TLP:CLEAR

Mengalihkan Keseimbangan Risiko Keselamatan Siber: Prinsip-Prinsip dan Pendekatan bagi Teguh-secara-Rekabentuk dan -Lalai

Diterbitkan pada: 13 April 2023

Agensi Keselamatan Keselamatan Siber dan Infrastruktur

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

Isi Kandungan

Isi Kandungan *2*

Pengenalan: Keterdedahan Tereka 3

Teguh-secara-Tereka *5*

Teguh-secara-Lalai *6*

Syor kepada Pengeluar Perisian Komputer 7

Prinsip-Prinsip Keselamatan Produk Perisian Komputer *7*

Taktik-Taktik Teguh-secara-Tereka *9*

Taktik-Taktik Teguh-secara-Lalai *11*

Panduan Pengetatan vs Pelonggaran 13

Syor Kepada Para Pelanggan 14

Penafian 15

Sumber-Sumber Rujukan 15

PENGENALAN: KETERDEDAHAN TEREKA

Teknologi sudah diintergasikan ke dalam hampir semua sudut kehidupan seharian. Sistem-sistem yang menghadap-Internet terhubung kepada sistem-sistem kritikal yang membawa kesan secara langsung ke atas kemakmuran ekonomi, sarahidup, malah soal kesihatan kami sekali, yang merangkumi pengurusan identiti peribadi sehingga ke penjagaan perubatan. Dengan mengambil satu contoh sahaja, pelanggaran siber telah mengakibatkan pembatalan pembedahan di hospital-hospital dan melencongkan penjagaan pesakit di seluruh dunia. Teknologi yang tidak teguh dan keterdedahan dalam sistem-sistem kritikal boleh mengundang pencerobohan siber berniat jahat, yang akan membawa kepada potensi risiko-risiko keselamatan[1] yang serius.

Kini, lebih daripada dahulu, ia adalah sangat penting bagi pengeluar teknologi untuk menjadikan Teguh-secara-Tereka dan Teguh-secara-Lalai titik-titik tumpuan bagi rekabentuk produk dan proses-proses pembangunan. Sesetengah vendor sudah pun mengorak langkah meluas dalam memacu industri ke hadapan dalam penjaminan perisian komputer, manakala yang lain pula tertinggal di belakang. Pihak agensi pengarang sangat menggalakkan setiap pengeluar teknologi untuk membina produk-produk mereka dalam cara yang menghalang para pelanggan daripada perlu senantiasa melakukan pemantauan, pengemaskinian rutin, dan kawalan kerosakan sistem mereka untuk mengehadkan pencerobohan siber. Pengeluar digalakkan untuk mengambil milik tanggungjawab untuk memperbaiki hasil keselamatan pelanggan mereka. Jika dilihat selama ini, pengeluar teknologi telah bergantung kepada pembaikan keterdedahan yang ditemui selepas para pelanggan mereka telah meletakaturkan produk-produk berkenaan, yang memerlukan pelanggan tersebut untuk menerapkan penampalan-penampalan berkaitan atas perbelanjaan mereka sendiri. Kitaran penciptaan dan penerapan pembaikan yang dahsyat hanya akan dapat dipatahkan dengan menggabungkan amalan-amalan Teguh-secara-Tereka sahaja.
Untuk mencapai tahap keselamatan perisian komputer yang tinggi ini, pihak agensi pengarang menggalakkan pengeluar untuk mengutamakan pengintegrasian keselamatan produk sebagai sebuah prasyarat kritikal kepada ciri-ciri dan kepantasan ke pasaran. Lambat laun, pasukan-pasukan kejuruteraan akan berupaya untuk menubuhkan sebuah ritma keadaan-stabil baharu di mana keselamatan benar-benar direka-dalam dan memerlukan lebih kurang usaha untuk dijaga. Mengimbas kembali perspektif ini, Kesatuan Eropah menegaskan kembali kepentingan keselamatan produk dalam Akta Daya Tahan Siber (Cyber-Resilience-Act), yang menegaskan bahawa para pengeluar harus melaksanakan keselamatan di dalam keseluruhan kitaran-hidup sesebuah produk bagi menghalang para pengeluar daripada memperkenalkan produk-produk berketerdedahan ke dalam pasaran.

Untuk mencipta sebuah masa hadapan di mana teknologi dan produk-produk berkaitan adalah selamat bagi pelanggan, pihak agensi pengarang menggesa para pengeluar untuk merombak program rekabentuk dan pembangunan mereka untuk membenarkan hanya produk-produk Teguh-secara-Tereka dan -Lalai untuk dikirim kepada para pelanggan.

