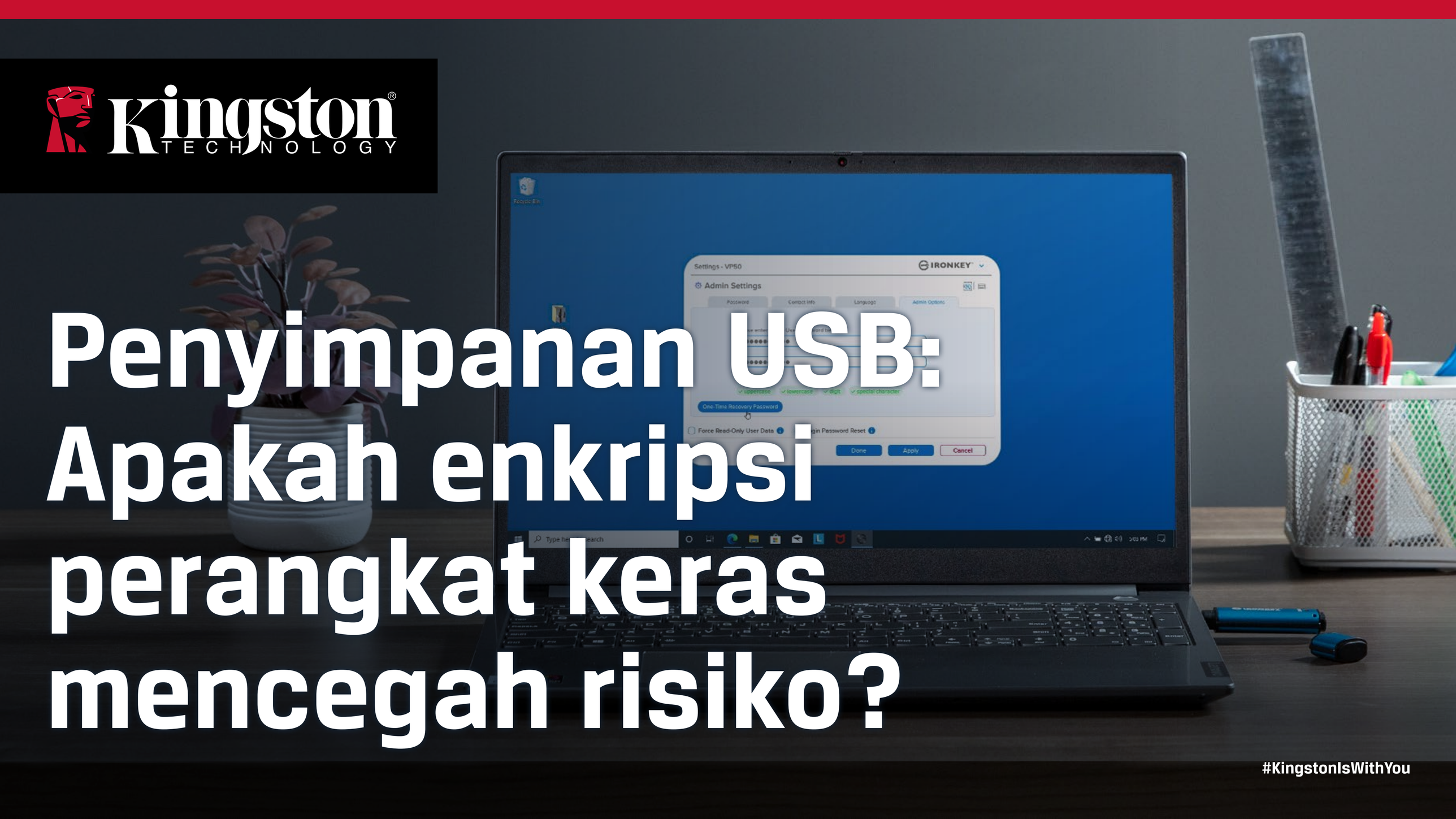

Penyimpanan USB: Apakah enkripsi perangkat keras mencegah risiko?

