Значимость безопасности печати для бизнеса

При финансовой поддержке:
HP

Авторы:
Анжель Бойд
Кейт Кметц
Мэтью Марден

Ноябрь 2015 г.

МНЕНИЕ IDC

Согласно исследованию IDC, 80% опрошенных компаний отметили, что ИТ-безопасность важна для выполнения их бизнес-процессов, но только 59% этих компаний заявили, что для их бизнеса важна безопасность устройств печати. Кроме того, высшее руководство с на 40% более высокой вероятностью будет принимать участие в принятии решений по общей ИТ-безопасности, чем в принятии аналогичных решений по безопасности устройств печати. Мы считаем, что такие результаты говорят о недостаточном внимании к безопасности среды печати, что может поставить под угрозу работу предприятий. Исследование IDC показало, что у предприятий есть веские основания обратить большее внимание на безопасность устройств печати, поскольку безопасная среда печати создает преимущества для ИТ и бизнеса, а именно:

- В ходе исследования IDC обнаружено, что более половины опрошенных компаний сталкивались с проблемами нарушения ИТ-безопасности в течение последних 12 месяцев, в том числе связанными с устройствами печати
- При работе с документами и печати можно обнаружить множество потенциальных угроз безопасности. Они могут возникать в результате вредоносных атак внутри и вне организации, а также неосторожного использования устройств печати и напечатанных материалов. Потенциальные нарушения безопасности, связанные с устройствами печати, могут возникать на уровне сетевых портов устройства, в результате перехвата заданий печати, копирования и сканирования, несанкционированного использования жестких дисков и памяти (ОЗУ) принтеров и МФУ, оставления напечатанных и скопированных документов в выходных лотках или незаконного использования бланков строгого учета (чеков, рецептов) и т. д.
- Компания IDC провела подробный опрос заинтересованных специалистов в организациях, в которых внедрена система безопасности документооборота и печати, и выявила два типа таких предприятий.
  - Компании, заботящиеся о безопасности и соблюдении нормативных требований, в которых реализована безопасная ИТ-инфраструктура в масштабах всего предприятия
  - Компании, которые видят выгоду от внедрения эффективной ИТ-инфраструктуры, достигаемую за счет внедрения мер обеспечения безопасности
- Опросы, проводимые IDC в организациях, в которых начали внедрять программу безопасности инфраструктуры печати, показали, что этим организациям удалось достичь

наиболее значительных преимуществ и экономической выгоды в трех областях: повышение безопасности печати, эффективность ИТ-специалистов и снижение затрат. Опрошенные организации сообщили о важных достижениях в области обеспечения безопасности в среде печати, в том числе:

- Сокращение числа нарушений безопасности при печати в среднем в шесть раз в результате внедрения решений безопасности устройств печати
- Сокращение времени, необходимого сотрудникам для поддержки среды печати, в среднем вдвое в результате внедрения решений безопасности устройств печати
- Сокращение расходов на бумагу, и картриджи в среднем на 15%

» То, каким образом внедряются решения безопасности печати, определяет не только их эффективность, но и их влияние на продуктивность работы сотрудников. Для достижения максимальных преимуществ необходимо учитывать основные требования к технологии, сотрудникам и процессам.

В данном информационном документе

В основу данного информационного документа легли основное и дополнительное исследования, проведенные компанией IDC по вопросам безопасности ИТ и среды печати. Компания IDC с июля по сентябрь 2015 г. проводила подробный опрос заинтересованных специалистов, отвечающих за внедрение решений безопасности устройств печати и управление ими в 16 организациях. Опросы были составлены IDC так, чтобы можно было оценить, какое влияние оказывают корпоративные решения безопасности устройств печати на работу организаций, как в количественном, так и в качественном отношении. Опросы отражают применение решений безопасности в различных организациях. В таблице 1 представлен обзор сред печати 16 опрошенных организаций.

ТАБЛИЦА 1

Фирмография по организациям, принявшим участие в опросе — подробный опрос

	Среднее	Срединное	Диапазон
Количество сотрудников	60 300	20 500	200–290 000
Число ИТ-специалистов	4500	610	40–25 000
Число ИТ-пользователей	57 200	19 500	180–290 000
Общее число устройств печати	8800	1200	4–100 000
Число пользователей, использующих печать	50 800	9000	200–280 000
Число страниц, напечатанных за год	51 миллион	10 миллионов	От 10 000 до 300 миллионов
Отрасли	Телекоммуникации, производство, финансовые услуги, издательское дело, авиакосмическая промышленность, биотехнологии, образование и здравоохранение		

n = 16 организаций

Источник: Опрос IDC по безопасности устройств печати, 2015 г.

