ENKRIPSI PERANGKAT LUNAK DAN KEPATUHAN REGULASI: SOLUSI LEBIH MURAH DENGAN RISIKO KEAMANAN UTAMA

PERSYARATAN REGULASI DAN KEPATUHAN

Dahulu, Keamanan Data hanya diserahkan kepada departemen TI, tetapi karena pelanggaran data konsumen yang terus terjadi, pemerintah di seluruh dunia memberlakukan lebih banyak persyaratan pada bisnis untuk mengenkripsi dan melindungi semua data yang dapat diidentifikasi secara pribadi.

Dari HIPAA dalam layanan kesehatan, hingga GDPR dalam EMEA, dan CCPA di California, enkripsi kelas data yang dilindungi diwajibkan melalui regulasi. Organisasi kepatuhan telah berkembang dengan pesat selama lebih dari 3 tahun terakhir karena regulasi ini dan risiko denda serta penghargaan hukum terkait telah meroket.

Akibat perubahan ini, departemen TI berjuang untuk mengimbangi keamanan dan kenaikan biaya. Selama pandemi COVID, anggaran dibelanjakan pada investasi perangkat keras dan firewall tambahan, dengan mengorbankan fokus pada enkripsi data.

Faktanya, enkripsi perangkat lunak dengan Microsoft BitLocker® atau perangkat lunak manajemen titik akhir dari perusahaan seperti Symantec, McAfee, dan lainnya sedang meningkat. Beberapa bisnis dan konsumen juga memanfaatkan drive USB standar dengan drive "vault" perangkat lunak seperti yang disediakan oleh beberapa vendor.

ENKRIPSI DAN DATA-IN-TRANSIT

Karyawan dan konsumen perlu selalu membawa data mereka. Mereka memiliki opsi seperti:

1. Layanan cloud: Cloud adalah layanan yang bagus, karena dapat diakses dari perangkat apa pun yang dapat terhubung ke internet. Akan tetapi, fleksibilitas memerlukan pengorbanan. Penyimpanan data pada Cloud menghilangkan kontrol data dari pengguna atau perusahaan dan memiliki potensi risiko seperti server Cloud yang tidak terkunci dan dapat diakses sembarangan.
2. Drive USB standar: Meskipun membawa drive USB tampak lebih aman, risiko terungkapnya data penting ketika drive hilang juga perlu diperhatikan. Misalnya, ada banyak cerita tentang hilangnya drive USB yang berisi informasi rahasia atau jasa laundry dengan laci-laci yang penuh dengan drive USB yang hilang.
3. Drive USB enkripsi perangkat keras: Drive USB ini memiliki arsitektur kustom yang menggabungkan pengontrol enkripsi onboard dan kontrol akses. Data dienkripsi secara umum menggunakan enkripsi terkuat AES-256 bit dalam mode XTS, ditambah kemungkinan pengaman lainnya untuk memitigasi serangan fisik atau berbasis firmware. Drive ini diproduksi oleh perusahaan yang berspesialisasi dalam perangkat keamanan, dan meskipun lebih mahal dari drive USB standar, drive USB ini menawarkan keamanan data yang lebih baik. Drive FIPS 197 atau FIPS 140-2 Level 3 dapat memberikan tingkat perlindungan yang lebih tinggi dan membuat Anda lebih tenang.
4. Drive USB standar dengan enkripsi perangkat lunak: Demi keamanan yang sesuai regulasi, penggunaan enkripsi perangkat lunak dengan BitLocker atau alat lainnya merupakan opsi yang baik karena relatif tidak mahal dan menawarkan enkripsi AES-256 XTS yang sama.

Tidak perlu heran jika di sebagian besar kasus, bisnis dan industri lebih memilih opsi 4, yaitu menggunakan drive USB Standar dengan enkripsi perangkat lunak. Alasan utamanya adalah enkripsi perangkat lunak seperti BitLocker atau utilitas vault data lainnya yang bersifat "gratis".

ENKRIPSI PERANGKAT LUNAK TIDAK MEMATUHI REGULASI

Bagi seorang profesional keamanan bisnis, enkripsi perangkat lunak dapat menawarkan kapabilitas enkripsi yang sama persis seperti drive USB enkripsi perangkat keras yang lebih mahal. Namun, apakah langkah itu tepat? Anggaran dibatasi, sehingga bisnis beralih ke enkripsi perangkat lunak untuk tujuan kepatuhan, tanpa menyadari sisi negatif enkripsi jenis ini.

