Александр Самарин

Безопасность в ИТ малого бизнеса

издание 2-е, дополненное

Александр Самарин

Безопасность в ИТ малого бизнеса

«Автор»
2017

Самарин А. М.

Безопасность в ИТ малого бизнеса / А. М. Самарин — «Автор», 2017

ISBN 978-5-532-07997-7

Безопасность информационных технологий среднего и малого бизнеса основана на мероприятиях, направленных на повышение и поддержание уровней защиты данных и информационных систем, а также предотвращения атак на критичные информационные ресурсы. Некоторые аксиомы безопасности, элементарные правила и несложные приёмы помогут решению задач, поставленных перед информационной и физической безопасностью на предприятии. О методиках, эффективных действиях и примерах защиты данных и информационной среды малого бизнеса в этой книге.

ISBN 978-5-532-07997-7

Содержание

Александр Самарин
Безопасность в ИТ малого бизнеса

Безопасность информационных технологий среднего и малого бизнеса основана на мероприятиях, направленных на повышение и поддержание уровней защиты данных и информационных систем, а также предотвращения атак на критичные информационные ресурсы. Некоторые аксиомы безопасности, элементарные правила и несложные приёмы помогут решению задач, поставленных перед информационной и физической безопасностью на предприятии. О методиках, эффективных действиях и примерах защиты данных и информационной среды малого бизнеса в этой книге.

Глава 1. Инвентаризация санкционированного и устранение постороннего ПО

Для начала коротко рассмотрим наиболее вероятные сценарии действий внешних злоумышленников. Начнем с ежедневно используемого в офисе или операционной среде предприятия программного обеспечения.

Достаточно серьезную опасность представляют «внешние» компьютеры, которые работают как интернет-ресурсы и оснащены устаревшими версиями ПО, например, веб-сервер Apache, BIND или Sendmail. Поиск и сканирование систем с такими уязвимыми версиями являются первым шагом злоумышленника к проникновению в систему или корпоративную сеть. Практически все хакеры пользуются сетевыми сканерами, позволяющими изучить сетевое окружение атакуемого и найти ресурсы сети, открытые для записи. Это предварительная стадия скрытого вторжения, за которой следует «фишинг». Операция фишинга заключается в подмене рабочего здорового файла «зараженным» или внедрение на сетевые ресурсы предприятия вредоносной программы под видом рабочей программы. Фишинг можно назвать одним из видов мошенничества, которое использует методики «социальной инженерии[1]» в электронной форме.

Другими способами проникновения посредством фишинга могут быть электронные письма с «вирусным» вложением, обман интернет-пользователей через «зараженный» контент уже взломанных сайтов или негласную подмену веб-страниц легальных сайтов сторонних владельцев страницами с вредоносным кодом.

Значительный риск в бизнесе несет использование постороннего программного обеспечения, которое попадает в локальную сеть через неграмотных в вопросах безопасности пользователей. Разъясняйте пользователям их ошибки, создайте в Политике информационной безопасности предприятия правила, которые своевременно пресекут загрузку ПО из сети интернет. Организационными мерами закрывайте такую возможность. Технические мероприятия по фильтрации парка программного обеспечения и устранению постороннего ПО стоят значительно дороже.

Когда пользователи выполняют доступ к вредоносному содержимому с помощью уязвимого браузера или клиентской программы, компьютер скрытно атакуется, предоставляя хакеру возможность проникновения в машину для получения долгосрочного контроля над чужой компьютерной системой. Некоторые сложные проникновения могут использовать уязвимости «нулевого дня»[2][3].

Когда один компьютер скрытно взломан и при этом продолжает эксплуатироваться, злоумышленники часто используют его в качестве «пункта наблюдения» для сбора конфиденциальной информации о пользователе и о других взаимодействующих компьютерах. Такая машина используется и в качестве стартовой точки для проникновения по всей сети. В результате хакер может быстро превратить одну скомпрометированную машину в армию подобных.

Предприятию, не имеющему полного реестра программ, как правило, не удастся устранить проблемы блокировки нарушителей и злоумышленников, а также выявить системы, работающие с уязвимым или вредоносным ПО. Контроль и управление всем ПО предприятия также

---

[1] Социальная инженерия – здесь понимается как незаконный метод получения доступа к закрытой информации, зачастую используемый в интернете, или подмены информации, которая представляет ценность и приводит к достижению цели со стороны хакера.