В дополнение к опросу заинтересованных специалистов компания IDC провела анализ полученных данных. Квалифицированные респонденты из 440 организаций разного размера являются их штатными сотрудниками. Респонденты должны были знать, какое оборудование для печати используется в компании, а также политику ИТ-безопасности компании.

Обзор ситуации

Почему предприятиям необходимо заботиться о безопасности инфраструктуры печати и документооборота

Большинство организаций считают ИТ-безопасность приоритетной задачей, и тому есть веская причина. Широкое распространение вычислительных, мобильных, облачных и других технологий способствует формированию ИТ-среды, в которой работникам умственного труда необходим доступ к деловой информации в «любое время, в любом месте». Однако компания IDC зачастую сталкивается с тем, что в стратегии ИТ-безопасности организаций устройства и технологии печати недооцениваются.

Так почему предприятиям необходимо изменить существующий подход к безопасности печати и защите своих устройств печати, как это делается для компьютеров, серверов, мобильных устройств и т. д.? Дело в том, что незащищенная инфраструктура печати ведет к нарушению защиты всей ИТ-инфраструктуры. Риск нарушений системы безопасности на уровне устройств печати выше, чем можно ожидать, что влечет за собой обязательства, требующие больших затрат.

В ходе исследования IDC обнаружено, что в течение последних 12 месяцев более половины опрошенных компаний сталкивались с проблемой нарушения ИТ-безопасности. Уязвимости могут возникать в результате вредоносных атак как изнутри, так и извне организации, а также неосмотрительного использования устройств печати и напечатанных документов. Потенциальные нарушения системы безопасности, связанные с устройствами печати, могут иметь место на уровне сетевых портов в результате перехвата заданий печати, копирования и сканирования, несанкционированного использования жестких дисков и памяти (ОЗУ) принтеров и МФУ, оставления напечатанных и скопированных документов в выходных лотках, незаконного использования бланков строгого учета (чеков, рецептов) и т. д. Подробнее:

В ходе исследования IDC обнаружено, что в течение последних 12 месяцев более половины опрошенных компаний сталкивались с проблемой нарушения ИТ-безопасности.

- Через незащищенные сетевые порты злоумышленники могут получить доступ к корпоративной сети и информационным ресурсам.
- При печати на сетевом принтере конфиденциальные документы (например, с данными пациентов или данными о финансовых сделках с клиентами) какое-то время остаются без присмотра, что повышает риск кражи и, соответственно, нарушения норм.
- Данные, передаваемые на печать или сканирование без шифровки, могут стать легкой добычей для злоумышленников.

Нарушения безопасности обходятся очень дорого. Можно выделить три основных источника затрат.

- **Ресурсы для устранения нарушения.** Когда в защите возникает брешь, компания вынуждена направлять много сил и средств на ее устранение и ликвидацию последствий. При этом приходится откладывать или закрывать проекты, приносящие прибыль.
- **Штрафы/санкции.** На компанию может быть наложен штраф за несоблюдение требований (например, закона HIPAA). Если клиент подаст в суд на нарушение конфиденциальности данных, возможны также судебные издержки.
- **Репутация.** При широкой негативной огласке компания будет нести финансовые потери даже после устранения инцидента.

Проблемы защиты интеллектуальной собственности, конфиденциальной информации или информации ограниченного пользования, необходимость соблюдения нормативных требований и потребность в безопасной и согласованной ИТ-инфраструктуре в масштабах всего предприятия — все это ключевые факторы, которые обуславливают внедрение программ безопасности печати.

Побудительные мотивы к обеспечению безопасности печати

Мы опросили представителей компаний, заботящихся о безопасности печати, и выяснили, что побуждает их делать это.