#KingstonIsWithYou

Penyimpanan USB: Apakah enkripsi perangkat keras mencegah risiko?

Kata pengantar dan isi

Bisnis saat ini lebih mengkhawatirkan keamanan siber dibandingkan sebelumnya, tetapi informasinya kurang diketahui oleh sangat banyak organisasi sehingga mereka kurang siap dalam menghadapi ancaman keamanan siber. Di Amerika Serikat, hanya 50% dari bisnis yang memiliki rencana keamanan siber, dengan 32% di antaranya belum memperbarui rencana keamanan sibernya sejak awal pandemi COVID-19, yang menurut UpCity, telah menyebabkan banyak organisasi beralih ke model kerja jarak jauh atau hybrid. Frekuensi serangan siber ternyata makin meningkat. Secara global, jumlah bisnis yang terkena serangan perangkat lunak pemeras (ransomware) meningkat dari 37% pada 2020 menjadi 66% pada 2021[1].

Keamanan siber yang terancam dapat berdampak sangat buruk pada bisnis. Selain kerugian keuangan, serangan siber juga menyebabkan kehilangan data, keamanan, dan reputasi yang dapat berdampak negatif bagi organisasi dalam banyak aspek, baik dalam jangka pendek maupun panjang.

Drive USB adalah media yang sering dipakai dalam ancaman keamanan siber. Drive USB telah menjadi sangat umum di banyak organisasi karena kesederhanaannya yang siap digunakan hanya dengan mencolokkannya ke komputer. Namun, kesederhanaan inilah yang menjadikan drive USB sangat rentan terhadap penyerangan. Kejadian seperti drive yang tidak disimpan dengan baik atau dicuri sudah cukup bagi pelaku kejahatan untuk mengakses data yang mungkin sensitif. Di sinilah enkripsi dapat berperan penting dalam mengamankan penggunaan drive USB dan mengurangi setiap risiko yang terkait bagi individu dan organisasi. Dalam eBook ini, kami memberikan jawaban atas beberapa pertanyaan penting berikut:

- Mengapa USB terenkripsi sangat penting dalam perlindungan terhadap serangan siber?
- Di mana terjadinya kerentanan organisasi yang disebabkan oleh dirinya sendiri?
- Apa yang dapat dilakukan organisasi untuk melindungi dirinya sendiri?

Daftar isi	Halaman

Penyimpanan USB: Apakah enkripsi perangkat keras mencegah risiko?

Kontributor

Penyusunan eBook ini dilakukan bersama sosok industri terkemuka di bidang TI dan teknologi yang muncul, bersama dengan ahli teknis kami sendiri.

David Clarke

David diakui sebagai satu dari 10 pemengaruh teratas berdasarkan daftar "30 pemuka pemikiran dan pemikir paling berpengaruh di media sosial, di bidang manajemen risiko, kepatuhan, dan teknologi regulasi di Inggris Raya" dari Thompson Reuter serta termasuk dalam daftar 50 Ahli Global oleh Kingston Technology.

Pasi Siukonen

Pasi bertanggung jawab untuk memimpin tim pakar yang mendukung berbagai departemen Kingston seperti Humas, Pemasaran, Penjualan Lapangan, Dukungan Teknis, dan Layanan Pelanggan terkait produk Kingston. Produk yang menjadi fokus utamanya adalah lini produk Flash dan SSD.

