Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Apa itu Heartbleed?
Bagaimana Bertindak?
Waspada serangan Phishing?

Heartbleed – Kenapa Harus Peduli?

Sekilas

Pada 7 April, ditemukan titik lemah pada salah satu implementasi protokol SSL yang dinamakan OpenSSL. SSL merupakan salah satu protokol keamanan sangat penting di dunia internet. SSL bukan hanya mengenkripsi komunikasi online namun juga memastikan Anda terhubung ke website yang benar pada saat melakukan layanan belanja dan perbankan online. Buletin ini memberikan ulasan sederhana perihal dampak kelemahan SSL dan tindakan perlindungan apa yang bisa dilakukan.

Editor Tamu

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) adalah Pimpinan Peneliti di CSRgroup Computer Security Consultants. Jake merupakan salah satu penulis materi pelatihan Memory Forensics (FOR526) dan Malware Reverse Engineering (FOR610) di SANS.

Apa Itu Heartbleed?

Kelemahan Heartbleed memungkinkan peretas terhubung ke webserver dan mendapatkan informasi sensitif, salah satunya adalah data userid (login) dan sandi (password). Dengan menggunakan informasi tersebut, seorang peretas bisa mengakses akun Anda. Kelemahan ini ditemukan dan diberitakan secara luas pada 7 April. Heartbleed tidak berdampak pada komputer berbasis Windows atau Mac. Heartbleed hanya berdampak pada website di internet seperti Facebook dan Gmail. Yang membingungkan adalah tidak semua website di internet terkena dampaknya. Untuk memeriksa apakah sebuah website sudah atau rawan terserang Heartbleed, gunakan https://lastpass.com/heartbleed/.

Bagaimana Bertindak?

Ada beragam langkah untuk perlindungan. Langkah ini tidak hanya membantu Anda aman dari kelemahan Heartbleed namun juga terhadap beragam serangan lainnya dimasa depan.

- Pertama, gantilah sandi pada website yang rentan, dimulai dari website yang terpenting. Jika Anda tidak yakin pada tingkat kerentanan sebuah website, lakukan saja penggantian sandi. Ini adalah saat yang tepat untuk memperbarui sandi dan meningkatkan keamanan online.
- Gunakan sandi yang kuat dan tidak mudah ditebak. Tambahan lagi, jika sebuah website memiliki fasilitas metode verifikasi dua langkah, aktifkan segera. Langkah tambahan ini perlu untuk menjadikan akun online Anda menjadi lebih aman.
- Pastikan Anda menggunakan sandi yang berbeda untuk setiap akun online. Dengan cara ini, jika salah satu akun diretas maka akun lainnya masih aman. Susah mengingat demikian banyak sandi? Itu artinya Anda memilih

Heartbleed – Kenapa Harus Peduli?

sandi dengan benar. Gunakan fasilitas pengelolaan sandi (password manager) untuk menyimpan sandi dengan aman. Fasilitas ini tidak hanya mempermudah aktifitas online namun juga menjadikannya lebih aman.

- Akun surel (email) jangan dilupakan. Jika fasilitas klien surel seperti Outlook atau Apple Mail, menggunakan SSL untuk sambungan ke server surel, Anda mungkin perlu mengganti sandinya juga.

Jika Anda membutuhkan informasi tambahan, silakan simak sumber pusataka dibagian akhir artikel ini.

Langkah perlindungan terbaik adalah mengubah sandi pada setiap akun utama dan pastikan menggunakan sandi yang kuat serta unik.

Waspada Serangan Phishing?

Pelaku kejahatan senantiasa menggunakan setiap peluang yang muncul. Mereka tahu berita Heartbleed sudah tersebar dan dibaca banyak orang termasuk Anda. Untuk itu, mereka menciptakan surel seakan-akan bersumber dari website yang Anda gunakan (bank atau belanja online). Mereka bahkan berpura-pura sebagai perusahaan keamanan menawarkan fasilitas bebas bayar guna melakukan pengecekan Heartbleed.

Taktik ini (dinamakan phishing) bukan hal baru. Mereka berusaha membujuk/memperdaya Anda agar mengakses website berbahaya atau membuka sebuah lampiran yang terinfeksi virus. Jika Anda merupakan salah satu korban taktik itu, bisa saja komputer Anda terinfeksi. Jika Anda perlu mengganti sandi, ketik (jangan mengklik alamat yang tercantum dalam surel yang dikirim kriminalis siber) alamat website (dikenal sebagai URL) kedalam browser dan lakukan perubahan sandi online. Dengan cara ini, Anda yakin akan terhubung ke website yang benar.

Sumber Pustaka

Which Sites Are Vulnerable:	https://lastpass.com/heartbleed/
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Technical Details:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Diterjemahkan oleh: T. Gunawan