- Высокие требования к безопасности и соблюдению норм (в том числе нежелание сталкиваться с негативными последствиями)
- Превентивная стандартизация защиты в ИТ-инфраструктуре
- Желание сэкономить и повысить эффективность ИТ

Безопасность и соблюдение норм

Проблемы защиты интеллектуальной собственности, конфиденциальной информации или информации ограниченного пользования, необходимость соблюдения нормативных требований и потребность в безопасной и согласованной ИТ-инфраструктуре в масштабах всего предприятия — все это ключевые факторы, обуславливающие внедрение программ безопасности печати. Нередко компании начинают внедрять более надежные программы после того, как сталкиваются с брешами в защите.

Технический директор в одной финансовой компании сформулировал это так: «Защита должна быть полной. На принтере постоянно печатают конфиденциальные, секретные и обычные данные. Любое сетевое устройство с доступом к закрытым данным должно соответствовать нормам и быть защищено. Это вынужденная мера».

Стандартизация защиты в ИТ-инфраструктуре

Стандартизация защиты во всей ИТ-инфраструктуре повышает безопасность печати и позволяет внедрить комплексную стратегию по устранению проблем, возникающих при эксплуатации оборудования. Вице-президент по информационным технологиям в издательской компании пояснил: «Нам нужна была защита на основе политик, автоматическое устранение проблем и базовая проверка сертификатов идентификации для принтеров — все это в рамках общего подхода и в сочетании с другими инфраструктурными функциями».

Снижение расходов и повышение эффективности ИТ

Руководство с радостью примет любую ИТ-инициативу, способную снизить эксплуатационные расходы. Экономия — это сопутствующее, однако от этого не менее важное преимущество, которое дает безопасная печать и соответствующий план обеспечения безопасности документов. Это, конечно, не главный аргумент, но вполне весомая причина, которую отметили треть опрошенных.

Старший ИТ-директор компании по оказанию финансовых услуг объяснил: «Необходимость защищать интеллектуальную собственность и нежелание нести убытки — вот главные аргументы в пользу данных решений. Очевидно, что ограничивая доступ, отсекая все посторонние распечатки, мы экономим на бумаге и материалах».

Экономия — это сопутствующее, однако от этого не менее важное преимущество, которое дает безопасная печать и соответствующий план обеспечения безопасности документов.

Конечно, у этой инициативы есть и другие преимущества в плане сокращения затрат. Представители некоторых компаний отметили, что в результате централизации печати и стандартизации защиты повысилась эффективность ИТ, что привело к экономии. Подобная оптимизация позволяет направить ИТ-ресурсы на реализацию других, более приоритетных технологических задач. ИТ-директор в университете сообщил: «Нам нужно было консолидировать контроль затрат и центральное управление в печатной среде».

Значимость безопасности печати для бизнеса

Обстоятельный опрос компанией IDC представителей 16 организаций, в которых используются корпоративные решения безопасности устройств печати, показал, что благодаря развертыванию этих решений они достигли значительных бизнес-преимуществ. В ходе опроса представители компании IDC просили респондентов описать их среду печати до и после развертывания решений. Результаты опроса свидетельствуют о том, что организациям удалось выполнить задачу по созданию более безопасной среды печати и одновременно с этим оптимизировать затраты на печать и рабочее время персонала.

- **Безопасность.** Повысился уровень безопасности инфраструктуры печати, и сократились затраты, связанные с предотвращением утечки данных и обеспечением соблюдения нормативных и аудиторских требований.
- **Эффективность работы ИТ-специалистов.** Сократилось время, затрачиваемое сотрудниками на управление и поддержку сред печати, а также на создание, изменение и применение политик печати, в результате чего у них появилось больше времени для работы над другими задачами.
- **Сокращение затрат.** За счет обеспечения большей прозрачности процесса печати и изменения подхода к нему снизились связанные с ним затраты, в том числе и затраты на печатную технику и расходные материалы.

Снижение рисков: повышенная безопасность печати и соблюдение требований

Организации, участвующие в опросе, сообщили, что корпоративные решения безопасности устройств печати внедрялись ими с целью сократить последствия нарушений безопасности печати и оптимизировать затраты времени и средств на соблюдение нормативных требований.

Компания IDC спросила участников опроса о том, как часто в их организациях происходят случаи нарушения безопасности устройств печати и утечки данных, а также попросила охарактеризовать основные виды подобных нарушений. Респонденты сообщили, что в результате внедрения в их организациях решений безопасности устройств печати число таких нарушений сократилось в среднем в шесть раз. За счет внедрения функций шифрования заданий печати, проверки подлинности и печати с авторизацией им удалось обеспечить надлежащий уровень учета и контроля, чтобы не допускать возникновения подобных нарушений безопасности. Кроме того, пытаясь защитить устройства печати, некоторые организации сумели выполнить задачу по обеспечению безопасности всей ИТ-инфраструктуры, устранив оставшиеся уязвимости. Участвующие в опросе организации привели свои примеры нарушений безопасности, связанные с устройствами печати. Приведем некоторые из них.

