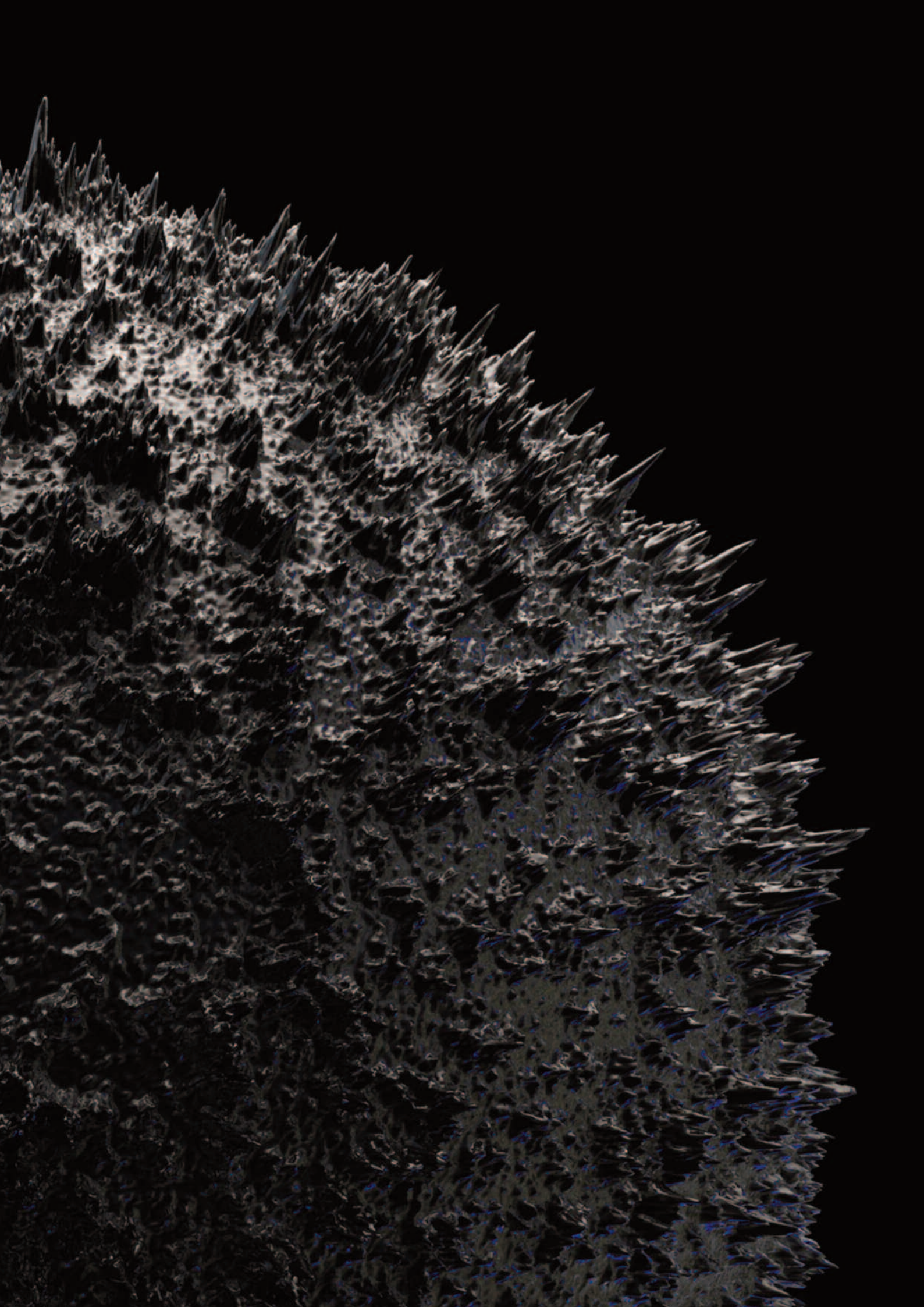
Check Point
SOFTWARE TECHNOLOGIES LTD.

