeb встроен сканер уязвимостей, он также может выполнять функции балансировщика нагрузки между веб-серверами. Как и FortiMail, FortiWeb сертифицирован ГСССЗИ. Для защиты рабочих станций и мобильных устройств компания предлагает FortiClient. Устройство обеспечивает антивирусную защиту, веб-фильтрацию, сканирование

уязвимостей, брандмауэр для приложений. Персональная версия FortiClient предоставляется бесплатно, однако для централизованного управления необходима лицензия.

Мирослав Мищенко: «Новый архитектурный подход к построению системы безопасности, называемый Security Fabric, впервые позволяет предприятиям объединить все свои дискретные решения по безопасности в единое целое»

В докладе, завершающем конференцию, Мирослав Мищенко рассмотрел систему обнаружения и реагирования на угрозы. Он отметил, что сегодня для обеспечения безопасности необходимо придерживаться концепции продвинутой защиты от угроз, которая предусматривает выполнение трех задач. Это предотвращение, обнаружение и минимизация последствий атаки, если она оказалась успешной. Однако компании не должны полагаться только на средства защиты, они должны уделять достаточное внимание людям, процессам и технологиям. Наибольшую обеспокоенность у бизнеса вызывает Интернет вещей и нехватка квалифицированных специалистов в области кибербезопасности. **По прогнозу аналитической компании Gartner, к 2020 г. около 60% компаний потерпят серьезные неудачи из-за неспособности сотрудников ИТ-служб управлять цифровыми рисками.**

Для противостояния киберпреступности организуются Network Operation Center (NOC) и Security Operation Center. Основное их отличие в том, что первый реагирует на атаку, когда она уже произошла, тогда как второй стремится ее предотвратить. В этих случаях говорят о реактивном и проактивном действии. Обе системы, как правило, между собой слабо взаимодействуют, что снижает эффективность противодействия атакам.

Для построения эффективной системы защиты Fortinet предлагает решение под общим названием Security Operations. В его состав входят FortiAnalyzer, выполняющий централизованный мониторинг Security Fabric, FortiManager, предназначенный для централизованного управления Security Fabric, в том числе для применения и управления политиками, и FortiSIEM для централизованного управления операциями по безопасности. В то же время все это является частью Security Fabric.

НЕ СТАВЬТЕ БЫТОВЫЕ SSD В СЕРВЕРЫ!

Источник: http://ko.com.ua/ne_stavte_bytovye_ssd_v_servery_120717

Тема пагубности использования не-серверных серий SSD в серверах отнюдь не нова. Об этом многократно говорилось на семинарах Intel и

других производителей дисков SSD. Часто это происходит как результат веры в маркетинговые лозунги. На последнем графике наглядно видно, что производительность бытовых SSD в режиме записи под серверной нагрузкой вполне сопоставима с бытовыми же HDD. А потом возникают легенды о том, что «SSD ничего не дает».

Данный материал – это краткий пересказ публикации Dan Lovinger на Microsoft Technet: **Don't do it: consumer-grade solid-state drives (SSD) in Storage Spaces Direct**

Логика SSD

SSD – устройство, состоящее из набора микросхем флэш-памяти NAND, подключенных к внутреннему контроллеру FTL (flash translation layer). Производительность и долгий срок службы SSD зависят от реализации контроллера и его набора процедур в буферной памяти (DRAM) с использованием резерва ячеек NAND (overprovisioning, spare): сбора мусора, освобождения страниц памяти под новую запись, выравнивания износа ячеек, фоновых проверок целостности данных.

Для защиты данных есть два механизма FTL: коррекция ошибок (ECC) и замещение ячеек, выработавших свой ресурс, ячейками из резерва. Когда их запас заканчивается, SSD приходит конец.

Буферная память работает во всех операциях SSD, связанных с размещением данных. Она энергозависима. В потребительских SSD защиты DRAM по питанию нет. В серверных SSD корректное завершение транзакций записи при обесточивании обеспечивают суперконденсаторы.

По сути, два определяющих отличия серверных SSD от бытовых:

- Наличие энергонезависимого кэша записи (Power loss protection)
- Большой ресурс перезаписи ячеек (3-10 DWPD против 0.1-0.2 DWPD)

Эксперимент с потребительскими SSD

Спецификация типичного SATA SSD потребительского класса емкостью 1 TB выглядит многообещающе:

- QD32 4K Read: 95,000 IOPS
- QD32 4K Write: 90,000 IOPS
- Endurance: 185TB при пятилетней эксплуатации.

QD ("queue depth") – количество отдельных запросов ввода-вывода к устройству во время теста. Расхожее значение 32 объясняется ограничением на число команд, обрабатываемых SATA-устройством. У SAS, а тем более NVMe, предел намного выше.

Переводя показатели endurance в более привычную метрику device-writes-per-day (DWPD), получим ресурс перезаписи:

185 TB / (365 days x 5 years = 1825 days) = ~ 100 GB в день, что составляет:

100 GB / 1 TB total capacity = 0.10 DWPD

Для начала тестовый файл размером 100 GB был последовательно записан на SSD несколько раз. Использовалась утилита DISKSPD 2.0.18 с

установками QD8 70:30 4 KB, смешанной нагрузкой чтения/записи в 8 потоков. Буфер записи активирован:

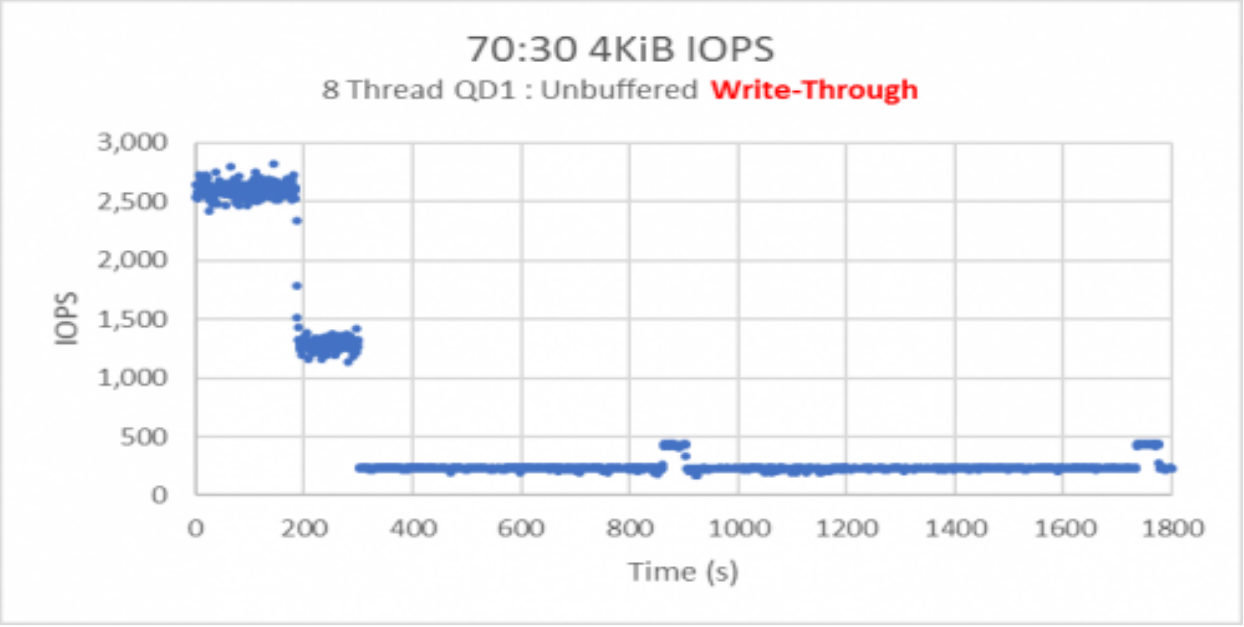
diskspd.exe -t8 -b4k -r4k -o1 -w30 -Su -D -L -d1800 -Rxml Z:\load.bin

Тест длился 30 минут. Падение производительности на ~ 10K IOPS примерно через две минуты - это нормально: у FTL закончился запас чистых страниц NAND под новые записи. По исчерпанию резерва SSD работает медленнее, в паузах контроллер предпринимает действия для восстановления производительности: убирает мусор, освобождает страницы. В типичных пользовательских сценариях - как загрузка веб-страниц - разницы никто и не заметит.

Тот же тест, но со сквозной записью, write-through (-Suw):

diskspd.exe -t8 -b4k -r4k -o1 -w30 -Suw -D -L -d1800 -Rxml Z:\load.bin

Режим write-through показывает истинные задержки NAND, обычно маскируемые FTL/буфером.



Ой! Это больше не “SSD”: через пять минут работы ***производительность записи упала до уровня HDD***, около 220 IOPS. FTL, лишенный буфера, записывает данные в ячейки, разруливает потоки чтения и записи, выполняет фоновую активность – но крайне медленно. Про “кэширование” на таких SSD можно забыть. Жить его ячейки будут недолго.

О важности энергонезависимого буфера.

Все серверные SSD имеют энергонезависимый буфер – это один из признаков этих устройств. С ним SSD гарантирует ОС и приложениям корректное завершение операций записи после попадании данных в буфер даже в случае исчезновения энергоснабжения. Как правило, он реализуется за счет установки на SSD блока суперконденсаторов.

Наличие энергонезависимого буфера обеспечивает предсказуемо высокую и стабильную производительность (как на первом графике), и ресурс ячеек вырабатывается равномерно. Все это обеспечивается серверным

SSD под смешанной интенсивной нагрузкой.

В финале…

Покупатели должны иметь возможность выбрать SSD, соответствующее задачам сервера. Да, они будут дороже, чем устройства потребительского класса. Но, надеюсь, мы убедили вас, почему серверные SSD того стоят.

Будьте в безопасности!

СЕРВЕРЫ И СИСТЕМЫ ХРАНЕНИЯ LENOVO – КРАТКИЙ ОБЗОР РЕШЕНИЙ

Источник: http://ko.com.ua/servery_i_sistemy_hraneniya_lenovo_120421

Хотя компания Lenovo совсем недавно вышла на украинский рынок серверов и систем хранения данных, в арсенале производителя широкий спектр решений и богатый опыт, который унаследован с приобретением бизнеса x86-серверов IBM.

В настоящее время Lenovo продвигает на украинском рынке всю имеющуюся у компании линейку серверов, куда входят системы башенного и стоечного типов, лезвийные платформы, решения для выполнения критически важных приложений, конвергентные и гиперконвергентные устройства, а также серверы высокой плотности. При необходимости с помощью решений Lenovo можно реализовать проекты любого уровня сложности или подобрать оптимальное по соотношению цены и производительности. В данном случае мы предлагаем познакомиться с наиболее актуальными для украинского рынка решениями, которые пользуются высоким спросом и отличаются оригинальными особенностями.

Начнем с односокетных серверов начального уровня, предназначенных для установки в стойку и ориентированных на малые и средние предприятия, а также на работу в распределенных ИТ-инфраструктурах. Кроме стандартных для данной категории устройств в линейке Lenovo имеется серия ThinkServer RS160 высотой 1U, претендующая на звание самой короткой в своем классе. Дело в том, что при размещении в стойке эти сервера занимают в глубину 411 мм. При этом по своему оснащению они не уступают аналогам других торговых марок, так как при своих компактных размерах позволяют установку от двухядерных процессоров Intel Pentium G4400/G4500 до четырехядреных Intel Xeon E3-1200 v5 с тактовой частотой 3,7 ГГц и до 8 МБ кэш-памяти. Оперативная память может быть увеличена до 64 ГБ с помощью четырех слотов для модулей DDR4 ECC UDIMM с частотой до 2133 МГц. А встроенная система хранения данных может быть организована с использованием двух 3,5-дюймовых или четырех 2.5-дюймовых накопителей с интерфейсами SAS/SATA без возможности горячей замены, а также M.2 SSD до 128 ГБ.

Think Server RS160 – самый короткий стоечный сервер

На борту устройства имеется ThinkServer Management Module (TMM), который предназначен для непрерывного мониторинга параметров системы, а при возникновении угрозы сбоя он выдает соответствующие предупреждения или предпринимает необходимые действия при отказах, что минимизирует время простоя платформы. При необходимости платформа может быть оснащена картой расширения с интерфейсом PCIe 3.0 x16. Есть возможность использования оптического привода. Для подключения к локальной сети предназначены два порта GbE, а еще один – для управления системой. Встроенный блок питания мощностью 300 Вт сертифицирован по требованиям 80 PLUS Gold.