Perbedaan antara drive komoditas dan terenkripsi

Dibandingkan drive biasa (tanpa enkripsi) yang sangat mudah diakses dan digunakan, enkripsi perangkat keras menambahkan beberapa lapisan keamanan, baik secara fisik maupun digital, yang menjadikan penyimpanan USB jauh lebih aman. Drive biasa tanpa enkripsi yang banyak tersedia, murah, dan portabel memberikan kenyamanan lebih kepada pengguna, namun juga memudahkan pelaku kejahatan yang bertujuan mencuri data sensitif, memasukkan perangkat lunak berbahaya (malware) atau perangkat lunak pemeras (ransomware) ke dalam jaringan perusahaan, dan perbuatan lainnya. Seringnya penggunaan USB menimbulkan banyaknya peluang serangan siber. Ada dua risiko utama yang terkait dengan drive biasa:

- **Serangan Ransomware:** serangan berbasis USB ini meliputi dimasukkannya perangkat lunak berbahaya (malware) ke dalam jaringan perusahaan, kemudian menyandera informasi dan/atau sistem perusahaan untuk tebusan dengan mengenkripsinya. Serangan ini sering disebabkan olehBadUSB dan telah menjadi jenis perangkat lunak berbahaya (malware) yang paling terkemuka.
- **Data yang dicuri:** pelaku kejahatan hanya memerlukan drive yang hilang, dicuri, atau tanpa penjagaan dan tanpa langkah keamanan yang tepat untuk dengan mudah mengakses data yang tersimpan di drive itu, yang bisa berupa informasi pelanggan, kode sumber, atau data keuangan dan kinerja yang sensitif.

BadUSB – adalah serangan yang dapat mengeksploitasi kerentanan drive USB dengan firmware yang tidak dilindungi, yang kemudian dapat diprogram dengan perangkat lunak berbahaya. Berbagai alat berbahaya ini sangat umum dan mudah diperoleh oleh penjahat siber, tetapi kesadaran akan adanya alat ini tetap rendah sehingga berbagai serangan terlalu mudah dilakukan dengan cara mengganti firmware drive biasa dengan firmware yang telah diretas sehingga drive USB dapat disamarkan sebagai keyboard dan dengan mudah menjalankan skrip untuk menyerang firewall. Karena begitu banyak serangan siber dilakukan melalui orang dalam yang tidak terduga, baik yang memang berniat jahat atau yang tidak, sangatlah penting bagi perusahaan untuk menggunakan drive terenkripsi yang menggunakan firmware yang dilindungi dan ditandatangani secara digital untuk mencegah serangan ini, sehingga dapat mengurangi peluang keberhasilan penjahat siber.

> **Biaya membangun kembali infrastruktur, dan mungkin membayar uang tebusan dan pemerasan lainnya, sangat besar dibandingkan dengan harga drive USB yang terkelola. - David Clarke**

Mengapa menggunakan USB terenkripsi?

Drive terenkripsi dirancang secara khusus untuk melindungi data di dalamnya dan juga setiap perangkat yang mungkin terhubung ke drive itu sehingga menjadikannya alat yang berharga dalam koleksi perlengkapan TI di setiap organisasi. Makin canggihnya ancaman keamanan siber diimbangi oleh makin canggihnya fitur pada drive terenkripsi sehingga drive dapat tetap lebih unggul dari para penjahat siber yang berusaha mengeksploitasi berbagai perangkat itu. Hal ini terlihat pada lini produk terenkripsi perangkat keras Kingston IronKey™, pada fitur seperti enkripsi AES 256 bit dalam mode XTS yang terkuat, casing yang kuat dan tahan gangguan, firmware yang ditandatangani secara digital, keyboard virtual, mode kata sandi kompleks atau passphrase, dan fitur lainnya yang telah dikembangkan dan ditambahkan selama bertahun-tahun untuk memastikan agar pengguna benar-benar terlindungi dengan baik dari segala macam serangan.

Karena risiko siber sering sekali kurang dipahami, banyak bisnis akan memilih penggunaan drive biasa tanpa mempertimbangkan berbagai kerentanan yang ditimbulkannya. Hal yang berperan dalam kasus ini adalah ketersediaannya yang mudah diperoleh, harga yang murah, dan penggunaan enkripsi perangkat lunak, serta kurangnya proses persetujuan perusahaan untuk penggunaan flash drive. Kebijakan praktik terbaik atau proses organisasi untuk memenuhi berbagai standar TI dan keamanan siber sangat jarang ditemukan, seperti praktik terbaik tata kelola ISO27001, GDPR, SOC2, dan WISP. Ini berarti penilaian risiko sering dilakukan berdasarkan opini daripada dengan bukti sehingga menyebabkan banyak organisasi rentan terhadap serangan.