---

[1] Pihak agensi pengarang mengambil maklum bahawa ungkapan “selamat” memiliki pelbagai maksud bergantung kepada konteks ia diguna. Bagi tujuan panduan ini, “keselamatan” merujuk kepada peningkatan tahap kepiawaian keselamatan teknologi untuk melindungi para pelanggan daripada aktiviti siber berniat jahat.

Produk-produk yang Teguh-secara-Tereka ialah produk di mana keselamatan pelanggan merupakan sebuah matlamat teras perniagaan, bukan sekadar sebuah unsur teknikal sahaja. Produk-produk Teguh-secara-Tereka bermula dengan matlamat tersebut sebelum pembangunannya dimulakan. Produk-produk Teguh-secara-Lalai ialah produk yang teguh dan selamat untuk diguna "bila ia dikeluarkan daripada kotaknya" tanpa memerlukan, atau hanya memerlukan sedikit perubahan konfigurasi manakala ciri-ciri keselamatannya sudah pun diakan tanpa memerlukan perbelanjaan tambahan. Secara bersama, kedua-dua prinsip ini memindahkan sebahagian besar beban untuk kekal teguh kepada pihak para pengeluar dan mengurangkan peluang bagi para pelanggan untuk menjadi mangsa insiden keselamatan akibat daripada kesilapan konfigurasi, penampalan yang tidak cukup pantas, atau isu-isu lazim yang lain.

Agensi Keselamatan Siber dan Keselamatan Infrastruktur (The Cybersecurity and Infrastructure Security Agency (CISA), Agensi Keselamatan Kebangsaan (National Security Agency) (NSA), Biro Penyiasatan Persekutuan (Federal Bureau of Investigation) (FBI) dan rakan-rakan antarabangsa[2] berikut menyampaikan syor-syor dalam panduan ini sebagai satu peta jalan hala tuju bagi pengeluar teknologi untuk menjamin keselamatan produk-produk mereka:

- Pusat Keselamatan Siber Australia (Australian Cyber Security Centre) (ACSC)
- Pusat Keselamatan Siber Kanada (Canadian Centre for Cyber Security) (CCCS)
- Pusat Keselamatan Siber Kebangsaan United Kingdom (United Kingdom's National Cyber Security Centre) (NCSC-UK)
- Pejabat Persekutuan untuk Keselamatan Maklumat Jerman (Germany's Federal Office for Information Security) (BSI)
- Pusat Keselamatan Siber Kebangsaan Netherlands (Netherlands' National Cyber Security Centre) (NCSC-NL)
- Pasukan Respons Kecemasan Komputer New Zealand (Computer Emergency Response Team New Zealand) (CERT NZ) dan Pusat Keselamatan Siber Kebangsaan New Zealand (New Zealand's National Cyber Security Centre) (NCSC-NZ).

Pihak agensi pengarang mengiktiraf sumbangan sebahagian besar rakan-rakan sektor swasta dalam memajukan teguh-secara-tereka dan teguh-secara-lalai. Produk ini berhasrat untuk mengetengahkan sebuah perbualan antarabangsa tentang keutamaan-keutamaan utama, pelaburan-pelaburan, dan keputusan yang perlu untuk mencapai sebuah masa hadapan di mana teknologi adalah selamat, teguh dan berdaya tahan secara tereka dan lalai. Untuk menuju ke arah ini, pihak agensi pengarang mengalu-alukan maklumbalas terhadap produk ini daripada pihak-pihak bermiat dan berhasrat untuk mengadakan sebuah siri sesi pendengaran untuk memperhalusi, memperinci dan memajukan lagi panduan kami bagi mencapai matlamat-matlamat yang dikongsi kita bersama.

Untuk maklumat lanjut tentang kepentingan keselamatan produk, sila lihat artikel CISA, The Cost of Unsafe Technology and What We Can Do About It.

[2] Selanjutnya dirujuk di sini sebagai "pihak agensi pengarang".

Teguh-secara-Tereka

"Teguh-secara-Tereka" bererti bahawa produk-produk teknologi dibina dalam cara yang memelihara secara sewajarnya daripada pemain-pemain siber yang berniat jahat untuk berjaya mendapatkan akses kepada alat-alat peranti, data dan infrakstruktur yang terhubung. Pengeluar perisian komputer harus melaksanakan sebuah penilaian risiko untuk mengenalpasti dan membutirkan ancaman siber kepada sistem kritikal yang sedia wujud, dan kemudian memasukkan perlindungan ke dalam pelan dasar produk yang mengambil kira landskap ancaman siber yang kian berubah.