Интерактивное 3D-знакомство с Think Server RS160

Одной из важных тенденций современного мира ИТ является борьба за энергоэффективность, поэтому все более востребованными становятся

серверы, способные работать при повышенных температурах. Это связано со стремлением сэкономить на охлаждении помещений для их установки. Имеются в арсенале Lenovo и такие решения, среди которых стоит остановиться на сериях Think Server RD550 и RD650. Они рассчитаны на работу при максимальной температуре 40°C благодаря эффективной системе охлаждения. Эти двухсокетные платформы имеют высоту 2U и могут оснащаться процессорами семейства Intel Xeon E5-2600 v4, что позволяет довести до 44 число задействованных ядер. На каждый из чипов приходится по 12 слотов для установки модулей памяти, поэтому ее максимальный объем составляет 1,5 ТБ в случае LRDIMM объемом по 64 ГБ. А масштабируемая встроенная система хранения включает до 28 2,5-дюймовых или до 14 3,5-дюймовых накопителей, в результате ее емкость может быть доведена до 215 ТБ. Все они поддерживают горячую замену. Эта же возможность обеспечена для двух блоков питания и кулеров системы охлаждения.

Think Server RD550 и RD650 – серверы, работающие при температуре до 40 градусов

Подсоединение к локальной сети обеспечивают четыре порта Gigabit Ethernet и один опциональный 10GE. Платформа предлагает 8 слотов PCIe 3.0. А удаленное управление сервером и мониторинг его состояния выполняются с помощью Integrated Management Module II (IMM2.1). Блоки питания платформы сертифицированы по требованиям 80 PLUS Platinum и Titanium.

Большое значение для бесперебойной работы ИТ-инфраструктур имеет своевременная замена компонентов сервера, которые могут выйти из строя. Особенно важно это при выполнении на нем критически важных приложений, будь то бизнес-приложения или облачные решения. Компания Lenovo располагает в своем арсенале технологией проактивного выявления отказов (Proactive Failure Analyses, PFA), которая ей досталась в результате приобретения бизнеса x86-серверов у IBM. Такая функциональность реализована в целом ряде серверов производителя, начиная с решений среднего уровня. Примерами таких платформ являются серии System

x3650 M5 и x3550 M5. Это универсальные мощные стоечные двухсокетные серверы высотой 2U с поддержкой процессоров Intel Xeon E5-2600 v4.

Максимальный объем ОЗУ в этих платформах составляет 1,5 ТБ, а встроенная система хранения строится с использованием интерфейса 12 Gbps SAS и может включать до 28 2,5-дюймовых или до 14 3,5-дюймовых накопителей. Конструкция серверов предусматривает 8 слотов расширения PCIe 3.0 и один слот PCIe 3.0 выделен специально для контроллера встроенной СХД.

Серверы System x3650M5 и x3550 M5 с поддержкой технологии PFA

Что же касается технологии PFA, то она предусматривает постоянный мониторинг состояния процессоров, регуляторов питающего напряжения, памяти, встроенной системы хранения на базе SAS/SATA HDD и SSD, NVMe SSD, модулей хранения M.2 , адаптеров флэш-накопителей, вентиляторов системы охлаждения, блоков питания, RAID-контроллеров, а также температуры внутри сервера и его ключевых компонентов. На основе этих данных принимается решение о том, насколько работоспособным является тот или иной компонент платформы, и не пора ли его заменить, пока не случилась аварийная ситуация.

Топовую же производительность в линейке серверов Lenovo обеспечивают серии x3850 X6 и x3950 X6. Модель x3850 X6 – четырехсокетная стоечная платформа высотой 4U с поддержкой процессоров Intel Xeon E7 v4, тогда как x3950 X6 – это восьмисокетная система высотой 8U. Они являются уже шестым поколением Enterprise X-Architecture, которая создавалась для обеспечения максимальной производительности и надежности в составе бизнес-критических решений.

О высокой масштабируемости этих платформ свидетельствует тот факт, что общее число используемых в серверах x3850 X6 DIMM составляет 96 при 24 DIMM на каждое процессорное гнездо. А в серии x3950 X6 имеется 192 DIMM. Максимальная частота работы памяти DDR4 равна 1866 МГц.

Встроенная система хранения в x3850 X6 может быть организована с использованием 16 1,8-дюймовых SSD или до восьми 2,5-дюймовых отсеков для накопителей. Эти показатели удваиваются в x3950 X6.

Серверы x3850 X6 и x3950 X6 показывают рекорды производительности

Выдающиеся показатели производительности платформы System x3850 X6 были подтверждены в тесте TPC-H@10,000GB, на которой в июле 2016 года был поставлен мировой рекорд 1,106,832.6 QphH @10,000GB (запросов в час H) при их удельной стоимости $0.89 USD / QphH @10,000GB.

Предприятия любого масштаба от малых и средних до крупных корпораций в своей работе используют большой объем данных. Поэтому спрос на надежные системы хранения не снижается даже в сложных экономических условиях. Компания Lenovo предлагает широкий спектр надежных СХД, включая NAS и SAN. Примерами сетевых хранилищ, ориентированных на бизнесы любого масштаба, являются Lenovo Storage S2200 и S3200.

Системы хранения Lenovo Storage S3200

Массивы для сетей хранения данных Lenovo Storage S2200 и S3200 предлагают предприятиям простой и удобный способ управления данными и обеспечивают производительность, необходимую для самых разных приложений, таких как веб-сервер или базы данных и аналитика, требующих высоких показателей операций ввода-вывода в секунду, и выдерживают

рабочие нагрузки, такие как видеонаблюдение и передача потокового видео, требующие высокую пропускную способность. Устройства поставляются в конфигурации с двумя контролерами в корпусе форм-фактора 2U, вмещающем 12 или 24 накопителя. Системы легко масштабируются по мере роста предприятия: Lenovo Storage S2200 расширяется до 96 дисков, а Lenovo Storage S3200 – до 192. Обе модели предлагают гибкие возможности подключения: они поддерживают интерфейсы Fibre Channel, iSCSI и SAS. Lenovo Storage S3200 также предоставляет многопротокольное подключение с возможностью одновременной работы через интерфейсы Fibre Channel и iSCSI. Благодаря этому достигается высокая гибкость и масштабируемость системы, которые позволяют ей вписаться практически в любую среду.