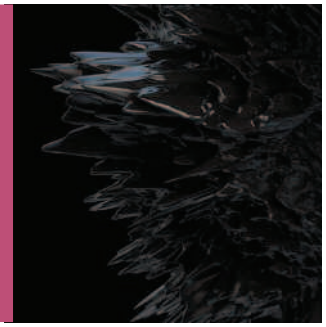
РУКОВОДСТВО ПО КИБЕР-БЕЗОПАСНОСТИ

10 ШАГОВ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ БИЗНЕСА



РУКОВОДСТВО ПО КИБЕРБЕЗОПАСНОСТИ

10 ШАГОВ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ БИЗНЕСА



БЕЗОПАСНОСТЬ НУЖНО ВОСПРИНИМАТЬ ВСЕРЬЕЗ

ПРЕДИСЛОВИЕ

Мы перестали реагировать на заголовки о киберпреступлениях, как будто мы просто выключили звук автомобильной сигнализации. И это несмотря на то, что киберпреступники похитили более 500 миллионов идентификационных записей[1] только за один 2014 год. Согласно статье[2] в Computer Weekly в декабре 2014 года, «выпуск вредоносного ПО продолжается в промышленных масштабах – наборы эксплойтов и сервисы по предоставлению в аренду вредоносного ПО, позволяющие реализовать сложные атаки, попадают в руки относительно неопытных киберпреступников». И, к сожалению, игнорировать этот факт уже нельзя.

Нравится Вам это или нет, для бизнеса защита информации так же важна, как и для правительств, защищающих свои секреты. Не важно, каким видом бизнеса занята ваша компания – технологическим, банковским, медицинским, спортивным или услугами быстрого питания – если вы что-то продаете, существует вероятность того, что в вашей сети хранятся персональные данные.

Цифровые активы вашего бизнеса нуждаются в круглосуточной защите так же, как и физическое имущество или банковские депозиты. Некоторые компании четко понимают, как это осуществить, в то время как для других безопасность остается таинственным предметом.

Понимание того, насколько вы открыты угрозам, и того, что действия по предотвращению этих угроз находятся не только в зоне ответственности руководства компании, критично для выживания бизнеса.

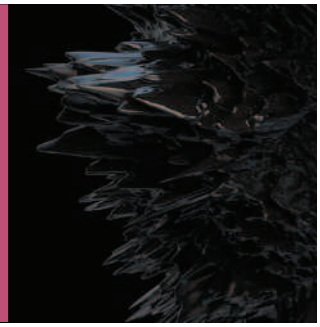
Далее в этой брошюре вы найдете 10 шагов, которые помогут вывести вашу организацию на более высокий уровень безопасности.

Мы хотим, чтобы ваш бизнес рос, процветал, и, самое главное, был безопасным.

> ВЫПУСК ВРЕДОНОСНОГО ПО ПРОДОЛЖАЕТСЯ В ПРОМЫШЛЕННЫХ МАСШТАБАХ.

[1] «Официальные представители предупредили, что 500 миллионов финансовых записей были взломаны», USA Today, октябрь 2014.
[2] «Top 10 Cybercrime Stories», Computer Weekly, Dec 2014.

ОСОЗНАНИЕ НЕОБХОДИМОСТИ



Открытость и доступ

Реальность риска для данных

Киберпреступность для большинства людей была тем, с чем сталкиваются только правительственные организации. Однако каждый год киберпреступность наносит удары все ближе и ближе к домам каждого из нас. В большинстве случаев, мы даже не подозреваем о существовании опасности до тех пор, пока не столкнемся с ней.

В 2014 году взломы Target, Home Depot и Sony попали на первые полосы изданий. Но, если вы не работаете в индустрии, вы может быть и не слышали о тысячах взломах других компаний, малых и больших, из разных отраслей экономики, коснувшихся всех типов данных. Хотя «малые взломы» сами по себе не выглядят значительными, каждый из них предоставляет возможность для проведения других взломов, так как большинство людей редко изменяют свои пароли и используют их для нескольких учетных записей.

