PASS Panda Security Summit | The European Cybersecurity Hub

КИБЕР-УСТОЙЧИВОСТЬ:

КЛЮЧ К БЕЗОПАСНОСТИ КОМПАНИИ

#PASS2018

Введение

Быстрый поиск термина "resilient companies" ("устойчивые компании") в Google выдает 44 400 000 результатов менее чем за секунду. Это понятие, определяемое как "способность быстро восстанавливаться после трудностей и становиться сильнее", стало ключевым для предприятий, которые сталкиваются с огромным количеством рисков, возникших в контексте глобальной экономики: кибер-атаки, крупномасштабные глобальные мошеннические аферы и кража персональных данных, потенциально негативные последствия технологических достижений, таких как искусственный интеллект, геоинженерия и синтетическая биология, которые способны влиять на окружающую среду, экономику и самих людей.

Мы наблюдаем трансформацию социальных отношений, работы предприятий и деятельности правительственных органов - трансформацию, которая основывает свой потенциал на технологиях, данных и искусственном интеллекте, которые собирают, фильтруют, классифицируют и сопоставляют огромные объемы данных для того, чтобы учиться на них и делать прогнозы.

Таким образом, цифровая трансформация влияет на повседневную жизнь и работу организаций в таких масштабах, что в настоящее время она стала источником благосостояния компании и инструментом обеспечения конкурентоспособности целых стран. Присваивание этого благосостояния уже не является результатом вооруженных конфликтов, а осуществляется в результате "всего" лишь цифровой передачи этого благосостояния, информационных активов, которые идентифицируют и отличают ту или иную страну. Поэтому все, что теперь нужно, - это кибер-битва, чтобы атаковать ключевые компьютеры и получить информацию, необходимую для свержения правительства или лишения страны ее конкурентного преимущества.

Если считать устойчивость императивом, то понятие термина "устойчивость" можно описать как "неотъемлемая способность организма, организации, компании или государства, которая позволяет им преодолевать кризис без тяжелых последствий для их деятельности". Речь идет не только о способности восстанавливаться, но также и о возрождении и расширении своих возможностей после неблагоприятного поворота событий.

В контексте безопасности кибер-устойчивость означает способность организации поддерживать свои основные функции и целостность при воздействии потенциальных атак с угрозой ее информационной безопасности.

Кибер-устойчивая компания - это компания, которая способна предотвращать, обнаруживать, сдерживать атаки и восстанавливаться после них, минимизируя свою подверженность атаке и ее влиянию на бизнес - т.е. противостоять бесчисленному количеству угроз данным, приложениям и ИТ-инфраструктуре, но особенно угроз устройствам, где находятся самые ценные информационные активы предприятия, т.к. их поражение будет означать также нарушение неприкосновенности предприятия и сотрудников.

При росте опасностей традиционных подходов для обеспечения кибер-устойчивости уже не хватает. Многие организации пребывают в условиях неустойчивого равновесия, и малейшие изменения, какими бы незначительными они ни были по сравнению с их размерами или важностью их деятельности, способны спровоцировать кризис. Чтобы избежать коллапса, управление информационной безопасностью потребует тщательного пересмотра и внедрения новых моделей защиты.

До недавнего времени основными объектами для кибер-атак были финансовые организации и правительственные органы. Сегодня развитие бизнеса любого размера и в любом секторе в той или иной мере зависит от Интернета, и, как следствие, угрозы стали более универсальными. По мере роста этих опасностей, текущие подходы к обеспечению кибер-устойчивости более не работают. Управление информационной безопасностью нуждается в тщательном пересмотре для внедрения новых и более усовершенствованных моделей безопасности.

Недавно мы стали свидетелями инцидентов с Meltdown и Specter, которые показали уязвимости не только в ПО, но и в "железе". Аналогично, в период с 2011 по 2014 года мы видели, как энергетические компании в Канаде, Европе и США были атакованы кибер-шпионской группировкой Dragonfly. В мае 2017 года вымогатель WannaCry удерживал в "заложниках" общественные и коммерческие организации в сфере телекоммуникаций, здравоохранения, логистики и пр. Также в 2017 году шифровальщик NotPetya нацелился на крупные европейские компании практически из всех сфер экономики.

Но пока коллективное сознание в этой области развивается медленно, вместе с этим растет и непонимание. Компании и их руководители обеспокоены этой проблемой. Согласно исследованию, выполненному в начале этого года Forrester Consulting for Hiscox[1], при опросе более чем 4100 руководителей, директоров по ИБ, ИТ-директоров и других ключевых сотрудников компаний и организаций в США, Германии, Великобритании, Испании, Нидерландах и других странах Евросоюза, 57% опрошенных компаний заявили, что они готовы реагировать на атаки безопасности. Однако более детальное изучение косвенных вопросов показывает, что 73% опрошенных компаний имеют низкий уровень компетенции и являются "новичками" в вопросах обнаружения и реагирования на кибер-атаки. И только 11% организаций имеют в своих департаментах безопасности экспертов, а значит, хорошо подготовлены к решению проблем ИБ.

Чтобы сохранить и повысить кибер-устойчивость к кибер-атакам, компании должны занять новую позицию: всеобъемлющую, стратегическую и активную с помощью нового подхода к своей программе безопасности, которая сможет защитить их предприятия без введения необоснованных ограничений на их бизнес. И эта новая позиция должна основываться на усилении превентивной защиты, предполагая, что они могут быть преодолены хакерами, или исходя из того, что хакеры уже проникли внутрь компании. Новые техники для преодоления защиты и сокрытия вредоносных программ позволяют угрозам оставаться в корпоративных сетях в течение длительного времени без их фактического обнаружения.

Нельзя забывать и о внутренних угрозах. Атаки сотрудников с привилегированными правами доступа представляют собой одну из самых больших угроз безопасности корпоративных и клиентских данных. Расследования, проведенные Ponemon Institute, указывают на хакеров и криминальных инсайдеров как на главных виновников дыр безопасности и утечек данных.

Данные взяты из 2016 DBIR

[1] 2018 Hiscox Cyber Readiness Report https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Сдвиг парадигмы в сторону устойчивости компании заключается в том, чтобы избежать компрометации активов компании и обнаруживать атаки в течение ограниченного периода времени до причинения ущерба. Настало время материализации таких тенденций, как Threat Hunting, экспертный анализ для выявления первопричин атаки, обнаружение атаки на конечном устройстве и реагирование на нее (EDR), а также непрерывный мониторинг конечных устройств. Крайне важно генерировать экспертные данные в реальном времени, чтобы тщательно расследовать инциденты.

В то же время, компания, которая стала устойчивой, будет признавать, что возникают сбои и ошибки, и будет иметь средства для восстановления нормальной работы по обеспечению безопасности активов и собственной репутации. Короче говоря, организация способна выйти из инцидента более сильной, применяя изменения, способные еще улучшить ее защиту.

Эволюция кибер-угроз

Кибер-преступность - это привлекательный и высокодоходный бизнес. Хакеры имеют в своем распоряжении все больше и больше ресурсов, чем когда-либо ранее, как технических, так и экономических. Это позволяет им разрабатывать все более сложные атаки. Результат - появление более сложных и более динамических угроз в дополнении к возрастающему числу атак.

Equifax, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, вмешательства в выборы… вот лишь некоторые персонажи историй с информационной безопасностью предприятий за последние месяцы. Они были главными действующими лицами массовых заражений, краж данных, атак шифровальщиков, взломанных приложений, использовавшихся для запуска атак против конкретных крупных компаний, или использования уязвимостей, повлиявших на миллиарды устройств.

Необходимо принять во внимание хаос, вызванный тремя недавними событиями. С 2011 до 2014 года кибер-шпионская группировка Dragonfly постоянно фигурировала в заголовках СМИ, быстро расширяя свою деятельность и ставя под угрозу энергетические компании Северной Америки и Евросоюза. Dragonfly использовал преимущества двух основных компонентов вредоносной программы, а именно инструментами удаленного доступа, получающими доступ к зараженным ПК и контролирующими их.

В 2017 году **было две атаки, которые особенно выделились своим влиянием и причиненным ущербом: WannaCry и GoldenEye / NotPetya.**

WannaCry появился в мае, распространяя и сея хаос в корпоративных сетях по всему миру, оказавшись одной из крупнейших атак в истории. Хотя мы видели и более мощные атаки в прошлом (такие как Blaster или SQLSlammer, если брать только два), хотя бы с точки зрения количества жертв и уровня распространения, но правда в том, что причиненный ими ущерб был всего лишь побочным. Однако WannaCry - это вымогатель с функциями сетевого червя, поэтому каждый зараженный компьютер кончил тем, что на нем были зашифрованы документы.