Респонденты сообщили, что в результате внедрения в их организациях решений безопасности устройств печати число таких нарушений сократилось в среднем в шесть раз.

- **Печать конфиденциальной информации с целью неправомерного использования.** Директор ИТ-отдела промышленной компании рассказал, что его компанией была утрачена интеллектуальная собственность, в том числе и по причине того, что ее сотрудники печатали строго конфиденциальную и служебную информацию и передавали ее конкурентам.
- **Печать и неправильное обращение с важными данными.** Директор ИТ-отдела компании по оказанию финансовых услуг объяснил, что их сотрудники поставили под угрозу разработки и другую интеллектуальную собственность компании, печатая все без разбора и оставляя задания печати в памяти принтера.

Опрашиваемые организации привели несколько примеров использования ими корпоративных решений безопасности печати для минимизации последствий нарушения безопасности при использовании принтеров.

- **Защита информации в процессе печати.** Вице-президент по информационным технологиям в издательской компании пояснил: «Данное решение стало важнейшим средством эффективной и надежной защиты потока содержимого и данных, поступающих на и исходящих с наших сетевых принтеров. Это позволило нам сократить число возможных нарушений безопасности».
- **Предотвращение излишней или неправомерной печати.** Директор ИТ-отдела компании по оказанию финансовых услуг сказал: «Часто важную документацию, которую мы используем внутри компании, вообще не следует печатать. Эти решения помогают минимизировать внутренние нарушения безопасности при печати, число которых растет вследствие намеренного злоупотребления или неизбирательного отношения».

Как видно из таблицы 2, хотя каждое нарушение безопасности, связанное с использованием устройств печати, само по себе сопряжено с затратами, для организаций особенно важно предотвратить значительные проблемы безопасности, поскольку устранение их последствий обходится слишком дорого. Согласно данным по пяти опрошенным организациям, заявившим, что в последние годы они сталкивались со значительным нарушением безопасности, причиной которого явились устройства печати, средний ущерб из-за такого нарушения выражается следующими цифрами: снижение производительности 54 сотрудников, 277 часов восстановительных работ и материальные затраты в сумме более 500 000 долларов США (за каждое нарушение), включая штрафы.

ТАБЛИЦА 2

Влияние корпоративных решений безопасности устройств печати на нарушения безопасности — подробный опрос

Общие данные по нарушениям безопасности	
Среднее число нарушений в год — до внедрения системы безопасности устройств печати	9,9
Среднее число нарушений в год — при внедрении системы безопасности устройств печати	1,5
Изменение в числе нарушений безопасности	Сокращение до 6 раз
Значительные нарушения безопасности	
Число опрошенных организаций, в которых имели место нарушения безопасности	5
Среднее число задействованных сотрудников	54
Среднее время, которое сотрудники тратят на устранение нарушений безопасности (в часах)	277
Средние совокупные затраты на восстановление каждого нарушения безопасности (включая штрафы)	521 400 долларов США

n = 16 организаций

Источник: Опрос IDC по безопасности устройств печати, 2015 г.

Кроме сокращения числа нарушений безопасности при печати, 10 из 16 опрошенных организаций отметили, что благодаря внедренным решениям безопасности устройств печати им удалось оптимизировать усилия, направленные на соблюдение нормативных требований и аудиторских стандартов. Расскажем о преимуществах, которые обеспечили усиление безопасности и контроля.

- **Усиление безопасности.** Директор ИТ-отдела компании по оказанию финансовых услуг отметил: «Ключевым преимуществом внедрения такой модели защиты является создание чрезвычайно надежной и безопасной среды, которая гарантирует сохранность данных и документов, повышенную конфиденциальность разработки и построения защищенной сети устройств печати. Наличие такой среды существенно помогает нам в соблюдении стандартов безопасности».
- **Контроль и прозрачность.** Вице-президент по ИТ компании, занимающейся медико-биологическими разработками, пояснил: «Мы сумели создать систему журналов аудита, пресечь возможности перехвата данных и показать, что мы строго ограничиваем пользовательский доступ к конфиденциальным данным. Кроме того, в процесс проверки и контроля мы включили такие этапы, как выявление рисков, анализ угроз и разработка действий по устранению проблем. Мы осуществляем глубокий анализ состояния систем и можем вести их мониторинг в режиме реального времени — полностью соблюдаем все политики безопасности».