Amalan-amalan pembangunan teknologi maklumat (IT) teguh dan lapisan pertahanan berganda – yang dikenali sebagai pertahanan-secara-mendalam – juga disyorkan bagi menghalang aktiviti seteru daripada mengkompromikan sistem atau memperolehi akses tanpa izin kepada data sensitif. Para agensi pengarang mensyorkan agar pengeluar menggunakan sebuah model ancaman terukur semasa tahap pembangunan produk untuk menangani semua potensi ancaman kepada sesebuah sistem dan mengambil kira proses peletakaturan setiap sistem.

Pihak agensi pengarang menggesa pengeluar untuk mengambil pendekatan keselamatan menyeluruh bagi produk-produk dan pelantar-pelantar mereka. Pembangunan Teguh-secara-Tereka memerlukan pelaburan sumber-sumber yang signifikan oleh pengeluar perisian komputer di setiap lapisan proses merekabentuk dan pembangunan produk yang tidak boleh "dipateri masuk" nanti. Ia memerlukan kepemimpinan kuat daripada para eksekutif perniagaan tertinggi para pengeluar untuk menjadikan keselamatan satu keutamaan perniagaan, dan bukan sahaja sebuah ciri teknikal. Usahasama antara para pemimpin perniagaan dan pasukan teknikal ini melunjur dari tahap-tahap awal merekabentuk dan pembangunan, seterusnya ke peletakaturan dan penyelenggaran pelanggan. Pengeluar digalakkan untuk membuat penggantian dan pelaburan yang sukar, termasuk yang "terselindung" daripada pelanggan, contohnya pemigrasian daripada bahasa pengaturcaraan yang melenyapkan keterdedahan yang meleluasa. Mereka harus mengutamakan ciri-ciri, mekanisme-mekanisme, dan penerapan peralatan-peralatan yang melindungi pelanggan daripada ciri-ciri produk yang kelihatan menawan tapi memperluaskan ruang serangan.

Tiada satu pun penyelesaian tunggal yang ada untuk menghentikan ancaman berterusan pemain siber berniat jahat dalam mengeksploitasikan keterdedahan teknologi, dan produk-produk yang "Teguh-secara-Tereka" akan terus menghidapi keterdedahan; namun begitu, sesebuah set keterdedahan yang besar adalah disebabkan oleh sebuah sub-set penyebab akar-umbi yang agak kecil. Para pengeluar harus membangunkan peta-peta jalan hala tuju bertulis untuk menyelaraskan portfolio-portfolio produk sedia ada dengan amalan-amalan Teguh-secara-Tereka, dengan memastikan bahawa ia hanya akan menyimpang dalam keadaan-keadaan yang luarbiasa sahaja.

Pihak agensi pengarang mengambil maklum bahawa pengambilan milik tanggungjawab ke atas hasil-hasil keselamatan bagi para pelanggan dan penjaminan tahap keselamatan pelanggan ini mungkin akan menaikkan kos-kos pembangunan. Tetapi, pelaburan dalam amalan-amalan "Teguh-secara-Tereka" sambil membangunkan produk-produk teknologi baru dan mengekalkan produk-produk yang sedia ada boleh memperbaiki kedudukan keselamatan para pelanggan secara meluas dan mengurangkan kemungkinan dikompromi. Prinsip-prinsip Teguh-secara-Tereka bukan sahaja akan memperkukuhkan kedudukan

keselamatan bagi para pelanggan dan reputasi jenama bagi para pembangun tetapi juga mengurangkan kos-kos penyelenggaraan dan penampalan bagi para pengeluar dalam tempoh jangkamasa panjang.

Seksyen Syor bagi Pengeluar Perisian Komputer yang tersenarai di bawah menyediakan sebuah senarai amalan dan dasar pembangunan produk yang disyorkan bagi pertimbangan para pengeluar.