Goldeneye / NotPetya был второй атакой в году с наибольшим воздействием, как вторая волна землетрясения после WannaCry. Несмотря на то, что его жертвы первоначально были ограничены определенной территорией (Украина), все же от него пострадали компании в более чем 60 странах.

Тщательно спланированная атака была выполнена на украинские компании через очень популярную бухгалтерскую программу M.E.Doc. Хакеры взломали ее сервер обновлений, в результате чего все компьютеры с установленным M.E.Doc могли немедленно и автоматически заразиться.

В дополнение к шифрованию файлов, если авторизованный пользователь имел права администратора, зловред уходил в главную загрузочную запись (MBR) жесткого диска. Сначала казалось, что это шифровальщик в стиле WannaCry, но после тщательного анализа **стало ясно, что его авторы не намерены позволять восстанавливать выкупленные файлы.** Спустя несколько дней украинское правительство открыто обвинило Россию в проведении этой атаки.

В области кибер-безопасности 2018 также начался плохо: дыра безопасности, обнаруженная в процессорах Intel, AMD и ARM, была смертельно серьезна. Эта ошибка в разработке архитектуры, сопровождаемая ошибками в операционной системе, стала "бомбой" в технологическом секторе, который круглосуточно работал над тем, чтобы оперативно устранить все проблемы.

Недостаток, используемый **эксплойтом Meltdown** в архитектуре Intel, особенно критичен с точки зрения извлечения конфиденциальных данных (регистрационные данные, письма, фотографии и другие документы), позволяя хакеру с помощью вредоносного процесса, запущенного на уровне пользователя на компьютере или сервере, считывать память у других процессов, включая привилегированные процессы ядра операционной системы.

Пострадали домашние пользователи и практически все корпоративные пользователи, т.к. Specter работает на компьютерах, ноутбуках, смартфонах с Android, а также на локальных и облачных серверах. Чем более критична обрабатываемая информация, тем выше риск стать целью для атаки, использующей этот инструмент.

Есть еще и другие инциденты с гигантами в различных секторах экономики. Например, **Apple**, которая "засветилась" историей с арестом в Китае 22 человек, которые якобы незаконно торговали корпоративными данными. Все указывает на работу инсайдера, т.к. некоторые из числа задержанных работали у подрядчиков Apple и имели доступ к продаваемым данным.

Американская кабельная и спутниковая телесеть **HBO** также пострадала от ряда кибер-атак за последние месяцы. В одной из них были взломаны серверы, с которых украли новые и еще не вышедшие на экраны сезоны ряда телесериалов, а также ряд внутренней информации.

InterContinental Hotels Group (IHG) стала жертвой кражи данных клиентов. Хотя компания заявила в феврале, что атака затронула только десяток ее отелей, но теперь стало известно, что у них пострадали POS-терминалы в более чем 1000 их учреждений. Среди многочисленных брендов, которыми владеет данная группа компаний, есть такие как Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels и Crowne Plaza.

Saber Corporation - это североамериканская компания, которая управляет бронированием номеров в 100 000 отелей и билетов у более чем 70 авиакомпаний по всему миру. Хакер получил учетные данные для доступа к одной из систем бронирования компании, получив доступ к платежной информации и подробным данным по бронированию. Эта система управляет бронированием номеров для физических лиц и туристических агентств в более чем 35 000 отелях. Их система оставалась взломанной в течение 7 месяцев с 10 августа 2016 г. до 9 марта 2017 г.

Но самое крупное нарушение безопасности в этом году (и одно из самых ужасных в истории) может произойти чуть позже, когда стало известно, что гигант кредитной отчетности **Equifax** был скомпрометирован. Компания предупредила, что общее количество пострадавших лиц может составлять 147,9 миллионов человек. Вопрос: можно ли было предотвратить такую атаку ? Ответ, конечно же, да. **Equifax оставил кибер-преступникам "открытую дверь", не обновив Apache Struts**, среду для разработки веб-приложений. Эта незакрытая уязвимость позволила хакерам получить номера социальных страховок, почтовые адреса и номера водительских удостоверений миллионов людей. Это пример того, как несоблюдение базовых мер безопасности (например, обновление ПО) может иметь колоссальные последствия.

С подобными реальными случаями неудивительно, что 75% компаний (согласно недавнему исследованию McKinsey[2]) считают, что информационная безопасность является приоритетом для их надлежащей работы. Быть готовым к кибер-атакам - это серьезная проблема в таких отраслях, как банковская деятельность или производство автомобилей, о которых можно подумать, что здесь следует больше беспокоиться о других серьезных изменениях и рисках. Мы имеем дело с универсальной и горизонтальной угрозой.

Угроза слишком велика, и слишком быстро растет количество хакеров, которые при этом становятся все более изощренными.

Чтобы поддерживать и повышать уровень своей устойчивости, компании должны внедрять новый подход, об основных характеристиках которого мы уже вкратце говорили.

[2] https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

Вызовы для организаций, желающих стать кибер-устойчивыми

Каждый субъект (компания, организация или государство) подвергаются напряжениям, вызванными событиями, изменениями и инцидентами, которые возникают в их среде. Такие ситуации стресса - это новые вызовы, разрешение которых будет влиять на функционирование организации до тех пор, пока нельзя будет управлять ею с помощью автоматизации.

Когда дело доходит до безопасности организаций, стрессовые ситуации, о которых идет речь, требуют реакции, которая включает в себя новый акцент на программе безопасности во всей организации. Компании должны определить активы, имеющие самую высокую ценность, и создать новую модель управления безопасностью, которая бы с помощью группы экспертов по безопасности централизовала надзор за всеми действиями внутри компании. Именно здесь руководитель такой группы получает видимость ситуации и участвует в принятии решений организации, входя в состав руководства.

Больше угроз - выше интенсивность

В США в январе 2008 года администрация Президента США Дж. Буша-младшего инициировала всеобъемлющую инициативу по национальной информационной безопасности (Comprehensive National Cybersecurity Initiative, CNCI). Данная инициатива вводила дифференцированный подход к выявлению существующих и возникающих угроз информационной безопасности, выявляя и блокируя существующие уязвимости, и изучая действия лиц, которые пытаются получить доступ к федеральным информационным системам. Президент Б. Обама выступил с заявлением о том, что "кибер-угрозы являются одним из наиболее серьезных вызовов экономике и национальной безопасности, с которыми мы сталкиваемся как нация", и что “экономическое процветание США в XXI веке будет зависеть от информационной безопасности".[3]

[3] https://www.es.w3eacademy.com/wiki/State_security

Двигаясь в сторону кибер-*устойчивости*

Способность быстро восстанавливаться от трудностей, становясь при этом еще сильнее.

7%

По прогнозам в 2018 году глобальные расходы на ИБ вырастут всего на 7% до 93 млрд $, а вот масштабы атак растут экспоненциально

Инвестировать в ИБ

Без инвестиций разрыв в готовности будет только усиливаться

36%

Только 36% специалистов по ИБ имеют возможность напрямую отчитываться руководителю компании

Получить место за столом

Без лучшей видимости ИБ по-прежнему будет лишена приоритетов

35%

По некоторым оценкам, только 35% специалистов по ИБ проверяют системы партнеров для кибер-целостности и готовности

Построить более надежную экосистему

Обнаружение угроз неэффективно без адекватной проверки

1,5м

Ожидается, что к 2020 году в глобальной ИБ будет свыше 1,5 миллионов вакантных должностей

Развивайте таланты у сотрудников

Нанимайте больше талантов и развивайте их профессиональный уровень

1/2

Специалисты по ИБ посчитали, что свыше половины предупреждений об угрозах имеют неверный приоритет и его следует корректировать вручную

Делайте обнаружение угроз более аккуратным

Системы должны быть более отточенными для все более опасной цифровой среды

Рис 1. Технологический процесс, несомненно, является движущей силой роста компаний. Организации и мир в целом более взаимосвязаны, чем когда-либо ранее, и темпы современного технологического развития являются самыми внушительными за всю историю. Такая взаимосвязь создает как новые возможности, так и риски.

В декабре 2017 года Администрация Президента США Дональда Трампа опубликовала документ о национальной стратегии[4], в котором десятки раз упоминались проблемы информационной безопасности и где авторы документа не уклонялись от того, чтобы назвать конкретные страны, которые, вероятно, будут использовать сети конечных устройств как оружие против США.

