Как обеспечить безопасность печати

Серия «Brother: переход на цифровые технологии»

Передовой опыт

Отчет основан на результатах исследования

www.brother.ru

Почему компании не инвестируют в безопасность печати

Угрозы хакерских атак и серьезных утечек конфиденциальной информации становятся все серьезнее. Большинство малых и средних предприятий понимают, что их ИТ-инфраструктура нуждается в защите.

Чтобы обеспечить ИТ-безопасность предприятия, требуется комплексный подход, предусматривающий в том числе защиту принтеров, сканеров и копировальных аппаратов. Иначе именно эти устройства могут стать слабым местом, которое откроет хакерам доступ к вашей конфиденциальной информации. Все больше малых и средних предприятий осознают значение этой угрозы, а **72 %** из них считают безопасность принтеров, сканеров и копировальных аппаратов критически важной. В сферах, где конфиденциальность данных особенно важна (здравоохранение и профессиональные услуги), таких предприятий еще больше: **81 %** и **82 %** соответственно.

Это означает, что около трети организаций все еще не придают должного значения безопасности печати. И в то же время почти половина респондентов считают, что их компании недостаточно в нее инвестируют.

Если предприниматели знают, как важно инвестировать в безопасность принтеров, то почему же они этого не делают?

Наше исследование показало, что есть две главные причины:

Отсутствие ответственных лиц

Отсутствие знаний об угрозах и стандартах безопасности

Наш отчет призван помочь руководителям малых и средних предприятий понять, почему безопасность печати важна и как ее обеспечить. Он входит в серию, посвященную эффективному использованию цифровых технологий на малых и средних предприятиях. Отчеты из этой серии основываются на результатах обширной программы исследований, которые проводились среди руководителей малого и среднего бизнеса в Европе, Африке и на Ближнем Востоке. В серию входят четыре отчета, которые посвящены следующим темам:

— Цифровые рабочие процессы
— Выбор и внедрение оптимального решения
— Безопасность
— Устойчивое развитие

Кто отвечает за безопасность печати?

Очень часто предприниматели не понимают, в чем заключаются конкретные обязанности по обеспечению безопасности печати. Почти в половине малых и средних предприятий Западной Европы **(44 %)** нет сотрудников, официально отвечающих за этот аспект. А когда ответственных нет, решения обычно принимаются и реализуются без оглядки на качество, что, в свою очередь, ставит бизнес под удар.

Традиционно считается, что в вопросах безопасности принтеры представляют намного меньший риск, чем, например, ноутбуки. Соответственно, в компаниях часто нет сотрудников, ответственных именно за безопасность печати. Наше исследование показывает, что в бизнесе начинают считать этот вопрос важным, но до кадрового состава малых и средних предприятий изменения еще не дошли.

Проблема отсутствия ответственных лиц особенно характерна для малых и средних компаний, поскольку в них аппаратным и программным обеспечением обычно занимается небольшая группа ИТ-специалистов. Если эти сотрудники не понимают, какие риски связаны с недостаточной безопасностью печати, то могут не придавать ей значения.

Но за безопасность конфиденциальных данных в той или иной мере отвечают все сотрудники компании.

Технические и ИТ-специалисты отвечают за защиту устройств, но остальные сотрудники, в свою очередь, обязаны следить за безопасностью конфиденциальной информации. В этой области риски особенно высоки.

В сфере информационной безопасности очень много угроз, например:

- Несанкционированный доступ к распечатанным документам
- Пользователи, забывающие выйти из учетной записи после печати конфиденциальных документов
- Невозможность отследить, кто получил доступ к тем или иным распечатанным документам

Почти в девяти из десяти компаний случались инциденты безопасности, связанные с печатью.

А семь компаний из десяти **(72 %)** считают защиту данных более серьезной проблемой, чем безопасность устройств. Но при этом менее трети компаний уверены в том, что их инфраструктура печати надежно защищена, и лишь **53 %** уверены в защите оборудования.