Благодаря подобным улучшениям системы защиты организациям удается также значительно сократить затраты времени и средств на обеспечение соответствия нормам и аудиторским требованиям. Организации, участвовавшие в опросе, отметили, что за счет внедрения решений безопасности устройств печати в среднем им удается в год сэкономить более 200 часов рабочего времени сотрудников и почти 250 000 долларов США на смежных расходах, включая расходы на услуги поддержки сторонних организаций по проведению аудита и проверок соответствия.

Повышение эффективности ИТ-специалистов

Организации, принявшие участие в опросе, заявили специалистам IDC, что в результате внедрения решений безопасности устройств печати у них в среднем в два раза сократилось время, необходимое для поддержки среды печати.

Организации, принявшие участие в опросе компании IDC, заявили, что с момента развертывания решений безопасности устройств печати они сократили время, необходимое на управление и поддержку сред печати. Столь эффективный результат был подкреплен такими факторами, как внедрение и расширение использования функциональных возможностей централизованного управления и автоматизации, а также сокращение сроков решения проблем, связанных с устройствами печати. Старший ИТ-директор компании по оказанию финансовых услуг объяснил: «Это [использование решений безопасности устройств печати] оказало ощутимое влияние на деятельность сотрудников, как в плане трудозатрат, так и в плане высвобождения дополнительного времени для выполнения более важных стратегических задач. Процесс реагирования на проблемы, связанные с устройствами печати, перестал быть разрозненным, теперь это комплексный и воспроизводимый процесс». Участвовавшие в опросе организации заявили специалистам IDC, что в результате внедрения решений безопасности устройств печати у них в среднем в два раза сократилось время, необходимое для поддержки среды печати.

Опрошенные организации отметили, что решения безопасности устройств печати повысили эффективность работы их сотрудников, ответственных за среду печати. Экономия времени персонала является результатом таких изменений, как автоматизация процессов поддержки и обслуживания, включая автоматизацию сертификатов, а также работы приложений и других воспроизводимых процессов. Например, вице-президент компании по оказанию финансовых услуг, в которой реализуются политики развертывания уникальных сертификатов

и аутентификации сотрудников, рассказал, каким образом его компании удалось на 60% сократить время сотрудников, затрачиваемое на мониторинг устройств: «Мы экономим время наших ИТ-специалистов, поскольку теперь можем легко создавать профили и устанавливать их одновременно на большое количество устройств, также нам удалось автоматизировать процесс управления сертификатами».

Кроме того, опрошенные организации отметили, что благодаря решениям безопасности устройств печати они сократили время, необходимое на разработку, внедрение и изменение политик печати. В среднем на работу с политиками печати персонал этих организаций теперь затрачивает на 59% меньше времени. Помимо экономии времени сотрудников, эффективное внедрение политики печати является залогом обеспечения таких преимуществ, как сокращение вероятности нарушений безопасности и разработка более действенных инструкций по работе с устройствами печати.

Как отмечают участники опроса, при возникновении проблем, связанных с использованием устройств печати, сотрудники эффективно используют для их устранения функциональные возможности внедренных решений безопасности, например, центральные консоли управления или удаленный доступ к принтерам. Все эти функции в сочетании с оптимизированной политикой безопасности печати помогли организациям снизить время реагирования на инциденты, связанные с устройствами печати, и время реагирования на обращения пользователей по данным инцидентам в среднем на 59% и 42% соответственно (см. рис 1). Вице-президент по ИТ издательской компании, в которой реализуются решения безопасности, включающие функции автоматического восстановления и управления уникальными сертификатами, пояснил, насколько эти решения повлияли на возможности его команды поддерживать работу принтеров: «В настоящее время проблемы возникают крайне редко, а на устранение существующих требуется значительно меньше времени. Это имеет положительное воздействие — появилось больше времени для поддержки и планирования других задач». ИТ-директор компании по финансовым услугам, в которой используется решение по управлению безопасностью устройств печати, заметил: «Наша служба поддержки теперь имеет четкое представление о настройках принтеров, разрешениях и проблемах и может действовать самостоятельно или обратиться за поддержкой уровня 2 к небольшой корпоративной группе, занимающейся проблемами печати».

