Сергей Груздев, компания Аладдин: Переоценка киберугроз, выявление и устранение точек отказа при построении безопасной доверенной ИТ-инфраструктуры

Сергей, тема вашего выступления на PKI-форуме была не вполне традиционной для этого уважаемого мероприятия. Регламент не позволил обсудить его непосредственно в зале, но по завершении сессии многие участники мероприятия подходили к вам за дополнительной информацией. Расскажите, пожалуйста, об этом.

Действительно, я затронул довольно больную тему, которая на конференциях обычно не поднимается, но в свете текущей ситуации она стала особенно актуальной.

На последних конференциях по информационной безопасности, проходивших после начала СВО, активно обсуждались проблемы, связанные с ушедшими зарубежными вендорами, необходимость замещения их решений российскими. Фиксируется рост успешных атак на наши организации, утечек персональных данных, баз данных, содержащих критическую информацию.

Ощущение, что для многих на рынке ИБ-ничего не изменилось. Вместо смещения фокуса нашего внимания на разработку и внедрение средств, направленных на недопущение утечек и успешных атак, по-прежнему предлагаются продукты по мониторингу атак, разбору инцидентов, улучшению инструментов для получения статистики и аналитики атак и инцидентов.

Мы по-прежнему движемся по инерции, боремся с "плохими парнями", пытающимися взломать наши информационные ресурсы, эксплуатировать уязвимости, подсаживать нам вирусы-шифровальщики, мы улучшаем защиту периметра, каналов связи…

Да, всё это надо делать и улучшать. Только мы совершенно упускаем из внимания, что мир кардинально изменился. Те риски и угрозы, которыми мы позволяли себе пренебрегать до СВО и считали их ничтожными, теперь "сыграли" по полной и стали нашей главной головной болью, часто затмевая все остальные.

Большинство до сих пор не до конца понимает, кто наш враг - кто нас атакует, от кого надо защищаться?

Многие до сих пор искренне считают, что их-то уж точно пронесёт! Что-то страшное может случиться, где угодно, только не у них.

Выполнил на бумаге основные требования Регуляторов – значит защищён. Типа "моё дело маленькое – что предписано, то я и сделал, значит, в случае чего, мне за это ничего не будет".

Мы до сих пор не верим, что ОНИ этого не сделают.

Так ведь сделали же, вопреки экономике, здравому смыслу и нашим ожиданиям: заблокировали работу западных платёжных систем, отключили ряд крупных банков от SWIFT, заблокировали производство российских процессоров и др. электроники на фабрике TSMC. А чего мы ждали, зачем сложили все яйца в одну корзину? Нам отключили облачные сервисы, в т.ч. и критичные для бизнеса – облачную аутентификацию корпоративных пользователей.

Так вот сейчас, как мне кажется, самое время остановиться, системно и всерьёз переоценить риски и угрозы для наших ИТ-инфраструктур. Оценить, что и как мы понастроили под сладкие рассказы западных вендоров, в т.ч. про облачные сервисы, Security as a Service и пр. модные веяния, выявить и устранить точки отказа.

Сегодня для всех должно быть совершенно понятно, что мы неправильно оценивали политические риски, архитектурные уязвимости, критические (технологические) зависимости. Мы продолжаем тратить бюджеты на ИБ на борьбу с навязанными нам угрозами.

Но жизнь показывает, что "прилетает" совсем не туда, куда ждёшь…

Здесь уместно вспомнить принятую в марте этого года новую национальную стратегию кибербезопасности США (почти дословно):

"Мы не будем дожидаться кибератак на объекты критической инфраструктуры США, мы должны бить первыми.

Мы знаем, кто наш враг, мы знаем, как и куда надо бить (объекты энергетики, органы государственного и военного управления, транспортной инфраструктуры).