Teguh-secara-Lalai

"Teguh-secara-Lalai" bererti produk-produk berdaya tahan terhadap teknik-teknik pengeksploitasian lazim yang tidak terjangka tanpa caj tambahan. Produk-produk ini memberi perlindungan daripada kebanyakan ancaman dan kerterdedahan lazim tanpa memerlukan pengguna-akhir untuk mengambil langkah-langkah tambahan untuk memperolehinya. Produk-produk Teguh-secara-Tereka direkabentuk untuk menjadikan menyedarkan para pelanggan secara ketara bahawa bila mereka menyimpang daripada kelalaian atau default yang selamat, mereka meningkatkan kemungkinan kompromi kecuali jika mereka menerapkan kawalan-kawalan pemampasan tambahan.

- Sebuah konfigurasi teguh harus dijadikan garis asas terlalai. Produk-produk Teguh-secara-Lalai secara automatik menggerakkan kawalan-kawalan keselamatan terpenting yang diperlukan untuk memelihara pihak-pihak perusahaan daripada pemain siber berniat jahat, selain menyampaikan keupayaan untuk mengguna dan melanjutkan konfigurasi kawalan keselamatan tanpa kos-kos tambahan.
- Kerumitan konfigurasi keselamatan tidak harus menjadi masalah kepada pelanggan. Para kakitangan IT sesebuah organisasi seringkali ditambahbebankan dengan tanggungjawab keselamatan dan pengendalian, yang mengakibatkan kesuntukan masa untuk memahami dan melaksanakan implikasi dan mitigasi keselamatan yang diperlukan bagi kedudukan keselamatan siber yang kuat lagi hebat. Melalui pengoptimuman konfigurasi produk teguh – meneguhkan "laluan lalai (default)" – para pengeluar boleh membantu pelanggan mereka dengan memastikan bahawa produk-produk mereka dikeluarkan, diedarkan dan digunakan dengan selamat dengan mematuhi tahap kepiawaian "Teguh-secara-Lalai".

Pengeluar produk-produk yang "Teguh-secara-Lalai" tidak mengenakan caj tambahan bagi melaksanakan konfigurasi keselamatan tambahan. Sebaliknya, mereka akan memasukkannya ke dalam produk dasar sebagaimana tali pinggang keledar tersedia dimasukkan dalam semua kereta baharu. Keselamatan bukan sebuah pilihan kemewahan tetapi lebih dekat kepada tahap kepiawaian yang harus diharapkan oleh setiap pelanggan tanpa perlu berunding atau membayar lebih.

SYOR BAGI PENGELUAR PERISIAN KOMPUTER

Panduan bersama ini menyampaikan syor-syor kepada para pengeluar untuk membangunkan sebuah peta hala tuju bertulis bagi melaksana dan menjaminkan keselamatan IT. Agensi-agensi pengarang panduan ini mengesyorkan agar pengeluar perisian komputer melaksanakan strategi-strategi yang digariskan dalam seksyen-seksyen di bawah ini untuk mengambil milik tanggungjawab ke atas hasil-hasil keselamatan para pelanggan mereka melalui prinsip-prinsip Teguh-secara-Tereka dan Teguh-secara-Lalai.

Prinsip-Prinsip Keselamatan Produk Perisian Komputer

Pengeluar teknologi disaran untuk mendokong sebuah fokus strategik yang mengutamakan keselamatan perisian komputer. Agensi-agensi pengarang panduan ini telah membangunkan tiga prinsip teras di bawah ini sebagai panduan bagi para pengeluar perisian komputer untuk membina keselamatan perisian komputer ke dalam proses rekabentuk sebelum membangun, mengkonfigurasi dan mengirim produk-produk mereka.