В большинстве малых и средних компаний **(64 %)** считают информационную безопасность одним из главных приоритетов и в то же время одной из самых серьезных проблем, способной заметно снижать эффективность работы.

Почти половина респондентов **(48 %)** отмечают, что в их компаниях невозможно или почти невозможно отследить, кто распечатывает и забирает документы. Неудивительно, что почти в девяти из десяти компаний **(86 %)** случались нарушения безопасности, связанные с печатью.

Сотрудники оставляли конфиденциальные документы в лотке без присмотра, не забирали их — или забирали чужие распечатки, на доступ к которым не имели полномочий.

По этой причине большинство малых и средних предприятий **(64 %)** начинают принимать меры для обеспечения безопасности печати: ограничивать доступ к определенным принтерам, вводить печать по PIN-кодам или с помощью идентификационных карт и т. д.

Это шаг в верном направлении. В ближайшие годы такие меры приобретут еще большее значение для всех компаний. Но на этом работа не заканчивается: далее необходимо улучшать контроль над печатью и вводить учет всех операций с принтерами и МФУ.

Чтобы обеспечить информационную безопасность предприятия, нужно достичь трех основных целей, касающихся защиты данных и устройств:

Конфиденциальность

Доступ к конфиденциальным бизнес-данным должны получать только уполномоченные лица. Для этого нужна система аутентификации и авторизации, чтобы перед использованием принтера пользователи подтверждали свою личность и право на печать соответствующего документа.

Целостность

Следует защитить микропрограммы устройств от взлома и прочих внешних угроз.

Доступность

Необходимо обеспечить исправность работы устройств и их доступность для авторизованных пользователей, чтобы они всегда могли распечатать необходимые документы.

Нехватка знаний не дает обеспечивать необходимую защиту

Менее трети **(32 %)** ИТ-руководителей малых и средних предприятий говорят, что хорошо разбираются в безопасности информационных технологий и возможных угрозах. А если сотрудники, ответственные за принятие решений, не знают, что может угрожать их предприятию, то они сталкиваются с большими трудностями, пытаясь обеспечить защиту. В компаниях малого и среднего размера ИТ-руководители обычно отвечают за много разных видов оборудования, и понятно, что они могут не иметь глубоких знаний о принтерах.

Часто проблема заключается в техническом жаргоне. Более половины респондентов **(51 %)** говорят, что не понимают профессиональных выражений, касающихся безопасности печати. Особенно остро эта проблема стоит в Италии и Франции.

И менее 60 % респондентов считают, что хорошо разбираются в стандартах безопасности печати.

Соответственно, руководители не знают, какие поставщики технологий печати могут предложить решение, наилучшим образом отвечающее потребностям компании в безопасности. В результате они часто выбирают принтеры от «знакомых» брендов, не понимая, есть ли в этих устройствах необходимые защитные функции.

Надежный поставщик должен не только продать принтеры, но и помочь клиенту разобраться во всех соответствующих стандартах безопасности и выбрать наиболее подходящее оборудование.

Советы от Brother

Brother предлагает семь ключевых рекомендаций, которые помогут малому и среднему бизнесу предотвратить утечки данных при печати и защититься от связанных с ними финансовых, юридических и репутационных проблем.

Привлеките высшее руководство

Кибератаки, утечки данных и нарушения Общего регламента по защите данных (GDPR) могут иметь серьезные последствия для бизнеса. По этой причине вопросами безопасности печати должен заниматься не только ИТ-отдел, но и высшее руководство компании, в частности директор по ИТ и руководитель по информационной безопасности.

Проведите тщательный аудит

Регулярный аудит системы и средств безопасности крайне важен для предприятий, так как позволяет своевременно выявлять потенциальные уязвимости инфраструктуры печати. Такой аудит особенно важен, если в компании есть не только современные, но и устаревшие устройства. Если же предприятие использует услуги по управлению печатью (MPS), то поставщик услуг обычно проводит не только тщательную оценку инфраструктуры печати в начале сотрудничества, но и осуществляет постоянный мониторинг парка устройств после его оптимизации и обеспечения защиты.

