WHITE PAPER

UNLOCKED DOORS

RISET MENUNJUKKAN PRINTER DIBIARKAN RENTAN BAHAYA DARI SERANGAN CYBER

Ketika tim IT fokus pada pengamanan endpoint lainnya, keamanan printer perusahaan kurang terlalu dipikirkan

Printer menjadi target yang mudah: Terlalu banyak printer yang terhubung dalam jaringan yang tidak memiliki batasan dan tidak dikunci dengan aman.

Tetapi ancaman ini nyata, dan tidak boleh diabaikan. Printer kelas enterprise berevolusi menjadi perangkat dalam jaringan yang semakin tangguh, namun memiliki kerentanan yang sama dengan endpoint lain pada jaringan Anda. Titik masuk yang biasanya kurang aman ini sangat memungkinkan serangan cyber yang sangat nyata; titik-titik ini juga memungkinkan akses ke data finansial dan pribadi di perusahaan Anda, sehingga memiliki konsekuensi bisnis yang sangat berat.

Meskipun begitu, survei terbaru Spiceworks pada lebih dari 300 pengambil keputusan IT perusahaan menunjukkan hanya 16% responden yang menganggap printer memiliki risiko tinggi terkena ancaman/pelanggaran keamanan, yang jauh lebih rendah dari desktop/laptop dan perangkat seluler.[1] Persepsi ini merusak metode pendekatan staf IT pada keamanan jaringan. Meskipun hampir tiga dari lima perusahaan menerapkan praktik keamanan untuk printer, persentasenya jauh di bawah persentase untuk endpoint lainnya, sehingga printer dibiarkan terancam bahaya. Namun faktanya, ada solusi mudah untuk mengamankan titik masuk khusus ini.

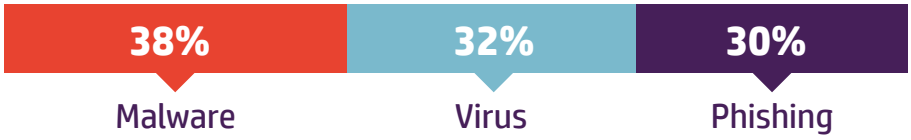
Laporan resmi ini menyediakan data keamanan printer berdasarkan hasil survei Spiceworks, dampak dari pelanggaran keamanan, dan beberapa fitur keamanan printer terpadu modern yang dirancang untuk melindungi dari serangan cyber.

HANYA 16% RESPONDEN YANG MENGANGGAP PRINTER MEMILIKI RISIKO TINGGI TERKAIT ANCAMAN/PELANGGARAN KEAMANAN.[1]

