TLP:CLEAR

Mengubah Keseimbangan Risiko Keamanan Siber: Prinsip dan Pendekatan untuk Aman-secara-Desain dan Bawaan

Publikasi: 13 April 2023

Badan Keamanan Siber dan Keamanan Infrastruktur

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Daftar Isi

IKHTISAR: RENTAN SECARA DESAIN

Teknologi terintegrasi ke dalam hampir setiap aspek kehidupan sehari-hari. Sistem-sistem yang menggunakan internet terhubung ke sistem-sistem kritis yang berpengaruh secara langsung terhadap kemakmuran ekonomi, mata pencaharian, dan bahkan kesehatan, mulai dari manajemen identitas pribadi hingga perawatan medis. Salah satu contohnya, penerobosan siber telah menyebabkan pembatalan operasi bedah di rumah sakit dan mengubah perawatan pasien secara global. Teknologi yang tidak aman dan kerentanan dalam sistem-sistem kritis dapat mengundang gangguan siber berbahaya, sehingga muncul potensi serius yang membahayakan keselamatan[1].

Sekarang, lebih dari sebelumnya, menjadikan Secure-by-Design (Aman-secara-Desain) dan Secure-by-Default (Aman-secara-Bawaan) sebagai titik fokus perancangan dan proses pengembangan produk merupakan hal krusial bagi produsen teknologi. Beberapa vendor telah melangkah jauh memajukan industri dalam jaminan perangkat lunak, sementara vendor-vendor lain tertinggal. Badan-badan penggagas sangat mendorong setiap produsen teknologi untuk membangun produk-produk mereka dengan cara yang dapat mencegah para pelanggan terus-menerus memantau, memutakhirkan, dan mengendalikan kerusakan pada sistem mereka guna mengurangi penyusupan siber. Para produsen didorong untuk bertanggung jawab dalam peningkatan keamanan bagi pelanggan mereka. Secara historis, produsen teknologi telah mengandalkan perbaikan kerentanan yang ditemukan setelah pelanggan menyebarkan produk, mengharuskan pelanggan untuk memperbaiki masalah tersebut dengan biaya mereka sendiri. Hanya dengan menggabungkan praktik-praktik Aman-secara-Desain kita akan memutus jahatnya siklus membuat dan menerapkan perbaikan.
Untuk mencapai keamanan perangkat lunak standar tinggi ini, badan-badan penggagas mendorong para produsen untuk memprioritaskan integrasi keamanan produk sebagai prasyarat kritis bagi fitur dan kecepatan ke pasar. Seiring waktu, tim rekayasa akan mampu mewujudkan ritme kondisi stabil baru, yaitu keamanan benar-benar terancang dan memerlukan sedikit usaha untuk pemeliharaannya. Mencerminkan perspektif ini, Uni Eropa memperkuat pentingnya keamanan produk dalam Undang-Undang Ketahanan Siber, yang menekankan bahwa para produsen harus mengimplementasikan keamanan selama masa pakai suatu produk agar menghindarkan produsen tersebut memperkenalkan produk rentan ke pasar.

Untuk menciptakan masa depan dengan teknologi dan produk-produk terkait lebih aman bagi para pelanggan, badan-badan penggagas mendorong produsen untuk memperbaiki desain mereka dan program pengembangan sehingga hanya produk Aman-secara-Desain dan Aman-

[1] Badan-badan penggagas mengakui bahwa istilah "safety" (keselamatan) memiliki makna ganda tergantung dari konteks yang digunakan. Untuk tujuan panduan ini, "safety" mengacu kepada meningkatkan standar keamanan teknologi untuk melindungi pelanggan dari aktivitas siber yang berbahaya.

secara-Bawaan yang sampai ke pelanggan. Produk-produk yang Aman-secara-Desain adalah produk yang keamanan pelanggannya menjadi tujuan bisnis utama, bukan hanya fitur teknis saja. Produk-produk Aman-secara-Desain bermula dari tujuan tersebut sebelum dimulai dengan pengembangan. Produk-produk Aman-secara-Bawaan adalah yang aman digunakan secara "dikeluarkan dari kotak" dengan sedikit atau tanpa perubahan konfigurasi dan fitur-fitur keamanan tersedia tanpa biaya tambahan. Bersama-sama, kedua prinsip ini memindahkan sebagian besar beban untuk tetap aman kepada produsen dan mengurangi peluang pelanggan menjadi korban insiden keamanan yang disebabkan oleh salah konfigurasi, tambalan kurang cepat, atau banyak masalah umum lainnya.

Badan Keamanan Siber dan Keamanan Infrastruktur (CISA), Badan Keamanan Nasional (NSA), Biro Investigasi Federal (FBI) dan mitra-mitra internasional[2] berikut ini memberikan rekomendasi dalam panduan ini sebagai kaidah bagi produsen teknologi guna memastikan keamanan pada produk mereka:

- Pusat Keamanan Siber Australia (ACSC)
- Pusat Keamanan Siber Kanada (CCCS)
- Pusat Keamanan Siber Nasional Kerajaan Inggris Raya (NCSC-UK)
- Kantor Federal untuk Keamanan Informasi Jerman (BSI)
- Pusat Keamanan Siber Nasional Belanda (NCSC-NL)
- Tim Respons Darurat Komputer Selandia Baru (CERT NZ) dan Pusat Keamanan Siber Nasional Selandia Baru (NCSC-NZ).