Мы задействуем все имеющиеся у нас возможности, весь ***заложенный арсенал средств*** *для блокирования и вывода из строя ИТ-инфраструктуры организаций КИИ противника - как с помощью кибератак, так и с проведением военных операций (силами зависимых от нас партнёров)".*

А теперь про имеющийся в ИХ распоряжении АРСЕНАЛ СРЕДСТВ для вывода из строя наших ИТ-инфраструктур.

Здесь уместно вспомнить знаменитую фразу Барака Обамы – "Мы порвём экономику России в клочья!". Тогда, в 2012 г., над ней все посмеялись и забыли. Но это были не пустые слова…

В 2012 г. Обамой были подписаны два важнейших документа – PPD-20 и Cloud Act:

- Решение о закладке в объекты критической информационной инфраструктуры России кибербомб, которые можно привести в действие,

для вывода из строя системы командования и контроля вооружённых сил противника, объектов его критически важной инфраструктуры.
- Решение, которое обязывает американских вендоров осуществлять сбор и передачу в АНБ, ЦРУ и ФБР так называемой "телеметрии".
- Запрет американским вендорам на передачу и/или раскрытие исходных кодов ПО и прошивок "железа" другим государствам.
- Задание ЦРУ по разработке маскировочных программных средств проведения компьютерных атак, в том числе под "чужим флагом".

Зачем? Они начали готовиться к серьёзному противостоянию с Россией, к войне. Знания, на каком оборудовании и в какой среде работает данная информационная система, о заложенных в её компоненты уязвимостях и закладках, позволят быстро и эффективно парализовать её работу и вывести из строя данный объект КИИ.

Т.о. арсенал средств, имеющихся в распоряжении наших противников, точнее – врагов, использован далеко не весь. Есть ощущение, что с нами пока лишь играют…

А раз так, то наш фокус сейчас должен быть сосредоточен на обеспечении живучести и работоспособности нашей ИТ-инфраструктуры и устранении узких мест, способных её "положить".

Насколько уязвимы наши ИТ-инфраструктуры, есть ли у них Ахиллесова пята?

Увы… Ключевой и самый критичный элемент практически в каждой российской ИТ-инфраструктуре – это корпоративный центр выпуска и обслуживания цифровых сертификатов Microsoft CA (Certificate Authority).

CA – это основа доверенного взаимодействия всех объектов и компонентов в корпоративной сети. CA выпускает и ПРОВЕРЯЕТ **машинные** сертификаты для аутентификации серверов, роутеров, маршрутизаторов, точек доступа и всего прочего оборудования в сети, а также программные и пользовательские сертификаты доступа.

Проблема №1 состоит в том, что работоспособность практически любой нашей ИТ-инфраструктуры на 100% зависит от работоспособности MS CA.

В 2022 г. Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя. С 30 сентября 2023 г. Microsoft перестала продлевать подписки корпоративным клиентам из России.

Проблема №2 – полноценной альтернативы или аналога MS CA под Linux нет, наши надежды на Open Source не оправдались от слова совсем. Всё, что там выложено, это либо "завлекалки", либо сделано на старых технологических стеках и платформах, не масштабируемые, без перспективы их сертификации (порядка 40% проектов в бинарниках, без исходных кодов).

Всё это плохо собирается и плохо работает под российскими ОС, кучу всего надо переписывать, словом, всё это совсем не для Enterprise.

По поводу "завлекалок" корпоративных СА – есть несколько интересных проектов СА действительно Enterprise уровня, но они закрытые и коммерческие. Удалось узнать цену (правда только на базовый модуль – центр выпуска сертификатов) – цена космическая.

Ни один коммерческий СА Enterprise класса в Россию не поставляется ни под каким предлогом. Мы связывались за год до СВО, было сказано (дословно) – "*Это стратегический товар, продать корпоративный PKI в Россию — это хуже, чем поставить ядерные технологии в Ирак, словом, забудьте!*".

Проблема №3 – мы вынуждены мигрировать с Windows на Linux, но в Linux'е нет PKI.