В этом документе конкретно говорится о том, что хакеры и правительственные структуры России, Китая, КНДР и Ирана имеют реальные возможности для дестабилизации экономики и созданию угроз для критической инфраструктуры страны, и что США будут сдерживать, защищаться и при необходимости уничтожать источники таких угроз, которые используют кибер-атаки против них.

Это - реальность: во всем мире растет количество кибер-угроз и интенсивность кибер-атак, а стремительное и неудержимое развитие цифровых трансформации помогает создавать новые возможности для хакеров. Вот некоторые цифры, иллюстрирующие явные признаки этой тенденции:

- 10 миллионов новых устройств подключаются к нашему миру каждый день. Прогнозируется, что к 2020 году количество взаимосвязанных устройств достигнет 20,8 миллиардов[5].
- Компании инвестируют до 500 миллионов долларов США в информационную безопасность6, и все же 50% руководителей компаний с оборотами свыше 500 миллионов долларов США не чувствуют, что их компании готовы гарантированно справиться с кибер-атаками7, а 82% руководителей обеспокоены или очень обеспокоены вопросами информационной безопасности[8].
- Во всем мире ежегодно создается свыше 100 миллиардов строк кода, генерируя миллионы новых уязвимостей на компьютерах и серверах.
- Многие компании сообщают о тысячах атак каждый месяц, начиная от тривиальных и заканчивая чрезвычайно опасными.
- Ежегодно нарушаются миллиарды записей данных.
- В 2017 году хакеры произвели порядка 120 миллионов новых вариантов вредоносных программ. На сегодняшний день общее количество вредоносных программ, зарегистрированных AV-TEST приближается к 800 миллионам[9].

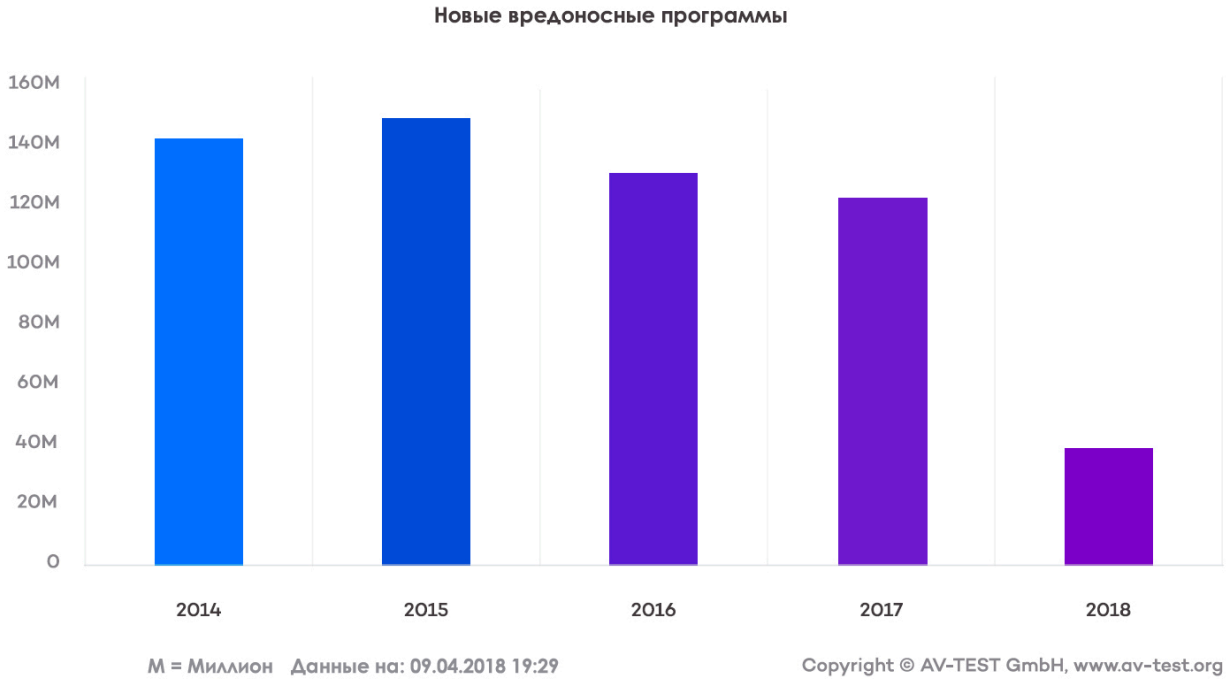
[4] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[5] https://www.isaca.org/chapters7/Monterrey/Events/Documents/20172408_Ciberseguridad_Fundamental_Trans_Digital.pdf [6] https://cybersecurityventures.com/cybersecurity-market-report/

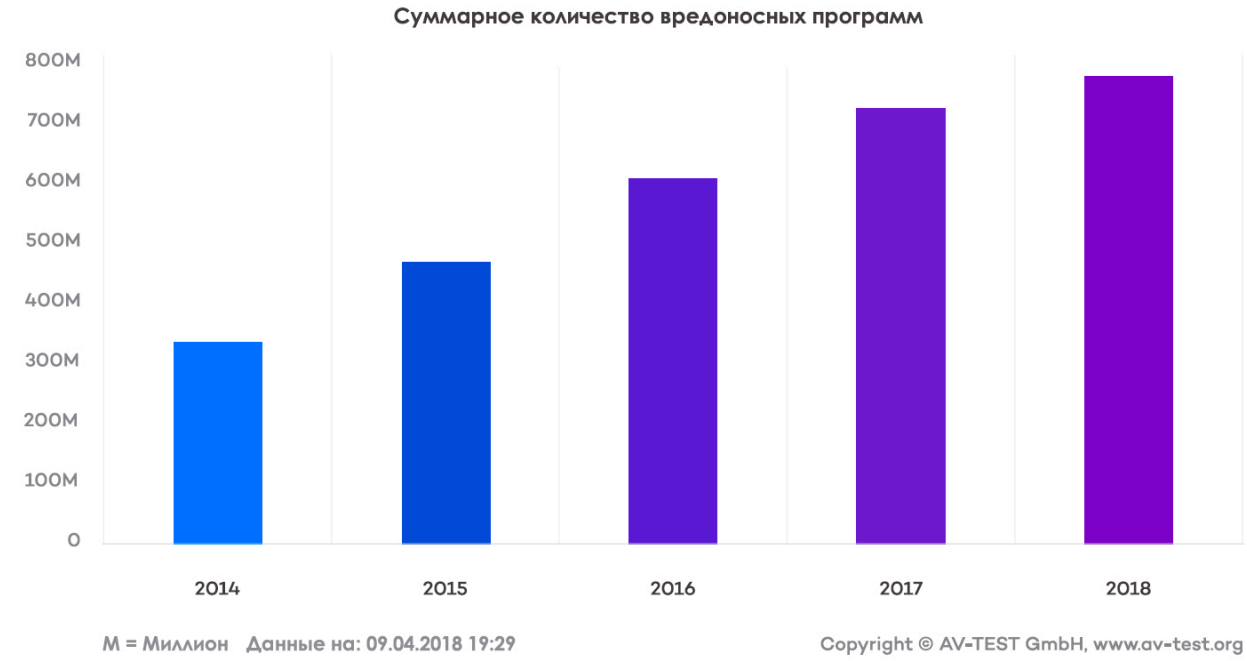
[7] Global CEO Outlook 2015 – KPMG. https://assets.kpmg.com/content/dam/kpmg/pdf/2015/08/global-ceo-outlook-2015.pdf

[8] ISACA/RSA Conference State of Cybersecurity study

[9] https://www.av-test.org/en/statistics/malware/



J.P. Morgan Chase & Co. удвоил годовой бюджет на информационную безопасность с 250 до 500 миллионов долларов США в 2017 году. Bank of America объявил о неограниченном бюджете, когда дело доходит до борьбы с кибер-преступностью.



https://www.av-test.org/en/statistics/malware/. Обновлен 9 апреля 2018 г.

Парадокс, но большинство компаний, которые стали жертвами NotPetya и WannaCry, возможно, сказали бы, что они были хорошо защищены во время атаки. Даже когда компания не является первоочередной целью, она рискует получить ущерб со стороны вредоносных программ при атаке против широко используемого ПО. И несмотря на все новые системы защиты, компаниям в среднем все еще требуется порядка 191 дня на обнаружение скрытой атаки, что все же несколько лучше, чем 201 день, который требовался организациям в 2016 году[10]. Не следует недооценивать ущерб, который может причинить хакер за этот период времени.