[2] Фишинг – phishing (от англ. слова fishing «рыбалка, удить рыбу».

[3] Уязвимостью «нулевого дня» называют уязвимость, которая ранее не была известна и поэтому для нее пока нет исправления/обновления.

играет важную роль в планировании и эксплуатации резервного копирования/восстановления информационных систем. Следовательно, без инвентаризации ПО проблемы по размеру больше и возникают чаще.

Инвентаризация ПО, внедренная в рамках всего предприятия, должна охватывать все типы используемых ОС на всех устройствах, включая серверы, рабочие станции и ноутбуки. Механизм инвентаризации должен записывать наименование системного и прикладного ПО, которое установлено на каждом сервере/станции, а также номер версии и релиза (уровень обновления) поименованного ПО.

Комплекс инвентаризации ПО должен быть интегрирован с инвентаризацией аппаратного оборудования таким образом, чтобы все устройства и соответствующее ПО отслеживались из единого центра. Проще говоря, аккуратная и полная инвентаризация ПО может быть противопоставлена обманным трюкам самых хитроумных хакеров. В любом случае без надлежащего контроля за программным обеспечением предприятия невозможно должным образом защитить свои информационные активы.

Глава 2. Применение «белого списка» ПО

Инвентаризация ПО является базисом для создания «белого списка». Этот список может быть внедрен путем применения специализированных коммерческих программ или с прикладными программами «белых списков», встроенными в антивирусные пакеты или ОС Windows. Системы инвентаризации ПО доступны и используются сегодня на многих предприятиях. Лучшие из них обеспечивают инвентаризацию сотни установленных и эксплуатируемых на предприятии приложений, извлекая информацию о версиях патчей каждой используемой программы, чтобы подтвердить актуальность и принадлежность программного приложения к общему перечню легального ПО.

Функции проверки по внедренным «белым спискам» разрешенных для запуска программ включены во многие современные комплексы безопасности. Более того, коммерческие решения все чаще комплектуются антишпионскими, антивирусными программами, персональным файерволом (firewall) и встроенными системами обнаружения вторжений (IDS) и предотвращения вторжений (IPS). Могут одновременно применяться и «белый» и «черный» списки. Большинство решений для такой защиты указывает наименование, расположение файловой системы и/или криптографический хэш[4], дающий исполнителю возможность определить, следует ли разрешить приложению работать на защищаемом компьютере.

Наиболее эффективны инструменты из специализированных «белых списков». Иногда применяются функции типа «серого списка», который составлен администраторами и определяет правила для выполнения конкретных программ только для уполномоченных пользователей и/или в определенное время суток.

Разрабатывая на предприятии список санкционированного ПО, необходимо учесть каждый тип системы и оборудования. Обязательно установите средства проверки целостности файлов для обеспечения гарантии того, что критические системные файлы (важных систем, исполняемых приложений, библиотечных модулей и настроек конфигураций) и файлы ПО из «белого списка» неизменны. Все изменения в таких файлах должны автоматически оповещать о событиях специалистов безопасности. Система оповещения должна иметь возможность отличить штатные изменения и выделять необычные события.

Внедренная технология «белых списков» приложений позволяет системе запускать ПО, если оно включено в «белый список», и запрещает запускать все остальное ПО. «Белый список» может быть очень обширным и включать дополнительные «белые списки» от вендоров коммерческих программ, чтобы пользователи не испытывали неудобства при использовании офисного ПО общего назначения. Для специальных систем, которые используют строго ограниченное число программ для своей необходимой бизнес-функциональности, «белый список» может быть довольно узкий. При защите системы со специализированным ПО возможно использование виртуальной среды, которая более защищена от вторжений и легко восстанавливается из копии предыдущего состояния.

Технологию «белых списков» необходимо поддерживать регулярным сканированием для обнаружения нелегального ПО. Чтобы обнаружить любые изменения или установки ПО на устройствах в сети, должен быть реализован строгий процесс контроля изменений. Например, с помощью контроля целостности файлов или состояния системы. Этот процесс включает оповещение, когда неопознанные объекты (исполняемые файлы, библиотеки DLL и т. п.) выявлены в системе. Контроль изменений должен включать проверку модифицированных версий ПО с использованием сравнения хэш-значений файлов. Злоумышленники часто используют

[4] Криптографический хэш – результат математического преобразования над файлом для контроля целостности этого файла.