И здесь мне часто приходится разрушать "картину мира" у очень многих, почти как в фильме "Стиляги". Помните сцену в конце фильма, когда герой возвращается из Америки и говорит: "У меня для тебя плохие новости – в Америке нет стиляг".

Примерно так же: "*Ребята, у меня для вас плохие новости, в Linux'е нет PKI. А без него всё это лишь консьюмерская история, а не полноценный Enterprise.Так же хорошо – всё необходимое органично встроено и доступно из всех сервисов, удобно, безопасно, так, как это сделано в Windows и к чему мы все привыкли, без поддержки PKI в Linux - никогда не будет*".

В Linux (как в российских, так и в международных проектах) нет не только полноценного аналога MS CA, но и клиентской части PKI, включая поддержку строгой двухфакторной аутентификации (2ФА) с использованием цифровых сертификатов, как это реализовано, например, в MS Smartcard Logon.

Напомню, что строгая двухфакторная аутентификация пользователей для критических и гос. систем – это must have, а также требование российских ГОСТов по идентификации и аутентификации. Большинство успешных атак и утечек происходит именно из-за неправильно реализованной подсистемы аутентификации пользователей или неиспользовании 2ФА и корпоративной PKI.

Это одна из ключевых и критически важных подсистем наших ИТ-инфраструктур, сделать её правильно – одна из первоочередных задач. Решив её, мы сможем предотвратить и большое количество инцидентов. Здесь хорошо работает правило Парето – 20% усилий (и ИБ-бюджета) даст 80% результата.

Проблема №4 – совместимость с разными экосистемами.

Многие российские вендоры создают собственные экосистемы. Я не очень люблю это понятие. Есть несколько разных определений. Одно из них говорит, что *экосистема – это замкнутое, самодостаточное и довольно*

хрупкое образование (пространство), любое вмешательство извне способно его разрушить.

Windows – это тоже замкнутая, большая и вполне устойчивая экосистема. Мы живём и работаем в ней много лет, привыкли, создали множество приложений. Взять и одномоментно перейти в другую замкнутую экосистему (на Linux) теперь никто не сможет. Мы обречены ещё достаточно долго как-то поддерживать её и пытаться работать сразу в двух экосистемах – Linux и Windows. Но в таком случае нужно сразу говорить про необходимость работы в сложной гетерогенной среде, а не обманывать себя, и не запутывать других.

Проблема миграции на Linux усугубляется необходимостью параллельно (пусть даже некоторое время) работать в двух экосистемах – Linux и Windows. Пользоваться сервисами и приложениями, которые ещё не портированы под Linux. Это требует разработки не просто аналога MS CA и MS Smartcard Logon, а гораздо более сложного инфраструктурного ПО, умеющего работать в двух параллельных "мирах", совместимого с разными домен-контроллерами и службами каталогов - MS Active Directory, Samba DC, FreeIPA, ALD Pro, РЕД АДМ, Альт Домен.

Построить доверенную ИТ-инфраструктуру Enterprise-уровня и выполнить требования регуляторов для организаций КИИ без разворачивания PKI не получится?

Верно, не получится. Давайте попробую объяснить почему.

Начну с ДОВЕРИЯ. К сожалению, в последнее время это понятие (и термин) сильно замусолили, не очень понимая его суть.

Что такое доверие?

В мире людей – *это открытые взаимоотношения между людьми (субъектами), содержащие уверенность в порядочности другого, в возможности поделиться с ним личной или сокровенной информацией, в его ответственности не воспользоваться этой информацией вам во вред*.

Применительно к ИТ-технологиям и информационной безопасности (ИБ) это определение тоже работает. *Если мы строим безопасную доверенную ИТ-инфраструктуру гос. организации, КИИ, то каждый её элемент должен быть доверенным, а значит надёжно (гарантированно) идентифицирован и аутентифицирован*.