Исследование Института SANS 2016 года по реагированию на инциденты[11] показало, что 21% организаций имели среднее время обнаружения (MTTD) от двух до семи дней, и только 29% были способны обнаруживать инциденты в течение не более 24 часов.

То же исследование показывает, что только 18% организаций могли бы перейти от обнаружения к реагированию(MTTR) в течение не более суток. Но по-прежнему плохо, что 38% опрошенных признали, что в целом они не могут реагировать должным образом в течение недели.

Согласно исследованию о важности устойчивости для усиления безопасности в компаниях, выполненному Ponemon Institute и опубликованному в марте 2018 года, чем больше времени требуется компании на устранение инцидентов, с которыми она сталкивается, тем выше их уровень серьезности и количество.

Как показано на рисунке 2, взятого из исследования Ponemon Institute о кибер-устойчивости, 64% опрошенных компаний указали на то, что увеличилось число инцидентов, а 65% - что возрос уровень их серьезности.

Как изменились количество и уровень серьезности инцидентов безопасности за последние 12 месяцев?

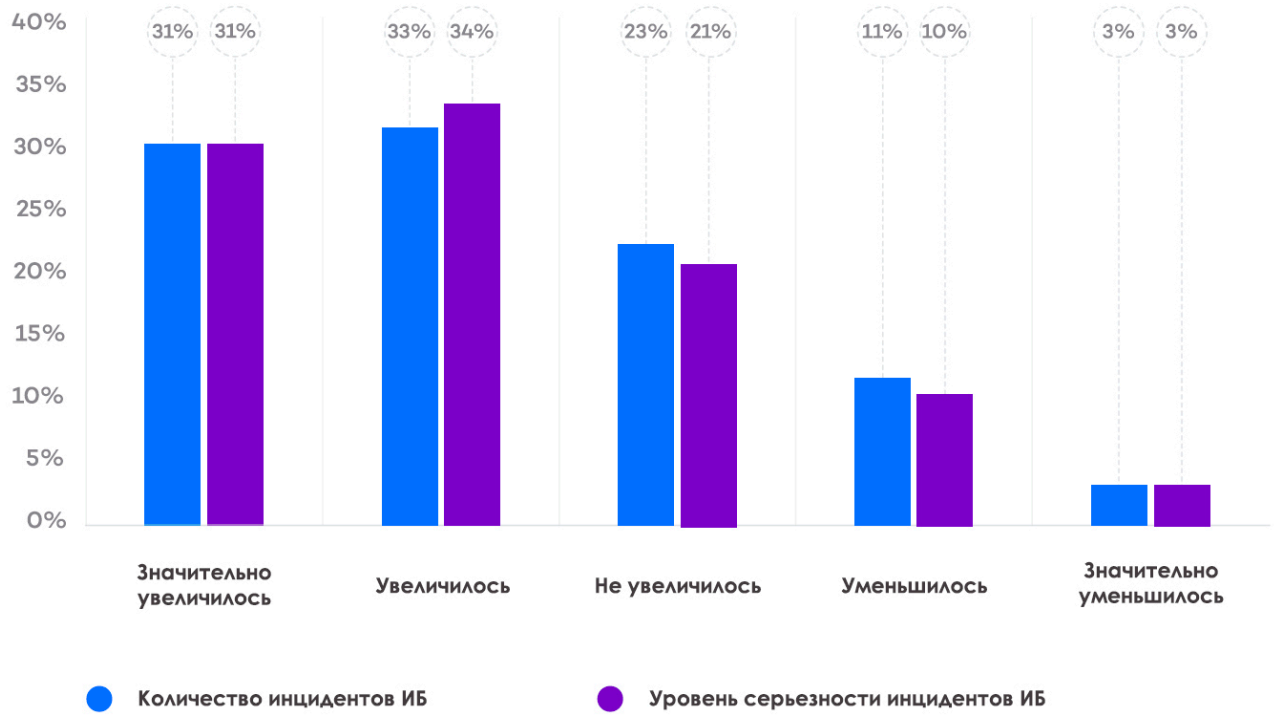


Рис 2. Изменение количества и уровня серьезности инцидентов безопасности за последние 12 месяцев, согласно исследованию Ponemon Institute, опубликованного в марте 2018 г.

[10] 2017 Cost of Data Breach Study (Ponemon Institute for IBM Security)

[11] https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

Увеличение количества и степени серьезности инцидентов имеет негативное воздействие на время, необходимое для их обнаружения и реагирования на них: оно значительно увеличивается. На рисунке 3 показано, что 57% опрошенных компаний сказали, что у них это время увеличилось.

Сложность ИТ-инфраструктуры

Усложнение инфраструктуры делает компании более уязвимыми. В то время как кибер-преступники совершенствуют свои навыки, компании становятся все более "цифровыми", открывая новые "двери" для уязвимостей и кибер-атак. Активы, которые варьируются от проектов новых продуктов до клиентских данных, теперь подвержены риску. Цифровое подключение также становится все более сложным, используя простое цифровое соединение для объединения тысяч людей, всевозможных приложений и серверов, рабочих станций и других устройств. Активы компаний теперь намного больше подвержены риску, чем когда-либо ранее.

Некоторые распространенные ошибки

Корпоративная информационная безопасность пытается поддерживать высокие темпы развития кибер-рисков[12], но во многих случаях это делается с ошибочным подходом и с неэффективной позиции. Некоторые широко распространенные негативные практики включают в себя:

- **Делегирование проблемы в ИТ-департамент**
  Многие руководители компаний рассматривают информационную безопасность как чисто техническую проблему, и делегируют ее решение в ИТ-департамент. Такая реакция, которая частично вызвана многими техническими проблемами, связанными с ИБ, не принимает во внимание тот факт, что защита бизнеса отличается от защиты серверов. Защита бизнеса требует понимания того, что поставлено на карту в соответствии с бизнес-приоритетами, бизнес-моделью и цепочкой создания добавленной стоимости, а также рисками, культурой, ролями, обязанностями и принципами управления в компании.

Как изменилось время для обнаружения, сдерживания и реагирования на кибер-преступления за последние 12 месяцев?

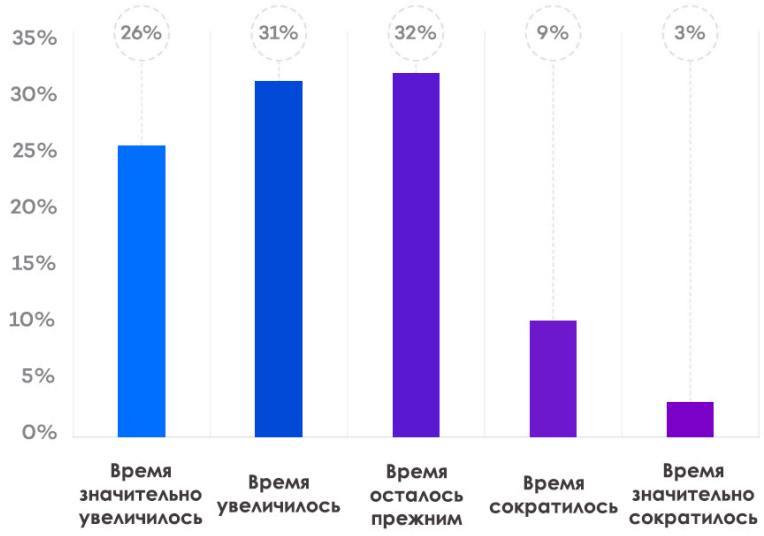


Рис. 3. Изменение среднего времени, необходимого для обнаружения и реагирования на инциденты безопасности за последние 12 месяцев согласно исследованию Ponemon Institute, опубликованному в марте 2018 г.

[12] AV-TEST Institute регистрирует свыше 250 000 новых вредоносных программ ежедневно. https://www.av-test.org/en/statistics/malware/

- **ИТ-департамент** не может в одиночку решать вопросы ИБ, которые следует рассматривать как проблему всей компании.

- **Следование тенденции использования статусных "хакеров" или экспертов для решения проблемы.** Некоторые компании предполагают, что угроза исчезнет, если они наймут достаточно крутых "хакеров". Но даже самые лучшие профессионалы не в состоянии предвидеть и защищать от всех атак на устройства в сложной корпоративной сети. Да, решение требует экспертов, но также и технологии и процессы, которые нацелены и адаптированы для работы. Это подразумевает инвестиции в среднесрочной перспективе, которые должны быть постоянны в течение определенного периода времени, чтобы повысить осведомленность и вовлеченность всех подразделений компании, чтобы правильно оценивать риски и их последствия, чтобы принимать участие в управлении.