Правило 1 и 3

Риск информационной безопасности является комбинацией трех факторов: активов, уязвимостей и угроз (активы, открытые посредством уязвимостей, через которые могут быть реализованы угрозы). Один взлом может иметь последствия в виде других взломов.

Все три фактора возросли за последние годы. И вот почему:

1. Повсеместное распространение интернета все больше делает нашу жизнь связанной с «всемирной паутиной», однако мы принимаем за данность, что наша информация и персональные данные не находятся в зоне риска. Пока мы ограничиваем использование интернета доступом к рабочим сайтам и не даем никому наши пароли, мы в безопасности. Правда? Нет.
2. Онлайн-бизнес предоставляет нам гораздо больше комфорта, однако и возможностей для организации атаки стало больше,
3. Киберпреступность сама стала индустрией. Объем угроз достиг ошеломляющих размеров и продолжает расти и развиваться.

Исследование, проведенное корпорацией Rand[3], показывает, что во многих случаях киберпреступный бизнес более доходен, чем торговля наркотиками, так как он легче в управлении, требует меньших людских ресурсов, несет в себе меньший риск обнаружения и даже меньший риск преследования.

Обозначить проблему

Взрывной рост угроз вызвал новый уровень озабоченности и действий, направленных на решение проблемы. Подключены правительственные органы и организации по обеспечению правопорядка. Настало время для компаний удвоить свои усилия по проактивному обеспечению безопасности.

[3]Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar, Rand Corp., 2014

Компании, осознающие важность управления рисками, как малые, так и большие, видят необходимость уделять безопасности самое пристальное внимание. И это не только вопрос защиты, но и предоставления возможностей.

С течением времени, компании поняли необходимость поднятия стандартов кибербезопасности до стандартов физической безопасности. Физический взлом требует силы и нахождения на самом объекте проникновения, после него легче проводить инвентаризацию и отслеживать потери. Киберпреступник, в свою очередь, может осуществить взлом за несколько секунд, находясь на другом конце земного шара. Могут потребоваться недели, чтобы оценить масштаб утечки, не говоря уже о том, чтобы отследить путь преступников. Кроме того, киберпреступление способно сильнее ударить по прибыли компании, нежели физическое преступление.

Хотя многие из руководителей компаний в настоящее время ставят кибербезопасность практически на один уровень с физической, они зачастую медлят выносить эти вопросы на собрания правления – до тех пор, пока не произойдет взлом. Для того, чтобы начать мыслить о безопасности проактивно, необходим другой подход.

Если компания вовлечена в бизнес с использованием персональных данных, ставки повышаются, и возникает необходимость соблюдения требований регулирующих органов и нормативных документов. Доступ к данным должен осуществляться согласно политикам, равно как и должны быть приняты определенные меры предосторожности. С персональными данными необходимо обращаться как с конфиденциальной информацией.

По состоянию на 2014 год, средняя ценность идентификационной записи оценивалась в $188. И хотя это может показаться маленькой суммой, необходимо учитывать, что идентификационная информация обычно хранится и похищается в объемах от десятков тысяч до миллионов записей за один раз. Что уже составляет достаточно существенные потери.

Доступ к конфиденциальной информации должен быть ограничен теми, кому она действительно необходима. В этом случае вы сможете эффективно отслеживать доступ к данным и пресекать любой взлом и существенно облегчить управление инфраструктурой безопасности.

Назначить ответственного

Причина, по которой люди не уделяют внимания киберпреступлениям, состоит в том, что они полностью не осознают их последствий. Большинство людей не понимают, что они могут потерять работу, если киберпреступники похитят проекты их компании; или то, что кража логина к игровому онлайн-сервису может привести к взлому банковского счета потому, что пользователь использовал один и тот же пароль для разных учетных записей.