Среди интересных функциональных возможностей массивов Lenovo Storage S2200 и S3200 – автоматическое распределение данных по уровням хранения (Intelligent Real-Time Tiering). Эта технология позволяет каждые пять секунд определять и автоматически перемещать часто используемые данные на диски с более высокой производительностью, а это значительно повышает эффективность работы системы хранения данных. Lenovo Storage S3200 с гибридной конфигурацией хранения и поддержкой технологии Intelligent Real-Time Tiering обеспечивает производительность, которая по уровню приближается к той, что предлагают флеш-массивы (All-Flash-Array): до 120 тысяч операций ввода-вывода в секунду. При этом стоимость Lenovo Storage S3200 в разы меньше.

Массивы поставляются в комплекте с резервным блоком питания, поддерживают горячую замену вентиляторов и дисков. Для Lenovo Storage S2200 и S3200 заявлен коэффициент готовности 99,999%. В них реализована технология резервирования каналов данных Multipathing. Кроме того, эти устройства предусматривают горячую замену контроллера, что избавляет от необходимости трудоемкой миграции данных и позволит не терять время из-за простоя системы.

Серии S2200 и S3200 поставляются с предустановленным ПО для администрирования SAN-среды, Lenovo SAN Manager, которое имеет интуитивно понятный графический интерфейс и стандартно включает следующие функции:

- распределение данных по разным уровням хранения (DataTiering) – автоматическое распределение подтомов по уровням, что обеспечивает повышение производительности системы;
- выделение емкости по требованию (ThinProvisioning) – оптимизированное предоставление ресурсов, что позволяет экономить средства ИТ-бюджета и приобретать только необходимую емкость дисков;
- возможность кеширования данных на твердотельных накопителях при чтении (SSDReadCaching) – приоритетный доступ к горячим (часто запрашиваемым) данным и увеличение, таким образом, скорости чтения;
- быстрое восстановление данных RAID-массивов (RapidRAIDRebuild) – минимизация временных затрат, необходимых для восстановления данных, и факторов риска, а также быстрое восстановление

данных;

• моментальные снимки файловой системы (Snapshot) – создание копии данных на определенный момент времени, что обеспечивает оптимизацию процесса восстановления данных и производительности системы;

• виртуализация системы хранения (StoragePooling) – объединение физических устройств хранения (дисков различных типов) в пулы, что обеспечивает повышение производительности по вводу-выводу до 2,5 раз, не влияя при этом на работу приложений.

Более вместительными являются массивы семейств Lenovo Storage V3700 V2 и V3700 V2 XP. Они позволяют организовать систему хранения с использованием до 240 накопителей с помощью до 9 полок расширения. Это позволяет достичь максимального объема 3,68 ПБ. При этом поддерживаются все применяемые для этого устройства, включая 2,5- и 3,5-дюймовые диски, SAS-накопители со скоростью вращения шпинделя 10000 или 15000 об/мин, NL SAS HDD со скоростью 7200 об/мин, а также SAS SSD.

Системы храения Lenovo Storage V3700 V2 и V3700 V2 XP

Если в Lenovo Storage V3700 V2 имеется 8 ГБ кэш-памяти, то в V3700 V2 XP ее объем составляет 16 ГБ на каждый контроллер, а кроме того в этой модели поддерживается интерфейс 12 Gb SAS. В обоих массивах в стандартной конфигурации доступны такие функции, как виртуализированное внутреннее хранилище, тонкое выделение, миграция данных, моментальные снимки FlashCopy (до 64 целей) и встроенный графический пользовательский интерфейс. Уровень готовности массивов

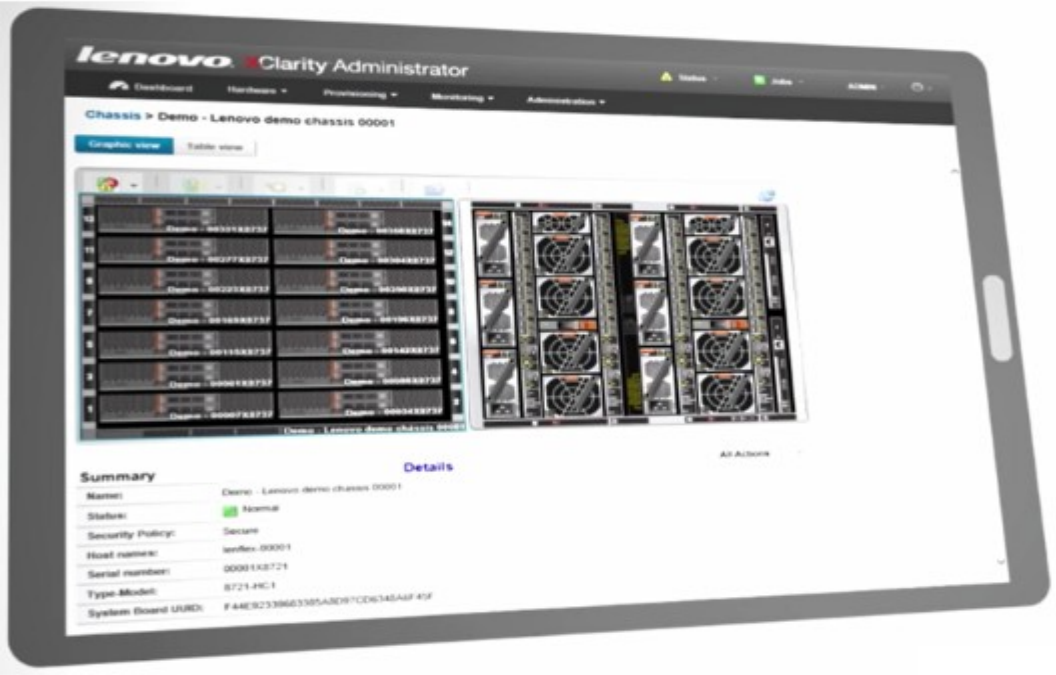
оценивается в 99,999%, что означает простой не более 5 минут в течение года эксплуатации.

