**Homework - [Lecture 1] - Introduction to information security – Prokhorov Andrey**

1. **Вредоносное ПО** - это любое программное обеспечение, намеренно предназначенное для нанесения ущерба компьютеру, серверу, клиенту или компьютерной сети. Сюда можно отнести различные малвари, которые выступают в роли кейлогера, в роли майнера, также может просто выстраивать топологию сети компании. Вообщем, для меня это топ один угроза, поскольку грамотно написанный малварь может принести огромные убытки для компании, вплоть до ее банкротства. Сюда также стоит добавить различные шифровальщики и инструменты шантажа – это тоже вредоносное ПО, которое шифрует данные, блокирует работу компании, требует за эти данные выкуп.

Первичным вектором может являться спам рассылки с вредоносным ПО, после открытия срабатывает макрос, который заставляет “пробудить” малварь.

Возьмем для примера WannaCry, первое место среди всех вымогательских ПО, от которого пострадало множество пользователей в более чем 100 странах мира. Жертвами стали такие известные компании, как Boeing, LG Electronics, автоконцерны и др. Американские эксперты оценили ущерб от масштабной хакерской атаки, которая в начале мая 2017 года обрушилась на компьютерные системы госорганов, крупных корпораций и других учреждений в 150 странах мира. Этот ущерб, уверены оценщики KnowBe4, составил $1 млрд. По этим данным, всего WannaCry поразил от 200 тыс. до 300 тыс. компьютеров.([https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:WannaCry\_(%D0%B2%D0%B8%D1%80%D1%83%D1%81-%D0%B2%D1%8B%D0%BC%D0%BE%D0%B3%D0%B0%D1%82%D0%B5%D0%BB%D1%8C)#.D0.9A.D0.B0.D0.BA\_.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D0.B0.D0.B5.D1.82](https://www.tadviser.ru/index.php/Статья:WannaCry_(вирус-вымогатель)" \l ".D0.9A.D0.B0.D0.BA_.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D0.B0.D0.B5.D1.82))

Для того, чтобы снизить риск попадания таких вредоносных ПО в инфраструктуры компаний, необходимо:

1) Держать основные ПО всегда обновленными;

2) Использовать антивирусы;

3) Обучать и поддерживать уровень знаний ИБ(митап, требования и т.д);

Если работники будут использовать сложные пароли, не переходить, открывать фишиноговые сайты, письма, не будут вставлять в рабочий ноутбук/ПК флешку, которую нашли на улице, то это значительно снизит риск попадания зловреда в инфраструктуру.

2. **Фишинговые сайты** – один из инструментов **социальной инженирии**, некий клон основного сайт. Представим кейс, когда человеку приходит письмо на почту, или смска, где его поздравляют с выйгрышем нового смартфона, но чтобы его забрать, нужно оплатить доставку, после чего деньги за доставку вернут. Что такое эти 5 000 рублей, когда бесплатно дарят смартфон в несколько раз дороже доставки. Недолго думая, жертва вводит свои креды от карты. Далее кто то продает данные карты в Даркнет, кто то скупает товары в интернете, кто то пробует зайти в банковское приложение, используя ситуацию, жертву можно заставить помочь войти в личный кабинет. Почему это для меня топ 2? Потому что очень легко проэксплуатировать. Нужен домен, тачка, на которой поднять “клон” нужнего сайта, поднять повыше в поиске, угроза готова. Страдают не топ компании, а наивные, доверчивые, пожилые люди.

Если брать пик активности, а именно локлаудн 2020года, то ущерб первого квартала мог достичь 3 млрд рублей.([https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3\_%D0%B2\_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8](https://www.tadviser.ru/index.php/Статья:Фишинг_в_России))

Фишинговые сайты в топах поиска долго не живут, основые поисковые системы банят такие домены. Но не стоит исключать спам рассылки. В наше время банки стараются учить людей не передавать чувствительные данные третьим лицам, придумывать сложные пароли, держать их у себя в голове, что сокращает число жертв социальной инженирии. Я считаю, чтобы снизить риск данной угрозы, нужно просто освещать данную проблему, учить людей цифровой гигиене.

