Почему каждое предприятие нуждается в грамотной стратегии в сфере услуг печати

Каждому предприятию требуется грамотная стратегия в сфере услуг печати, которая позволит повысить безопасность и производительность. Консультанты HP в области безопасности печати — Джейсон О›Киф и Майкл Ховард — объясняют, почему.

Узнать больше

«Большинство компаний не считают, что нуждаются в защите своих инфраструктур печати, поэтому сфера печати в их стратегии безопасности стоит на одном из последних мест»

Джейсон О›Киф, Консультант HP в области безопасности печати

Подключенные к сети принтеры обладают меньшей степенью защищенности, чем думают в большинстве организаций. В условиях роста угроз безопасности, несущих за собой просто катастрофические последствия, предприятия всех размеров нуждаются в стратегиях услуг печати, которые смогут обеспечить надежную защиту и свести к минимуму риски. Для многих предприятий основой построения надежной и грамотной стратегии является сотрудничество с поставщиком услуг по аутсорсингу и управлению инфраструктурой печати (MPS), который может выявлять и блокировать угрозы безопасности и решать сопутствующие проблемы (то есть, обслуживать оборудование), делая все, чтобы процессы печати никоим образом не снижали общий уровень производительности.

Решение проблемы незащищенности принтеров

Согласно опросу Ponemon Institute, в котором приняли участие более 2000 специалистов-практиков в области безопасности ИТ, 60 процентов респондентов признали, что сталкивались с утечками данных, наверняка связанными с подключенным к сети принтером, и большинство респондентов прогнозируют, что в следующие 12 месяцев также будут иметь место утечки данных, связанные с принтерами, подключенными к сети.

Однако только 34 процента респондентов отметили, что в их организации практикуется ограничение доступа к принтерам повышенного риска, включая доступ к напечатанным на них бумажным документам. Эти явные бреши в системе безопасности делают малые и средние предприятия практически незащищенными перед атаками, которые в лучшем случае приведут к финансовым потерям, а в худшем — к разрушению бизнеса.

Джейсон О›Киф, консультант HP в области безопасности печати, отметил, что большинство организаций недооценивают свою уязвимость через инфраструктуру печати. «Большинство компаний не считают, что нуждаются в защите своих инфраструктур печати, поэтому сфера печати в их стратегии безопасности стоит на одном из последних мест, — заявил он. — Мы представляем структуру, включающую до 200 компонентов, которые мы контролируем и оцениваем на предмет уязвимостей в масштабах инфраструктуры печати. Беда приходит неожиданно, и все меняется. Начальный скептицизм уступает место неверию и шоку, и уже после этого наступает время честной и активной дискуссии».

Грамотная стратегия в сфере услуг печати должна начинаться с оценки уязвимостей. Согласно мнению Майкла Ховарда, главного консультанта HP по безопасности, большинство уязвимостей, источник которых — инфраструктура печати, сводится к четырем факторам: устаревающие технологии, ненадлежащее внедрение средств управления безопасностью, неоднородный парк устройств, и недостаточный контроль за событиями в среде печати.

Знаете ли вы, что в организациях одним принтером пользуются в среднем шесть человек? В то время как компьютеры и ноутбуки защищены паролями, у принтеров такой функции нет, поэтому уязвимы будут данные всех шести пользователей. «Многие специалисты по безопасности даже не знают, сколько устройств печати установлено в организации. А ведь их число может достигать 5000. И все эти устройства открыты для атак, — говорит Ховард. — Когда думаешь, насколько широко используется печать в большинстве организаций, отсутствие средств безопасности в них пугает и шокирует».

Почему каждое предприятие нуждается в грамотной стратегии в сфере услуг печати

«Безопасность печати, как и корпоративная безопасность»

Майкл Ховард, Консультант HP в области безопасности печати

Важная роль стратегий в сфере услуг печати

Грамотная и эффективная стратегия в сфере печати блокирует доступ к принтерам (как и в случае с компьютерами), ограничивает привилегии администраторов, добавляет защиту паролем и именем пользователя и обеспечивает полноценный мониторинг. Это важнейшее условие видимости, возможности отслеживания и подотчетности.