Badan-badan penggagas mengakui kontribusi oleh banyak mitra sektor swasta dalam mempercanggih keamanan-secara-desain dan keamanan-secara-bawaan. Produk ini ditujukan untuk melanjutkan pembahasan internasional mengenai prioritas kunci, investasi, dan keputusan yang diperlukan untuk mencapai masa depan dengan teknologi yang tidak berbahaya dan aman, serta tahan secara desain dan bawaan. Demi tujuan tersebut, badan-badan penggagas mencari umpan balik tentang produk ini dari pihak-pihak yang tertarik dan bermaksud mengadakan rapat sesi menyimak agar lebih lanjut menyaring, menetapkan, dan meningkatkan panduan kami untuk mencapai tujuan-tujuan bersama.

Untuk informasi lebih lanjut tentang pentingnya keamanan produk, bacalah artikel CISA, Akibat Teknologi Tidak Aman dan Hal Yang Bisa Dilakukan Untuk Mengatasinya .

[2] Selanjutnya disebut sebagai "badan-badan penggagas".

Aman-secara-Desain

"Secure-by-Design" (Aman-secara-Desain) berarti bahwa produk-produk yang dibangun dengan cara yang melindungi agar pelaku siber berbahaya tidak berhasil mendapatkan akses ke perangkat, data, dan infrastruktur yang tersambung. Produsen perangkat lunak harus melakukan penilaian risiko untuk mengidentifikasi dan memperhitungkan ancaman siber yang meluas ke sistem kritis, dan kemudian mencakup proteksi dalam cetak biru produk yang menjelaskan lanskap ancaman siber yang berkembang.

Praktik-praktik pengembangan teknologi informasi (TI) yang aman dan lapisan pertahanan ganda— yang dikenal sebagai defense-in-depth—juga direkomendasikan untuk mencegah aktivitas lawan dalam menyusupi sistem atau mendapatkan akses tidak sah ke data sensitif. Badan-badan penggagas merekomendasikan produsen menggunakan sebuah model ancaman yang disesuaikan selama tahap pengembangan produk untuk menunjukkan semua potensi ancaman terhadap suatu sistem dan menjelaskan setiap proses penyebaran sistem.

Badan-badan penggagas mendorong produsen untuk melakukan pendekatan holistik pengamanan bagi produk dan platform mereka. Pengembangan Aman-secara-Desain memerlukan investasi sumber daya yang signifikan dari produsen-produsen perangkat lunak di setiap lapisan desain produk dan proses pengembangan yang tidak dapat "ditambahkan" kemudian. Ini memerlukan kepemimpinan yang kuat dari eksekutif bisnis tertinggi produsen tersebut untuk menjadikan keamanan sebagai prioritas bisnis, bukan hanya fitur teknis. Kolaborasi antara para pemimpin bisnis dengan tim-tim teknis ini berlangsung sejak tahap awal perancangan dan pengembangan, hingga penyebaran oleh pelanggan dan pemeliharaan. Produsen didorong untuk melakukan tukar-pilih dan berinvestasi, termasuk hal-hal yang akan "tidak terlihat" oleh para pelanggan, seperti bermigrasi ke bahasa pemrograman yang menghilangkan kerentanan yang meluas. Mereka harus memprioritaskan fitur, mekanisme, dan implementasi alat yang melindungi pelanggan daripada fitur-fitur produk yang tampak menarik tetapi memperbesar permukaan serangan.

Tidak ada satu solusi untuk mengakhiri ancaman terus-menerus dari pelaku siber berbahaya yang mengeksploitasi kerentanan teknologi, dan produk-produk yang "Aman-secara-Desain" akan terus mengalami kerentanan; akan tetapi, sekumpulan besar kerentanan disebabkan oleh sekumpulan kecil akar masalah. Produsen harus mengembangkan kaidah tertulis agar selaras dengan portofolio produk mereka yang sudah ada dengan lebih banyak praktik Aman-secara-Desain, guna memastikan hanya akan menyimpang dalam situasi luar biasa saja.

Badan-badan penggagas mengakui bahwa bertanggung jawab atas keamanan bagi pelanggan dan memastikan level keamanan ini bagi pelanggan dapat meningkatkan biaya pengembangan. Akan tetapi, berinvestasi dalam praktik-praktik "Aman-secara-Desain" saat mengembangkan produk teknologi baru dan memelihara yang sudah ada dapat meningkatkan postur keamanan pelanggan secara substansial dan mengurangi kemungkinan disusupi. Prinsip-prinsip Aman-secara-Desain

tidak hanya menguatkan postur keamanan bagi pelanggan dan reputasi merek bagi pengembang tetapi juga menurunkan pemeliharaan dan biaya patching (tambalan) bagi produsen dalam jangka waktu lama.

Bagian Rekomendasi bagi Produsen Perangkat Lunak yang terdaftar di bawah memberikan daftar praktik-praktik pengembangan produk yang disarankan agar dipertimbangkan oleh produsen.