И здесь недостаточно декларации о том, что защита информации в компании является обязанностью каждого сотрудника. Люди должны быть ответственными на индивидуальном уровне и ощущать свой вклад в безопасность компании. И, конечно, необходимые механизмы безопасности должны быть встроенными, запланированными частями инфраструктуры, а не добавленными постфактумом.

Чтобы создать политику информационной безопасности, вам следует помнить о трех аспектах:

А. Сконцентруйтесь. Уделите пристальное внимание тому, как работает ваша компания и ваши сотрудники. Затем создайте концепцию, позволяющую реализовать видение, используя безопасность как двигатель.

Б. Смотрите вперед. Изучите необходимые регулирующие документы, информацию о угрозах и уязвимостях. Но также не забывайте смотреть на полную картину для того, чтобы заставить безопасность работать на конечный результат не только в данный момент, но и на протяжении всего пути.

В. Помните о деталях. Постоянно напоминайте высшему руководству компании о политике безопасности и осуществляйте ее с четко определенными обязанностями.

И, наконец, не усложняйте вещи. Чем проще и яснее написана ваша политика безопасности, тем больший процент сотрудников будет ей следовать.

10 ШАГОВ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ БИЗНЕСА

А | СКОНЦЕНТРИРУЙТЕСЬ

Б | СМОТРИТЕ ВПЕРЕД

В | ПОМНИТЕ О ДЕТАЛЯХ

A. СКОНЦЕНТРИРУЙТЕСЬ

1 ИСПОЛЬЗУЙТЕ БЕЗОПАСНОСТЬ ДЛЯ ИННОВАЦИИ

Безопасность не должна становиться врагом инноваций. Здравый подход к безопасности может не только защитить компанию от атаки; он может также способствовать переходу к более комплексным базовым технологиям, что поможет усовершенствовать ваш бизнес. Важность баланса между рисками и преимуществами, которые могут приносить новые технологии, не должна преуменьшаться. Зачастую инновация может одновременно и обеспечить защиту и увеличить производительность.

Когда вы внедряете инновационные решения и технологии, оценка рисков безопасности должна быть частью процесса внедрения. Примите необходимые меры безопасности на ранних стадиях процесса внедрения. Планируя ваши бизнес-задачи, сразу продумайте вашу инфраструктуру, а именно, как бизнес-требования, под которые данная инфраструктура создается, будут сочетаться с требованиями по обеспечению информационной безопасности.

Обязательно вовлекайте эксперта по безопасности в планирование IT инфраструктуры, для того, чтобы безопасность была встроена в систему, а не просто «прикручена» к ней. Это даст более глубокий уровень защиты, который необходим вам для внедрения инноваций.

ДАЛЕЕ >

2 ПРОВЕРЯЙТЕ ГРАНИЦЫ

Одна из распространенных ошибок, которую совершают некоторые компании, заключается в предположении, что как только они внедрили меры безопасности, работа завершена. В современном мире это далеко от истины. Угрозы изменяются и киберпреступники учатся по ходу своей деятельности, постоянно возрастает уровень сложности. Бдительность в применении к ландшафту угроз, а также контроль за использованием ваших информационных систем и политик безопасности являются критическими факторами.

Постоянная оценка устойчивости вашей компании к киберугрозам и уязвимостям помогает оценить прогресс и адекватность мероприятий по обеспечению безопасности. Постоянно проверяйте вашу инфраструктуру на предмет обнаружения вторжений и проводите аудит на местах. Рассмотрите возможность привлечения третьих компаний для идентификации уязвимостей. Обменивайтесь опытом с другими компаниями в индустрии и будьте в курсе новых угроз.

3 СФОКУСИРУЙТЕСЬ

При существующем объеме угроз в современном мире, управление информационной безопасностью в вашей организации может походить на постоянные попытки заделать пробоины в судне. Ключом к решению проблемы является понимание того, какая информация или какие данные являются критичными для поддержания вашего бизнеса «на плаву».