Здесь мне хочется процитировать В.В. Путина - "*В деле, которым я занимаюсь, нужно оперировать другими категориями - здесь вопрос не в доверии, а в гарантиях*".

Для ИБ (которой мы занимаемся) также *важнее не доверие, а гарантии*.

Необходимые гарантии даёт криптография - гарантированная стойкость, PKI (централизованная инфраструктура открытых ключей), безопасность закрытых ключей - в средствах 2ФА - USB-токенах и смарт-картах с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом.

Основа доверительных отношений – надёжная АУТЕНТИФИКАЦИЯ всех субъектов ИТ-инфраструктуры: "железа" (сервера, роутеры, маршрутизаторы и т.п.), ПО (ОС, системное, прикладное ПО, службы, сервисы и пр.), пользователей.

Согласно принятым российским ГОСТам по идентификации и аутентификации (которые, кстати разрабатывала наша компания), есть 3 типа аутентификации с разными уровням доверия:

1) Простая – обеспечивающая некоторую уверенность в том, что данный пользователь является тем, за кого себя выдаёт. Как правило, в информационных системах – это пара Логин-Пароль.

2) Усиленная – обеспечивающая достаточно высокую уверенность, которую даёт, как правило, наличие второго фактора (токена или смарт-карты).

3) Строгая – обеспечивающая очень высокую степень уверенности, добиться её можно только с использованием криптографических средств 2ФА.

Для организаций с высоким уровнем значимости информации в ИС, высокой вероятностью и размером возможного ущерба (гос. организации, КИИ) необходимо применять СТРОГУЮ аутентификацию.

Реализовать строгую аутентификацию пользователей в ИС можно только с использованием средств 2ФА – USB-токенов и смарт-карт с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом – невзламываемых и неклонириуемых, разворачиванием инфраструктуры открытых ключей (PKI). Главным компонентом PKI является корпоративных центр выпуска и обслуживания сертификатов доступа (аутентификации) – CA, а также поддержка средств 2ФА и PKI на клиентском ПО.

Напомню, что в Windows – это Microsoft CA (CS) на сервере (входит в состав Windows Server как "бесплатный сыр") и MS Smartcard Logon, обеспечивающий для пользователей простой и понятный интерфейс для 2ФА.

Для Linux же, как я уже говорил, картина совсем другая – доверенный CA Enterprise-класса отсутствует (*здесь не путать УЦ под Linux для выпуска и обслуживания сертификатов электронной подписи по 63-ФЗ и корпоративным центром сертификации!*). Полнофункционального аналога MS Smartcard Logon, умеющего работать с сертификатами, тоже нет. Чтобы реализовать поддержку средств 2ФА и аутентификацию в Linux с их помощью, придётся самостоятельно доработать, установить и настроить порядка 34 пакетов – не каждому под силу…

То есть на текущий момент выполнить требования по реализации строгой аутентификации и построить безопасную доверенную ИТ-инфраструктуру организаций КИИ в соответствии с требованиями регуляторов практически невозможно?

С помощью имеющихся средств, предоставляемых разработчиками российских ОС на базе Linux – нет.

Но мы с ними активно работаем в этом направлении и уже выпустили на рынок набор ключевых компонентов, необходимых для разворачивания корпоративной PKI на Linux с поддержкой средств 2ФА.

Первый ключевой компонент для построения безопасной доверенной ИТ-инфраструктуры – это Aladdin Enterprise CA – корпоративный центр выпуска и обслуживания сертификатов.

Он позволяет заместить такой критичный элемент в инфраструктуре, как MS CA – единую точку её отказа, о которой я говорил, объединить все компоненты ИТ-инфраструктуры в единый домен безопасности, обеспечить их аутентификацию и безопасное взаимодействие, одновременно работать с различными службами каталогов, как в Windows, так и Linux.