Смените пароли администраторов, заданные по умолчанию

Одна из уязвимостей, связанных с корпоративными принтерами, — это предустановленные пароли для доступа с правами администратора, которые может узнать кто угодно. К счастью, это легко исправить: просто сразу устанавливайте на каждом новом устройстве надежный пароль.

Обновите микропрограммы

Многие потенциальные уязвимости можно исключить, если обновить микропрограмму на устройстве и настроить автоматическую установку обновлений. Если у вас возникнут вопросы, обратитесь за помощью к производителю оборудования.

Защитите задания печати

В защите нуждаются не только принтеры, но и распечатываемые документы. Используйте сквозное шифрование сетевого трафика, чтобы задания печати безопасно передавались на принтер. Обычно документы некоторое время хранятся на печатных устройствах, поэтому данные должны быть зашифрованы.

Следите за устройствами

Зная текущее состояние принтеров, вы сможете получить представление об инфраструктуре печати в целом. Существуют специальные программные средства для мониторинга оборудования, позволяющие сразу решать возникающие проблемы. Устройства генерируют большой объем данных, которые можно использовать для отслеживания потенциальных угроз и быстрого реагирования на атаки. Компании, использующие услуги по управлению печатью (MPS), могут также регулярно получать отчеты по соответствию требованиям безопасности и мониторингу утечек данных.

Обучайте сотрудников

Часто утечки данных происходят по недосмотру сотрудников и незнанию возможных угроз. Поэтому крайне важно обучать персонал правильному обращению с конфиденциальной информацией. Поставщики MPS часто предоставляют и услуги обучения.

Заключение

Раньше безопасности печати уделялось очень мало внимания. Сейчас она становится приоритетом для малого и среднего бизнеса, но на практике с ней все еще возникают серьезные проблемы.

Важно четко определить конкретные обязанности по обеспечению безопасности печати и назначить ответственных за их выполнение. Для эффективной борьбы с угрозами необходимо защитить не только устройства, но и информацию. Чтобы свести риски к минимуму, требуется участие не только ИТ-отдела, но и всех остальных сотрудников.

Также серьезными проблемами являются недостаток знаний в сфере безопасности печати и профессиональный жаргон, из-за которого неспециалистам трудно разобраться в этой теме. Поэтому важно обращаться к надежным поставщикам, которые посоветуют оптимальное решение.

Безопасность — это лишь одно из требований к эффективной печатной инфраструктуре: нужно еще внедрить цифровые решения для организации рабочих процессов, выбрать эффективное оборудование для печати и не забывать об устойчивом развитии. Этим аспектам посвящены другие отчеты в серии «Переход на цифровые технологии».

