Latar Belakang Toolkit Keamanan Siber GCA: Perbarui Kotak Peralatan Pertahanan Anda

Penjahat siber terus mencari cara untuk mendapatkan akses ke sistem dan data Anda. Salah satu cara untuk mencapainya adalah dengan menemukan kelemahan dalam konfigurasi atau dalam kode pengembang yang dapat direplikasi di seluruh basis pengguna dan dieksploitasi untuk keuntungan penjahat siber.

- Produsen dan pengembang perangkat lunak secara berkala merilis pembaruan sistem operasi dan aplikasi mereka untuk mengatasi kelemahan atau kerentanan yang baru ditemukan.
    - Perbaikan ini biasanya disebut sebagai tambalan, dan prosesnya dikenal sebagai penambalan.

Tambalan harus diterapkan secepatnya, dan sedapat mungkin secara otomatis, agar tambalan tidak digunakan dalam serangan siber.

- Serangan ransomware WannaCry pada Mei 2017 mengambil keuntungan dari kecacatan yang diidentifikasi dalam Sistem Operasi Windows dan memiliki konsekuensi yang menghancurkan secara global.
    - Serangan tidak menargetkan sektor tertentu, tetapi menargetkan jenis perangkat yang digunakan.
        - Serangan berdampak individual.
        - Berdampak pada organisasi kecil, menengah, dan besar.
        - Berdampak pada kepolisian, kesehatan, transportasi, telekomunikasi, layanan perbankan, dll.
    - Diperkirakan bahwa dalam waktu 24 jam, terdapat lebih dari 230.000 sistem komputer yang terdampak di 150 negara, dengan kerugian sebesar miliaran dolar AS.
- Tambalan telah dirilis oleh Microsoft pada Maret 2017 untuk semua perangkat yang didukung.
    - Mereka yang belum menerapkan tambalan sebelum serangan dimulai berisiko.
    - Mereka yang telah menerapkan tambalan (secara manual atau otomatis) tidak berisiko.
    - Mereka yang menggunakan Windows XP sangat berisiko karena Windows XP adalah produk End of Life (meskipun tambalan dengan cepat dikembangkan karena tingkat keparahan WannaCry).

End of Life

Semua perangkat dan sistem operasi memiliki tanggal 'End of Life' (Akhir Manfaat), setelah itu pemeliharaan produk tidak lagi disediakan; dukungan dihentikan, dan tidak ada tambalan lebih lanjut yang dirilis. Produk juga menjadi amat berisiko dan memiliki

berbagai kerentanan baru. Keadaan ini juga dapat terjadi jika produsen atau pembuat sistem mengakhiri usahanya dan tidak ada perusahaan lain yang mengambil alih pengembangan jajaran produknya. Contoh:

- Windows 7 melewati End of Life pada Januari 2020.
- Windows XP melewati End of Live pada April 2014.
- *Sistem yang tidak didukung harus dihapus dari jaringan, dimutakhirkan, atau diganti.*

Perangkat IoT

Pertumbuhan perangkat Internet of Things (IoT), terutama di pasar produk konsumen, seringkali keputusan membeli didasarkan pada harga, kemudahan penggunaan, fungsionalitas, dan minim keamanan, dapat menciptakan potensi titik akses bagi penyerang. Banyak perangkat yang memiliki fitur keamanan terbatas dan tidak dilengkapi kemampuan penambalan. Sehingga, apabila terdapat kekurangan, keadaan ini akan membuat jaringan Anda terbuka terhadap serangan sampai perangkat tersebut dihapus secara fisik dari jaringan atau metode mitigasi yang tepat diterapkan. Jika ada kekurangan, tindakan pencegahan yang minimal dapat dilakukan untuk mengantisipasi risiko ini.

Aplikasi lama yang tidak lagi digunakan dan peralatan warisan (peralatan lama yang telah 'diadaptasi' untuk digunakan pada jaringan atau melalui Internet) lebih baik dihapus saja. Idealnya, hal ini harus diidentifikasi dan diatasi/diperbarui saat menyelesaikan kotak peralatan 'Ketahui Aset Anda', memastikan bahwa tingkat akses minimum untuk fungsionalitas 'bisnis rutin' diterapkan.

Singkatnya:

- Tambalan/pembaruan mencakup perbaikan keamanan penting untuk melindungi dari kerentanan yang baru ditemukan dan harus segera diimplementasikan, idealnya melalui opsi pembaruan otomatis jika ini ada.
    - *Kegagalan untuk menambal secara tepat waktu akan membahayakan sistem komputer Anda – dan karenanya, organisasi Anda – berisiko.*
- Hapus perangkat yang tidak dapat ditambal (yakni, berbagai perangkat IoT konsumen) dan perangkat atau aplikasi apa pun yang tidak lagi didukung – keadaan ini mungkin menimbulkan risiko bagi organisasi Anda.
    - *Jika perangkat diperlukan untuk bisnis, isolasikan perangkat sebaik mungkin dan cegah seluruh tingkat akses internet dan akses ke perangkat lain.*
- Pastikan tingkat akses yang minimum untuk kelancaran usaha dan segera hapus akses bagi karyawan yang telah berhenti dari organisasi atau perusahaan pihak ketiga yang sudah tidak menyediakan layanan (atau pelanggan).
- Pastikan semua perangkat lunak dan sistem adalah versi terbaru – ditambal ke revisi terbaru dan ditinjau secara teratur. Selalu perbarui (update) secara berkala!

Maka, gunakan Kotak Peralatan Perbarui Pertahanan Anda! Menerapkan kebijakan yang memastikan peninjauan inventaris, rantai pasokan, dan pembaruan dilakukan secara rutin.

https://gcatoolkit.org/id/umkm/perbarui-pertahanan-anda/?_tk=memperbarui-perangkat-dan-aplikasi