Meskipun sebagian organisasi mungkin menggunakan drive biasa dengan peralatan enkripsi perangkat lunak yang telah ada, langkah ini sering merupakan tindakan ekonomi yang keliru karena banyak drive terenkripsi perangkat lunak dapat diretas dengan alat gratis atau berbayar yang tersedia di Internet untuk siapa pun. Enkripsi perangkat lunak juga dapat dihapus dari drive dengan memformat ulang drive secara mudah oleh pengguna yang dilakukan untuk kemudahan pemakaian atau untuk menggunakan drive itu pada platform OS yang tidak didukung. Sementara itu, USB terenkripsi perangkat keras memiliki enkripsi yang selalu aktif dan tidak dapat dinonaktifkan sehingga menjadikannya tepat untuk tujuannya. Drive ini juga dibuat tahan terhadap gangguan, meninggalkan bukti jika ada upaya perusakan (tamper-evident), dan menggunakan firmware yang ditandatangani secara digital untuk memastikan keaslian dan integritas drive. Membatasi percobaan kata sandi (perlindungan serangan Brute Force) dan keyboard virtual (perlindungan dari perekam ketikan dan perekam layar) adalah dua fitur lain pada drive terenkripsi seperti IronKey VP50, yang menjadikannya memenuhi praktik terbaik di industri terhadap pelaku kejahatan yang hendak mengekstrak kata sandi dari pengguna yang tidak menyadarinya.

> Jika drive IronKey mendeteksi adanya upaya mengubah firmware, drive akan menjadi tidak berfungsi sama sekali dan tidak menyala setelah di-booting, sehingga meningkatkan keamanan siber.
> - Pasi Siukonen

Siapa yang mengalami risiko?

Setiap perusahaan yang tidak dapat mengendalikan akses USB di tempatnya pasti akan mengalami risiko. Seringnya perusahaan tidak menyadari risiko itu dengan baik. Namun, ada beberapa faktor yang dapat membuat perusahaan tertentu menjadi sasaran yang lebih menarik - dan lebih rentan - terhadap serangan siber.

Perusahaan di sektor kesehatan dan keuangan memiliki data yang tidak hanya jauh lebih menarik bagi para penjahat siber, tetapi juga berdampak lebih serius baik kepada organisasi maupun pelanggannya. Di Inggris Raya, serangan siber pada 2017 yang menargetkan Pelayanan Kesehatan Nasional (NHS) menyebabkan pembatalan lebih dari 19.000 janji pertemuan dan merugikan NHS sebesar £92 juta dalam bentuk kehilangan output dan juga biaya untuk memulihkan data dan sistem. Hal ini tidak hanya menghalangi penerimaan perawatan kesehatan dari pasien yang terdampak, tetapi NHS dikritik dengan keras karena tidak memberikan respons yang cukup besar atau cepat terhadap peringatan ancaman siber sebelumnya. Semua organisasi harus selalu mengikuti perkembangan terakhir dan terinformasikan dengan baik mengenai keamanan siber, sedangkan pihak yang menangani informasi sensitif - terutama data berkategori khusus - harus dua kali lebih waspada terhadap risiko siber.

Makin tinggi nilai perusahaan, yang diukur dengan pendapatannya, makin besar keuntungan pelaku kejahatan, sehingga makin besar pula risiko yang dihadapi dari ancaman siber. Namun, hal itu tidak berarti bahwa organisasi yang lebih kecil tidak perlu khawatir tentang keamanan siber; meskipun perusahaan besar mungkin menjadi sasaran penyerangan yang lebih menarik, perusahaan itu juga sering memiliki sumber daya dan staf khusus untuk mengatasi ancaman siber. Di sisi lain, banyak UKM tidak memiliki tim keamanan siber khusus dan membuat pengecualian bagi para eksekutif seniornya untuk mengabaikan manajemen USB sehingga menjadikan para eksekutif itu sangat rentan dengan akibat yang sangat merugikan. Beberapa studi menunjukkan bahwa perusahaan kecil dan menengah sebenarnya lebih banyak ditargetkan oleh serangan siber.