- **Оценка риска как проблемы соответствия действующим правилам.** Некоторые компании, видимо, вводят новые протоколы безопасности и чек-листы верификации каждые два дня. Но эти усилия зачастую провоцируют чрезмерное внимание к формальному их соблюдению, а не к реальной устойчивости.

Внедрение кибер-устойчивости

Принимая во внимание данную сложную и реальную панораму, как компании, намеревающиеся защитить свои активы наиболее эффективным способом, могут достичь этого более адаптивного, комплексного и совместного подхода?

Информационную безопасность следует рассматривать как проблему управления корпоративными рисками, а не как проблему, связанную только с ИТ. При таком подходе ключевые элементы управления содержат:

- Приоритезация наиболее ценных активов компании.

- Приоритезация, знание и понимание наиболее актуальных противников и угроз для каждой организации.

- Знание и внедрение лучших средств защиты от текущих и потенциальных угроз.

- Быть готовым к моменту, когда противники смогут преодолеть все технологии безопасности и их обнаружения, сдерживая их и как можно быстрее препятствуя их действиям для минимизации корпоративного ущерба.

- Принятие кризисной позиции, в рамках которой осуществляется постоянный и активный поиск угроз, и обнаружение уязвимых точек, которые впоследствии могут использоваться источниками угроз, для уменьшения поверхности атаки.

- Управление на корпоративном уровне любыми коммуникациями инцидента.

- Определение и непрерывное выполнение инициатив по минимизации рисков и возобновлению цикла непрерывного усовершенствования в управлении корпоративной безопасностью.

Адаптация имеет очень важное значение. Корпоративные процессы, технологии, инструменты и сервисы безопасности должны пересматриваться и корректироваться по мере развития угроз в процессе постоянного совершенствования, основанного на осторожности. "Быть устойчивым" означает, что такая адаптация должна выполняться в минимально короткие периоды времени с максимальной скоростью (желательно даже в реальном времени).

Полный подход к управлению информационной безопасностью в компаниях

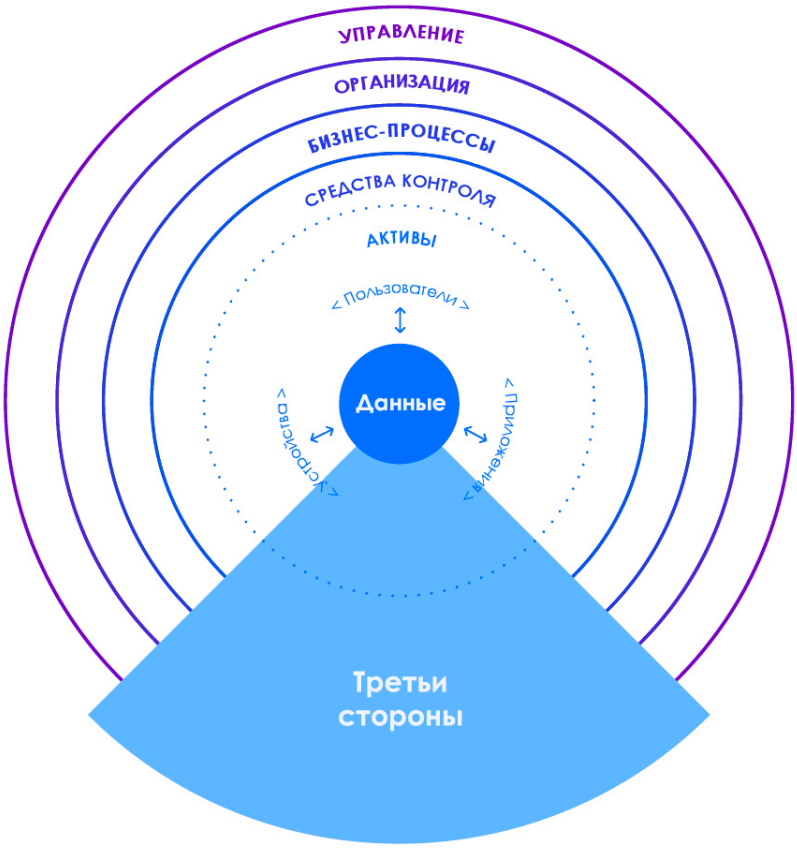


Рис 4. Полный подход к управлению информационной безопасностью в компаниях.

Компании должны искать риски и снижать их на всех уровнях. Описание всех активов от данных до приложений и мониторинг всех действий, которые выполняются по отношению к ним, - это длинный и утомительный процесс, но необходимый. Компании должны использовать инструменты и сервисы, которые автоматизируют эти задачи для профилирования, каталогизирования и мониторинга своих активов (люди, данные, инфраструктура) с целью предотвращения и/или раннего обнаружения противников.

Создание "цикла устойчивости"

Организации должны понимать и внедрять процесс "цикла устойчивости", который поможет сотрудникам ИБ постоянно работать с учетом опыта заблокированных и/или обнаруженных угроз.

Это требует того, чтобы они изучали и применяли ключевые фазы устойчивости:

- **На этапе, предшествующему инциденту**, лучше предотвращать и противостоять угрозы, используя усовершенствованные технологии, которые обнаруживают известные и неизвестные ("нулевого дня") вредоносные программы.
- **Во время инцидента** быстро реагировать за счет обнаружения, сдерживания и реагирования на внезапные события, которые угрожают организации, чтобы минимизировать их последствия для бизнеса, а также воспользоваться новыми парадигмами, которые возникают как результат использования возможностей мониторинга и видимости, предоставляемых решениями с технологиями EDR.

Рис 5. Риски и средства управления, которые должны быть внедрены на всех уровнях от данных и до конечных устройств и приложений, работающих на них.

- **На этапе после завершения инцидента** необходимо анализировать его последствия наряду с непрерывным достижением стратегических целей безопасности и восстановлением операционной среды таким образом, чтобы устранять будущие источники подобных проблем. Это именно то, что называется "уменьшение поверхности атаки".

Предотвращение, обнаружение и реагирование

Лучше всего считать, что рано или поздно, но любая компания будет скомпрометирована в результате кибер-атаки. В такой момент решающее значение будет иметь время обнаружения атаки и реагирования на нее. Баланс должен быть найден между оперативным реагированием и восстановлением нормального уровня работы предприятия и анализом инцидента, источника атаки и установлением мер во избежание ее в будущем.

Как мы уже говорили во введении, кибер-устойчивость относится к способности предприятия поддерживать свои основные функции и целостность в борьбе с атаками на информационную безопасность. Кибер-устойчивая компания - это такая компания, которая способна предотвращать, обнаруживать, сдерживать атаки и восстанавливаться после них, минимизируя время ее воздействия и влияние на бизнес бесчисленных серьезных угроз данным, приложениям и ИТ-инфраструктуре, особенно конечным устройствам, где хранятся самые ценные активы предприятия, и учетным данным пользователей.

Хотя мы знаем, что невозможно гарантировать полное предотвращение, все же компании должны стремиться минимизировать ущерб от кибер-атак, усиливая профилактику на предварительном этапе, не позволяя хакеру выполнять вредоносный код на рабочих станциях и серверах.

Не менее важно дополнить стратегию информационной безопасности быстрым обнаружением атак и реагированием на них на этапах выполнения и завершения инцидента, чтобы выявлять повреждения, восстанавливать системы и как можно скорее возвращать нормальный ход выполнения операций. Между тем, слабые места и уязвимости могут быть вновь обнаружены для их коррекции и во избежание атаки в будущем.

Реализация непрерывных процессов обнаружения аномалий в поведении пользователей, конечных устройств и приложений

Когда дело доходит до минимизации влияния на бизнес, время от возникновения инцидента до его обнаружения - это решающий фактор в конечном ущербе от инцидента.

Мониторинг, видимость конечного устройства и технологии, которые позволяют автоматизировать процессы обнаружения и анализа, способны значительно сократить это время. Обнаружение аномального поведения пользователей, приложений и устройств, которое является симптомами присутствия хакера в системе, является очень критичным.

Управление кибер-рисками требует комплексного и совместного управления

Многие компании проводят различия между физической и информационной безопасностью, между ИТ и операциями, между управлением непрерывностью бизнеса и защитой данных, между внутренней и внешней безопасностью. В цифровую эпоху эти разделения устарели. Распределенная ответственность может подвергнуть серьезному риску всю компанию. Дублирование функций должно быть ограничено, а ответные меры должны приниматься быстрее, чтобы повысить устойчивость компании в целом.