1. Beban tanggungan keselamatan tidak sepatutnya terletak di atas bahu para pelanggan sahaja. Para pengeluar perisian komputer harus mengambil milik tanggungjawab ke atas soal hasil keselamatan pembelian pelanggan mereka dan mengolah produk-produk mereka dengan sewajarnya.
2. Alu-alukan ketelusan dan kebertanggungjawaban radikal. Pengeluar perisian komputer harus berbangga dengan penyampaian produk-produk selamat dan teguh, selain membezakan diri mereka daripada komuniti pengeluar yang lain berdasarkan keupayaan mereka untuk berbuat dmeikian. Ini mungkin merangkumi perkongsian maklumat yang mereka pelajari daripada peletakaturan pelanggan mereka, contohnya pengambilan mekanisme pengesahsahihan yang kuat secara lalai. Ia juga termasuk sebuah komitmen kuat untuk memastikan nasihat-nasihat keterdedahan dan rekod-rekod keterdedahan dan pendedahan (CVE) biasa berkaitan adalah lengkap dan tepat. Namun begitu, berwaspadalah terhadap keinginan untuk mengira CVE sebagai sebuah metrik negatif, memandangkan angka-angka ini juga merupakan sebuah tanda komuniti kod analisis dan ujian yang sihat.
3. Membina struktur dan kepemimpinan organisasi untuk mencapai matlamat-matlamat ini. Walaupun kepakaran bidang tajuk teknikal ialah kritikan kepada keselamatan produk, eksekutif-eksekutif kanan merupakan para pembuat keputusan utama bagi melaksanakan perubahan di dalam sesebuah organisasi. Komitmen tahap-eksekutif bagi pengeluar perisian komputer untuk mengutamakan keselamatan sebagai sebuah elemen kritikal pembangunan produk memerlukan pembangunan perkongsian bersama pelanggan sesebuah organisasi untuk memahami:
    a. Panduan senario peletakaturan produk bersama model ancaman terukur
    b. Pelaksanaan yang dicadangkan bagi kawalan keselamatan agar ia selaras dengan prinsip-prinsip Teguh-secara-Lalai
    c. Strategi-strategi peruntukan sumber yang diukur kepada saiz syarikat berkenaan dan keupayaan untuk menggantikan amalan-amalan pembangunan yang dipusakai dengan amalan-amalan Teguh-secara-Tereka

d. Keperluan untuk mengekalkan talian komunikasi terbuka bagi maklumbalas dalaman dan luaran (contohnya maklumbalas pekerja dan pelanggan) berkenaan isu-isu keselamatan produk. Keselamatan perisian komputer harus ditekankan dalam forum-forum dalaman (contohnya, all-hands atau brown bags), selain penglibaturusan pemasaran dan pelanggan produk luaran.

e. Pengukuran keberkesanan dalam peletakaturan pelanggan. Pemimpin eksekutif kanan akan ingin mengetahui di mana pelaburan dalam teguh secara tereka dan lalai sedang membantu pelanggan dengan memperlahankan kelajuan penampalan keselamatan, mengurangkan kesilapan konfigurasi, dan meminimumkan ruang serangan.

Untuk melaksanakan ketiga-tiga prinsip ini, para pengeluar harus mempertimbangkan beberapa taktik pengendalian untuk mengolah proses pembangunan mereka.

Mengadakan mesyuarat rutin bersama kepemimpinan eksekutif syarikat untuk menegaskan kepetingan Teguh-secara-Tereka dan Teguh-secara-Lalai di dalam sesebuah organisasi. Dasar-dasar dan prosedur-prosedur harus diwujudkan sebagai ganjaran kepada pasukan-pasukan pengeluaran yang membangunkan produk-produk yang mematuhi prinsip-prinsip ini, yang boleh meliputi anugerah bagi pelaksanaan amalan-amalan keselamatan perisian komputer yang luarbiasa kehebatannya atau insentif-insentif bagi tangga kerjaya dan kriteria kenaikan pangkat.

Pengendalian di sekitar kepentingan keselamatan perisian komputer bagi kejayaan perniagaan. Contohnya, pertimbangkan pelantikan seorang “pemimpin keselamatan perisian komputer” atau sebuah “pasukan keselamatan perisian komputer” yang memartabatkan amalan-amalan perniagaan dan IT yang menghubungkan tahap kepiawaian keselamatan perisian komputer dan kebertanggungjawaban pengeluar secara langsung. Pengeluar harus memastikan mereka mempunyai program-program penaksiran dan penilaian keselamatan produk yang bebas, lagi kuat dan hebat bagi produk-produk mereka.

Gunakan model ancaman terukur semasa proses pembangunan untuk mengutamakan produk-produk paling kritikal dan berimpak-tinggi. Model-model ancaman menimbangkan kes-kegunaan khusus sesesuatu produk dan membolehkan pasukan-pasukan pembangunan untuk memperkukuhkan produk-produk itu. Akhirnya, kepemimpinan kanan harus mempertanggungjawabkan pasukan-pasukan berkenaan untuk menyampaikan produk-produk teguh sebagai sebuah elemen utama kecemerlangan dan kualiti produk.