Aman-secara-Bawaan

“Secure-by-Default” (Aman-secara-Bawaan) artinya produk-produk tahan terhadap teknik-teknik eksploitasi yang meluas di luar batasan tanpa biaya tambahan. Produk-produk ini melindungi dari ancaman dan kerentanan paling meluas tanpa membuat pengguna akhir harus mengambil langkah tambahan untuk mengamankannya. Produk-produk Aman-secara-Bawaan dirancang untuk membuat pelanggan mengetahui bahwa ketika mereka menyimpang dari bawaan yang aman, mereka meningkatkan kemungkinan penyusupan kecuali mereka mengimplementasikan kontrol tambahan.

- Konfigurasi yang aman harus menjadi garis dasar bawaan. Produk-produk Aman-secara-Bawaan secara otomatis mengaktifkan kontrol keamanan paling penting yang dibutuhkan untuk melindungi perusahaan dari pelaku siber berbahaya, serta memberikan kemampuan untuk menggunakan dan lebih jauh mengonfigurasikan kontrol keamanan tanpa biaya tambahan.
- Kekompleksan konfigurasi keamanan tidak boleh menjadi masalah pelanggan. Staf TI organisasional sering dibebani terlalu banyak tanggung jawab keamanan dan operasional, sehingga menyebabkan terbatasnya waktu untuk memahami dan mengimplementasikan implikasi keamanan dan mitigasi yang diperlukan untuk postur keamanan siber yang kokoh. Melalui optimasi konfigurasi produk yang aman— mengamankan “default path” (jalur bawaan)— produsen dapat membantu pelanggannya dengan memastikan produk mereka diproduksi, didistribusikan, dan digunakan dengan aman sesuai dengan standar "Aman-secara-Bawaan".

Produsen produk yang "Aman-secara-Bawaan" tidak mengenakan biaya ekstra untuk mengimplementasikan konfigurasi keamanan tambahan. Sebaliknya, itu sudah termasuk dalam produk dasar seperti sabuk pengaman yang sudah termasuk dalam semua mobil baru. Keamanan bukanlah pilihan mewah tetapi lebih dekat ke standar yang diharapkan setiap pelanggan tanpa bernegosiasi atau membayar lebih.

REKOMENDASI BAGI PRODUSEN PERANGKAT LUNAK

Panduan gabungan ini memberikan rekomendasi kepada produsen agar mengembangkan sebuah kaidah tertulis untuk mengimplementasikan dan menjamin keamanan TI. Badan-badan penggagas menyarankan produsen perangkat lunak untuk mengimplementasikan strategi yang ditegaskan di bagian bawah ini untuk bertanggung jawab atas keamanan bagi pelanggan melalui prinsip-prinsip Aman-secara-Desain dan Aman-secara-Bawaan.

Prinsip-Prinsip Keamanan Produk Perangkat Lunak

Produsen teknologi didorong untuk mengadopsi sebuah fokus strategis yang memprioritaskan keamanan perangkat lunak. Badan-badan penggagas mengembangkan tiga prinsip inti berikut ini untuk memandu produsen perangkat lunak dalam membangun keamanan perangkat lunak menjadi proses desain mereka sebelum mengembangkan, mengonfigurasi, dan mengirimkan produknya.

1. Beban keamanan tidak seharusnya ditanggung oleh pelanggan. Produsen perangkat lunak harus bertanggung jawab atas hasil keamanan dari pembelanjaan pelanggannya dan dengan demikian mengembangkan produk mereka.
2. Rangkul transparansi dan akuntabilitas yang radikal. Produsen perangkat lunak harus bangga dengan memberikan produk yang tidak berbahaya dan aman, serta membedakan dirinya di antara komunitas produsen lain berdasarkan kemampuannya. Ini termasuk berbagi informasi yang mereka dapatkan dari penyebaran pelanggannya, seperti penyerapan mekanisme autentikasi yang kuat secara bawaan. Ini juga bisa mencakup komitmen kuat untuk menjamin catatan saran kerentanan serta kerentanan dan paparan umum terkait (CVE) lengkap dan akurat. Akan tetapi, berhati-hatilah dengan godaan untuk menghitung CVE sebagai metrik negatif, karena angka-angka demikian juga merupakan tanda analisis kode dan komunitas pengujian yang sehat.
3. Bangun struktur dan kepemimpinan organisasional untuk mencapai tujuan-tujuan ini. Sementara keahlian materi bidang teknis adalah hal kritis bagi keamanan produk, eksekutif senior merupakan pembuat keputusan utama bagi implementasi perubahan dalam suatu organisasi. Komitmen dari level eksekutif agar produsen perangkat lunak memprioritaskan keamanan sebagai elemen kritis pengembangan produk memerlukan pengembangan kemitraan dengan pelanggan suatu organisasi untuk memahami:
    a. Panduan skenario penyebaran produk bersama dengan model ancaman yang disesuaikan
    b. Implementasi yang diajukan untuk pengendalian keamanan harus sejalan dengan prinsip-prinsip Aman-secara-Bawaan
    c. Strategi-strategi alokasi sumber daya disesuaikan dengan ukuran perusahaan dan kemampuan mengganti praktik-praktik pengembangan warisan dengan praktik-praktik Aman-secara-Desain

