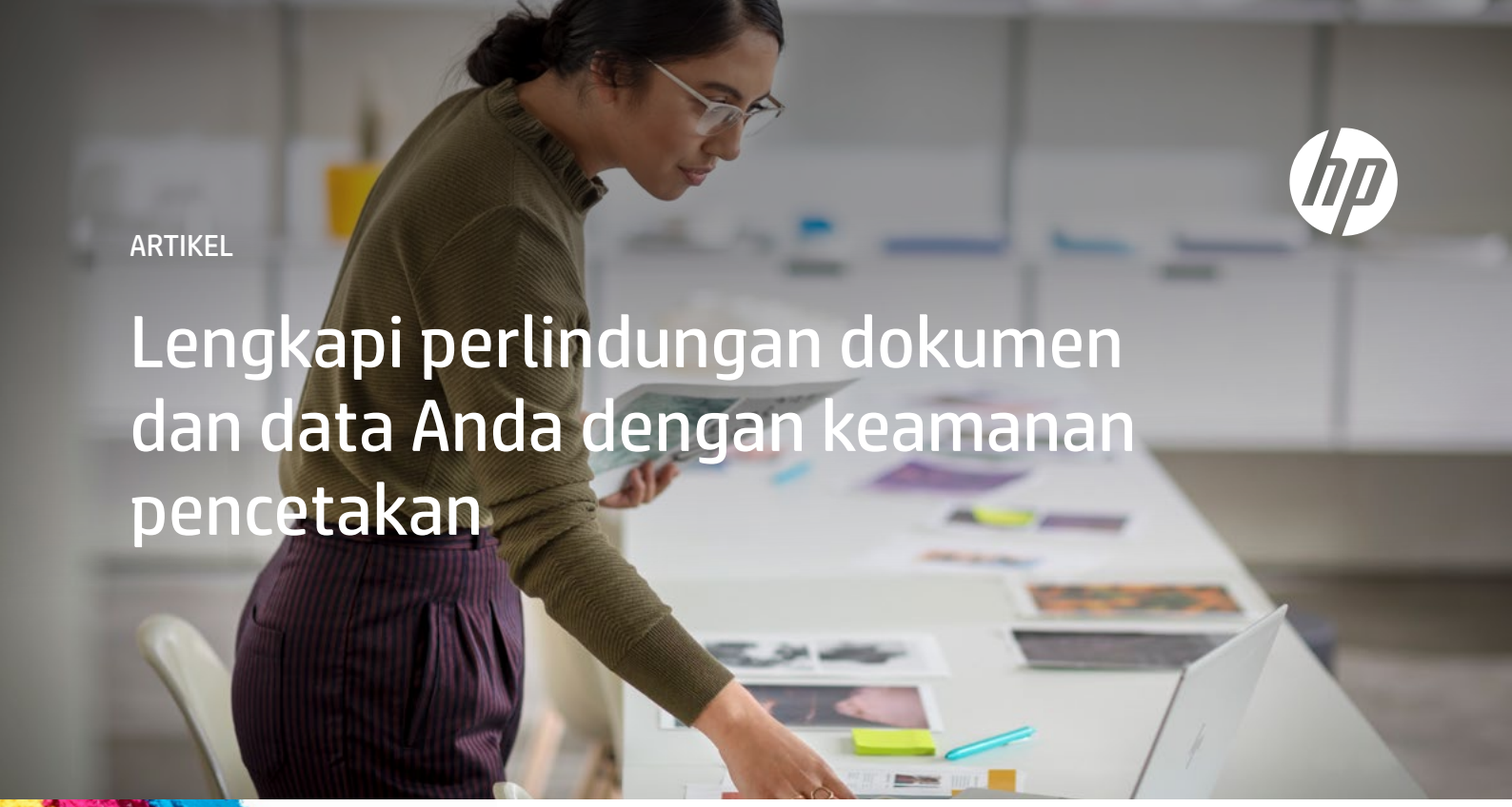


ARTIKEL

Lengkapi perlindungan dokumen dan data Anda dengan keamanan pencetakan

Peretas adalah sekumpulan orang-orang kreatif. Serangan dimulai dari awal rantai pasokan hingga rekayasa sosial dan peretasan dengan dukungan AI[1], mereka melancarkan teknik serangan baru tanpa henti dan mencari celah keamanan yang tersembunyi pada sistem keamanan perusahaan – salah satu celah tersebut adalah jaringan printer terkoneksi.

Sebagai mitra teknologi terkemuka, selama ini HP aktif merekomendasikan dan mendukung sistem keamanan pencetakan yang lebih baik bagi perusahaan di seluruh dunia. Meskipun perangkat jaringan, server, dan komputer masih menjadi sasaran utama peretasan, printer-printer milik perusahaan juga merupakan endpoint jaringan. Dan bagi peretas, endpoint yang memiliki celah keamanan adalah potensi masuknya serangan cyber.