РИС. 1

Средний показатель экономии времени сотрудников, ответственных за среду печати, — подробный опрос заинтересованных специалистов

n = 16 организаций

Источник: Опрос IDC по безопасности устройств печати, 2015 г.

Снижение затрат, связанных с печатью

Возможности снизить затраты в ходе реализации той или иной ИТ-инициативы только повышают ее привлекательность. В итоге для организаций, участвовавших в опросе, возможность сократить затраты за счет развертывания решений безопасности устройств печати стала существенным дополнительным преимуществом. Опрос показал, что в этих организациях, помимо прочего, широко используются такие практические решения, как аутентификация пользователей и печать с авторизацией (более двух третей из организаций). Эти решения обеспечивают защиту конфиденциальности документов и способствуют снижению затрат, требуя от пользователей выполнения ряда действий для получения разрешения на печать и сокращая число несанкционированных или нецелевых заданий печати. Возможность использования решений безопасности устройств печати в качестве механизма снижения затрат в сфере печати настолько очевидна, что некоторые из опрошенных организаций заявили, что оптимизация затрат являлась для них главным аргументом в пользу развертывания таких решений.

Организации объяснили, что за счет перечисленных ниже возможностей решения безопасности устройств печати помогли сократить затраты:

- **Сокращение объемов печати за счет изменения подхода к процессу печати.** Финансовый директор одной из компаний пищевой отрасли сообщил: «Используемая нами функция печати с авторизацией позволяет отправлять материалы на печать, но чтобы они были напечатаны, нужно дойти до нужного принтера и приложить к нему свой бейджик. Думаю, что это позволило сократить объемы печати в среднем на 21–24 процента».
- **Постоянная доступность информации об использовании устройств печати.** ИТ-директор одного университета сообщил: «Теперь мы можем отслеживать затраты на печать страниц и взыскивать возмещение с факультетов». Возможность приписывать затраты на печать факультетам позволяет университету перекладывать обязанность поиска эффективных способов рационального использования принтера на администрацию этих факультетов.
- **Списание ненужных или устаревших принтеров.** Вице-президент организации по финансовым услугам отметил: «Мы сокращаем число ненужных заданий печати, поскольку сотрудники знают, что использование устройств печати контролируется. Мы также списываем и заменяем устаревшее оборудование печати, не способное обеспечить выполнение основных требований в отношении безопасности предприятия».

Благодаря инициативам в сфере безопасности устройств печати сотрудники компаний получили доступ к данным об использовании принтеров и смогли вносить свой вклад в сокращение затрат на печать и обслуживание печатного оборудования. Участники подробного опроса заинтересованных специалистов отметили, что их сотрудники в среднем отправляют на 43% меньше заданий печати не на тот принтер. В результате меньше заданий печати отменяются или печатаются повторно. Как показано на рис. 2, все эти улучшения повысили общий уровень эффективности использования устройств печати, обеспечив сокращение общего объема печати (в среднем на 6%), увеличение объемов двусторонней печати (на 19%) и сокращение объемов цветной печати (на 2%). Эти факторы, а также большая наглядность работы сред печатного оборудования, обеспечили организациям, участвовавшим в опросе, значительную экономию затрат на поддержку своих сред печати, включая затраты на развертывание и обслуживание принтеров (уменьшение на 1% или в среднем 115 принтеров в каждой организации), а также экономию затрат на бумагу и картриджи (уменьшение на 15%, 14% и 16%, соответственно).

Благодаря инициативам в сфере безопасности устройств печати сотрудники компаний получили доступ к данным об использовании принтеров и смогли вносить свой вклад в сокращение затрат на печать и обслуживание печатного оборудования.

РИС. 2

Средние показатели экономии затрат и повышения эффективности устройств печати в среде печатного оборудования — подробный опрос

(% эффективности или улучшения)

n = 16 организаций

Источник: Опрос IDC по безопасности устройств печати, 2015 г.

Проблемы

Практически в любой организации заблаговременное планирование помогает исключить целый ряд проблем. При развертывании системы безопасности печати в группе организаций, участвовавших в исследовании, проблемы возникали на всех трех этапах: планирования, внедрения и поддержки после внедрения.