Определите самые критичные для взлома информационные системы и назначьте задаче по их защите наивысший приоритет. Учитывайте такие последствия взлома, как потеря конфиденциальной информации, репутация компании, несоответствие требованиям регуляторов. Затем сфокусируйтесь на том, где вы можете минимизировать риск.

ДАЛЕЕ >

4 БУДЬТЕ ГОТОВЫ

Этот пионерский девиз с не меньшим основанием должен быть девизом любого ответственного за обеспечение безопасности в компании. Не важно, насколько вы аккуратны – инциденты безопасности будут происходить. В текущих условиях угроз и уязвимостей вы должны исходить не из предположения «если инцидент случится», а из предположения «когда он случится». То, как вы реагируете на инцидент, и не только на сам инцидент, может стать решающим моментом. Ни одна из компаний, подвергшихся взломам в 2014 году, не ожидала, что она станет жертвой до того, как это случилось. Те из них, кто имел готовый план, восстановились быстро и с наименьшими негативными последствиями.

Возьмите за правило иметь план восстановления работоспособности. Чем больше и сложнее организация, тем больше типов инцидентов вы должны в нем учесть. Проконсультируйтесь с экспертом из сторонней организации для лучшего понимания и предупреждения возможных сценариев угроз. Определяя их заранее, вы существенно снизите время реакции в случае реального взлома.

Уделяйте должное внимание вашей способности реагировать и помните, что коммуникация является ключевым моментом. Те, кто игнорирует важность этого правила, могут обнаружить себя в ситуации нежелательного внимания, когда их безопасность дает сбой.

Приготовьте хорошо выверенные планы сообщений в случаях инцидентов безопасности со сдержанной, подходящей информацией, как это требуется для внутренней аудитории, внешней аудитории и для властей.

Б. СМОТРИТЕ ВПЕРЕД

5 НАУЧИТЕСЬ ВИДЕТЬ ЛЕС ЗА ДЕРЕВЬЯМИ

При проведении аудита информационной безопасности важно получить информацию об угрозах и уязвимостях. Но не менее важно знать о первопричинных факторах и видеть целостную картину того, куда вы хотите вести вашу организацию.

Согласно отчету о Сервисах Безопасности IBM[4] за 2014 год, более чем в 95% всех расследуемых инцидентов человеческий фактор был указан в числе оказавших влияние. Некоторыми факторами, повлекшими инцидент, явились неправильное конфигурирование систем или плохой патч- менеджмент, однако пятью наиболее частыми причинами инцидентов явились потерянные ноутбуки и мобильные устройства, раскрытие конфиденциальной информации вследствии отправки сообщений электронной почты ошибочному адресату, запуск вредоносных приложений и открытие вредоносных веб-сайтов.

По большому счету, обеспечение информационной безопасности - это задача каждого сотрудника в организации. Наиболее подготовленные компании знают, что политика безопасности должна брать свое начало из стратегических целей, бизнес-задач и корпоративной политики, и быть связанной с процедурами и требованиями компании, оценкой производительности и, конечно, с людьми на всех уровнях организации.

Если вы хотите иметь здоровый лес, вы должны позаботиться о его экосистеме в целом.

Обучайте людей тому, как риск может быть снижен и как продуманная информационная безопасность может улучшить бизнес, а не мешать ему.