Второй важнейший компонент – это клиент под Linux – Aladdin SecurLogon, обеспечивающий строгую 2ФА пользователей по цифровым сертификатам с использованием выпускаемых нами USB-токенов и смарт-карт JaCarta PKI. Это третий важнейший компонент инфраструктуры. Он позволяет обеспечить усиленную 2ФА с использованием одноразовых паролей (OTP) и др. методов для тех, кто ещё не развернул у себя в инфраструктуре PKI.

Отмечу, что SecurLogon позволяет аутентифицироваться как в Linux, так и в Windows. Причём, и это принципиально, решение "свой-чужой" и разрешение на вход в систему здесь принимаем мы (наше доверенное ПО), а не чужое, как в случае с Windows Smartcard Logon.

SecurLogon имеет привычный для многих интерфейс, как у Windows Smartcard Logon, так что проблем с переходом не возникнет.

Четвёртый компонент также относится к инфраструктурным. Это корпоративная система централизованного управления жизненным циклом сертификатов, токенов и смарт-карт, средств криптографической защиты и пр. – JMS (JaCarta Management System). Именно она позволяет обеспечить учёт и контроль выдаваемых сертификатов, средств 2ФА и ЭП, автоматизировать большинство рутинных операций и применение политик безопасности для различных групп пользователей.

JMS также включает в себя высокопроизводительный сервер аутентификации Enterprise-класса.

Внедрять средства 2ФА и PKI без подобной системы централизованного управления – просто утопия.

И здесь я хотел бы отметить ещё одну важнейшую компоненту - пятую. Это подсистема современной ИТ-инфраструктуры любой достаточно крупной организации. Это обеспечение безопасной дистанционной работы сотрудников.

Пандемия показала, что удалёнка крайне востребована и прочно вошла в нашу жизнь. Пандемия прошла, кто-то сохранил у себя созданные в период пандемии решения, кто-то удалёнку у себя запретил, понимая, что это была крайне вынужденная и очень опасная мера…

Соглашусь, применяемые многими решения для организации дистанционной работы своих сотрудников на базе "служебного ноутбука", очень небезопасны. Потому что поверхность атаки такого сложного решения огромна – и через недоверенное "железо", и через заложенные уязвимости в процессорных чипсетах, UEFI, протоколах, спецификациях USB и пр.

Мы в своё время сделали и сертифицировали специализированное решение для обеспечения безопасной дистанционной работы сотрудников органов исполнительной власти при использовании ими недоверенных (личных) средств вычислительной техники – Aladdin LiveOffice.

Это решение сделано на базе технологии LiveUSB, позволяет загружать со специализированного защищённого USB-носителя изолированную замкнутую доверенную программную среду практически на любом компьютере, из неё по защищённому каналу подключаться к своему виртуальному рабочему столу (VDI) или к своему служебному компьютеру и безопасно работать на нём.

Такое специализированное решение соответствует требованиям Регуляторов к средствам безопасной дистанционной работы, имеет гораздо меньшую поверхность атаки по сравнению со служебным ноутбуком, его не нужно дополнительно аттестовывать в составе ГИС или ИСПДн, не нужно обеспечивать контролируемую зону при работе с информацией ограниченного доступа (ДСП) и различными видами служебной тайны.

В общем, применение специализированных средств для организации безопасной дистанционной работы с возможностью подключения к ГИС, ИСПДн и пр. – это и намного безопаснее, и дешевле. Да и риски новых эпидемий и пандемии никто не отменял – все мы под Богом ходим…

Ещё один важный момент. Было несколько инцидентов с "прилётом" в министерские башни Москва-Сити. Работа на несколько дней парализована, сотрудников отправили на удалёнку.

Какие ещё выводы из этого надо сделать? С учётом того, что я уже говорил про новую стратегию кибербезопасности США?

Теперь любая организации КИИ и органов госуправления стали целями и мишенями не только для кибернападения, но и для точечного военного нападения с целью уничтожения её инфраструктуры и блокирования работы.