Taktik Teguh-secara-Tereka

Kerangka Pembangunan Perisian Komputer Teguh (Secure Software Development Framework) (SSDF), yang juga dikenali sebagai SP 800-218, Institut Kepiawaian dan Teknologi Kebangsaan (National Institute of Standards and Technology) (NIST), ialah satu set amalan teras bagi pembangunan perisian komputer peringkat tinggi yang boleh diintegrasikan ke dalam setiap tahap kitaran hidup pembangunan perisian komputer (software development lifecycle) (SDLC). Penurutan amalan ini boleh membantu pengeluar perisian komputer untuk menjadi lebih berkesan dalam mencari dan mengeluarkan keterdedahan dalam perisian yang dikeluarkan, mengehadkan potensi kesan terhadap pengeksploitasian keterdedahan tersebut, serta menangani penyebab akar-umbi keterdedahan ini bagi mengelakkannya daripada berulang pada masa hadapan.

Pihak agensi pengarang menggalakkan penggunaan taktik Teguh-secara-Tereka, termasuk prinsip-prinsip yang merujuk kepada amalan-amalan SSDF. Pengeluar perisian komputer harus membangunkan sebuah peta hala tuju bertulis untuk mendokong lebih banyak amalan pembangunan perisian komputer Teguh-secara-Tereka ke seluruh portfolio mereka. Berikut ialah sebuah senarai tidak muktamad tentang amalan terbaik bagi peta hala tuju yang digambarkan:

- Bahasa pengaturcaraan memori selamat (SSDF PW.6.1): Mengutamakan penggunaan bahasa memori selamat sejauh mana yang boleh. Pihak agensi pengarang mengambil maklum bahawa mitigasi khusus terhadap memori, misalnya perawakan rekaletak ruang alamat (address space layout randomization) (ASLR), integriti pengawalan-aliran (control-flow integrity) (CFI), dan 'fuzzing' adalah berguna bagi pangkalan kod lama, tetapi tidak memadai untuk dianggap sebagai teguh-secara-tereka kerana ia tidak mencukupi untuk menghalang pengeksploitasian. Beberapa contoh bahasa memori selamat moden termasuklah C#, Rust, Ruby, Java, Go, dan Swift. Sila baca risalah maklumat keselamatan memori NSA untuk butiran lanjut.
- Yayasan Perkakasan Komputer Teguh: Menggabungkan ciri-ciri senibina yang membolehkan perlindungan memori butiran-halus, seperti yang dinyatakan oleh Arahan RISC Perkakasan Keupayaan yang Dipertingkatkan (Capability Hardware Enhanced RISC Instructions) (CHERI) yang boleh melanjutkan Senibina Set Arahan (Instruction-Set Architectures) (ISAs) perkakasan komputer konvensional. Untuk maklumat lanjut, sila layari laman web CHERI Universiti Cambridge.
- Komponen Perisian Komputer Teguh (SSDF PW 4.1): Memperoleh dan mengekalkan komponen-komponen perisian komputer yang sangat-teguh (contohnya, perpustakaan perisian komputer, modul-modul, perisian tengah, kerangka-kerangka), dari pembangun komersial yang ditentusahkan, sumber terbuka dan pihak ketiga lain bagi memastikan keselamatan yang hebat dan teguh dalam produk-produk perisian komputer pengguna.
- Kerangka pencontoh sesawang (SSDF PW.5.1): Gunakan kerangka pencontoh sesawang yang menerapkan pelepasan automatik bagi input pengguna untuk mengelakkan serangan sesawang seperti penskripan silang-tapak.
- Pertanyaan berparameter (SSDF PW 5.1): Menggunakan pertanyaan berparameter daripada memasukkan input pengguna dalam pertanyaan, untuk mengelakkan serangan suntikan SQL.
- Ujian keselamatan aplikasi statik dan dinamik (SAST/DAST) (SSDF PW.7.2, PW.8.2):

  - Menggunakan peralatan ini untuk menganalisis kod sumber produk dan tingkahlaku aplikasi untuk mengesan amalan yang sering-salah. Peralatan ini meliputi pelbagai isu-isu, daripada kesalahgunaan pengurusan memori kepada pembinaan pertanyaan pangkalan data yang sering-salah (contohnya, input pengguna yang tidak terlepas yang membawa kepada suntikan SQL). Peralatan SAST dan DAST boleh digabungkan ke dalam pembangunan proses dan boleh dijalankan secara automatik sebagai sebahagian daripada pembangunan perisian komputer. SAST dan DAST harus melengkapi jenis-jenis ujian lain, misalnya ujian unit dan ujian pengintegrasian, untuk memastikan produk-produk mematuhi keperluan keselamatan yang dikehendaki. Bila isu-isu dikenalpasti, para pengeluar harus melakukan analisa penyebab akar-umbi untuk menangani pendedahan kepada bahaya secara sistematik.