Apa masalah drive USB enkripsi perangkat lunak? Apakah data-at-rest dan in-transit tidak dienkripsi dengan AES-256 XTS? Pada umumnya, dienkripsi. Masalahnya adalah: Enkripsi perangkat lunak termasuk "enkripsi yang dapat dihapus".

Tunggu – Dapat dihapus? Apakah itu artinya pengguna drive USB yang dienkripsi perangkat lunak dapat menonaktifkan enkripsi?

Jawabannya adalah Ya. Pengguna dapat menghapus fitur enkripsi perangkat lunak dari drive USB mereka. Jika Anda bertanya, untuk apa? Karena hal itu mungkin, dan karena mereka ingin mengakses file tanpa menggunakan kata sandi atau mereka lupa kata sandi, tetapi perlu menggunakan drive USB.

CARA MENGHAPUS ENKRIPSI PERANGKAT LUNAK DARI DRIVE USB TERENKRIPSI

Untuk pengguna yang tidak ingin berurusan dengan kata sandi yang rumit untuk mengakses data mereka, prosesnya simpel:

1. Colokkan drive enkripsi perangkat lunak ke komputer
2. Format drive
3. Setelah drive diformat, semua enkripsi terhapus
4. Salin file dengan informasi rahasia ke drive untuk mempermudah akses

Ini mudah dilakukan jika pengguna menggunakan komputer yang tidak dibatasi, karena departemen TI umumnya membatasi penggunaan perintah format pada komputer perusahaan, tetapi ini dapat dilakukan di komputer non-perusahaan lainnya.

Berkenaan dengan Kepatuhan, kemudahan menghapus enkripsi data artinya drive yang disediakan perusahaan kini tidak lagi dienkripsi, dan akibatnya, data yang dienkripsi pada drive dianggap hilang selamanya setelah enkripsi dihapus melalui metode di atas (kunci enkripsi terikat ke data). Data apa pun yang disalin pada perangkat setelah enkripsi dihapus dianggap tidak aman dan berkemungkinan tidak patuh atau melanggar regulasi dari HIPAA, GDPR, CCPA, dan banyak lagi lainnya.

KONSEKUENSI KEHILANGAN DRIVE YANG TIDAK DIENKRIPSI

Jika drive USB yang ditetapkan perusahaan hilang lalu ditemukan, bahkan jika perusahaan tidak menyadarinya di awal kemudian mengetahuinya lewat media sosial, perusahaan akan diwajibkan memenuhi persyaratan kepatuhan khusus, yaitu:

1. Melakukan investigasi forensik untuk mengidentifikasi data apa yang hilang
2. Menentukan apakah terjadi pelanggaran hukum melalui konsultasi dengan Hukum
3. Menentukan apakah harus memberi tahu pelanggan

Inilah alasan mahalnya biaya satu drive USB yang hilang. Dengan tarif Hukum melebihi ratusan dolar per jamnya, proses kepatuhan ini dapat berakhir dengan pengeluaran hingga ribuan dolar, belum lagi potensi denda, gugatan dari pelanggan, dan rasa malu atas terungkapnya data.

Ketika enkripsi perangkat lunak dipertimbangkan karena implementasinya yang hemat biaya, risiko-risiko dan konsekuensi finansialnya yang sangat besar tidak dipikirkan.

Ada bahaya lain akibat membiarkan penggunaan drive USB tidak dienkripsi pada jaringan perusahaan. Umumnya ini dikenal sebagai "BadUSB". BadUSB adalah sejenis malware yang digunakan oleh aktor jahat untuk menjebol firewall perusahaan dan memasukkan malware ke pertahanan siber perusahaan melalui perangkat penyimpanan USB.

BadUSB

Ketika drive USB dicolokkan ke komputer, pengontrol chipset komputer memulai handshake (komunikasi komputer) dengan pengontrol drive USB melalui firmware. Pertukaran ini terjadi sebelum Sistem Operasi, seperti Microsoft/macOS/Linux bahkan menyadari bahwa ada drive USB yang disambungkan. Setiap drive USB memiliki firmware yang berjalan ketika drive dicolokkan ke port USB.