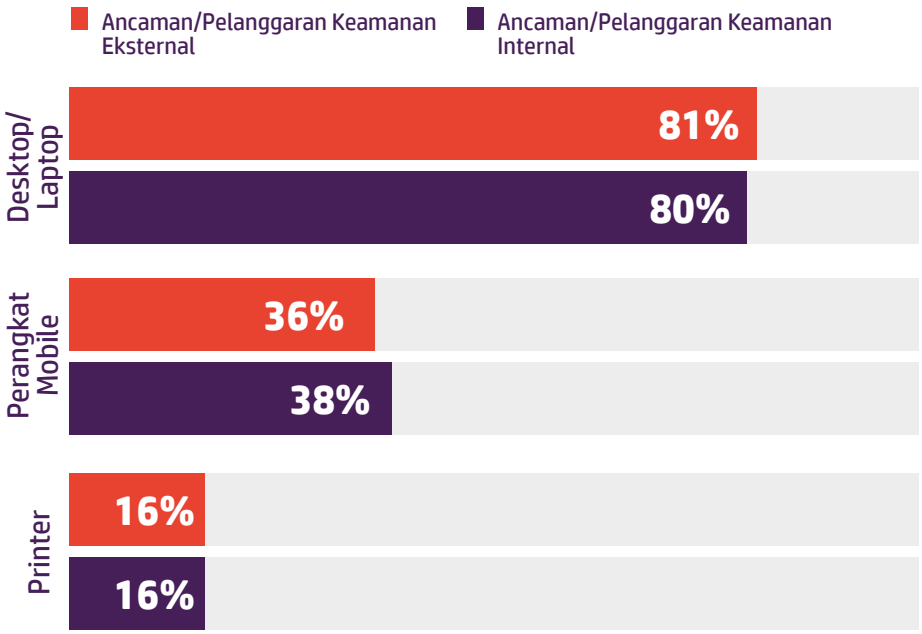
PINTU MASUK SERANGAN

Dalam survei Spiceworks, 74% responden mengatakan bahwa perusahaan mereka pernah mengalami setidaknya beberapa jenis ancaman atau pelanggaran keamanan IT eksternal pada tahun lalu. Dan 70% mengalami ancaman atau pelanggaran keamanan IT internal, sebagian besar karena kesalahan pengguna, penggunaan perangkat pribadi untuk bekerja, atau karyawan yang menggunakan jaringan rumah atau umum untuk tujuan bekerja.[1]

ANCAMAN/PELANGGARAN KEAMANAN IT EKSTERNAL TERATAS YANG PERNAH DIALAMI



Ancaman teratas utamanya menyelinap melalui desktop dan laptop, serta yang lain berasal dari perangkat seluler dan printer.[1] (Ancaman 16% yang berasal printer jauh lebih tinggi dibandingkan hasil 4% yang ditemukan pada penelitian Spiceworks serupa di tahun 2014.) Jumlah serangan yang melalui printer mungkin juga diremehkan, karena printer tidak dipantau secara ketat melalui PC dan perangkat seluler.



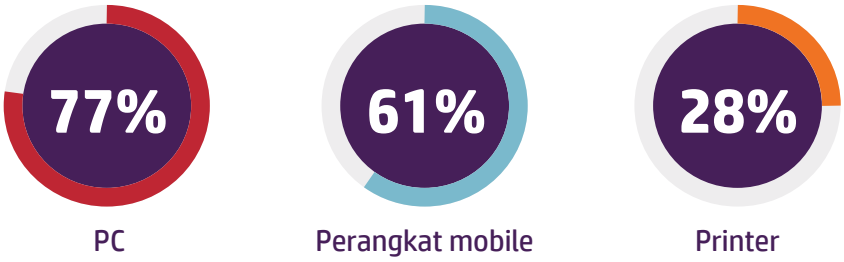
KAMI MENGABAIKAN PRINTER KAMI

Apa pun kasusnya, survei Spiceworks semakin memperjelas bahwa keamanan printer biasanya hanya dipikirkan sebagai tambahan.

Perusahaan sangat sadar pentingnya dari jaringan, endpoint, dan keamanan data. Faktanya, lebih dari empat puluh tiga responden menggunakan keamanan jaringan, akses kontrol/manajemen, perlindungan data, atau keamanan endpoint—atau kombinasi dari semua itu.[1]

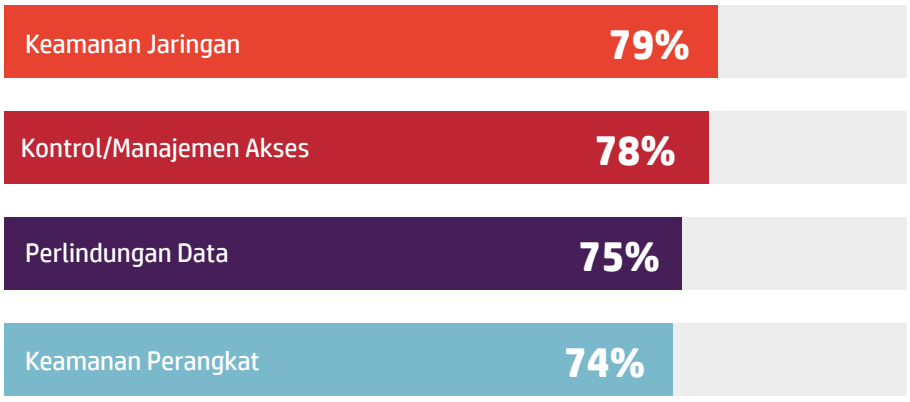
Tetapi solusi ini sangat jarang diterapkan pada printer. Sementara 83% dari responden menggunakan keamanan jaringan pada desktop/laptop dan 55% pada perangkat mobile, hanya 41% yang menggunakannya pada printer.[1]

Ketimpangan ini bahkan lebih jauh pada keamanan endpoint:



Ditambah lagi, bahkan tidak sampai sepertiga (28%) dari responden menerapkan sertifikat keamanan untuk printer. Sebaliknya, 79% responden menerapkannya untuk PC dan 54% untuk perangkat mobile.[1]

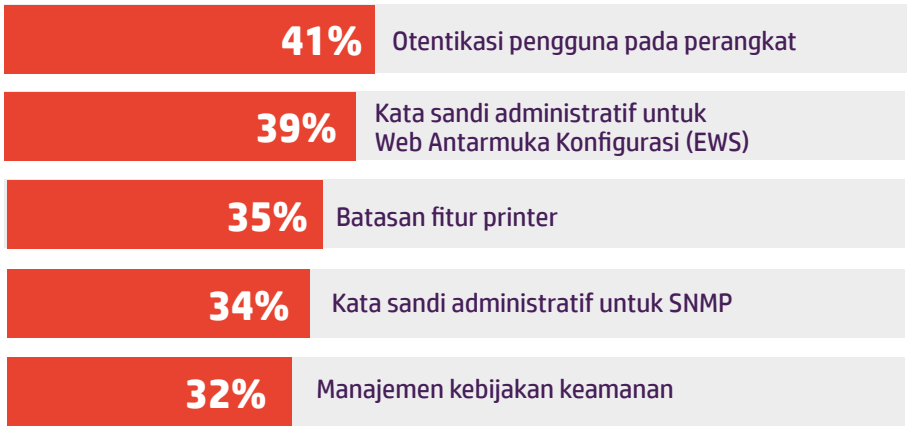
PRAKTIK KEAMANAN ENDPOINT TERATAS



Di antara perlindungan yang digunakan pada perangkat endpoint pada umumnya, tindakan keamanan yang paling banyak digunakan untuk printer adalah keamanan dokumen, keamanan jaringan, dan kontrol akses, tetapi kurang dari setengah responden mengatakan perusahaan mereka menggunakan tindakan-tindakan tersebut pada printer mereka.[1]

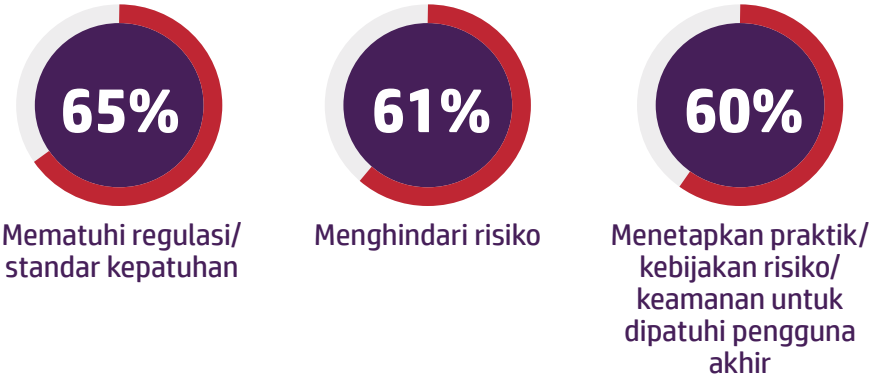
Beberapa perusahaan memang memiliki praktik keamanan khusus printer, tetapi itu pun jumlahnya masih timpang. Lebih dari 40% perusahaan yang menerapkan otentikasi pengguna, dan kurang dari 40% menggunakan kata sandi administrator untuk konfigurasi antarmuka web (web configuration interface).[1] Untuk pertahanan yang kuat, setiap perusahaan harus menggunakan gabungan dari semua pendekatan ini—dan lebih banyak lagi.

PRAKTIK KEAMANAN KHUSUS PRINTER TERATAS



Bila berhubungan dengan endpoint compliance dan kebijakan audit, kontrol keamanan printer tertinggal hampir dari semua endpoint lainnya. Hampir 90% perusahaan menerapkan kebijakan keamanan informasi, tetapi kebijakan ini biasanya tidak mencakup printer. Misalnya, meskipun 57% responden mengatakan mereka menerapkan perlindungan malware pada PC, hanya 17% yang menerapkannya pada printer.[1]

HAMPIR 9 DARI 10 PAKAR TI MENYATAKAN BAHWA ORGANISASI MEREKA MENERAPKAN KEBIJAKAN KEAMANAN INFORMASI, KARENA ALASAN BERIKUT:



Jelas, perusahaan tidak terlalu menganggap penting keamanan printer—tetapi seharusnya iya.