Risiko ini bahkan lebih besar bagi karyawan di posisi eksekutif senior. Individu seperti ini mudah dilacak dan sering memiliki hak istimewa eksekutif di organisasinya yang berarti bahwa kontrol siber - seperti prosedur manajemen USB - tidak diterapkan kepadanya sehingga menjadikannya target yang menguntungkan bagi penjahat siber. Di sinilah faktor seperti drive dengan enkripsi perangkat keras yang selalu aktif, pengetahuan yang baik tentang keamanan siber, serta kepatuhan pada praktik dan proses terbaik dapat sangat membantu dalam mengurangi risiko dan melindungi dari serangan.

> Banyak dari pelanggaran yang baru-baru ini terjadi dilakukan oleh pelaku jahat yang secara khusus menggunakan bantuan orang dalam, baik atas keinginan sendiri ataupun tanpa disadarinya.
> - David Clarke

Siapa yang mengalami risiko?

> Organisasi tidak berbuat cukup banyak untuk melawan ancaman keamanan siber. - David Clarke

Rantai pasok adalah titik kerentanan potensial lainnya bagi organisasi, dan serangan terhadap rantai pasok sudah sangat umum terjadi. Pada tahun 2013, perusahaan peritel AS, Target, terkena satu dari serangan pembobolan data terbesar dalam sejarah peritel, yang mengekspos informasi kartu debit dan kartu kredit dari 40 juta lebih pelanggannya. Meskipun Target sendiri sangat memperhatikan keamanan siber, dengan baru saja menginstal sistem keamanan siber yang ekstensif, enam bulan sebelum terjadinya serangan, para penyerang telah menyusup ke satu pemasok pihak ketiga dari Target, dan memperoleh akses ke jaringan data utama Target melalui pemasok itu. Secara keseluruhan, ada 90 tuntutan hukum diajukan terhadap Target, dan perusahaan mengalami kerugian sebesar 61 juta dolar dalam menanggapi pelanggaran itu. Meskipun Target mungkin tidak bertanggung jawab langsung terhadap serangan itu, kelemahan pada keamanan siber di rantai pasoknya sudah cukup untuk menyebabkan kerusakan, baik finansial maupun reputasi.

Solusi pintas karyawan juga dapat menjadi sumber kerentanan. Meskipun solusi pintas ini memungkinkan karyawan menjadi lebih efektif dalam pekerjaan sehari-harinya, namun pengabaian proses keamanan dasar dan praktik terbaik, seperti manajemen kata sandi, terlalu sering terjadi. Meskipun panduan dari NCSC dan CISA cukup mudah, seringkali panduan itu lebih sulit diterapkan dalam praktik, terutama dialami oleh anggota tim yang kurang berpengalaman dalam TI dan keamanan siber. Selain bantuan yang pasti didapatkan dari tim keamanan siber yang khusus, tindakan memberi karyawan peralatan yang tepat, seperti drive terenkripsi perangkat keras, dapat sangat membantu dalam mengurangi risiko karena solusi pintas karyawan.

> Drive USB terenkripsi perangkat keras dewasa ini mudah digunakan dan diintegrasikan ke dalam kebijakan keamanan siber yang telah ada; dari beragamnya antarmuka (grafis, keypad, layar sentuh) hingga luasnya dukungan sistem operasi, serta dengan kapasitas yang memenuhi kebutuhan setiap organisasi. - Pasi Siukonen

Bagaimana organisasi dapat mengurangi risiko serangan siber?