3. **Веб уязвимости**. Уровень защищенности веб-приложений продолжает постепенно расти, но все еще остается довольно низким. Кто то соблюдает процессы безопасной разработки, тратя время на тестирование безопасности, другие же предпочитают выливаться быстрее и чаще. У таких компаний как правила есть серьезные проблемы с безопасностью. Эти уязвимости могут привести компанию к потери репутации у клиентов. Базовые уязвимости из OWASP TOP 10 постоянно обновляются, меняются местами, потому что все это актуально. Баг баунти программы позволяют снизить риск, но не у всех есть на это деньги. Я считаю этот тип уязвимостей топ 3, поскольку каждое мобильное, веб приложение имеет свои недостатки, которые порой могут привести к эксплуатации уязвимостей. Огромные компании-гиганты совершают маленькие ошибки, которые могут привести к угрозам, например, Apple(<https://xakep.ru/2021/10/01/airtags-xss/>). Просто не добавили экранирование, пример xss. Эксплуатировал ли кто то данную уязвимость и ее ущерб, не известно. Обычно такие инциденты не афишируются, базы данных с ПдН клиентов без шума благодаря sql атакам идту на продажи.

Чтобы предотвратить все эти уязвимости, необходимо на каждом этапе развития продукта прорабатывать риски безопасности(использовать SecureSDLC), консультировать разработчиков писать безопасный код, следить за окружением для разворачивания сервисов.

4. **0-day уязвимости**. Уязвимости нулевого дня являются огромным риском для компаний, чей продукт подвержен риску. Все приложения используют third party библиотеки, которые написаны сторонними компаниями. Такие зависимости могут содержать известные уязвимости, поэтому также важно проверять их. Но когда всплывает уязвимости нулевого дня, компания должна принимать какие то меры. Для начала, нужно понять все точки входа, все приложения, которые уязвимы. Возможно стоит прикрыть сервисы, что торчит наружу, дабы исключить риск атаки. А далее остается ждать фикса и в незамедлительном порядке, обновиться.

Для примера можно взять Log4j. Это уязвимость нулевого дня в Log4j, популярной среде ведения журналов Java, включающая выполнение произвольного кода

Насчет инцидентов, очень много компаний пострадало, таких как Amazon, Steam, даже Майнкрафт был уязвим. Многие приложения на Apache содержали эту библиотеку, что позволяло проэксплуатировать RCE. Чтобы снизить риск, необходимо придерживаться ряду рекомендаций:

1) Следить за тем, чтобы программы регулярно обновлялись;

2) Использовать файерволлы, dmz зоны;

3) И список рекомендаций из первой угрозы про вредоносные ПО. 0-day уязвимости очень часто существуют в малварях, которые закидывают через спам.

5. **DdoS-атаки**. DdoS-атаки – атаки из типа “отказ в обслуживании”. (<https://itelon.ru/blog/zashchita-servera-ot-ddos-atak/>)

DoS (Denial of Service) – это перегрузка сети паразитным трафиком (т.н. флуд), когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания входного маршрутизатора. Существует куча типов атак, но все они нацелены на перегрузку серверов. Каждая секунда недоступности сервиса несет огромные убытки для компании как в денежном эквиваленте, так и в доверии людей к ресурсу. DdoS используют как оружие для устранения конкурентов. Разные сервисы пытаются вывести друг друга из ”строя”. Вот один из примером(<https://xakep.ru/2021/11/30/cannazon-closed/>), атака привела к закрытию “магазина” в интернете.

Чтобы предотвратить подобного рода атаки, необходимо использовать аппаратные и программные средства анти-DdoS;

Cпециальные защитные средства, защищать DNS-сервер;

Увеличить полосу пропускания.