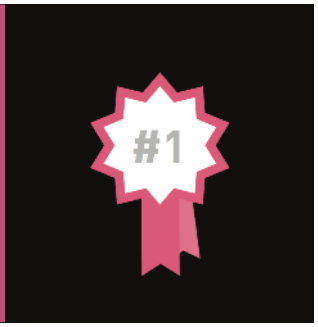
[4] IBM Security Services 2014 Cyber Security Intelligence Index report

ДАЛЕЕ >

6 ВЫЙТИ ЗА ПРЕДЕЛЫ ДОСТАТОЧНОГО

Соответствие требованиям регуляторов среди прочего включает в себя обширный список законов и регулирующих документов, которым должны следовать компании. К сожалению, многие думают, что если они соответствуют данным требованиям, то они полностью защищены. Такой подход существенно сужает охват и эффективность оценки состояния безопасности. Соответствие требованиям регуляторов обычно сконцентрировано на специфических угрозах, например, на охране персональных данных и не является комплексным подходом, каким должна быть оценка состояния информационной безопасности. Например, если требования регуляторов не затрагивают вопросы обеспечения безопасности сети, это не должно становиться основой вашей политики информационной безопасности. Имея это в виду, выходите за пределы требований регуляторов. Создавайте более строгую политику безопасности, которая защищает информацию и обеспечивает ответную реакцию. Действуя так, вы встроите требования регуляторов внутрь политики.

7 СДЕЛАЙТЕ БЕЗОПАСНОСТЬ ОФИЦИАЛЬНЫМ ТРЕБОВАНИЕМ



Назначая корпоративные политики безопасности официальными документами и распространяя их внутри компании, вы достигаете чрезвычайно важных преимуществ:

- Вы создаете для всех сотрудников компании стандарт для обращений, который становится частью культуры;
- Большее число людей будет вовлечено в этот процесс и будет вносить свой вклад в защиту жизненно важных информационных активов;
- Ваша открытость угрозам станет более управляемой.

Привлекая большее количество сотрудников к внедрению политики информационной безопасности, вы помогаете ее более эффективной реализации. Например, в городах с населением свыше 50000 человек, на 600 жителей в среднем приходится один офицер полиции. Когда большинство населения вовлечено в соблюдение законов, граждане подчиняются правилам.

Точно так же происходит и в бизнесе. Привлеките ваших работников к совершенствованию информационной безопасности, обучая их тому, как они могут в этом помочь. Создавайте такие политики информационной безопасности, которые сотрудники смогут понять и помочь их усилить.

ДАЛЕЕ >

B. ПОМНИТЕ О ДЕТАЛЯХ

8 ЗАИНТЕРЕСУЙТЕ ЛЮДЕЙ

Глобальные цели имеют огромный эффект, когда они приходят сверху. Защита информации вашей организации должна быть глобальной целью. Для большинства менеджеров высшего звена информационная безопасность не стоит в числе высокоприоритетных задач; вы должны включить ее туда.

За последние пять лет взломы, случившиеся почти в каждой отрасли экономики, дали достаточно данных для того, чтобы не игнорировать приоритеты информационной безопасности. Найдите примеры компаний, похожих на вашу и подчеркните вашему руководству потенциальные риски. Если они еще не осознают их, эти данные помогут им прийти к пониманию. Выделение адекватных ресурсов, как финансовых, так и людских, играет важную роль в обеспечении защиты компании. Подпись исполнительного директора под политикой информационной безопасности компании демонстрирует активную поддержку.

Помогите каждому участнику на всех уровнях понять важность устранения кибер-рисков для защиты интеллектуальной собственности. Одно это защитит сердце компании и поможет поддерживать конкурентное преимущество.

Все мы знаем, что числа и данные говорят громче всяких слов. Создайте систему метрик, которая поможет вам регулярно отчитываться о прогрессе в деле информационной безопасности. Также, как минимум раз в год, предоставляйте эти метрики высшему руководству компании.

Скорее всего,вы захотите указать ключевые показатели безопасности и отобразить на графиках эффективность применяемых мер. Это даст важный материал для постоянной оптимизации вашей политики безопасности, равно как и для будущих инвестиций в эту область.

9 СОЗДАЙТЕ АТМОСФЕРУ ОТВЕТСТВЕННОСТИ

Эффективное управление информационной безопасностью требует инструментов, тренировки и методов контроля. И, так как сотрудники зачастую негативно смотрят на применение политик безопасности, необходима хорошая внутренняя коммуникация. Жизненно необходимо быть уверенным, что методы, технологии контроля и инициативы в области безопасности были обнародованы и объяснены сотрудникам. Пусть ваши коллективы знают о новых угрозах и инвестициях компании в обеспечение полной защиты.