- Pewasitan kod (SSDF PW.7.1, PW.7.2): Berusaha untuk memastikan agar kod yang diserahkan ke dalam produk-produk melalui pewasitan oleh pengeluar lain untuk memastikan kualiti yang lebih tinggi.
- Bil Perisian Bahan (Software Bill of Materials) (SBOM) (SSDF PS.3.2, PW.4.1): Menggabungkan pengewujudan SBOM[3] untuk menyampaikan keterlihatan ke dalam set perisian komputer yang dimasukkan ke dalam produk-produk.
- Program-program pendedahan Keterdedahan (SSDF RV.1.3): Menubuhkan program-program pendedahan keterdedahan yang membenarkan pengkaji keselamatan untuk melaporkan keterdedahan dan menerima perlindungan perundangan yang selamat dalam berbuat demikian. Sebagai sebahagian daripada hal ini, para pembekal harus mewujudkan proses-proses untuk menentukan penyebab akar-umbi bagi keterdedahan yang ditemui. Proses-proses sebegini harus termasuk juga penentuan sama ada dokongan mana-mana amalan Teguh-secara-Tereka dalam dokumen ini (atau amalan-amalan sama yang lain) sudah boleh menghalang kemasukan keterdedahan itu.
- Pelengkapan CVE: Memastikan CVE yang diterbitkan akan mengandungi pembutiran penyebab akar-umbi atau kelemahan lazim (CWE) untuk membolehkan analisis penyebab akar-umbi keselamatan perisian komputer di serata pelusuk industri. Walaupun usaha untuk memastikan setiap CVE adalah betul dan lengkap boleh memakan masa yang berlebihan, ia akan membenarkan entiti-entiti berbeza dan berasingan untuk mengesai trend-trend industri yang memanfaatkan semua pengeluar dan pelanggan. Untuk maklumat lanjut tentang pengurusan keterdedahan, sila lihat CISA's Stakeholder-specific SVCC guidance.
- Pertahanan-secara-Mendalam: Merekabentuk infrastruktur supaya pengkompromian satu kawalan keselamatan tunggal tidak akan menghasilkan pengkompromian keseluruhan sistem. Contohnya, memastikan agar hak-hak istimewa pengguna akan diperuntukkan secara ketat dan senarai-senarai kawalan akses boleh diterapkan untuk mengurangkan kesan ke atas sebuah akaun yang dikompromi. Selain itu, teknik-teknik 'sandboxing' perisian komputer boleh menguarantinakan sebuah kelemahan untuk mengehadkan pengkompromian keseluruhan sesebuah aplikasi.

[3] Sesetengah agensi pengarang sedang meneroka pendekatan-pendekatan alternatif untuk memperolehi jaminan keselamatan di sekitar rantaian bekalan perisian komputer

- Memenuhi Matlamat Prestasi Siber (Satisfy Cyber Performance Goals) (CPGs): Merekabentuk produk-produk yang memenuhi amalan-amalan keselamatan asas. CISA's Cybersecurity Performance Goals menggariskan langkah-langkah keselamatan siber asasi dan garis asas yang harus dilaksanakan organisasi-organisasi. Selanjutnya, bagi cara-cara untuk menguatkan kedudukan organisasi anda, sila lihat Kerangka Penilaian Siber UK (UK's Cyber Assessment Framework) yang berkongsi keserupaan dengan CPG-CPG CISA. Jika sesebuah pengeluar gagal untuk memenuhi CPG-CPG - misalnya dengan tidak memerlukan pengesahsahihan pelbagai-faktor yang menahan pemancingan data bagi semua pekerja – mereka kemudian tidak akan dapat dianggap sebagai menyampaikan produk-produk Teguh-secara-Tereka.

Pihak agensi pengarang mengambil maklum bahawa perubahan-perubahan ini merupakan anjakan signifikan dalam kedudukan sesebuah organisasi. Oleh yang demikian, pengenalannya harus diutamakan berdasarkan kekritikalan, kerumitan, dan kesan terhadap perniagaan. Amalan-amalan ini boleh diperkenalkan bagi perisian komputer baharu dan meluaskannya secara berperingkat untuk menampung kes-kes dan produk-produk kegunaan tambahan. Dalam sesetengah kes, kekritikalan dan kedudukan risiko sesuatu produk tertentu mungkin mewajarkan jadual yang dipercepatkan bagi mendokong amalan-amalan ini. Dalam kes lain, amalan-amalan boleh diperkenalkan ke dalam pangkalan kod yang dipusakai dan dipulihkan dalam tempoh masa yang akan datang.