Одним из важных трендов при построении современных ИТ-инфраструктур является использование программно-определяемых компонентов. Lenovo также предлагает программно-определяемые системы хранения данных DX8200C, DX8200N, DX8200D, которые основаны, соответственно, на программных платформах от Cloudian, Nexenta и DataCore. DX8200N и DX8200D поддерживают унифицированное файловое и блочное хранение для масштабируемых внедрений в флэш-, HDD- и гибридных конфигурациях. DX8200C использует модель объектного хранения, идеальную для крупномасштабных сред, а благодаря возможностям платформы Cloudian достигается совместимость с публичным облаком Amazon S3.

Программно-определяемые системы хранения DX8200C

Программно-определяемые системы хранения Lenovo базируются на аппаратных платформах высотой 2U с использованием процессоров Intel Xeon E5-2630 v4, каждая из которых представляет собой узел в многоузловой конфигурации. Возможности масштабирования этих решений предусматривают объединение нескольких сотен таких узлов. В состав узла в зависимости от его типа входит набор накопителей: для DX8200C и DX8200N он включает 12 3,5-дюймовых и два задних 3,5-дюймовых жестких диска, а также два 2,5-дюймовых жестких диска/твердотельных накопителя (SSD); тогда как конструкция DX8200D позволяет установить 24 и 2 жестких диска/твердотельных накопителя (2,5-дюймовых). Возможность горячей замены предусмотрена для блоков питания, вентиляторов и накопителей HDD/SSD.

Обзор серверных платформ и систем хранения Lenovo был бы неполным без рассказа о программном инструменте Lenovo XClarity, которое обеспечивает автоматизированное обнаружение, мониторинг, настройку и обновление инфраструктуры Lenovo. Теперь XClarity поддерживает управление серверами линейки ThinkServer в дополнение к System x. Также среди новых функций – мониторинг энергопотребления и управление инфраструктурой с мобильных устройств в любое время и в любом месте.



Система управления Lenovo Xclarity

Решение Lenovo XClarity позволяет сократить общее время развертывания инфраструктуры с 60 до 6 минут (при уменьшении количества действий на 75 % по сравнению с использованием стандартных консолей управления), что экономит время ИТ-администраторов.

F5 SOLUTION DAYS: В ФОКУСЕ — ДОСТАВКА ПРИЛОЖЕНИЙ И КИБЕРБЕЗОПАСНОСТЬ

Источник: http://ko.com.ua/f5_solution_days_v_fokuse_dostavka_prilozhenij_i_kiberbezopasnost_119655
Автор: Леонид Бараш

В конце марта в Киеве впервые состоялась конференция из серии международных мероприятий F5 Solution Days, посвященная доставке приложений и кибербезопасности. Это событие стало возможным благодаря двум факторам: результату семилетней работы компании БАКОТЕК по развитию бизнеса F5 Networks в Украине и высокому уровню заинтересованности производителя в отечественном рынке.

Работа конференции началась с представления ежегодного отчета «2017 State of Application Delivery Report», которое сделал директор F5 Networks по работе с партнерами в Восточной Европе и СНГ Дмитрий Тихович. Опрос включал три категории вопросов: сервисы приложений, облачные вычисления и безопасность.

Сервисы приложений (Application Services) разрабатываются для обслуживания нужд приложений на протяжении всего их жизненного цикла. Они могут включать разработку и модернизацию приложений, аутсорсинг, тестирование и другие процессы и технологии, обеспечивающие эффективную и надежную работу приложений. Согласно опросу 2200 клиентов F5, в ТОП-5 самых популярных сервисов, развернутых сегодня корпорациями, входят брандмауэры (83 %), антивирусы (83 %), SSL VPN (78 %) и средства подавления спама (72 %). При этом три четверти респондентов имеют 10 или более развернутых сервисов, а около 20 % используют 20 и более сервисов приложений. На вопрос о том, что самое худшее может случиться при разворачивании приложений, 39 % респондентов ответили, что это не позаботиться о безопасности, а 33 % – о доступности. Однако еще в 2015 г. безопасность не была на первом месте.

Исследование отношения компаний к облакам показало, что за последний год тенденция Cloud First существенно усилилась. Здесь первое место занимают компании из Азиатско-Тихоокеанского региона (54 %), далее идут Америка и Япония (41 %) и тройку лидеров замыкают страны EMEA. Примечательно, что 20 % компаний к концу 2017 г. развернут в облаках более 50 % своих приложений.

Что касается предпочтений в выборе типа облака и облачных сервисов, то 46 % из опрошенных компаний предпочитают вкладывать средства в частные облака, расположенные на своей площадке, 15 % – в частные облака в удаленных областях, остальные предпочтения примерно поровну разделились между совместным размещением и использованием облачных сервисов SaaS, IaaS и PaaS.

Алексей Ясинский: «В новой линейке реализована технология TurboFlex, которая позволяет использовать FPGA для различных задач, снижая нагрузку на центральный процессор»

В качестве наиболее волнующих проблем были выделены сомнения в состоятельном уровне безопасности по всему облаку (28 %), отсутствие необходимой аналитики для понимания, где лучшее место для разворачивания приложений (25 %) и недоступность к опыту других компаний.

При ответах на блок вопросов о безопасности, 50 % респондентов указали на возрастающую сложность атак как основную проблему. Далее по значимости стоят несоблюдение сотрудниками политик безопасности (44 %) и ТОП-5 проблем замыкают недостаток квалификации, безопасность мобильных приложений и сложность решений. Для усиления уровня безопасности в текущем году 25 % корпораций планируют развернуть системы защиты DNS, 21 % – системы ослабления атак DDoS и 20 % опрошенных – брандмауэры веб-приложений.

Подводя итоги своего выступления, докладчик отметил, что цифровая экономика стимулирует распространение сервисов приложений, а ускорение

перехода в облака создает повышенный запрос на сервисы безопасности и решающим в этом процессе является опыт.

Актуальную тему защиты веб-приложений поднял старший системный инженер F5 Александр Серебряков. Рассказав о некоторых типах атак на веб-приложения, он выделил ряд особенностей продукта F5 ASM (Application Security Manager), которые отличают его от традиционных решений WAF (Web Application Firewall). Так, обнаруживаются бот-сети, проверяется человек или робот находится на связи, анализируется, соответствует ли поведение паттерну человека, формируются и проверяются характерные особенности клиента, так называемый «отпечаток пальца» и другие подобные методы.