«Видимость имеет огромное значение, — говорит О›Киф. — Я бы еще отметил совместную работу, которая также повышает безопасность печати. Для получения всей необходимой аналитической информации, повышающей надежность безопасности, компании должны объединить и согласовать работу администраторов печати, специалистов по безопасности и внутренних аудиторов. Эти группы должны стремиться к сотрудничеству, совместно повышая эффективность этого компонента работы сети, который долгие годы не принимался в расчет».

Еще ряд дополнительных мер позволит организациям устранить уязвимости в инфраструктуре печати:

- Постоянное обновление микропрограммного обеспечения
- Сокращение администрирования в рамках инфраструктуры печати
- Обновление версий баз данных печати с Express до Enterprise
- Внедрение процессов и документации, обеспечивающих согласованность и измеримость процедур обеспечения безопасности
- Обучение администраторов печати в сфере безопасности

«Безопасность печати, как и корпоративная безопасность, — процесс непрерывный, — говорит Ховард. — Поэтому так важно непрерывно совершенствовать процедуры оценки и консультирования». Более глубокая и постоянная оценка неразрывно связана с управлением. В сфере печати процесс управления должен включать управление учетными данными пользователей, осуществляющих доступ к инфраструктуре печати, соблюдение корпоративных политик, управление рисками, ведение документации по безопасности и ведение журнала событий.

Управляемые или не управляемые — вот в чем вопрос

Грамотная и надежная стратегия невозможна без целого ряда компонентов. Для большинства предприятий, главным образом малых и средних, разработка и реализация такой стратегии собственными силами в планы не входят. Они скорее потратят время и энергию на ведение самого бизнеса. В этом случае верным решением станет сотрудничество с поставщиками услуг по аутсорсингу и управлению инфраструктурой печати (MPS), которые смогут позаботиться о повседневных мелочах и обеспечить такой уровень безопасности, который необходим предприятиям для бесперебойной и эффективной работы.

Первым шагом к созданию эффективной стратегии безопасности является определение круга вопросов, на которые необходимо дать ответы. Какие принтеры необходимы нашей организации, чтобы приступить к реализации такой стратегии? Будут ли это струйные или лазерные принтеры? Какие функции печати нам необходимы? Для ответа на эти вопросы требуется определить оптимальное соотношение надежности, затрат и производительности. Затем следует проанализировать аспекты безопасности, технического обслуживания и поддержки. Будут ли использоваться собственные принтеры, или лучше прибегнуть к услугам поставщика? Этот вопрос влечет за собой множество других: Достаточно ли оснащены наши ИТ-специалисты, чтобы решать проблемы принтеров? Не окажется ли в долгосрочной перспективе, что собственные услуги печати обойдутся дороже? Для малых предприятий наиболее часто ответ утвердительный.

Предприятия, делающие выбор в пользу услуг по аутсорсингу и управлению инфраструктурой печати (MPS), должны знать, в каких случаях необходим контракт, и с каким поставщиком лучше сотрудничать. В связи с этим необходимо ответить на следующие вопросы: Какие услуги нам необходимы? Что должно включать соглашение об уровне обслуживания? Во сколько это обойдется? Как быстро будет расти наша сеть принтеров? Какие изменения должны вноситься в стратегию по мере роста организации?

Опасности, возможные в результате незащищенности подключенных к сети принтеров, очевидны, и предприятия всех размеров должны делать все, чтобы услуги печати стали неотъемлемой частью их стратегии безопасности и производительности. К счастью, имеется множество поставщиков решений, готовых сделать за вас всю грязную работу.

Узнать больше
hp.com

4AA7-1720RUE, Ноябрь 2017г.