d. Kebutuhan untuk mempertahankan komunikasi terbuka untuk umpan balik secara internal dan eksternal (misalnya, umpan balik karyawan dan pelanggan) mengenai isu keamanan produk. Keamanan perangkat lunak harus ditekankan di forum-forum internal (misalnya, rapat terbuka atau rapat makan siang), serta pemasaran produk eksternal dan keterlibatan pelanggan
e. Pengukuran keefektifan dalam penyebaran pelanggan. Para pimpinan eksekutif senior akan ingin tahu bagaimana investasi dalam keamanan secara desain dan bawaan membantu pelanggan dengan memperlambat laju tambalan keamanan, mengurangi galat konfigurasi, dan meminimalkan permukaan serangan.

Untuk mengaktifkan ketiga prinsip ini, produsen harus mempertimbangkan beberapa taktik operasional untuk mengembangkan proses pengembangannya.

Adakan rapat rutin dengan pemimpin eksekutif perusahaan untuk mendorong pentingnya Aman-secara-Desain dan Aman-secara-Bawaan dalam organisasi tersebut. Kebijakan dan prosedur harus didirikan untuk menghargai tim-tim produksi yang mengembangkan produk menurut prinsip-prinsip ini, yang bisa berupa penghargaan untuk mengimplementasikan praktik keamanan perangkat lunak yang luar biasa atau insentif untuk kriteria jenjang pekerjaan dan promosi.

Wujudkan pentingnya keamanan perangkat lunak bagi kesuksesan bisnis. Sebagai contoh, pertimbangkan menugaskan seorang "pemimpin keamanan perangkat lunak" atau satu "tim keamanan perangkat lunak" yang menguatkan praktik bisnis dan TI untuk mengaitkan secara langsung standar keamanan perangkat lunak dan akuntabilitas produsen. Produsen harus menjamin mereka memiliki penilaian keamanan produk yang kokoh dan independen serta program evaluasi bagi produk mereka.

Gunakan model ancaman yang disesuaikan selama pengembangan untuk memprioritaskan produk-produk paling kritis dan berdampak tinggi. Model ancaman mempertimbangkan kasus pengguna tertentu suatu produk dan memungkinkan tim pengembangan untuk membentengi produk. Akhirnya, kepemimpinan senior harus meminta pertanggungjawaban tim agar memproduksi produk yang aman sebagai elemen kunci keunggulan dan kualitas produk.

Taktik-taktik Aman-secara-Desain

Kerangka Kerja Pengembangan Perangkat Lunak Aman (Secure Software Development Framework/SSDF), juga dikenal sebagai Institut Nasional Standar dan Teknologi (NIST) SP800-218, adalah kumpulan inti praktik pengembangan perangkat lunak aman tingkat tinggi yang dapat diintegrasikan ke dalam setiap tahap daur hidup pengembangan perangkat lunak (software development lifecycle/SDLC). Mengikuti praktik ini dapat membantu produser perangkat lunak menjadi lebih efektif dalam menemukan dan menghilangkan kerentanan dalam perangkat lunak yang dirilis, memitigasi potensi dampak dari eksploitasi kerentanan, dan mengarahkan akar

masalah kerentanan untuk mencegah pengulangan nantinya.

Badan-badan penggagas mendorong penggunaan taktik Aman-secara-Desain, termasuk prinsip-prinsip yang mengacu ke praktik SSDF. Produsen-produsen perangkat lunak harus mengembangkan kaidah tertulis untuk mengadopsi lebih banyak praktik pengembangan perangkat lunak Aman-secara-Desain di sepanjang portofolio mereka. Berikut ini daftar tidak lengkap praktik terbaik kaidah ilustratif:

- Bahasa pemrograman aman memori (SSDF PW.6.1): Memprioritaskan penggunaan bahasa aman memori di mana pun sebisa mungkin. Badan-badan penggagas mengakui bahwa mitigasi spesifik memori lainnya, seperti pengacakan tata letak ruang alamat (address space layout randomization/ASLR), control-flow integrity (CFI), dan fuzzing berguna bagi basis kode warisan, tetapi tidak cukup untuk dianggap sebagai secure-by-design karena tidak cukup mencegah eksploitasi. Beberapa contoh bahasa aman memori modern termasuk C#, Rust, Ruby, Java, Go, dan Swift. Bacalah lembar informasi keamanan memori NSA lebih lanjut.
- Fondasi Perangkat Keras Aman: Masukkan fitur-fitur arsitektural yang memungkinkan proteksi memori berdetail tingkat tinggi, seperti yang dijelaskan oleh Capability Hardware Enhanced RISC Instructions (CHERI) yang dapat memperpanjang Arsitektur Perangkat Instruksi (ISA) perangkat keras konvensional. Untuk informasi lebih lanjut kunjungi, halaman web CHERI Universitas Cambridge.
- Komponen-komponen Perangkat Lunak Aman (SSDF PW 4.1): Peroleh dan pelihara komponen-komponen perangkat lunak yang diamankan dengan baik (misalnya, pustaka perangkat lunak, modul, middleware, kerangka kerja,) dari usaha yang terverifikasi, open source, dan pengembang pihak ketiga lainnya untuk memastikan keamanan kokoh dalam produk perangkat lunak pelanggan.
- Kerangka kerja templat web (SSDF PW.5.1): Gunakan kerangka kerja templat web yang mengimplementasikan pelarian otomatis input pengguna untuk menghindari serangan web seperti *cross-site scripting*.
- Kueri berparameter (SSDF PW 5.1): Gunakan kueri-kueri berparameter daripada memasukkan input pengguna dalam kueri, untuk menghindari serangan injeksi SQL.
- Pengujian keamanan aplikasi statis dan aplikasi dinamis (SAST/DAST) (SSDF PW.7.2, PW.8.2)