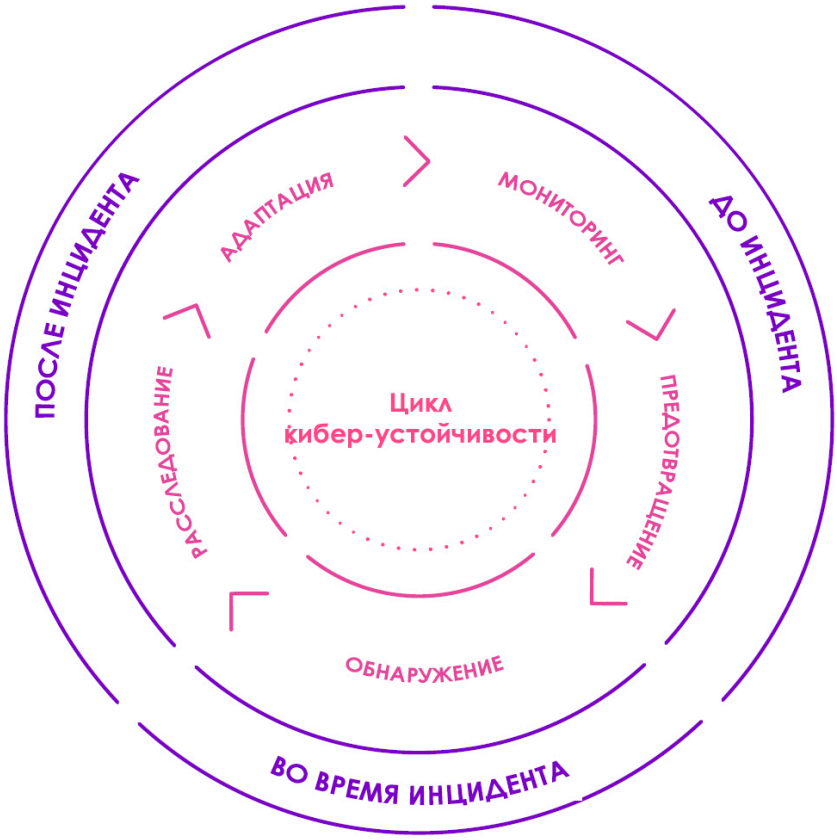
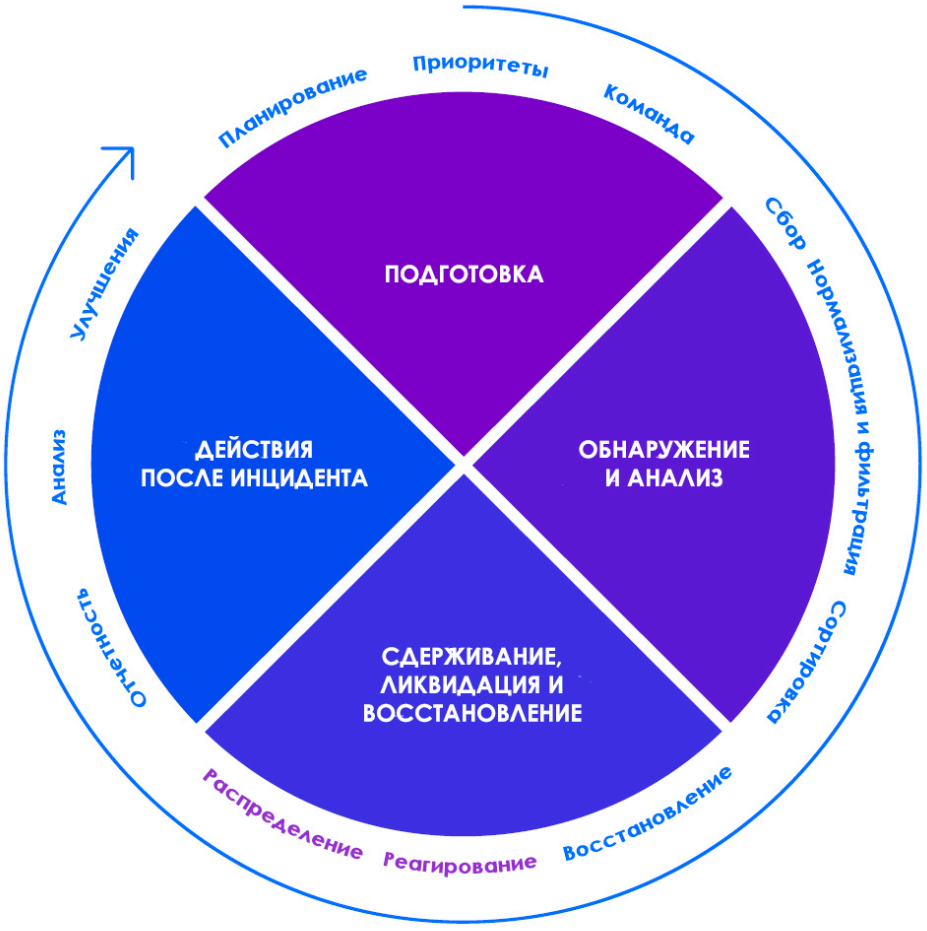


Рис 6. Цикл непрерывного совершенствования кибер-устойчивости, который должен быть разработан и внедрен в каждой организации.

Следующий рисунок был взят из отчета Gartner от 25 января 2018 г.: “Повышение операционной устойчивости за счет совместного процесса реагирования на инциденты". Он показывает области цикла управления и реагирования, в которых необходимы совместные усилия и координация (синие секторы), и функции, в которых применяются конкретные возможности каждого отдела (красные секторы) с целью обнаружения и реагирования в максимально короткие сроки при идентификации зон для усовершенствования.

Компании, которые придерживаются этих принципов, как правило, гораздо более устойчивы к атакам, чем те, которые их не придерживаются.

Обработка инцидентов



Пояснения: ● Схожая задача и практика
● Отличающаяся задача и практика

Рис 7. Координация между операционными департаментами и департаментом безопасности при управлении инцидентом безопасности. Gartner: “Improve Operational Resilience Through to More Collaborative Incident Response Process”. 25 января 2018 г. Аналитики: Мэттью Т. Стампер, Кеннет Гонсалес

Как моя компания оценивает кибер-устойчивость?

В рамках "Третьего ежегодного исследования кибер-устойчивости организаций"[13], выполненного IBM и Ponemon Institute в этом году, были определены характеристики организаций с высокой степенью кибер-устойчивости.

Компаниям рекомендуется оценивать свое состояние по этим характеристикам и предпринимать соответствующие меры для того, чтобы сократить разрыв между той точкой, где они сейчас находятся, с той, где они должны быть. Эти меры многообразны как по своему характеру, так и по объему. Внедрение соответствующих технологий, решений и сервисов, предлагаемых производителями решений безопасности и сервис-провайдерами, может привести к тому, что компании сразу начнут их применять без огромных первоначальных инвестиций, что окупится в краткосрочной перспективе за счет сокращения операционных расходов, связанных с инцидентами и нарушениями данных.

Для компаний с высокой степенью кибер-устойчивости характерно:

Наличие программы информационной безопасности с высоким уровнем зрелости, полностью или, по крайней мере, частично развернутой по всей организации, которая постоянно совершенствуется.

Согласно отчету SANS Institute "Behind the Curve? A maturity Model for Endpoint Security"[14], где модель зрелости определяется с точки зрения безопасности конечного устройства, организация в состоянии высокой зрелости способна предотвратить кибер-атаки до момента их выполнения. Или внести изменения в системах, которые влияют на конечные устройства, обнаруживать атаки, которые были способны преодолевать внедренные решения безопасности, сообщать о статусе инцидента и предотвращать распространение новых атак в компании. Если говорить коротко, они имеют внедренную в компании программу безопасности, основанную на проактивной обороне и существенно повышающей общую устойчивость организации.