Компании-участники говорили о том, что им катастрофически не хватало времени для разработки стратегии и плана. Чтобы снизить нагрузку на ИТ-специалистов на этапах после внедрения, требуется длительная предварительная работа. Кроме того, необходимо автоматизировать процесс соблюдения требований сотрудниками. Чтобы уменьшить число обращений в службу поддержки по вопросам и проблемам печати, такой процесс должен включать инструменты мониторинга, процесс эскалации и процедуры устранения недостатков.

При планировании пользователи устройств печати в любой организации должны учитывать следующие аспекты:

- **Баланс между строгими требованиями к безопасности печати и устойчивым снижением производительности сотрудников.** Безопасности предприятия следует уделять особое внимание, однако организациям необходимо разработать систему, которая бы свела к минимуму негативное влияние на производительность. Например, некоторые организации, внедряющие печать с авторизацией для решения своих потребностей в безопасности печати, могут встретить сопротивление со стороны пользователей, поскольку сначала им потребуется проходить через этап аутентификации (например, вводить пароль), а затем ждать, когда будет распечатан весь документ. В таком сценарии стоит выбор между защитой информации, включенной непосредственно в документ (например, никто не может просмотреть документы, оставленные в лотке для бумаги), и необходимостью ожидания распечатки документа (например, печать инициируется только после аутентификации пользователя в системе устройства).

» **Обучение сотрудников.** Для сохранения и повышения производительности сотрудников план обеспечения безопасности печати должен включать процессы и время, необходимые для обучения сотрудников новым политикам и процедурам. Предприятия должны быть готовы к периодическому проведению обучения в самых разнообразных форматах, соответствующих возрасту и учебным предпочтениям сотрудников.

Основные указания

IDC был определен ряд причин, по которым связанные рабочие процессы печати и документооборота должны стать неотъемлемой частью системы безопасности ИТ корпоративного масштаба. Разумеется, одно из основных преимуществ тесно связано с предоставлением комплексной программы по обеспечению безопасности ИТ. Такая программа включает и аспекты печати, однако предлагает еще множество существенных преимуществ и помимо безопасности. Два из них — заметная экономия затрат и повышение эффективности ИТ-инфраструктуры.

IDC рекомендует использовать технологию защиты печати/документов, применяемую в организации. Организации должны понимать, что эффективное решение этой задачи возможно только в случае полной согласованности людей и процессов в ходе выполнения намеченного плана.

Технологии

Что касается безопасности, то внедрение соответствующих технологических решений — это вопрос, требующий однозначного ответа. В организации безопасность либо есть, либо ее нет.

IDC рекомендует всем организациям как можно скорее внедрить следующие функциональные компоненты. ИТ-специалисты и поставщики решений для инфраструктуры печати отвечают также за настройку и активацию этих компонентов и возможностей в масштабе всех устройств печати, используемых в организации.

IDC рекомендует использовать технологию защиты печати/документов, применяемую в организации.

» Обеспечьте все устройства печати, подключенные к сети, следующими функциональными возможностями, или хотя бы следите, чтобы их микропрограммное обеспечение было всегда обновлено.

» Убедитесь, что устройства используют только протоколы зашифрованной связи, и отключите остальные.

» Внедрите систему, которая будет удалять или разрушать данные на жестких дисках устройств в рамках процедуры вывода устройств из эксплуатации.

» Используйте хотя бы одну форму аутентификации пользователей (предпочтительно — две или три). Мы также рекомендуем внедрить функцию печати с авторизацией в средах, в которых печатаются большие объемы конфиденциальной информации или установлены высокие требования к соблюдению нормативов.

» Используйте последнюю актуальную версию официального микропрограммного обеспечения.

» Обеспечьте безопасность всех жестких дисков устройств печати (периодически шифруйте и удаляйте данные).

- Начните применять средства защиты от несанкционированного вскрытия или используйте устройства печати с запирающимися лотками, если имеете дело со специальными материалами. Это обеспечит безопасность материалов, подверженных потенциальному риску мошенничества, — чеков, медицинских рецептови т. п.