Printer kerap menjadi target serangan

Berbeda dengan persepsi umum, printer yang terkoneksi jaringan cukup sering menjadi sasaran peretasan oleh para penjahat cyber. Menurut laporan Global Print Security, hampir dua per tiga perusahaan melaporkan kehilangan data terkait pencetakan, sehingga menimbulkan kerugian pada perusahaan-perusahaan di Amerika sebesar lebih dari $1 juta[2]. Studi lain yang dikutip dari perusahaan konsultasi Booz Allen Hamilton menemukan bahwa 61% responden telah melaporkan insiden kehilangan data pada tahun 2016, dan setidaknya 50% pernah mengalami insiden tersebut melalui serangan keamanan pada printer[3].

Menurut perkiraan Cybersecurity Ventures, kejahatan cyber akan membebani ekonomi dunia sekitar $6 triliun pada 2021[4], maka perusahaan -perusahaan kini tidak bisa lagi mengabaikan sistem keamanan pencetakan mereka.

Lebih dari

30%

responden melaporkan satu atau lebih insiden kehilangan data terkait pencetakan.[3]

Risiko keamanan yang berhubungan dengan printer

Sebelum perusahaan menentukan strategi keamanan cyber untuk printernya, mereka harus terlebih dahulu memahami risiko keamanan yang harus ditanggulangi. Dari serangan cyber eksternal hingga penyusupan malware melalui kartrid toner tiruan yang tidak aman, dokumen sensitif yang tertinggal di printer, dan lainnya, jaringan printer terkoneksi memiliki berbagai kerentanan, seperti[5]:

Akses tanpa izin ke data pencetakan

Meskipun keamanan data kerap dikaitkan dengan ancaman digital, pelanggaran data dapat terjadi hanya karena seseorang menggunakan printer dan mengakses dokumen milik orang lain.

Risiko malware

Tidak seperti Kartrid HP Asli yang memiliki perlindungan terhadap perusakan, banyak kartrid tiruan menggunakan chip yang bisa diprogram ulang sehingga rentan disusupi malware.

Re-routing saat mencetak

Dengan sejumlah perubahan konfigurasi, peretas dapat mengalihkan tugas pencetakan ke printer mereka.

Manipulasi data

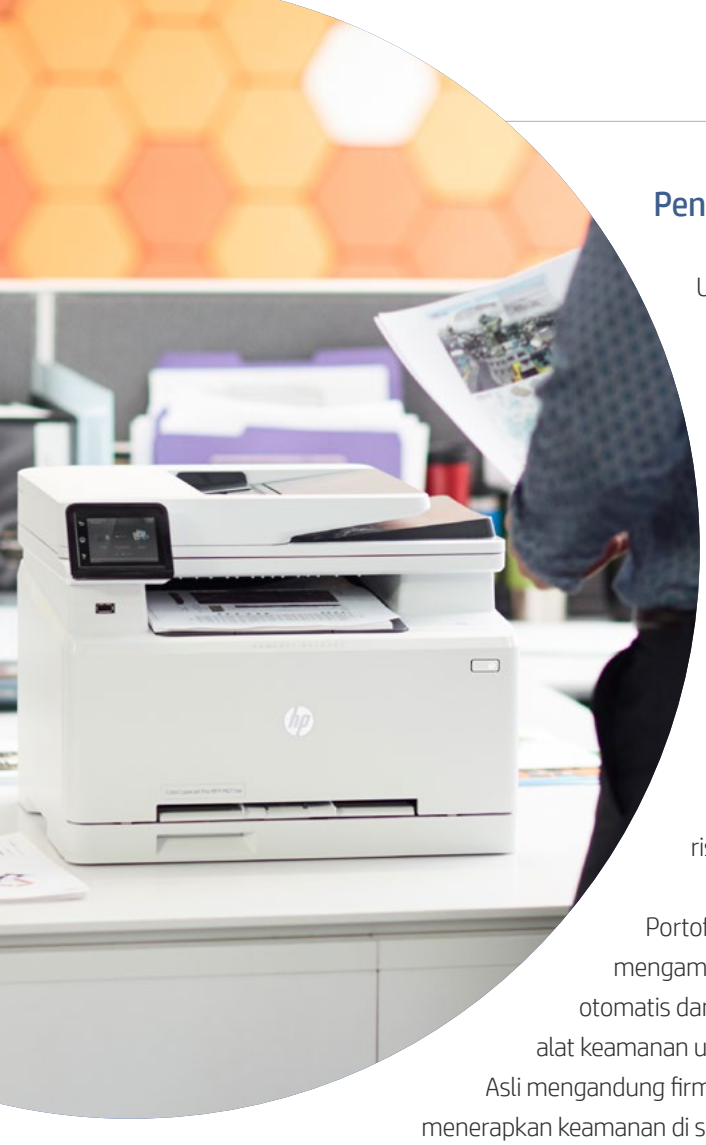
Printer yang rentan dapat memudahkan peretas mengganti atau menyisipkan konten tertentu ke dalam materi yang akan dicetak.