измененные версии известных программ для нападения, а сравнение файлового хэша укажет на взломанные программные компоненты.

С практическим контролем списка исполняемых модулей при помощи программы «СКЗИ инфо» можно ознакомиться в рекомендациях Банка России http://www.cbr.ru/mcirabis/po/recommend.pdf [1].

Глава 3. Использование стандартных безопасных системных образов для ноутбуков, рабочих станций и серверов

При поставке оборудования от производителей и поставщиков настройки по умолчанию для устройств, операционных систем и приложений, как правило, ориентированы на легкость внедрения, но не на безопасность. Конечно, возможно и обратное, когда в процессе внедрения системы приходится разрешать некоторые функции в ущерб безопасности. Тем не менее здесь необходим осознанный, квалифицированный подход, так как основные элементы управления, открытые службы и порты, аккаунты и пароли по умолчанию, устаревшие (уязвимые) протоколы, предустановленное ненужное ПО – все это потенциально может быть использовано для несанкционированного проникновения.

Вместо того, чтобы с нуля разрабатывать базовые настройки безопасности для каждой программно-аппаратной системы, предприятие должно использовать публично распространяемые, проверенные, сопровождаемые настройки безопасности, а также руководства по обеспечению безопасности и/или чек-листы.

Необходимую информацию содержат следующие порталы:

The NIST National Checklist Program [2];

Информационный портал по безопасности [3];

Информационно-аналитический портал [4];

Инвентаризация ПО Microsoft SAM [5];

Поставщики услуг и техники [6].

Далее предприятию необходимо расширять или корректировать публичные исходные настройки безопасности для удовлетворения местных политик и требований, а также обосновывать и документировать принимаемые отклонения, чтобы облегчить последующие осмотры или служебные проверки.

Для большого комплексного предприятия создание единой базовой конфигурации безопасности (например, один установочный образ для всех рабочих станций по всему предприятию) иногда неприемлемо или невозможно. Вполне вероятно, что необходимо поддерживать различные стандартные образы на основе соответствующих конфигураций систем и необходимых функций для первоначального старта (например, рабочая станция бухгалтера с приложением 1С или станция разработчика ПО и тому подобные). Число вариаций лучше свести к минимуму, чтобы ясно понимать свойства безопасности и управлять ими. Однако необходимо быть готовым управлять несколькими базовыми линейками образов.

ПО управления настройками можно использовать для сопоставления параметров ОС, как и для сопоставления параметров приложений, контролируемых машин при поиске отклонений от стандартной конфигурации образа.

Типичные инструменты отслеживания настроек используют некоторый комплекс: проверка через агента, установленного на каждой управляемой системе, или проверка систем без участия агентов, с удаленным входом на каждую управляемую машину. Кроме того, иногда используется гибридный подход, в процессе которого инициируется удаленный сеанс и временный или динамический агент устанавливается на целевой системе для сканирования, а затем агент удаляется.

Старайтесь аккуратно и строго управлять конфигурациями. Создайте исходный безопасный образ и используйте его для создания всех новых систем, которые появляются в IT-среде предприятия. Всякую востребованную систему, которая «сломана», можно повторно восстано-

вить с помощью такого образа. Периодические обновления и/или исключения из этого образа важно интегрировать в процессы управления изменениями на предприятии. Образы необходимо создать для базовых вариантов рабочих станций, серверов и, возможно, для некоторых виртуальных машин предприятия.

Типовые образы компонуются как сконфигурированные версии базовой операционной системы и приложений. Конфигурирование обычно включает в себя: блокирование или удаление избыточных учетных записей, удаление или отключение ненужных служб, установку необходимых обновлений, закрытие открытых и неиспользуемых сетевых портов, удаление неисполняемых скриптов, а также включение файрволов и систем обнаружения вторжений. Типовые образы должны пересматриваться и обновляться на регулярной основе, чтобы поддержать необходимый уровень безопасности в противодействии «свежим» уязвимостям и модифицированным хакерским атакам.

