Чому кожній компанії потрібно розробити розумну стратегію керування послугами друку

Усім компаніям потрібні стратегії безпечного та продуктивного керування послугами друку. Консультанти з безпеки друку HP Джейсон О'Кіф та Майкл Говард пояснюють чому.

Learn more

«Більшість компаній вважає, що їм не потрібен захист інфраструктури друку, тому він має низький пріоритет,

Jason O'Keefe

Підключені до мережі принтери захищені не так добре, як уявляє переважна частина компаній. Кількість загроз збільшується — а їх характер стає надзвичайно серйозним, — тому компаніям усіх розмірів необхідні стратегії керування послугами друку, які дозволяють забезпечити захист і звести до мінімуму ризики. Для багатьох підприємств надійна стратегія ґрунтується на співпраці з постачальником послуг зовнішнього керування друком, який може виявляти й нейтралізувати вразливості, а також усувати поточні проблеми (тобто виконувати технічне обслуговування обладнання), в результаті чого друк ніколи не стає на заваді продуктивності.

Вирішення проблем із захистом принтерів

За результатами опитування, проведеного Ponemon Institute, в якому взяло участь понад 2000 фахівців з IT-безпеки зі всього світу, 60 відсотків респондентів визнає, що в їхній компанії використання підключеного до мережі принтера ймовірно призвело до витоку даних. Більшість респондентів також прогнозує можливість витоку даних в результаті недостатнього захисту підключених до мережі принтерів протягом наступних 12 місяців.

Але лише 34 відсотки респондентів заявляє, що в їхніх компаніях використовуються процедури обмеження доступу до принтерів з високим рівнем ризику, зокрема до роздрукованих документів. Ці очевидні недоліки в захисті роблять малі й середні компанії особливо вразливими до атак, що можуть не лише призвести до фінансових втрат, але й похитнути саму структуру організації.

Джейсон О'Кіф, консультант з безпеки друку HP, каже, що більшість компаній недооцінює, наскільки великою вразливістю є їхня інфраструктура друку. «Більшість компаній вважає, що їм не потрібен захист інфраструктури друку, тому він має низький пріоритет, — зазначає він. — Ми розповідаємо про свою платформу, що має до 200 засобів контролю, за допомогою яких можна оцінити вразливості в інфраструктурі друку. Тут у співрозмовника кардинально змінюється точка зору. Початковий скептицизм перетворюється на недовір'я та шок, що відкривають шлях для дуже відвертого й жвавого обговорення».

Надійна стратегія керування послугами друку починається з оцінювання вразливостей. За словами Майкла Говарда, головного консультанта з безпеки HP, більшість вразливостей безпеки друку зводиться до чотирьох факторів: старіння технологій, неправильного впровадження засобів контролю захисту, різнорідності середовищ у постачальників та відсутності елементів керування умовами друку.

Чи знали ви, що в пересічній компанії кожен принтер використовує приблизно шість

Чому кожній компанії потрібно розробити розумну стратегію керування послугами друку

співробітників? Комп'ютери та ноутбуки можна блокувати між періодами використання, але з принтерами так ніхто не робить, через що вразливими стають усі шестеро користувачів. «Співробітники служби безпеки часто не знають, скільки принтерів використовується в компанії. А їх може бути до 5000, і всі відкриті, — каже Говард. — Якщо замислитись над тим, наскільки активно використовуються принтери в більшості компаній, відсутність профілактичного захисту просто лякає».

Чому стратегії керування послугами друку є важливими

У розумній стратегії друку принтери блокуються (як комп'ютери), обмежуються права адміністраторів, впроваджуються вказівки з використання імені користувача та пароля, а також здійснюється моніторинг. Це дозволяє забезпечити відкритість, можливість відстеження та відповідальність за дії.

«Відкритість є дуже важливою, — зазначає О'Кіф. — Крім того, ключем до ефективного захисту друку є співпраця. Щоб зібрати комплексні дані, необхідні для надійного захисту, компаніям доведеться зламати бар'єри між адміністраторами пристроїв друку, фахівцями з безпеки та внутрішніми аудиторами. Ці групи повинні працювати разом, щоб захистити ключову частину мережі, яка протягом багатьох років залишалася без уваги».

Крім того, компанії можуть зарадити своїм вразливостям, пов'язаним з друком, таким чином:

- регулярно оновлювати мікропрограми;
- зменшити обсяги адміністрування в інфраструктурі друку;
- модифікувати бази даних друку з експрес-версій до корпоративних;
- впровадити процедури та документацію, щоб забезпечити послідовність та кількісний контроль захисту;
- організувати тренінги з підвищення рівня безпеки для адміністраторів пристроїв друку.

«Безпека друку, як і корпоративна безпека, є постійним процесом, — пояснює Говард. — Саме тому дуже важливо завжди вдосконалюватися завдяки поглибленому аналізу й експертним консультаціям.

«Безпека друку, як і корпоративна безпека, є постійним процесом,

Michael Howard

Безперервний поглиблений аналіз пов'язаний з важливістю управління. У сфері друку до управління входять контроль за обліковими записами користувачів (тих, хто має доступ до інфраструктури друку), забезпечення дотримання корпоративних правил, керування ризиками, документація з безпеки та реєстрація подій.

Чи потрібне зовнішнє керування друком

Надійна стратегія вимагає використання широкого спектра компонентів. Для більшості компаній, особливо малих та середніх, самостійна розробка та виконання такої стратегії здаються неможливими. Їм краще присвятити час та енергію своєму бізнесу. Найкраще рішення — співпраця з постачальниками послуг зовнішнього керування друком, які можуть контролювати найменші деталі щоденної роботи та підтримувати рівень безпеки, який дозволить компанії спокійно працювати.

Перший крок до створення розумної стратегії друку — поставити собі декілька запитань. По-перше, які принтери краще використовувати в нашій компанії? Нам краще підійдуть струменеві або лазерні принтери? Які функції друку нам потрібні? Відповідаючи на ці запитання, потрібно дотримуватися балансу надійності, витрат та продуктивності.

Після цього слід поміркувати про безпеку, технічне обслуговування та підтримку. Нам краще самим керувати принтерами або найняти зовнішніх спеціалістів? Це залежить від відповідей на додаткові запитання, наприклад: Чи спроможний наш IT-відділ вирішувати проблеми з принтерами? Чи буде дорожче керувати послугами друку самостійно в довгостроковій перспективі? У малих компаніях на це запитання часто відповідають «так».

Компанії, які обирають зовнішнє керування послугами друку, повинні поміркувати про те, чи слід підписати угоду, а також з яким постачальником працювати. Для цього потрібно поставити такі запитання: Які послуги нам потрібні? Що необхідно включити в угоду про рівень послуг? Скільки це буде коштувати? Як швидко ми плануємо розширити нашу мережу принтерів? Як має змінюватися стратегія друку зі зростанням компанії?

Загрози, які становлять незахищені принтери, під'єднані до мережі, є очевидними, й компанії всіх розмірів мають включити послуги друку до загальної системи безпеки та продуктивності. На щастя, існують постачальники готових рішень, які допоможуть вам виконати брудну роботу

Learn more
hp.com

4AA7-1720EEE, November 2017