Aktor jahat telah belajar bahwa mereka dapat memasukkan malware melalui mekanisme handshake ini dengan mengganti firmware yang berjalan pada drive USB dengan firmware jahat yang menyuntikkan malware ke sistem komputer target saat komunikasi terjadi dengan drive USB. Drive USB Standar tidak memiliki keamanan pada firmware internal yang dieksekusi oleh pengontrolnya, sehingga BadUSB adalah hasil dari drive USB biasa yang dipersenjatai untuk menembus firewall dan menjebol pertahanan siber.

Banyak perusahaan mencoba untuk melarang penggunaan drive USB pada sistem mereka, bahkan sampai mengisi port USB dengan epoksi. Akan tetapi, mereka menyadari bahwa beberapa kelas karyawan perlu membawa data mereka menggunakan drive USB. Misalnya, eksekutif ingin membawa data untuk kerja atau data yang tidak ada di Cloud perusahaan yang perlu diberikan ke penasihat Legal atau Finansial eksternal; kontraktor perusahaan yang perlu data, tetapi akses ke database perusahaan dibatasi; analis finansial yang harus segera menutup laporan bulanan dan perlu mengerjakannya di rumah.

Seperti yang ditunjukkan analisis sebelumnya, terdapat risiko signifikan dari penggunaan solusi drive USB standar + enkripsi perangkat lunak. Sekilas, apa yang terlihat lebih murah ternyata membawa potensi bahaya besar dan mengakibatkan biaya yang jauh lebih mahal. Uang yang dapat digunakan untuk solusi yang lebih murah justru terpakai untuk sekadar 2-3 jam konsultasi dengan pengacara tentang potensi pelanggaran data.

DRIVE USB ENKRIPSI PERANGKAT KERAS ADALAH OPSI TERBAIK UNTUK KEPATUHAN REGULASI

Yang membuat drive USB enkripsi perangkat keras menjadi pilihan terbaik untuk aplikasi kepatuhan regulasi adalah:

1. Enkripsi yang ada pada drive USB enkripsi perangkat keras selalu AKTIF: Pengguna tidak akan dapat mematikan enkripsi, mengatur ulang aturan kata sandi (panjang minimum, kerumitan), dan mematikan percobaan ulang kata sandi otomatis. Berbeda dari enkripsi perangkat lunak yang tidak mencegah kata sandi ditebak berulang-ulang melalui serangan kamus perangkat lunak, versi perangkat keras membatasi percobaan ulang kata sandi dan akan mengunci data jika salah memasukkan kata sandi 10 kali atau bahkan lebih sedikit. Ini adalah cara yang sangat aman di era komputer canggih.
2. Drive enkripsi perangkat keras menggunakan pengontrol enkripsi premium dan menggabungkan banyak fitur keamanan: Meskipun kami tidak selalu mengungkap semua penanggulangan keamanan, ada satu penanggulangan untuk perlindungan terhadap BadUSB. Di pabrik, ketika firmware hanya dimuat pada drive enkripsi perangkat keras, firmware ditandatangani secara digital lalu dimuat. Ini berarti, ketika USB terenkripsi ini dicolokkan, pengontrol enkripsi memeriksa terlebih dahulu integritas dari firmware melalui tanda tangan digital tersebut, dan hanya memuatnya jika lolos verifikasi. Percobaan apa pun untuk mengganti firmware akan memblokir drive dan membuatnya tidak berfungsi, tanpa ancaman.
3. Drive USB enkripsi perangkat keras dapat memiliki ID Produk (PID) yang diatur untuk perusahaan tertentu: Drive premium ini dapat memiliki pengidentifikasi digital yang diprogram ke dalamnya, sehingga, jika sebuah drive tersambung ke firewall dalam atau luar perusahaan, drive tersebut diidentifikasi sebagai drive milik perusahaan. Misalnya, jika karyawan menghilangkan drive perusahaan dan membeli model yang sama di ritel, drive yang baru dibeli tersebut tidak akan divalidasi pada jaringan perusahaan. Kustomisasi ini menambah lapisan keamanan pada penggunaan drive USB.
4. Drive enkripsi perangkat keras menghemat uang dengan sangat cepat: Sekadar pengurangan dan eliminasi risiko membuat siklus balik modal menjadi sangat singkat.

Kingston adalah produsen drive USB Terenkripsi terbesar di dunia dan menawarkan jajaran drive dengan bermacam-macam fitur dan rentang harga. Hubungi Kingston secara langsung untuk mendiskusikan tentang bagaimana kami dapat membantu Anda tetap patuh terhadap regulasi dengan solusi USB Terenkripsi untuk eksekutif, karyawan, kontraktor, dan banyak lagi lainnya.