Хранить мастер-образы рекомендуем на надежно защищенных серверах, оснащенных инструментами проверки целостности файлов, руководствуясь принципом постоянного контроля и управления изменениями, чтобы гарантировать возможность только авторизованных изменений. В качестве альтернативы мастер-образы могут быть сохранены на автономных машинах, отключенных от производственной сети. Иногда образы могут быть скопированы на безопасные, надежные носители для их перемещения между серверами и станциями производственной сети. В общем случае мастер-образ является частным случаем «резервной копии», так называемого бэкапа, о котором немного позже.

Глава 4. Дистанционные инструменты – корпоративный ноутбук, персональный смартфон

Сразу отметим, что информация корпоративного ноутбука зачастую стоит дороже самого ноутбука. Как пользоваться переносным устройством вне офиса, защитить оборудование и его данные, пойдет речь в этой главе.

Корпоративная техника обычно является предметом коллективного использования. Не является исключением и такое устройство, как ноутбук, принадлежащий организации. Переносной компьютер представляет удобную возможность выполнять служебные обязанности вне помещений и офисов, занимаемых бизнесом, но это удобство несет определенные риски. Именно поэтому наличие в ноутбуке служебной, коммерческой информации или программ с возможностью доступа в корпоративную сеть вынуждает применять к этому устройству три главных принципа информационной безопасности: конфиденциальность, целостность, доступность. А это, в свою очередь, означает, что нарушения принципов или правил использования ноутбука, регламентированных на предприятии, в большинстве случаев приведут к возникновению инцидентов информационной безопасности.

Самый опасный инцидент, который может произойти с переносным компьютером, – это потеря или утечка конфиденциальной информации с устройства. Стоимость такой информации с учетом вероятных рисков во много раз превышает стоимость самого ноутбука.

Для использования вне офиса при временном владении и эксплуатации устройства, переходящего из рук в руки, применяются различные превентивные меры безопасности. Оговоримся сразу, речь идет о переносном компьютере, совместимом с архитектурой IBM PC, причем этот компьютер не попадает в разряд устройств BYOD[5].

Мобильное рабочее место на базе ноутбука обычно подготавливается специалистом IT в соответствии с типовой конфигурацией, предписанной политикой ИБ предприятия.

– При выдаче в служебном журнале или базе регистрируется серийный номер ноутбука для исключения возможности его подмены. Комплект с переносным устройством включает в себя силовой шнур и соответствующий блок питания.

– Устанавливается пароль на BIOS[6]/UEFI[7] ноутбука во избежание изменения аппаратной конфигурации и/или замены внутренних компонент устройства.

– Специальными средствами (BitLocker, TrueCrypt, SecretDisk[8]) шифруется системный диск для защиты собственного содержимого, предотвращая несанкционированный доступ к операционной системе и доступ посторонних к параметрам и конфигурациям программ ноутбука, включая удаленный вход в корпоративную сеть.

---

[5] BYOD – Bring Your Own Device, мобильное устройство (ноутбук, нетбук, планшет или смартфон), владельцем которого является пользователь, а не предприятие [7].

[6] BIOS – Basic Input/Output System, интерфейс для управления набором микропрограмм, представляющих «базовую систему ввода-вывода» для IBM PC-совместимого компьютера [8].

[7] UEFI – Unified Extensible Firmware Interface, интерфейс между операционной системой и микропрограммами IBM PC-совместимого компьютера. Идет на смену устаревшему BIOS [9].

[8] BitLocker, TrueCrypt, SecretDisk 4 – наиболее часто используемые продукты для шифрования дисков, томов рабочих станций в среде Windows [10].

– При необходимости выдается идентификационная карта или токен (ESMART Token, eToken PRO, JaCarta PKI[9]) с привязкой к логину пользователя для однозначной аутентификации пользователя в корпоративной сети.

– Дополнительно к ноутбуку могут быть выданы мышь и металлизированный трос с ключом для физической привязки переносного компьютера к рабочему месту, например, на время командировки.