Gunakan alat-alat ini untuk menganalisis kode sumber produk dan perilaku aplikasi untuk mendeteksi praktik mudah-galat. Alat-alat ini menyelesaikan masalah mulai dari manajemen memori yang tidak tepat hingga konstruksi kueri basis data yang mudah galat (misalnya, input pengguna yang tidak lolos menyebabkan injeksi SQL). Alat-alat SAST dan DAST dapat dicakup ke dalam proses pengembangan dan secara otomatis berjalan sebagai bagian dari pengembangan perangkat lunak. SAST dan DAST dapat melengkapi tipe lain pengujian, seperti pengujian unit dan pengujian integrasi, guna memastikan produk mematuhi persyaratan keamanan yang

diharapkan. Ketika ditemukan masalah, produsen harus melakukan analisis akar masalah untuk mengarahkan kerentanan secara sistemik.

- Tinjauan kode (SSDF PW.7.1, PW.7.2): Berusaha memastikan bahwa kode yang dikirimkan ke dalam produk telah melalui tinjauan sejawat oleh pengembang lain demi kualitas lebih baik.
- Daftar Bahan-Bahan Perangkat Lunak (Software Bill of Materials/SBOM) (SSDF PS.3.2, PW.4.1): Masukkan pembuatan SBOM[3] untuk memberikan visibilitas ke dalam set perangkat lunak yang menjadi produk.
- Program-program pengungkapan kerentanan (SSDF RV.1.3): Selenggarakan program-program pengungkapan kerentanan agar para peneliti keamanan dapat melaporkan berbagai kerentanan dan menerima perlindungan hukum karenanya. Sebagai bagian darinya, pemasok harus menjalankan proses untuk menentukan akar masalah dari kerentanan yang ditemukan. Proses seperti itu harus mencakup penentuan apakah mengadopsi praktik Aman-secara-Desain dalam dokumen ini (atau praktik serupa) akan dapat mencegah kerentanan.
- Kelengkapan CVE: Pastikan bahwa CVE yang diterbitkan mencakup akar masalah atau enumerasi kelemahan umum (CWE) untuk mengaktifkan analisis seluruh industri dari akar masalah keamanan perangkat lunak. Walaupun proses memastikan bahwa setiap CVE benar dan komplit dapat memakan waktu ekstra, tetapi memungkinkan entitas berbeda-beda menemukan tren industri yang menguntungkan semua produsen dan pelanggan. Untuk informasi lebih lanjut tentang mengelola kerentanan, bacalah Pemangku Kepentingan CISA- pedoman SVCC khusus.
- Defense-in-Depth: Rancanglah infrastruktur agar penyusupan terhadap satu kontrol keamanan tidak menyebabkan penyusupan terhadap keseluruhan sistem. Sebagai contoh, pemastian hak khusus pengguna agak disediakan dan daftar kontrol akses bekerja dapat mengurangi dampak terhadap akun yang terganggu. Selain itu, teknik-teknik sandboxing perangkat lunak dapat mengarantina kerentanan untuk membatasi gangguan pada seluruh aplikasi.
- Penuhi Tujuan-Tujuan Kinerja Siber (CPG): Rancang produk-produk yang memenuhi praktik-praktik keamanan dasar. Tujuan-Tujuan Kinerja Keamanan Siber CISA menggarisbawahi tindakan-tindakan keamanan siber garis dasar fundamental yang harus diimplementasikan oleh organisasi. Selain itu, untuk cara lain memperkuat postur organisasi Anda, kunjungi Kerangka Kerja Penilaian Siber Inggris Raya yang mirip dengan tujuan CPG CISA. Jika suatu produsen gagal memenuhi CPG— seperti tidak mengharuskan autentikasi multifaktor anti phishing (pesan penipuan) bagi semua karyawan— maka mereka tidak dapat dianggap membuat produk Aman-secara-Desain.

[3] Sebagian badan penggagas mengeksplorasi pendekatan alternatif untuk mendapatkan jaminan keamanan dalam rantai pasokan perangkat lunak.