- Чтобы обеспечить соблюдение политик безопасности, используйте инструмент управления парком оборудования для централизованного управления, мониторинга и восстановления устройств. Это позволит любой организации исключить этап конфигурирования и обслуживания вручную каждого устройства отдельно. Этот инструмент должен упростить такие операции, как создание и администрирование политик безопасности, выявление факта подключения устройств к сети, управление уникальными сертификатами устройств, регистрация инцидентов несоблюдения политик безопасности и решение этих инцидентов в рамках процесса эскалации и устранения недостатков. Его работа должна быть согласована с инструментами управления безопасностью ИТ, которые действуют в масштабах всей организации и осуществляют мониторинг конечных устройств на предмет инцидентов и аномалий, связанных с несоблюдением нормативов. Благодаря этому будет обеспечено быстрое выявление любых потенциальных нарушений безопасности.

- Чтобы обеспечить полную защиту данных, имеющих отношение к печати, убедитесь, что материалы, напечатанные и отсканированные на настольных и мобильных устройствах (которые передаются или хранятся), шифруются. Это означает, что необходимо открывать и обрабатывать даже вложения, которые планируется напечатать. Инструмент, выполняющий мониторинг печати и сканирующий содержимое, является ключевым элементом, гарантирующим высочайший уровень безопасности и соблюдение политик компании и стандартов отрасли.

Люди

Организация, которая серьезно относится к своим потребностям в области безопасности ИТ, наверняка позаботится о том, чтобы ее специалисты по безопасности обладали навыками эффективной защиты устройств печати и связанных процессов документооборота. Специалисты по безопасности могут входить в штат организации и/или привлекаться со стороны. Эти специалисты должны быть в состоянии проконсультировать по поводу будущих проблем безопасности печати и сопутствующего рабочего процесса, а также оказать помощь в интеграции плана обеспечения безопасности ИТ в масштабах всего предприятия.

Чтобы работа по обеспечению безопасности устройств печати и связанных процессов документооборота не привела к снижению производительности сотрудников, в процессе планирования необходимо получить соответствующие данные и поддержку от ряда сотрудников организации. Также рекомендуется привлечение эксперта по управлению изменениями, особенно если требуется большое число изменений. Такой эксперт может также порекомендовать эффективный способ развертывания и обучения.

Большинство организаций не обладают знаниями и навыками, необходимыми для обеспечения должной безопасности инфраструктуры печати и документооборота. Поэтому любой организации следует поинтересоваться у своего поставщика устройств печати, сможет ли он в дальнейшем предоставлять ресурсы своего ИТ-отдела. К этим ресурсам относятся функции безопасности, которыми оснащены принтеры и МФУ организации, программные инструменты для обеспечения безопасности и услуги безопасности (например, профессиональные услуги по

безопасности, услуги оценки уровня безопасности, услуги управления изменениями и поддержка в соблюдении нормативов для конкретных отраслей).

Процесс

Важно, чтобы инициатива в сфере безопасности в любой организации начиналась с оценки текущего состояния среды печати и разработки плана, в котором намеченный уровень безопасности соответствовал бы состоянию и потребностям всей остальной ИТ-среды. Такая инициатива должна включать анализ основных требований по безопасности, характерных для отрасли, в которой работает организация, а также план по мониторингу, эскалации, восстановлению и соблюдению этих политик на постоянной основе.

Этот план следует периодически переоценивать, используя данные, собранные в течение определенного периода времени. Это позволит определить, требуется ли внести какие-либо корректировки, а также узнать, имеют ли место нарушения безопасности печати/документов за пределами компании. Любые корректировки будут определяться собранными данными, а также уровнем риска и затрат на безопасность, приемлемых для организации.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Сведения об IDC

Компания IDC (International Data Corporation) — ведущий поставщик информации и консультационных услуг, организатор мероприятий на рынках информационных технологий, телекоммуникаций и потребительской техники. Компания IDC помогает ИТ-профессионалам, руководителям и инвесторам принимать обоснованные решения о закупке техники и выборе бизнес-стратегии. Более 1100 аналитиков IDC в 110 странах по всему миру изучают технологии, тенденции и возможности отрасли на мировом, региональном и местном уровнях. Вот уже 50 лет IDC предлагает своим клиентам стратегический анализ, который помогает решить их важнейшие бизнес-задачи. IDC — дочернее предприятие IDG, компании, лидирующей на мировом рынке ИТ-изданий, исследований и специализированных мероприятий.

IDC Analyze the Future