Соблюдая формальности, с временного владельца берется расписка с указанием срока и цели использования ноутбука, а со стороны предприятия специалист IT вместе с ноутбуком может вручить пользователю памятку о необходимых мерах безопасности. Предприятию не лишним будет рассмотреть возможность страхования ноутбуков, выдаваемых своим сотрудникам во временное пользование. Стоимость страхования может зависеть от стоимости обрабатываемой информации. Очень важно, чтобы выданный ноутбук внутри и вне предприятия поддерживал принятые требования информационной безопасности. Как раз об этом далее.

[9] Рутокен, ESMART Token, eToken PRO, JaCarta PKI – это типы самых распространенных специальных устройств, применяемых для авторизации пользователя [11].

Глава 4.1. Передача ноутбука в пользование и возврат

При выдаче/возврате ноутбуков соответствующий регламент обязан учитывать принципиальные различия в функционале пользователей ноутбуков. Например, если ноутбук использовался топ-менеджером, а затем переходит в руки программиста, то высока вероятность несанкционированного доступа к конфиденциальной информации. Для недопущения подобных случаев информация на жестком диске ноутбука после предыдущего владельца удаляется и на ноутбук устанавливается типовой исходный образ операционной системы – билд[10]. Подобное действие полезно практиковать независимо от того, был ли зашифрован жесткий диск или нет.

Разумно поддерживать два-три различных стандартных образа, предназначенных для ноутбуков с необходимыми функциями для первоначального старта (например, ноутбук для презентаций, ноутбук бухгалтера или ноутбук разработчика ПО и т. п.). Число вариаций лучше свести к минимуму, чтобы ясно понимать уровни безопасности и управлять ими. Если ноутбук возвращается после использования, то пользователя, безусловно, необходимо предупредить, что вся информация на жестком диске будет удалена и несвоевременное информирование в большинстве этих случаев заканчиваются негативно.

Ноутбук может выдаваться пользователю краткосрочно, что не вызывает особых проблем с точки зрения контроля и безопасности. Если же устройство передается на длительный срок, то специалистам IT и безопасности предприятия необходимо периодически проверять наличие устройства у пользователя, например, через соединение в корпоративной сети. Сеансы соединения должны быть регламентированы (например, не менее одного раза в неделю) и кроме контроля обычно несут функциональную нагрузку. Загружаются свежие антивирусные базы, устанавливаются обновления для компонент операционной системы, возможно выполнение удаленного резервного копирования и т. п.

Ноутбук и комплектное к нему оборудование должны быть предоставлены для проверки по первому требованию ответственного IT-специалиста или сотрудника безопасности предприятия. Это необходимо для оперативного устранения «вирусных атак», каких-либо опасных уязвимостей или при реагировании на чрезвычайные ситуации. Рекомендуется поддерживать документируемую связь с пользователем через корпоративную электронную почту или мобильный телефон. В экстренных случаях доступ ноутбука в корпоративную сеть незамедлительно блокируется.

[10] Build – билд, в нашем случае сборка содержимого системного жесткого диска ноутбука, ориентирована на типовой обобщенный функционал пользователя. Обычно в Windows-среде формируется с помощью ПО Drive Image, Acronis, Symantec и пр. [12].

Глава 4.2. Ноутбук у пользователя вне предприятия

Допустим, ноутбук передан пользователю. Вместе с ноутбуком пользователю вручается памятка о необходимых мерах безопасности. Обязательство ознакомиться с памяткой и использовать мобильное устройство должным образом закреплено в расписке пользователя с указанием срока и цели использования ноутбука. Основные рекомендации памятки могут быть следующими.

– Переносите ноутбук в надежной сумке, защищающей устройство от влаги, ударов и повреждений. Не размещайте одновременно с оборудованием в сумке письменные принадлежности, пищу или напитки. Риск того, что ваша карьера может зависеть от бутылки газировки – недопустим.

– Перед транспортировкой завершите работу и выключите ноутбук. Отключите все кабели и периферийные устройства. По возможности не сдавайте ноутбук в багаж на время перелета. Известны случаи, когда ноутбук волшебным образом исчезал из багажа.

– Адаптируйте ноутбук к переменам температурных условий и влажности окружающей среды минимум 15—20 минут. Опасайтесь высокой влажности, т. к. внутри ноутбука образуется конденсат, что может привести к короткому замыканию. Если смотреть на обстоятельства реально, то пользоваться ноутбуком в сауне – опасно для жизни.