Badan-badan penggagas mengakui bahwa perubahan-perubahan ini merupakan pergeseran signifikan dalam sebuah postur organisasi. Dengan demikian, pengenalannya harus diprioritaskan berdasarkan kekritisan, kekompleksan, dan dampak bisnisnya. Praktik-praktik ini dapat diperkenalkan untuk perangkat lunak baru dan diperluas secara bertahap untuk meliputi kasus pengguna dan produk tambahan. Dalam banyak kasus, kekritisan dan postur risiko produk tertentu memerlukan jadwal cepat untuk mengadopsi praktik-praktik ini. Dalam kasus lain, praktik dapat diperkenalkan ke dalam basis kode warisan dan diperbaiki dari waktu ke waktu.

Taktik-taktik Aman-secara-Bawaan

Selain pengadopsian praktik pengembangan Aman-secara-Desain, badan-badan penggagas menyarankan produsen perangkat lunak agar memprioritaskan konfigurasi Aman-secara-Bawaan dalam produk mereka. Konfigurasi tersebut harus berusaha memutakhirkan produk agar sesuai dengan praktik-praktik ini seiring dilakukan penyegaran. Sebagai contoh:

- Hapuskan kata sandi bawaan: Produk tidak boleh beredar dengan kata sandi bawaan yang dibagikan secara universal. Untuk menghapus kata sandi bawaan, badan-badan penggagas menyarankan agar produk mewajibkan administrator mengatur kata sandi yang kuat selama instalasi dan konfigurasi.
    - Mandat Autentikasi Multi Faktor (MFA) untuk para pengguna khusus. Kami mengamati bahwa banyak penyebaran dalam perusahaan dikelola oleh para administrator yang belum memproteksi akun-akun mereka dengan MFA. Mengingat bahwa para administrator merupakan target nilai tinggi, produk harus membuat MFA opt-out daripada MFA opt-in. Lebih jauh, sistem sebaiknya secara teratur meminta administrator untuk mendaftarkan MFA hingga mereka berhasil mengaktifkannya di akun mereka. NCSC Belanda memiliki pedoman yang sejalan dengan pedoman CISA, kunjungi Lembar Fakta Autentikasi Sempurna mereka untuk informasi lebih lanjut.
- Sistem masuk tunggal (SSO): Aplikasi-aplikasi TI harus mengimplementasikan teknologi sistem masuk tunggal melalui standar terbuka modern. Contohnya termasuk Bahasa Markup Pernyataan Keamanan (SAML) atau OpenID Connect (OIDC). Kemampuan ini harus tersedia secara bawaan tanpa biaya tambahan.
- Log Aman: Sediakan log audit berkualitas tinggi bagi pelanggan tanpa biaya tambahan. Log audit bersifat krusial dalam mendeteksi dan meningkatkan potensi insiden keamanan. Ini pun bersifat krusial selama investigasi suatu insiden keamanan yang dicurigai atau sudah dikonfirmasi. Pertimbangkan praktik-praktik terbaik seperti menyediakan integrasi yang mudah dengan sistem informasi keamanan dan manajemen acara (SIEM) dengan akses antarmuka pemrograman aplikasi (API) yang menggunakan waktu universal terkoordinasi (UTC), format zona waktu standar, dan teknik-teknik dokumentasi yang kuat.

- Profil Otorisasi Perangkat Lunak: Pemasok perangkat lunak harus memberikan rekomendasi tentang peranan profil yang diotorisasi dan masalah penggunaan tertentu mereka. Produsen harus memunculkan peringatan yang memberitahukan pelanggan tentang naiknya risiko jika mereka menyimpang dari otorisasi profil yang disarankan. Sebagai contoh: Dokter medis dapat melihat semua rekam medis pasien, tetapi penjadwal medis memiliki akses terbatas untuk mendapatkan informasi yang diperlukan untuk menjadwalkan janji temu.
- Keamanan masa depan daripada kompatibilitas masa lampau: Terlalu sering, fitur warisan kompatibel-mundur dimasukkan, dan sering diaktifkan dalam produk-produk walaupun menimbulkan risiko bagi keamanan produk. Prioritaskan keamanan daripada kompatibilitas mundur, memberdayakan tim keamanan untuk menghilangkan fitur-fitur tidak aman bahkan jika harus melakukan perubahan.
- Lacak dan perkecil ukuran "panduan pengerasan" (hardening guide): Perkecil ukuran "panduan pengerasan" yang dibuat untuk produk dan berusaha memastikan bahwa ukuran terus berkurang seiring versi baru perangkat lunak dirilis. Integrasikan komponen-komponen "panduan pengerasan" sebagai konfigurasi bawaan pada produk. Badan-badan penggagas mengakui bahwa panduan pengerasan yang diperpendek disebabkan oleh kemitraan berkelanjutan dengan pelanggan yang ada dan termasuk usaha oleh banyak tim produk, termasuk pengalaman pengguna (UX).
- Pertimbangkan konsekuensi pengalaman pengguna akan pengaturan keamanan: Setiap pengaturan baru menaikkan beban kognitif pada pengguna akhir dan seharusnya dinilai bersamaan dengan manfaat bisnis yang diperolehnya. Idealnya, satu pengaturan seharusnya tidak ada; alih-alih, pengaturan paling aman harus dipadukan ke dalam produk secara bawaan. Ketika konfigurasi diperlukan, opsi bawaan harus aman secara luas terhadap ancaman-ancaman umum.