Обучайте сотрудников, чтобы они поняли, насколько они ответственны и какова их роль в деле защиты от угроз. Особенно важно сделать упор на тематике социальной инженерии, в силу ее чрезвычайного распространения при осуществлении атак.

Независимо от размера вашей компании, проведите среди сотрудников обучение по политике безопасности для того, чтобы подчеркнуть ее значение.

В больших компаниях выделите время и определите сотрудников, которые будут помощниками в деле внедрения политики информационной безопасности. Каждому должны быть назначены четкие обязанности, с ясным пониманием взаимодействия между сотрудниками. Задокументируйте это и распространите информацию среди всех участников для ознакомления.

Также не забудьте поделиться информацией с другими компаниями в отрасли. Это может создать неоценимые связи в деле выработки лучших практик и противодействия новым атакам.

ДАЛЕЕ >

10 НИКОГДА НЕ УПРОЩАЙТЕ

В некоторых компаниях в силу нехватки ресурсов или экспертизы управление безопасностью отдано на аутсорсинг. Часто такие сервисы, как резервное копирование и восстановление, шифрование и защита данных могут быть особенно привлекательными для малых компаний. Но аутсорсинг приносит свои риски.

Внешние компании, которые не прилагают адекватных усилий к защите информации или информационных систем, могут оказаться серьезной проблемой для бизнеса организации, ее репутации и стоимости бренда.

Вот некоторые моменты, которые необходимо иметь в виду:

1. Требуйте от ваших сервис-партнеров или поставщиков соблюдения политик информационной безопасности вашей организации.
2. Убедитесь, что определены и соблюдаются соглашения об уровне сервиса (SLA, Service Level Agreement), в которые включены параметры доступности систем и времени восстановления их работы. Периодически проводите аудит соблюдения вашим провайдером SLA. Проверяйте журналы активности для анализа и выявления угроз.
3. При использовании облачных сервисов учитывайте необходимость специальных политик информационной безопасности. Если вы работаете с провайдером в области хранения, обработки или управления данными в сети, ознакомьтесь с его политиками безопасности, а также областью их действия.

Независимо от того, IT-сервис провайдер ли это, облачный провайдер или аутсорсинговая компания, если они имеют доступ или управляют любыми важными для работы вашей компании данными, убедитесь, что вы понимаете их политики безопасности и механизмы защиты.

ЗАКЛЮЧЕНИЕ

ПРЕВРАТИТЕ БЕЗОПАСНОСТЬ В ДВИГАТЕЛЬ

Учитывая тот факт, что данные являются краеугольным камнем бизнеса, современные руководители не могут позволить себе игнорировать вопросы безопасности. Без надлежащей политики, как компания, так и ее клиенты подвергаются риску. Понимая потенциальные угрозы и уязвимости, создайте надежный план, соотнесенный с вашим бизнесом, и убедитесь, что механизмы защиты интегрированы в вашу IT-инфраструктуру. Тогда вы можете превратить безопасность в двигатель бизнеса, а не в его тормоз.

Сделайте проактивный шаг – убедитесь, что Вваша организация защищена. Подпишитесь на **CHECK POINT'S SECURITY CHECKUP** – бесплатную онлайн проверку, которая поможет выявить потенциальные риски Вашей сети.

http://www.checkpoint.com/campaigns/securitycheckup/index.html

Check Point®
SOFTWARE TECHNOLOGIES LTD.

WE SECURE THE FUTURE

Дополнительную информацию о том,
как обеспечить безопасность вашей организации,
вы можете найти на сайте www.checkpoint.com

НАШИ КОНТАКТЫ

Международная штаб-квартира | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com

Представительство в России и СНГ | Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com