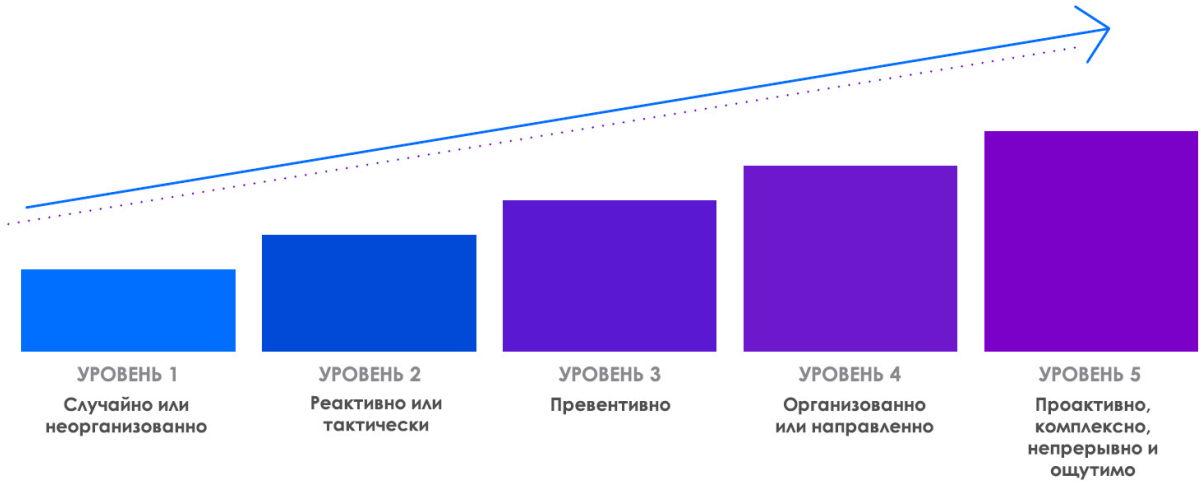


Рис 8. Модель зрелости безопасности на рабочих станциях и серверах по мнению SANS Institute, в которой определены пять уровней зрелости в отношении разработанной и внедренной программы безопасности.

[13] http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study .

[14] http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study

Очень кибер-устойчивые организации внедрили надежные инструменты предотвращения, обнаружения, сдерживания кибер-атак и восстановления после них.

Как описано в исследовании устойчивости, выполненным Ponemon Institute, большинство устойчивых компаний - это те, кто инвестировал в развитие своих способностей по предотвращению, обнаружению атак и реагированию на них.

Организации, уверенные в своих возможностях предотвращать, обнаруживать, сдерживать атаки и реагировать на них

1 = низкая способность, 10 = высокая способность

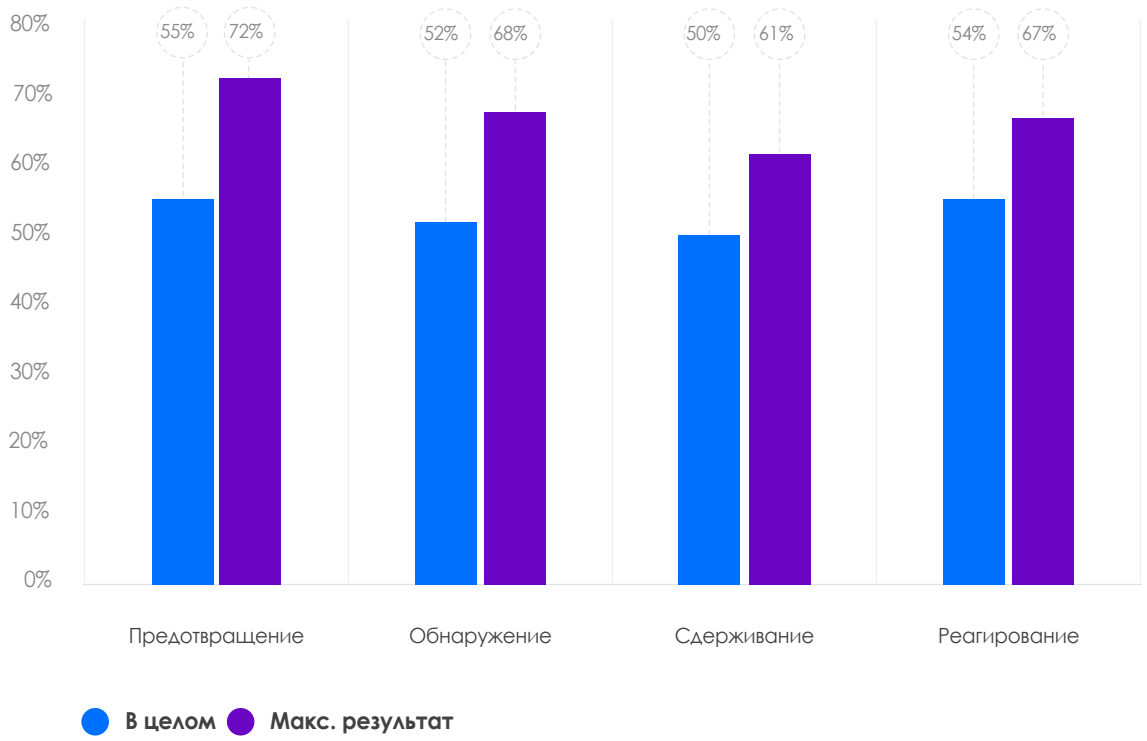


Рис 9. Ponemon Institute: соотношение между кибер-устойчивостью и способностью предотвращать, обнаруживать, сдерживать кибер-атаки и реагировать на них.

Очень кибер-устойчивые компании внедрили План реагирования на инциденты информационной безопасности (CSIRP). Данный план основан на непрерывном мониторинге и сопоставлении событий, используя данные, собираемые сенсорами на сетевых устройствах и/или конечных устройствах, а также на механизмах обнаружения, анализа и автоматизированного реагирования и/или реагирования, управляемого экспертами по безопасности или командой Threat Hunters.

Что лучше всего описывает План вашей компании по реагированию на инциденты ИБ (CSIRP)?

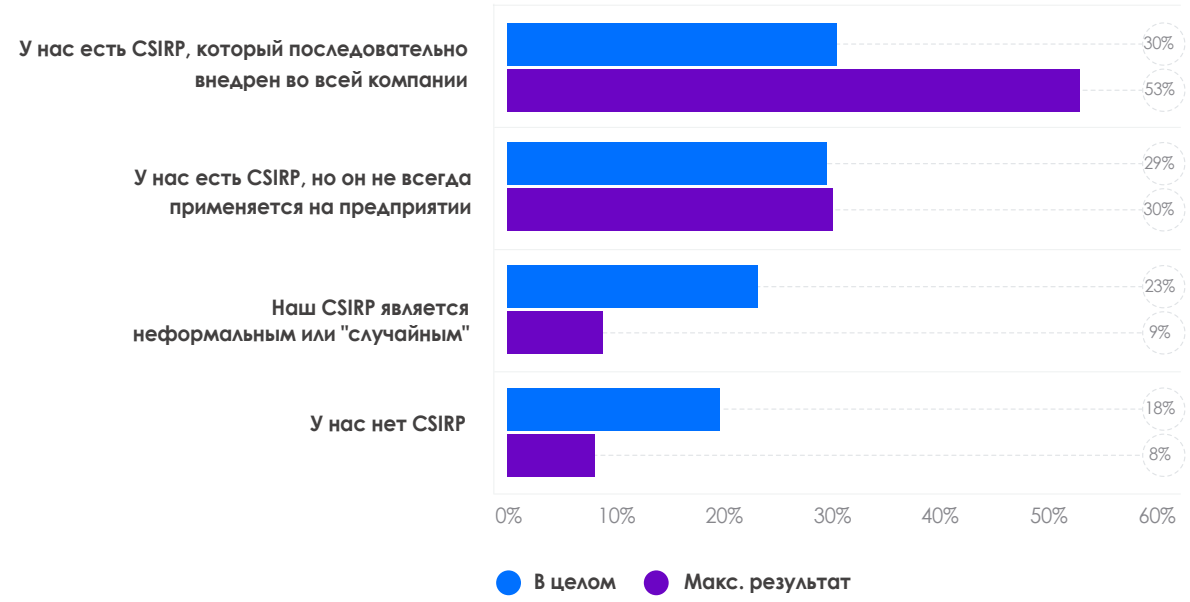


Рис 10. Ponemon Institute: соотношение между кибер-устойчивостью и внедрением плана по реагированию на инциденты информационной безопасности.

Более того, почти все компании с высоким уровнем кибер-устойчивости считают необходимым иметь в рамках собственной команды безопасности или внешнего SoC высококвалифицированный персонал, подключаемый при реализации плана по реагированию на инциденты.

Очень важно иметь высококвалифицированных специалистов по ИБ в своем CSIRP?