Badan-badan penggagas mengakui perubahan-perubahan ini dapat mempengaruhi cara perangkat lunak beroperasi. Dengan demikian, input pelanggan bersifat kritis dalam menyeimbangkan pertimbangan operasional dan keamanan. Badan-badan penggagas yakin bahwa pengembangan kaidah tertulis dan dukungan eksekutif yang memprioritaskan ide-ide ini ke dalam produk paling kritis dari organisasi merupakan langkah pertama menuju perubahan menuju praktik pengembangan perangkat lunak yang aman. Walaupun input pelanggan itu penting, badan-badan penggagas telah mengamati kasus-kasus penting di mana para pelanggan tidak ingin atau tidak mampu mengadopsi standar yang telah meningkat, seringkali protokol jaringan. Bagi produsen, menciptakan insentif bermakna bagi pelanggan agar tetap terkini dan tidak membiarkan mereka tetap rentan selamanya itu hal yang penting.

PANDUAN PENGERASAN (HARDENING GUIDE) VERSUS PANDUAN PELONGGARAN (LOOSENING GUIDE)

Panduan pengerasan dapat disebabkan oleh kurangnya kontrol keamanan produk yang melekat dalam arsitektur produk sejak awal pengembangan. Akibatnya, panduan pengerasan dapat juga menjadi jalan bagi musuh untuk menentukan dan mengeksploitasi fitur-fitur yang tidak aman. Merupakan hal yang umum bagi banyak organisasi untuk tidak menyadari panduan pengerasan, dengan demikian mereka membiarkan pengaturan konfigurasi perangkat dalam postur tidak aman. Sebuah model kebalikannya yang dikenal dengan panduan pelonggaran dapat menggantikan panduan pengerasan semacam itu dan menjelaskan perubahan mana yang harus dibuat oleh para pengguna selama mendaftar risiko-risiko keamanan yang disebabkannya.

Daripada mengembangkan panduan pengerasan yang mendaftar metode-metode untuk mengamankan produk, badan-badan penggagas menyarankan produsen perangkat lunak agar beralih ke pendekatan Aman-secara-Bawaan dengan menyediakan panduan pelonggaran. Panduan-panduan ini menjelaskan keputusan risiko bisnis dalam bahasa yang mudah dimengerti, dan dapat meningkatkan kesadaran organisasi akan risiko terhadap intrusi siber berbahaya. Tukar-pilih keamanan harus ditetapkan oleh eksekutif senior pelanggan, guna menyeimbangkan keamanan dengan persyaratan bisnis lainnya.

REKOMENDASI BAGI PELANGGAN

Badan-badan penggagas menyarankan organisasi untuk meminta pertanggungjawaban produsen teknologi pemasok mereka atas keamanan produknya. Sebagai bagian dari hal ini, badan-badan penggagas merekomendasikan bahwa para eksekutif organisasi memprioritaskan kepentingan membeli produk-produk Aman-secara-Desain dan Aman-secara-Bawaan. Hal ini terwujud melalui penetapan kebijakan yang memerlukan departemen TI menilai keamanan produsen perangkat lunak sebelum dibeli, serta memberi wewenang kepada departemen TI untuk menolak, jika perlu. Departemen TI seharusnya diberi kuasa untuk mengembangkan kriteria pembelian yang menekankan pentingnya Aman-secara-Desain dan Aman-secara-Bawaan (keduanya yang diringkas dalam dokumen ini dan lainnya yang dikembangkan oleh organisasi). Lagi pula, departemen TI harus didukung oleh manajemen eksekutif ketika memperkuat kriteria tersebut dalam membuat keputusan membeli. Keputusan-keputusan organisasi untuk menerima risiko terkait dengan produk-produk teknologi tertentu harus didokumentasikan secara formal, dan di setujui oleh seorang eksekutif bisnis senior, dan dipresentasikan secara rutin ke Dewan Direksi.

Layanan kunci IT perusahaan yang mendukung postur keamanan organisasi, seperti jaringan perusahaan, identitas perusahaan dan manajemen akses, dan operasi keamanan serta kapabilitas respons, harus tampak sebagai fungsi bisnis kritis yang didanai selaras dengan kepentingannya bagi kesuksesan misi organisasi. Organisasi-organisasi harus mengembangkan sebuah rencana untuk meningkatkan kapabilitas ini guna memanfaatkan produsen-produsen yang menganut

praktik-praktik Aman-secara-Desain dan Aman-secara-Bawaan.

Di mana pun bisanya, organisasi harus berusaha menempa hubungan kemitraan strategis dengan pemasok utama IT mereka. Hubungan semacam itu mencakup kepercayaan di berbagai level organisasi dan memberikan cara untuk menyelesaikan masalah dan mengidentifikasi prioritas bersama. Keamanan harus menjadi elemen kritis dari hubungan semacam itu dan organisasi harus berusaha memperkuat pentingnya praktik Aman-secara-Desain dan Aman-secara-Bawaan di kedua dimensi hubungan formal (misalnya, kontrak atau perjanjian vendor) dan informal. Organisasi harus mengharapkan transparansi dari pemasok teknologi mereka mengenai postur kontrol internalnya serta kaidah mereka terhadap pengadopsian praktik Aman-secara-Desain dan Aman-secara-Bawaan.