“Banyak printer masih menggunakan kata sandi default, atau tidak memiliki kata sandi sama sekali, atau sepuluh printer menggunakan kata sandi yang sama,” Michael Howard, ketua penasihat keamanan untuk HP, menuturkan kepada Computerworld pada bulan Juni. “Printer tanpa perlindungan kata sandi adalah tambang emas bagi hacker. Salah satu pelanggaran yang sering kami temui adalah serangan man-in-the-middle, yaitu mereka mengambil alih printer dan mengalihkan [dokumen masuk] ke sebuah laptop sebelum dicetak. Mereka dapat melihat semua hal yang sedang dicetak CEO.”[2]

POTENSI DAMPAK INTRUSI PRINTER

Menurut analis e-threat senior dari Bitdefender, Bogdan Botezatu, printer memunculkan potensi lubang keamanan yang cukup besar. “Kami mendapatkan banyak telemetri di lab penilaian kerentanan milik kami. Router bukan lagi perangkat terburuk di internet. Sekarang adalah printer.”[3]

Kerentanan ini dapat memberikan pengaruh besar pada bisnis. Bila ada satu printer yang tidak aman, Anda dapat membuat seluruh jaringan perangkat yang saling terhubung rentan terhadap serangan, memberi kesempatan peretas untuk memata-matai perangkat yang terhubung jaringan—dan membuka celah keamanan seluruh jaringan.

Kita semua memahami dampak dari pelanggaran keamanan. Dalam survei Spiceworks, responden mengatakan lima dampak pelanggaran teratas adalah:[1]

Tetapi pelanggaran printer dapat lebih parah dari itu, terutama jika Anda menggunakan printer multifungsi yang mampu menyimpan data cetak secara elektronik. Pekerjaan pencetakan yang disimpan pada cache printer

memungkinkan hacker dapat mengakses informasi bisnis atau informasi pribadi yang sensitif.

Bahkan yang lebih mengkhawatirkan, hacker dapat mengakses jaringan perusahaan lebih luas melalui printer yang tidak aman, mencuri sesuatu seperti nomor Jaminan Sosial, informasi finansial, atau memo dan dokumen internal. Informasi yang dicuri ini tidak hanya dapat memengaruhi karyawan secara perorangan, tetapi juga digunakan oleh pesaing atau membahayakan reputasi perusahaan secara serius.

SOLUSI MUDAH: FITUR KEAMANAN TERPADU

Pastinya, perusahaan harus mengatasi keamanan bahkan pada printer mereka. Dewasa ini, beberapa printer modern tingkat perusahaan mengunggulkan keamanan terpadu yang mudah digunakan, yang memerangi ancaman pada printer. Keamanan ini mencakup:

- **Deteksi, perlindungan, dan pemulihan serangan otomatis**
- **Melacak penggunaan untuk mencegah penggunaan tidak sah**
- **Opsi masuk sederhana seperti PIN atau smartcard**
- **Alat pembaca proximity card yang memungkinkan pengguna mengotentikasi dan mencetak dengan cepat dan aman pada printer menggunakan badge karyawan mereka**
- **Pencetakan terenkripsi yang aman untuk dokumen sensitif**

Saat mempertimbangkan membeli printer lagi, baik single atau multifungsi, telitilah pencegahan keamanan terpadunya—dan pastikan untuk mengaktifkannya. Dengan fitur sederhana, khusus untuk printer, seperti itu, Anda tidak akan lagi rentan diserang melalui printer; selain itu, dengan adanya Internet of Things, masih banyak lagi titik akses yang perlu dikhawatirkan—**tapi printer Anda tidak termasuk di dalamnya.**

ANDA MENCARI PRINTER YANG LEBIH AMAN?
PELAJARI SELENGKAPNYA ›

Sumber:

[1] Survei Spiceworks dari 309 pembuat keputusan TI di Amerika Utara, EMEA, dan APAC, atas nama HP, November 2016.

[2] "Printer Security: Is your company's data really safe?" *Computerworld*, 1 Juni 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet," *The Register*, September 8, 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/