Pengungkapan data

Data yang akan dicetak bisa terungkap jika peretas memiliki akses ke sistem memori atau file printer, atau secara fisik dari hard drive printer yang dibuang.

Risiko pencetakan nirkabel

Printer yang bisa mencetak lewat jaringan Wi-Fi juga rentan terhadap serangan, di sini peretas dapat menghubungkan printer dengan jaringan yang tidak aman dan menjalankan kode berbahaya.



Pengamanan data printer dan pencetakan Anda

Untuk melindungi endpoint yang sangat penting ini, HP merekomendasikan sejumlah tindakan keamanan yang mendasar. Sebagai langkah awal, pilih printer atau layanan cetak terkelola dari vendor dengan kapabilitas keamanan yang telah terbukti, dan hindari penggunaan kartrid tiruan untuk menciptakan fondasi sistem keamanan pencetakan yang kokoh. Selanjutnya, lengkapi dengan patching sistem operasi printer yang tepat waktu, rutin mengubah PIN dan kata sandi, menonaktifkan layanan yang tidak terpakai, menerapkan autentikasi multi-factor, serta memberikan pelatihan pada karyawan terkait praktik terbaik keamanan data untuk memperkuat sistem keamanan perusahaan Anda.

Dengan menerapkan langkah-langkah di atas, Anda dapat menutup kelemahan yang tersembunyi pada strategi keamanan Anda dan mengurangi risiko pelanggaran data yang berasal dari printer yang tidak terlindungi.

Portofolio printer HP menggunakan sistem keamanan berlapis untuk mengamankan sistem pencetakan perusahaan, dari pendeteksi malware otomatis dan kemampuan self-healing[6] hingga firmware yang dapat diupgrade[7] dan alat keamanan untuk manajemen printer.[8] Selain itu, chip yang terdapat pada Kartrid HP Asli mengandung firmware anti-perusakan[9], serta didesain, diproduksi, dan dikirim dengan menerapkan keamanan di seluruh rantai pasokan demi memastikan integritas produk.[8]

Lindungi data Anda dengan solusi pencetakan yang dirancang untuk keamanan. Pelajari lebih lanjut di sini

REFERENSI:

[1] ZDNet, Artificial intelligence will be used to power cyberattacks, warn security experts, April 2020.

[2] Quocirca, The Print Security Landscape, 2020, Louella Fernandes, Desember 2020

[3] DarkReading.com, How Hackers Hit Printers, 2018.

[4] Cision, Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021, Desember 2018.

[5] Business News Daily, Is Your Printer Your Weak Security Link?, April 2020.

[6] Fitur keamanan bawaan paling canggih dari HP tersedia di perangkat HP Enterprise dan HP Managed dengan firmware HP FutureSmart 4.5 atau lebih tinggi. Klaim berdasarkan tinjauan HP terhadap fitur yang dipublikasikan pada tahun 2019 dari printer yang bersaing di kelasnya. Hanya HP yang menawarkan kombinasi fitur keamanan yang dapat secara otomatis mendeteksi, menghentikan, dan memulihkan dari serangan dengan reboot otomatis, sesuai dengan panduan NIST SP 800-193 untuk ketahanan siber perangkat. Untuk daftar produk yang kompatibel, kunjungi: hp.com/go/PrintersThatProtect. Untuk informasi lebih lanjut, kunjungi: hp.com/go/PrinterSecurityClaims.

[7] Sejumlah fitur keamanan printer yang didukung oleh upgrade firmware HP FutureSmart di masa mendatang mungkin tidak tersedia di perangkat yang lebih lama, jika misalnya, karakteristik produk fisik membatasi fungsi fitur baru tersebut.

[8] HP JetAdvantage Security Manager harus dibeli secara terpisah. Untuk mempelajari selengkapnya, kunjungi hp.com/go/securitymanager.

[9] Sistem pencetakan kelas office HP merupakan perangkat Perusahaan dan Terkelola pilihan dengan FutureSmart firmware 4.5 dan lebih tinggi, perangkat Pro, LaserJet model 200 ke atas, dengan Toner HP Asli, PageWide, dan Kartrid Tinta masing-masing. Tidak termasuk kartrid printhead terintegrasi dari HP. Pelacakan rantai pasokan digital, perangkat keras, dan fitur keamanan kemasan berbeda menurut lokasi berdasarkan SKU. Lihat https://www8.hp.com/id/en/cartridge/supplies-security.html dan hp.com/go/SuppliesSecurityClaims.