В конце прошлого года F5 Networks полностью обновила линейку оборудования корпоративного класса, которая получила название iSeries. По словам руководителя отдела развития бизнеса F5 Networks из BAKOTECH Алексея Ясинского, сегодня это наиболее программируемая и готовая к облакам платформа ADC (Application Delivery Controller) на рынке. Под готовностью к облакам здесь подразумевается, в частности, поддержка не только установленных, но и появляющихся приложений, быстрая пользовательская настройка и интеграция с любыми облачными оркестраторами и системами управления с помощью полноценного API, поддержка множества облачных шаблонов, программно-определяемая производительность.

Мариуш Савчук: «Решение F5 SSL Orchestrator обеспечивает видимость зашифрованного трафика пользователя для любых систем информационной безопасности»

Одним из основных изменений в новой линейке является поддержка эллиптической криптографии – Elliptic Curve Cryptography (ECC), характеризующейся высокой устойчивостью к взлому при относительно коротком ключе. Оборудование F5 также может использоваться в качестве коннектора приложений. С его помощью можно отделить внутреннюю сеть корпорации от внешней сети и уменьшить площадь атаки, а также отделить пользовательскую сеть от сети приложений и сделать невидимым для пользователей исходное окружение.

iSeries позволяет наращивать производительность платформы по мере роста бизнеса, изменяя возможности оборудования с помощью программных ключей лицензирования. В новой линейке реализована технология TurboFlex. Она позволяет использовать FPGA (Field-Programmable Gate Array) для различных задач, снижая нагрузку на центральный процессор. Способность обеспечить гибкий рост производительности позволяет использовать BIG-IP iSeries как центральный элемент ЦОД нового поколения в частных и в публичных облачных архитектурах.

Сегодня быстро увеличивается объем зашифрованного с помощью SSL трафика в сети. Этот метод шифрования используют и хакеры, чтобы скрыть свою деятельность. Поэтому для обеспечения необходимого уровня защиты

нужно не только уметь зашифровывать трафик, но и расшифровывать его. Решение F5 SSL Orchestrator обеспечивает видимость зашифрованного трафика пользователя для любых систем информационной безопасности. О нем рассказал специалист из группы системных инженеров F5 в регионе Северной и Восточной Европы Мариуш Савчук (Mariusz Sawczuk).

Рафаль Хрущел: «В режиме прокси F5 Silverline DDoS Protection направляет весь трафик к клиенту через центры фильтрования компании»

Некоторые брандмауэры нового поколения (NGF) могут расшифровывать трафик SSL. Однако здесь возникают проблемы с производительностью, когда множество устройств безопасности, установленных на маршруте, расшифровывают, инспектируют, а затем вновь шифруют трафик. Потери производительности могут составлять 75–79 %%. Однако дело не только в этом. Последние алгоритмы шифрования часто не поддерживаются устройствами. Как эти проблемы решает F5?

Устройство BIG-IP позволяет однократно расшифровывать трафик и перенаправлять его на устройства обеспечения безопасности уровня L2/L3, устройства для сканирования вирусов и фильтрации контента, работающие по протоколу ICAP (Internet Content Adaptation Protocol) и т. п. Затем трафик можно вновь зашифровать и отправить дальше. В процессе презентации докладчик привел пример конфигурирования BIG-IP, а также продемонстрировал работу устройства в комплексе с устройствами NGF от Palo Alto (L2) и Check Point SG (L3).

Темой второго выступления Мариуша Савчука было решение F5 Hybrid DDoS Protection по защите от атак DDoS.

Атаки DDoS могут выполняться как на сетевом уровне, так и на уровнях сессий и приложений модели OSI. Существуют также смешанные атаки, выполняющиеся на уровне TCP/IP или на более высоком. Поэтому средство для защиты от DDoS-атак должно работать не только на сетевом уровне, но и на уровне сессий и приложений.

Почему же эти атаки так популярны и так опасны? Дело в том, что существует много доступных инструментов, которые просто можно загрузить из Интернета, и на самом деле не нужно быть экспертом, чтобы ими пользоваться.

Решение F5 Hybrid DDoS Protection включает две части: облачную и локальную. В облачной части используется F5 Silverline DDoS Protection, а в локальной – устройства BIG-IP и DHD (DDoS Hybrid Defender). Silverline осуществляет мониторинг приходящего в корпоративную инфраструктуру трафика, ослабляет DDoS-атаки и снижает количество ложных срабатываний в режиме 24/7. Если на площадке заказчика установлены устройства BIG-IP и DHD, то при обнаружении атаки информация о ней передается в облако и подавление атаки начинается на уровне облака.

Анализ реальных атак и средства защиты от них F5 Networks представил старший аналитик по безопасности Рафаль Хрущел (Rafal Chrusciel). В частности он боле подробно остановился на особенностях

функционирования F5 Silverline DDoS Protection. Его можно настроить на прокси-режим, когда весь трафик к клиенту направляется через центры фильтрования, два из которых расположены в США, по одному – в Европе и Азии. Режим прокси требует, чтобы заказчики меняли записи на серверах DNS. Продукт можно также использовать в режиме маршрутизации. При этом запрос к сайту в Интернете выполняется через прокси, а ответ приходит непосредственно к источнику запроса.

При борьбе с мошенничеством в основном приходится иметь дело с фишингом и вредоносным ПО. Для защиты от этого типа атак F5 предлагает использовать опять-таки BIG-IP. Устройство устанавливается на границе сети за демилитаризованной зоной. Обращение к веб-сайту, на котором находится нужное приложение, выполняется через устройство BIG-IP, которое внедряет в трафик некоторый java script, выполняющий мониторинг трафика на наличие вредоносного ПО. При обнаружении такового генерируется предупреждение на соответствующий сервер тревоги, который может располагаться в облаке или на площадке заказчика. BIG-IP может контролировать сайты, выявлять внешние инъекции кода, определять доступность доменов и выполнять ряд других защитных функций. Устройство может также осуществлять шифрование в режиме реального времени, обрывать сессии с инфицированным кодом, перенаправлять трафик веб-приложения.

Познакомиться с работой решений F5 Networks участники конференции могли на нескольких демостендах, развернутых партнерами компании. Были представлены примеры интеграции продуктов F5 с продуктами технологических партнеров Cisco, Palo Alto Networks и Tenable, в тандеме с которыми возможно построение комплексной инфраструктуры, ориентированной на безопасную и быструю работу приложений.