Selain menjadikan Aman-secara-Bawaan sebuah prioritas dalam suatu organisasi, pemimpin TI harus berkolaborasi dengan sejawat industri mereka untuk memahami produk dan layanan mana yang paling mencerminkan prinsip-prinsip desain ini. Para pemimpin ini harus mengkoordinasikan permintaan mereka untuk membantu produsen memprioritaskan inisiatif keamanan mendatang. Dengan bekerja sama, pelanggan dapat membantu memberikan input bermakna bagi produsen dan membuat insentif baginya untuk memprioritaskan keamanan.
Ketika memanfaatkan sistem cloud, organisasi-organisasi seharusnya memastikan mereka memahami model tanggung jawab bersama dengan pemasok teknologinya. Yakni, organisasi harus memiliki kejelasan mengenai tanggung jawab keamanan pemasok daripada tanggung jawab pelanggan saja. Organisasi harus memprioritaskan penyedia cloud yang transparan mengenai postur keamanan mereka, kontrol internal, dan kemampuan memenuhi kewajiban mereka dalam model tanggung jawab bersama.

PENAFIAN

Informasi dalam laporan ini disediakan "sebagaimana adanya" untuk tujuan yang bersifat informasi saja. CISA, dan badan-badan penggagas tidak mendukung produk komersial atau layanan apa pun, termasuk subjek analisis apa pun. Referensi apa pun untuk entitas komersial khusus atau produk komersial, proses, atau layanan oleh merek layanan, merek dagang, produsen, atau sebaliknya, bukan merupakan atau menyiratkan dukungan, rekomendasi, atau favoritisme oleh CISA dan badan-badan penggagas. Dokumen ini merupakan inisiatif bersama dari CISA yang tidak berfungsi secara otomatis sebagai dokumen pengatur.

SUMBER

CISA

- Panduan SBOM CISA
- Tujuan-Tujuan Kinerja Keamanan Siber Lintas Sektor CISA
- Garis Pedoman Mengenai Interoperabilitas Teknologi

- Mempertahankan Diri Dari Serangan Rantai Pasokan Perangkat Lunak CISA dan NIST
- Akibat Teknologi Tidak Aman dan Hal Yang Bisa Dilakukan Untuk Mengatasinya | CISA
- Berhenti Mencari Kambing Hitam untuk Keamanan Siber: Mengapa Perusahaan Harus Membangun Keamanan Pada Produk-Produk Teknologi (foreignaffairs.com) Products (foreignaffairs.com)
- Pedoman Kategorisasi Kerentanan Khusus-Pemangku Kepentingan CISA (SSVC)
- Lembar Fakta MFA Anti Phising CISA
- Pedoman Siber bagi Bisnis Kecil | CISA

NSA

- Lembar Informasi Keamanan Siber NSA tentang Keamanan Memori
- Mengamankan Rantai Pasokan Perangkat Lunak ESF NSA: Praktik Terbaik bagi Pemasok

FBI

- Memahami dan Merespons Serangan Rantai Pasokan SolarWinds: Perspektif Federal
- Ancaman Siber - Respons dan Pelaporan
- Strategi Siber FBI

Institut Nasional Standar dan Teknologi (NIST)

- Pedoman Identitas Digital NIST
- Kerangka Kerja Keamanan Siber NIST
- Kerangka Kerja Pengembangan Perangkat Lunak Yang Aman NIST (SSDF)

Pusat Keamanan Siber Australia (ACSC)

- Kode Internet untuk Segala ACSC untuk Pedoman Praktis bagi Produsen

Pusat Keamanan Siber Nasional Kerajaan Inggris Raya (UK)

- Kerangka Kerja Penilaian Siber Inggris Raya
- Panduan Pengembangan dan Penyebaran Aman NCSC UK
- Panduan Manajemen Kerentanan NCSC UK
- Toolkit Pengungkapan Kerentanan NCSC UK
- CHERI Universitas Cambridge
- Sekian dan terima kasih untuk semuanya – NCSC.GOV.UK

Pusat Keamanan Siber Kanada (CCS)

- Panduan Perlindungan Terhadap Serangan Rantai Pasokan Perangkat Lunak CCCS

- Rantai pasokan siber: Sebuah pendekatan untuk menilai risiko
- Pedoman ransomware CONTI Pusat Keamanan Siber Kanada

Kantor Federal untuk Keamanan Informasi Jerman (BSI)

- Pedoman ransomware CONTI Pusat Keamanan Siber Kanada
- Standar Internasional IEC (International Electrotechnical Commission) 62443, bagian 4-1
- Laporan Situasi Keamanan TI di Jerman, 2022
- Praktik-Praktik Keamanan Aplikasi Web BSI

Pusat Keamanan Siber Nasional Belanda

- Lembar Fakta Autentikasi Sempurna NCSC-NL

Lainnya

- Bagaimana Sistem-Sistem Kompleks Gagal
- New Look dalam kegagalan sistem kompleks