– Избегайте попадания на ноутбук прямых солнечных лучей. Сложная бытовая техника не дружит с солнцем. Старайтесь не оставлять ноутбук в жару в салоне автомобиля или в багажнике. В солнечный день температура внутри машины всегда выше допустимых для компьютера норм.

– Используйте ноутбук на ровном твердом столе, подставке. Не ставьте работающий компьютер на мягкие поверхности, такие как ковер, одеяла, подушка. Неровные мягкие поверхности препятствуют воздушному охлаждению устройства, а следствием является недолгий срок работы.

– Как минимум раз в неделю подключайте ноутбук к корпоративной сети для обновления антивирусных баз и модулей операционной системы. Не используйте посторонние источники обновлений в интернете. Не устанавливайте постороннее программное обеспечение, в случае необходимости обращайтесь в подразделение IT. В противном случае вас с большой вероятностью обвинят в распространении «вредоносного кода».

– Не рекомендуется использовать ноутбук и дополнительное оборудование в общественных местах, где есть вероятность насильственного захвата ноутбука или его кражи. Строго оградите ноутбук от использования посторонними лицами. Пользователь несет ответственность за безопасность использования вверенного оборудования. Потеря или кража ноутбука доставят вам немало досады и «служебной горечи».

– Соблюдайте правила и требования корпоративных политик информационной безопасности. Не допускайте передачи и случайного ознакомления посторонних лиц с паролями доступа к ноутбуку и служебными сервисами дистанционного доступа. Если вы семейный чело-

век, то для познания электронного мира купите детям или «второй половине» личный компьютер.

– В случае утери или кражи устройства пользователь обязан в течение двух часов проинформировать службу безопасности предприятия о данном инциденте, а затем обратиться в правоохранительные органы по факту пропажи оборудования. Своевременные адекватные меры помогут предотвратить утечку информации и, возможно, вернуть утерянное устройство.

В общем случае рекомендации по использованию, переноске и защите ноутбука опубликованы на сайте производителя, например, HP [13].

Помните, читатель, что ноутбук не Ваш, а корпоративный. Следовательно, работодатель имеет полное право знать, что происходит и как вы пользуетесь переносным компьютером компании. Возникают определенные риски, которые несет Работодатель, вверяя вам компьютер для дистанционного использования, имеет серьезные основания ограничить действия, которые возможны при соединении ноутбука компании с интернетом. Выполнение прописных элементарных правил будет способствовать вашей успешной работе.

Глава 4.3. Персональные мобильные устройства.

Для персональных ноутбуков и смартфонов требования к защите информации ужесточаются. Повсеместный доступ в Интернет и легкая доступность к недостаточно защищенным мобильным устройствам диктуют новые правила к безопасности информационного обмена.

Для работы через Интернет желательно сохранить анонимность работы в глобальной сети, что возможно, если использовать VPN[11]. Эта технология позволяет заходить на интернет-ресурсы скрывая источник соединения так, что никто не узнает настоящее местоположение источника данных. Это важно, если вы решили из-за границы совершить операцию в российской финансовой организации или подключиться к сервису для просмотра иностранных новостей и медиа-файлов из России. До использования VPN такая возможность достигалась через соединение, состоящее из цепочки прокси-серверов. VPN реально поможет сохранить местонахождение источника запросов или воспользоваться сервисом, доступным только для конкретной страны. Полная анонимность возможна, если VPN-провайдер не хранит данные о вашем соединении и имеет много стран, где расположены VPN-серверы.

Наиболее популярны VPN-сервисы: RusVPN[12], TunnelBear[13] и Hideman[14]. У этих сервисов есть приложения для iOS, Android, а также версии для персональных компьютеров. Для браузеров Chrome и Opera есть соответствующие расширения (плагины). Запускайте программу, выбирайте исходную страну для вашего соединения, и вы получите необходимую степень анонимности. Более мощной альтернативой VPN-службам является небезизвестный браузер Tor[15]

[11] VPN – англ. Virtual Private Network, виртуальная частная сеть.

[12] RusVPN – https://rusvpn.com

[13] TunnelBear – https://www.tunnelbear.com

[14] Hideman – https://www.hideman.net

[15] Tor – https://torproject.org

Конец ознакомительного фрагмента.