Dari sudut pandang organisasi, ada sejumlah hal yang dapat dilakukan untuk mengamankan titik akhir dan melindungi data. Keamanan siber akan gagal tanpa GRC atau Tata Kelola, Risiko, dan Kepatuhan (Governance, Risk, Compliance), sehingga mempelajari dan mengikuti proses adalah hal yang sangat penting bagi perusahaan untuk melindungi dirinya sendiri. Memiliki kesiapan perangkat lunak keamanan titik akhir yang kuat juga dapat meniadakan sejumlah ancaman siber. Demikian juga berupaya seresponsif mungkin menginstal patch untuk setiap kerentanan keamanan.

> **Pertanyaan apakah akan menggunakan kebijakan pemberlakuan enkripsi atau tidak adalah sama pentingnya atau bahkan mungkin lebih penting untuk manajemen risiko dengan pertanyaan apakah Anda memilih untuk mencadangkan data ... atau tidak.**
> - Pasi Siukonen

Namun, pada tingkat individu, perangkat keras terenkripsi dapat secara drastis mengurangi kerentanan terhadap ancaman keamanan siber. Dengan meningkatnya dan akan bertahannya pola kerja jarak jauh dan hybrid, terutama disertai peningkatan serangan siber tahun lalu, hal yang menjadi lebih penting dari sebelumnya adalah memastikan agar karyawan di setiap tingkat organisasi dapat menangani, mentransfer, dan membaca data perusahaan secara aman. USB terenkripsi perangkat keras memungkinkan pengguna untuk tetap mendapatkan manfaat dari portabilitas dan kesederhanaan flash drive, sambil mengurangi secara drastis risiko yang terkait dengan perangkat. Drive biasa yang hilang atau dicuri dapat mengakibatkan kehilangan data, uang, reputasi, dan lainnya, sedangkan drive terenkripsi perangkat keras dirancang untuk melindungi data sensitif dari berbagai macam serangan. Selagi penjahat siber mengembangkan cara penyerangan baru, drive terenkripsi akan terus dikembangkan untuk memenuhi tantangan baru ini.

Secara keseluruhan, biaya menangani serangan siber bisa sangat besar. Sebenarnya, meskipun penerapan dan penggunaan drive terenkripsi pada tingkat organisasi mungkin memerlukan lebih banyak keterlibatan dalam persetujuan dan pengaturan, langkah ini dapat menghemat dana perusahaan dalam jumlah besar secara jangka panjang, baik terkait biaya pemerasan maupun kehilangan pendapatan karena rusaknya reputasi. Biaya hukum karena satu kasus pelanggaran saja dapat membiayai pengeluaran tambahan membeli drive USB terenkripsi perangkat keras.

> **Melalui komitmen jangka panjang untuk menyediakan solusi USB terenkripsi yang unggul, portofolio Kingston memungkinkan setiap organisasi memenuhi konfigurasi keamanan siber mereka, seperti pemberlakuan enkripsi perangkat keras standar industri, desain yang sesuai dengan kebijakan titik akhir, dan kemampuan manajemen perangkat.** - Pasi Siukonen

Ringkasan

Di Kingston, kami selalu mengamati perkembangan di dunia keamanan siber, untuk memastikan agar drive terenkripsi IronKey kami selalu mutakhir untuk kebutuhan terbaru dan memenuhi kebutuhan keamanan siber dari organisasi besar maupun kecil. Karena keamanan siber terus menjadi perhatian yang makin meningkat secara global, kami yakin bahwa dengan kesiapan peralatan dan pengetahuan yang tepat, organisasi dapat melengkapi dirinya dengan baik untuk menghadapi tantangan ini secara langsung, sambil melindungi dirinya sendiri, karyawannya, dan pelanggannya.

Tentang Kingston

Dengan pengalaman lebih dari 35 tahun, Kingston memiliki pengetahuan untuk mengidentifikasi dan menyelesaikan tantangan data seluler Anda – memudahkan tenaga kerja untuk bekerja dengan aman tanpa mengorbankan organisasi Anda.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021

©2022 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. Hak cipta dilindungi undang-undang. Semua merek dagang dan merek dagang terdaftar adalah hak milik dari pemiliknya masing-masing.