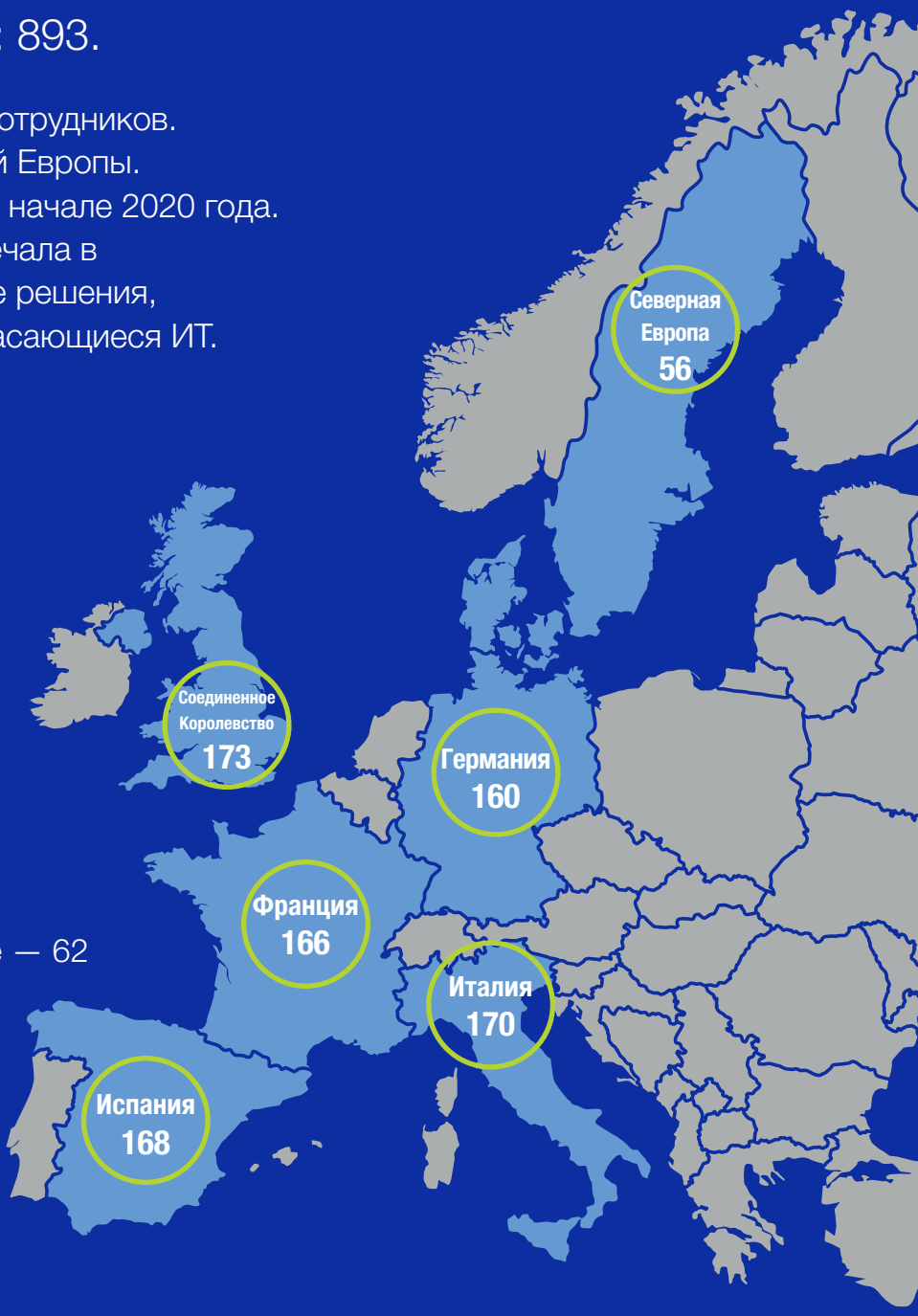
Наша методология

Отчет составлен по результатам онлайн-опроса, проведенного среди руководителей предприятий малого и среднего бизнеса, а также глав ИТ-отделов. Количество респондентов: 893.

Штат предприятий: от 10 до 499 сотрудников.
Регион: несколько стран Западной Европы.
Опрос проводился в 2019 году и в начале 2020 года.
Половина респондентов (448) отвечала в своей компании за стратегические решения, а половина (445) — за решения, касающиеся ИТ.

Основные отрасли

- Здравоохранение — 152
- Торговля — 117
- Логистика — 113
- Гостинично-ресторанный бизнес — 81
- Транспортировка и хранение — 62
- Профессиональные услуги — 65
- Промышленность — 54
- Финансовые услуги — 53
- Образование — 51
- Строительство — 39



Кроме того, опрашивались руководители из других отраслей: энергетической, фармацевтической, сельскохозяйственной, оборонной, а также представители индустрии спорта, развлечений и рынка недвижимости.

Исследование проводила компания Savanta, которая занимается анализом рынков.

Результаты последних исследований

Другие отчеты из серии «Brother: переход на цифровые технологии».

Скоро

brother
at your side

www.brother.ru

ООО «Бразер»
125047, Москва, ул. 1-я Тверская-Ямская, д. 21
БЦ «Четыре ветра», 8-й этаж
Горячая линия: 8-800-700-08-09 (круглосуточно)