ДОВОЛЬНЫЙ КЛИЕНТ – УСПЕШНЫЙ БИЗНЕС

Источник: http://ko.com.ua/dovolnyj_klient_uspeshnyj_biznes_119178
Автор – Евгений Куликов

Главным отличием второй конференции Perform Day Kyiv, организованной компаниями Dynatrace и БАКОТЕК, стал акцент на обсуждении практических примеров внедрения решений для мониторинга производительности приложений (APM) в компаниях различных отраслей. Партнерами форума выступили украинские SK Consulting и «ИТ Специалист», а также польская Omnilogy.

Современный розничный бизнес, будь то сфера финансовых услуг, торговля или телекоммуникации, невозможно представить без множества

цифровых сервисов. В тоже время по мере усложнения ИТ-систем специалистам становится все труднее отслеживать, оперативно обнаруживать и устранять возникающие сбои или задержки. Особенно в условиях современного ИТ-ландшафта, когда простой с точки зрения клиента сервис обеспечивается взаимодействием десятков систем, которые обслуживаются разными отделами, а то и компаниями. Между тем пользователь становится все более требовательным, он не хочет ждать и стремится получать искомое немедленно, независимо от местоположения, а в случае недовольства готов сразу же транслировать негатив в социальные сети. Поэтому быстрое решение проблем и удовлетворенность клиентов становится для бизнеса критически важной задачей.

Евгений Бадах: «Мы наблюдаем повышенный интерес к APM в нашем регионе, который трансформируется в растущее количество проектов в разных странах и отраслях»

Помочь в этом деле призваны системы класса APM (Application Performance Monitoring), а ключевым преимуществом платформы управления производительностью приложений от компании Dynatrace, одного из лидеров в данной области по версии Gartner, считается проактивность. Благодаря ей заказчик может отслеживать и оптимизировать работу традиционных, мобильных и веб-приложений, различных цифровых сервисов. Причем, в отличие от многих конкурирующих решений, есть возможность оценить ситуацию не только изнутри, со стороны инфраструктуры, а и с позиции пользовательского опыта. Это позволяет сократить время вывода продукта или услуги на рынок, уменьшить расходы на управление приложениями и сервисами, повысить их производительность, упростить и ускорить выявление и устранение возникающих проблем.

Платформа Digital Performance Management от Dynatrace может предложить два принципиально разных подхода к задачам APM – на базе программных агентов и, когда нет доступа к исходному коду приложения, на основе анализа копии сетевого трафика. Оба, как водится, имеют свои сильные и слабые стороны, но, по сути, являются взаимодополняющими и вместе позволяют получить наиболее полную картину происходящего. (Прим. ред.: рекомендуем также к прочтению интервью с Луишем Поремом, региональным вице-президентом Dynatrace).

Открывая Perform Day Kyiv 2017, генеральный директор БАКОТЕК Евгений Бадах сообщил, что его компания занимается вопросами APM уже около пяти лет, а конкретно продвижением разработок Dynatrace – два года. У компании наработана техническая экспертиза и накоплен немалый опыт в данной предметной области. Об актуальности темы APM и высоком интересе к ней свидетельствуют как значительное количество реализованных за минувший год проектов, так и существенно выросшее число участников киевского форума, в этот раз собравшего примерно 150 человек. Если же говорить о Dynatrace, то, по данным спикера, это технологический лидер в своем сегменте с рыночной долей около 14%, а одним из важных достоинств предлагаемой платформы является скорость развертывания. Причем с

прошлого года разработчик взял курс на расширение ее возможностей и охвата, отражением чего призван стать вводимый в обиход термин Digital Performance Management.

Владимир Поздняков: «Не надо далеко ходить за успешными примерами цифровой трансформации бизнеса. Таких компаний уже хватает и у нас в стране»

Знакомство аудитории с актуальными рыночными тенденциями продолжил Владимир Поздняков, региональный менеджер компании IDC. В своем докладе он затронул тему цифровой трансформации бизнеса и привел множество примеров того, как прорывные технологии и подходы за считанные годы меняют сложившиеся практики и целые отрасли. С учетом же нарастающего темпа развития человечества это означает, что в наше время ни одна компания не застрахована от стремительного упадка. **Ресурсный бизнес постепенно утрачивает значение и на первое место выходит экономика знаний.** Лидерам цифровой трансформации удается в разы, а то и на порядок улучшать свои ключевые показатели и получать значительное конкурентное преимущество. В том числе за счет удачного прикладного применения компонентов третьей платформы – мобильных устройств и приложений, социальных сетей, аналитики больших данных и облачных сервисов. Причем важное значение имеют не только сами изменения бизнес-процессов, но и скорость реализации новшеств. **Поэтому поиск и внедрение инноваций должны стать нормой существования для успешных компаний.** Бизнесу жизненно необходимо научиться тонко чувствовать клиентов и оперативно реагировать на переменчивые рыночные тенденции. Для этого требуется уже упоминавшаяся проактивность и в ряде технических моментов хорошим подспорьем на данном пути могут стать APM-решения.

Евгений Гончаренко: «В современных условиях на первое место выходят клиентский опыт и проактивный мониторинг»

Далее тему цифровой трансформации развил Евгений Гончаренко, руководитель департамента компании БАКОТЕК. Он справедливо заметил, что просчитать косвенные последствия наблюдаемых технологических сдвигов в различных отраслях попросту невозможно. К примеру, кто может сказать наверняка, как набирающие популярность электромобили с функцией автопилота повлияют на сферу автострахования или градостроения? Однако, тренд очевиден и бизнесу необходимо предпринимать меры, чтобы подняться на гребне волны, а не оказаться за бортом. Согласно Forrester, 93 % руководителей компаний считают, что цифровые технологии значительно преобразят их бизнес, а по версии Gartner, к 2020 г. они будут приносить до 40 % оборота.