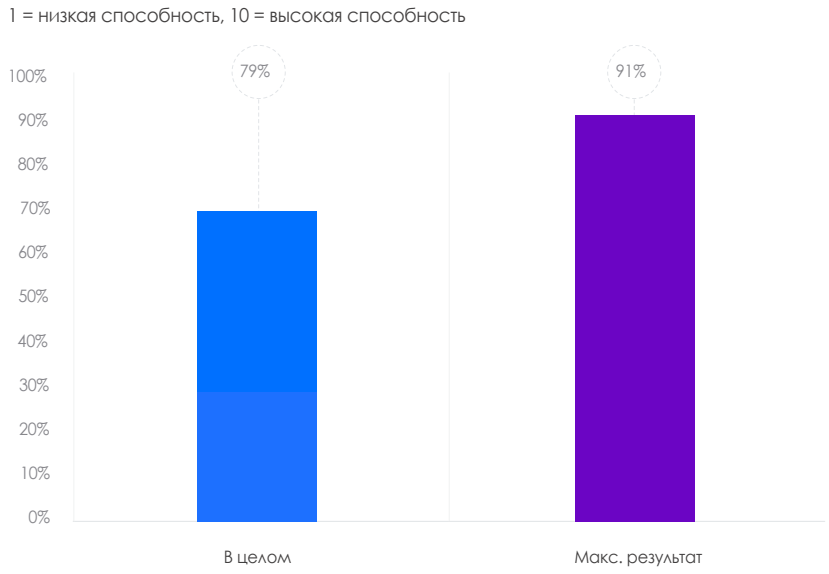


Рис 11. Ponemon Institute: соотношение между кибер-устойчивостью и необходимостью иметь высококвалифицированные и специализированные ресурсы, выделенные на информационную безопасность

Кибер-устойчивое корпоративное управление: Руководители компаний с высоким уровнем кибер-устойчивости чувствительны к положительной связи, которая существует между этим фактором и экономическим ростом, а также усилением бренда и репутации их компании.

Осведомленность высшего руководства о положительном влиянии кибер-устойчивости на предприятие

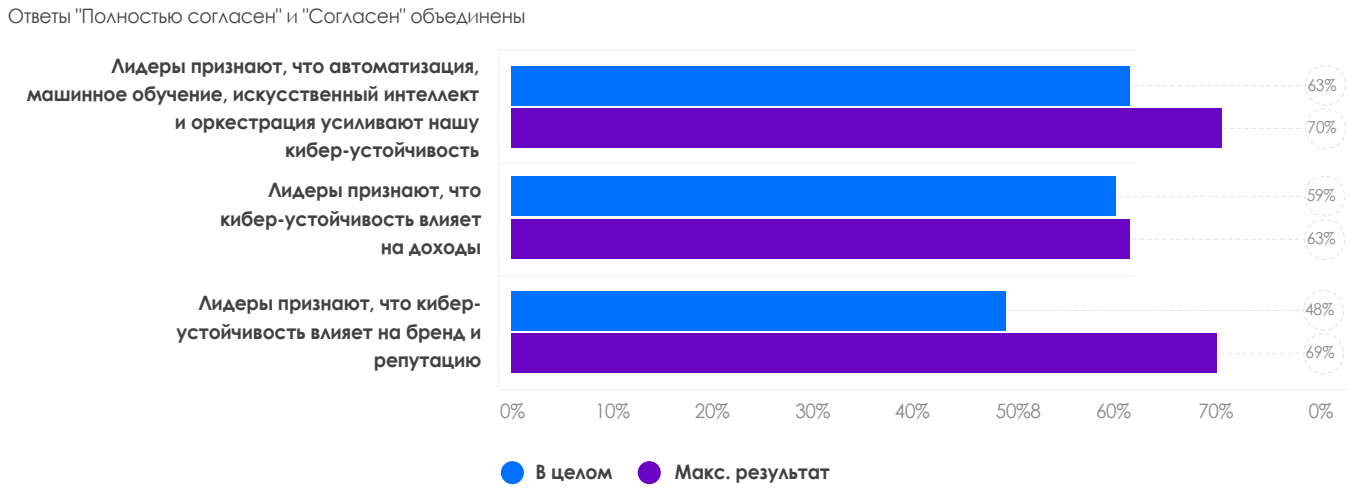


Рис 12. Ponemon Institute: Важность вовлеченности высшего руководства в построении компании с высоким уровнем кибер-устойчивости.

Выводы

Цифровая трансформация, происходящая практически во всех сферах нашей жизни, имеет особое значение при рассмотрении эволюции компаний, организаций и государственных структур, взаимосвязанных устройств, приложений, инструментов и производственных процессов.

С точки зрения конкуренции поиск путей оптимизации с использованием новых и усовершенствованных инструментов, средств, возможностей и процессов является источником почти всех инициатив в частном и государственном секторе.

Однако есть еще один аспект, который мы не можем игнорировать на пути к цифровой трансформации: преобразования должны быть глубоко встроены в управление безопасностью и рисками предприятия.

Более того, если учитывать рост числа угроз и повышение степени их изощренности. Кибер-преступность - это привлекательный и очень прибыльный бизнес. Злоумышленники имеют все больше и больше ресурсов (технических и экономических), которые позволяют им разрабатывать все более изощренные и усовершенствованные атаки. Все это приводит к появлению более сложных и динамических угроз в дополнении к росту числа атак.

Equifax, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, **WannaCry**, **Goldeneye/NotPetya**, Meltdown/Specter, **вмешательство в выборы...** Вот лишь некоторые персонажи недавних случаев массовых заражений, кражи и утечки персональных данных, атак шифровальщиков, взломанных приложений для запуска атак против целой страны или выполнения атак, направленных против конкретных крупных компаний, а также использования уязвимостей, повлиявших на миллиарды устройств.

При наличии таких реальных случаев, неудивительно, что 75% компаний (согласно недавнему исследованию McKinsey[15]) считают, что информационная безопасность является приоритетом для надлежащего развития их деятельности. "Стрессовая ситуация", описанная выше, требует реакции, которая подразумевает фокусировку всей компании на программу безопасности, которая развивает и укрепляет кибер-устойчивость предприятия.

Кибер-устойчивость - это способность предприятия поддерживать свои основные функции и целостность перед лицом потенциальной угрозы атаки на информационную безопасность предприятия.

Кибер-устойчивая компания - это такая компания, которая способна предотвращать, обнаруживать, сдерживать атаки и восстанавливаться после них, минимизируя время воздействия и влияния на предприятие бесчисленных серьезных угроз данным, информации, приложениям и ИТ-инфраструктуре, а особенно - устройствам, на которых расположены самые ценные активы компании. Если атака достигла устройства, то это также означает атаку против целостности бизнеса и пользователей.

Чтобы стать кибер-устойчивой компанией, необходимо, чтобы новый подход к безопасности охватывал, как минимум, следующие направления:

1. **Управление информационной безопасностью как проблема управления корпоративными рисками,** а не как ИТ-проблема, **и применение "цикла устойчивости".** Ключевые элементы цикла кибер-устойчивости:
    1) Приоритезация самых ценных активов предприятия.
    2) Приоритезация, знание и понимание наиболее актуальных противников и угроз для каждой организации.
    3) Знание и применение лучших средств защиты от текущих и потенциальных угроз.
    4) Готовность к моменту, когда противники смогут преодолеть все технологии безопасности, оперативно обнаруживая и сдерживая их, а также препятствуя их действиям для минимизации ущерба для компании.

[15] https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

5) Принятие кризисной позиции для непрерывного и активного поиска угроз и обнаружение уязвимых точек, которые позже могут использоваться источниками угроз, для уменьшения поверхности атаки.

6) Управление на корпоративном уровне любыми коммуникациями инцидента.

7) Определение и постоянное исполнение инициатив по минимизации риска и возобновлению цикла непрерывного усовершенствования процессов управления корпоративной безопасностью.

2. **Укрепление четырех ключевых компонентов: профилактика, обнаружение, Threat Hunting, сдерживание, реагирование и уменьшение поверхности атаки.**

3. **Постоянная адаптация к новым техникам и тактикам хакеров и других злоумышленников.** "Быть устойчивым" означает, что данная адаптация должна выполняться в минимально короткие периоды времени с максимальной скоростью и желательно даже в реальном времени.

4. **Определение приоритетов и снижение рисков на всех уровнях организации.** Компании должны использовать преимущества управляемых инструментов, продуктов и сервисов, которые автоматизируют эти функции для профилирования, каталогизирования, мониторинга активности (людей, данных и инфраструктуры), и анализируют их, чтобы системы безопасности были способны прогнозировать и ускорять предотвращение и/или раннее обнаружение противников за счет снижения уровня организационных рисков без несоразмерных затрат, особенно операционных расходов.

5. **Управление кибер-рисками с помощью комплексного и совместного управления.**

PASS Panda Security Summit | The European Cybersecurity Hub

#PASS2018