Это означает, что у таких организаций на подобный случай (не дай Бог) должен быть реализован план-Б, не допускающий простоя и причинения неприемлемого ущерба. У каждого сотрудника в кармане должен быть такой USB-токен (Aladdin LiveOffice).

Кстати, LiveOffice можно использовать не только как специализированное средство для безопасной дистанционной работы, но и как обычный USB-токен для 2ФА, как средство ЭП, как защищённую флешку для хранения и переноса служебных документов.

В общем, при нынешних временах это становится must have.

В начале нашего разговора вы упоминали про рост утечек критически важной информации и персональных данных. Вы же давно занимаетесь защитой данных от подобных утечек?

Да, в начале нашего разговора я говорил, что многие аналитики и российские вендоры фиксируют большой рост утечек. Но вместо того, чтобы фокусироваться на защите самих данных, нам опять навязываются какие-то странные решения по мониторингу хакерской активности, отслеживанию действий нарушителей внутри взломанного периметра сети, применение искусственного интеллекта для выявления поведенческих аномалий и пр.

Что, все смирились с неизбежностью таких утечек, невозможностью защититься от внутреннего нарушителя? Ведь мы-то хорошо понимаем, что утекают базы не через взломы, а изнутри. Мы научились эффективно защищать базы данных и обезличивать персональные данные в них. Копировать и воровать их (даже имея полный административный доступ) бесполезно.

Мы отработали эффективную технологию импортозамещения встроенных в иностранные СУБД иностранных средств защиты, позволяющую изолировать критически важные данные от самой СУБД и решить проблему со старыми унаследованными приложениями, которых у организации может быть сотни. Быстро и просто их не перепишешь и не перенесёшь на отечественный Postgres Pro. Проблемы с миграцией именно в этом, не в самих СУБД.

Крипто БД обеспечивает защиту главных информационных активов организации (ERP, CRM, ИБС, ИСПДн и др.) от утечек, кражи, от внесения несанкционированных изменений и искажения чувствительной информации,

от несанкционированного доступа к критически важным данным администраторов СУБД (внутренних нарушителей). Решение обеспечивает получение некорректируемой юридически значимой доказательной базы для проведения расследований инцидентов.

Это достаточно зрелый продукт, ему уже порядка 10 лет. В начале октября, кстати, мы получили на него новый сертификат ФСБ России.

И ещё один очень важных продукт для защиты критически важных данных от утечек – это Secret Disk – система защиты данных на дисках.

Этот продукт также из разряда must have. Вся служебная информация, выносимая за пределы организации, должна быть зашифрована.

На конференциях часто задаю аудитории вопрос – *данные на своих ноутбуках шифруете? Да-ааа! Чем? BitLocker'ом!*

Красавцы! Лучший способ похоронить свои данные – это продолжать добровольно пользоваться бесплатным продуктом MS Windows BitLocker.

Это лучший вирус-шифровальщик! Всё, дальше говорить об этом даже не хочу – все материалы про ЭТО есть на нашем сайте (www.aladdin.ru) – читайте, смотрите вебинары, думайте.

Что бы вы хотели сказать в заключение?

Только то, что говорю обычно – мы живём с вами в интересное время, сейчас нам дали уникальную возможность перезагрузиться, другими глазами посмотреть на всё то, что нам вещали западные провидцы, что нам так настойчиво насаждали, и попытаться сделать всё правильно.

Не пытаться затыкать дыры, заменяя одни продукты ушедших из России западных вендоров другими, часто наспех собранными из Open Source, а начать с проектирования правильной и безопасной ИТ-инфраструктуры, без наследования "родимых пятен" и навязанных нам ИХ "ценностей".

На банковском рынке нам удалось это сделать. Россия совершила "квантовый скачок", перепрыгнула целую эпоху платёжных карт с магнитной полосой, сразу на смарт-карты, и стала одним из лидеров.

Так что у нас есть исторический шанс! Давайте стараться делать всё правильно и безопасно! …и немного на вырост.