Возвращаясь к разработке ПО, исследования показывают, что для многих пользователей скорость работы приложений важнее каких-то отдельных особенностей. В условиях, когда рынок перенасыщен

конкурентными предложениями, лояльность потребителя к бренду стремительно сокращается. На первое место выходит клиентский опыт и проактивный мониторинг. При этом ускорение темпов индустрии неплохо иллюстрирует пример самой Dynatrace. Так, если в 2011 г. вышло два крупных обновления ее флагманского продукта, то всего спустя пять лет – уже целых 26 за год, не считая сотен улучшений SaaS-решения. Чтобы соблюсти баланс между потребностями бизнеса в быстром запуске новых сервисов с одной стороны и возможностями разработчиков и отдела технической поддержки с другой, Dynatrace и развивает свою платформу DPM, которая призвана помочь этим трем звеньям сообща добиваться оптимизации пользовательского опыта, ускорения инноваций и совершенствования эксплуатации.

Яцек Куява: «Сегодня бизнесу жизненно необходимо иметь возможность анализировать пользовательский опыт в режиме реального времени»

Ряд прогнозов касательно перспектив рынка APM участникам конференции представил Яцек Куява (Jacek Kujawa), генеральный директор польской компании Omnilogy, которая является региональным представителем Dynatrace в Польше. Согласно оценкам экспертов, уже к 2018 г. взаимодействие бизнеса с пользователями на 50 % будет зависеть от аналитики в реальном времени. **Через два года около 40 % ИТ-проектов будут направлены на создание новых цифровых сервисов и источников дохода, включая монетизацию данных.** Доля пользователей технологий APM за пределами традиционных организаций, эксплуатирующих ИТ, вырастет с 40 % в 2016 г. до 70 % в 2020 г.

Не только разработчики, но и аналитики в своих исследованиях профильного сегмента управления производительностью переходят от масштаба приложений к более обширному понятию DPM, которое объединяет все возможные цифровые каналы взаимодействия с клиентом. Цифровой опыт позволяет компаниям сократить накладные расходы, увеличить базу клиентов и повысить их лояльность. Однако для этого необходимо иметь возможность анализировать пользовательский опыт в режиме реального времени. Что в свою очередь подразумевает наличие соответствующего инструментария сбора и обработки данных.

Для упрощения управления клиентским опытом взаимодействия с цифровым сервисом компания Omnilogy разработала и продвигает продукт Omniflow. Он позволяет на основе интеграции потока данных Dynatrace PureLytics и плагина Kibana визуализировать карту веб-приложения или сайта, облегчая изучение ситуации в различных бизнес-контекстах и поиск проблемных точек. Также Omnilogy берется помочь освоить технологию контейнеризации и повысить эффективность инфраструктуры приложений с использованием продукта JLupin Next Server.

Владислав Самойленко: «Нередко попутно проекты АРМ помогают решить такую непростую задачу, как улучшение взаимопонимания ИТ и бизнеса»

Переходя к практике, Владислав Самойленко, старший инженер поддержки проектов БАКОТЕК, рассмотрел ряд аспектов реализации проектов в области АРМ. Он отметил, что на стадии пилотного внедрения перед специалистами компании, как правило, возникает непростая задача улучшения взаимопонимания между бизнесом и айтишниками заказчика. Для прояснения текущей ситуации до выезда инженеров на место клиенту высылается опросник. Уже на этом этапе зачастую становятся очевидными отличия в подходах и ожиданиях представителей разных отделов. Между тем, как показывает опыт множества проектов, наиболее распространенными требованиями являются: отображение архитектуры взаимодействия компонентов, мониторинг активности пользователей и выявление связанных с ней ошибок, улучшение кода приложений.

Затем докладчик проиллюстрировал возможности решения этих и других задач с использованием продуктов Dynatrace на примере четырех проектов для заказчиков из разных отраслей и стран Балтии. Одному из них помогли выявить узкие места, найти общий язык со сторонним разработчиком и сократить сроки вывода в эксплуатацию нового сервиса. Другому предоставили возможность изучения активности пользователей портала интернет-банкинга с сегментацией по разным целевым группам. Третьему помогли разобраться с влиянием тех или иных действий посетителей на инфраструктуру и оптимизировать производительность веб-сервиса, а также оценить степень удовлетворенности клиентов. Наконец, четвертому – всесторонне проанализировать и усовершенствовать код приложений.

Валерия Янковская: «Бизнес-подразделениям "Киевстар" проект АРМ помогает глубже понять сложности клиентов и лучше контролировать ситуацию в случае возникновения неисправностей»

Опытом построения системы контроля цифровых сервисов в компании «Киевстар» делились Игорь Козенко, руководитель департамента автоматизации и управления ИТ-сервисами, и Валерия Янковская, руководитель электронных платформ. Отметим, что, по данным Евгения Гончаренко, на сегодня это одно из крупнейших внедрений в странах присутствия БАКОТЕК. Проект рассчитан на три года, с постепенным расширением охвата мониторинга на все цифровые каналы взаимодействия оператора с абонентами, а со временем, возможно, и на используемые сервисы третьих сторон, например, облачные.

Говоря о предпосылках проекта Игорь и Валерия фактически подтвердили уже звучавший тезис о том, что ожидания ИТ и бизнеса заметно отличаются, по меньшей мере на начальном этапе. Однако, коротко говоря, основная цель заключалась в улучшении мониторинга веб-сервисов оператора и повышении их качества с позиции пользователя. В частности,

одной из первоочередных задач была разработка наглядной приборной панели (dashboard), позволяющей сделать работу технических систем более прозрачной для бизнес-подразделений и руководства.

Уже сейчас можно говорить о некоторых результатах использования APM от Dynatrace в «Киевстаре». Проблемные ситуации стали прозрачнее для всех вовлеченных подразделений, что способствует созданию более конструктивной обстановки для их устранения, а соответственно зачастую сокращает сроки (примерно на 20%). Также за первый год проекта удалось ориентировочно вдвое уменьшить количество инцидентов и жалоб со стороны пользователей.

Помимо уже описанных докладов, в рамках Perform Day Kyiv 2017 участники мероприятия получили возможность ознакомиться с опытом: компании Playtech в части анализа производительности систем с проприетарным протоколом, компании SK Consulting в создании системы мониторинга клиентского опыта для крупного медиа-портала и компании Azerpay по контролю качества пользовательского опыта платежного сервиса. Также несколько презентаций были посвящены техническим вопросам анализа производительности закрытого ПО и мониторинга шин данных. Активность аудитории на протяжении всего дня дополнительно подчеркнула актуальность темы управления опытом пользователей цифровых сервисов в современных условиях.

ЗМІСТ