Taktik-Taktik Teguh-secara-Lalai

Selain mendokong amalan-amalan pembangunan Teguh-secara-Tereka, pihak agensi pengarang mengesyorkan pengeluar perisian komputer untuk mengutamakan konfigurasi Teguh-secara-Lalai dalam produk-produk mereka. Ia harus berusaha ke arah mengemaskinikan produk-produk itu agar ia selaras dengan amalan-amalan ini bila ia dimuat semula. Contohnya:

- Melenyapkan kata laluan lalai: Produk-produk tidak harus dtang bersama kata laluan lalai yang dikongsi secara sejahat. Untuk melenyapkan kata laluan lalai, pihak agensi pengarang mengesyorkan agar produk-produk memerlukan para pentadbirnya untuk menetapkan kata laluan yang kuat semasa ia dipasang dan dikonfigurasi
    - o Memandatkan Pengesahsahihan Pelbagai-Faktor (Multifactor Authentication) (MFA) bagi penggunaan teristimewa. Kami memerhatikan bahawa ramai peletakaturan enterprise diuruskan oleh pentadbiran yang tidak melindungi akaun-akaun mereka dengan MFA. Memandangkan pentadbir merupakan sasaran nilai tinggi, produk-produk harus menjadikan MFA sesuatu untuk dipilih-keluar daripada sesuatu untuk dipilih-masuk. Seterusnya, sistem itu harus mengingatkan pentadbir secara kerap untuk mendaftar masuk ke dalam MFA sehingga mereka telah menghidupkannya dengan berjaya pada akaun mereka. NCSC Netherlands mempunyai panduan yang selari dengan panduan CISA, sila lihat Risalah Fakta Pengesahsahihan Matang (Mature Authentication Factsheet) mereka untuk mendapatkan maklumat lanjut.

- Daftar-masuk Tunggal (Single sign-on) (SSO): Aplikasi IT harus menerapkan daftar-masuk tunggal pada teknologi melalui tahap kepiawaian terbuka moden. Contohnya termasuk Bahasa Markup Penegasan Keselamatan (Security Assertion Markup Language) (SAML) atau Hubungan IDTerbuka (OpenID Connect) (OIDC). Keupayaan ini harus disediakan secara lalai tanpah sebarang kos tambahan.
- Pengelogan Teguh: Menyediakan log audit berkualiti-tinggi kepada pelanggan tanpa sebarang caj tambahan. Log audit adalah sangat penting untuk mengesan dan melonjakkan insiden-insiden keselamatan yang berpotensi berlaku. Ia juga sangat penting semasa sesuatu penyiasatan sebuah insiden keselamatan yang disyaki atau disahkan. Pertimbangkan amalan terbaik seperti menyediakan pengintegrasian mudah dengan maklumat keselamatan dan sistem-sistem pengurusan kejadian (Event Management Systems) (SIEM) dengan akses pengantaramuka pengaturcaraan aplikasi (Application Programming Interface) (API) yang menggunakan waktu universal yang diselaraskan, (Coordinated Universal Time) (UTC), pemformatan zon waktu standard, dan teknik-teknik pendokumentasian yang kuat dan hebat.
- Profil Pengesahsahihan Perisian Komputer: Pembekal perisian komputer harus menyediakan syor-syor terhadap peranan profil yang disahsahihkan dan kes penggunaannya yang sudah terpilih. Pengeluar harus meletakkan sebuah amaran jelas yang memberitahu pelanggan tentang penambahan risiko jika mereka menyimpang daripada pengesahsahihan profil yang disyorkan. Contohnya: Doktor perubatan boleh melihat semua rekod-rekod pesakit, tetapi seorang penjadual perubatan mempunyai akses terhad untuk menangani maklumat yang diperlukan untuk menjadualkan temujanji.
- Keselamatan memandang ke hadapan daripada keserasian ke belakang: Ciri-ciri yang dipusakai yang berkeserasian ke belakang terlalu kerap dimasukkan sekali, dan sering dibolehkan, dalam produk-produk walaupun ia membawakan risiko kepada keselamatan produk tersebut.
- Menjejak dan mengurangkan saiz “panduan pengetatan”: Mengurangkan saiz “panduan pengetatan” dihasilkan bagi produk-produk dan berusaha untuk memastikan bahawa saiz tersebut menyusut dengan tempoh perjalanan masa apabila versi-versi baharu perisian komputer itu dikeluarkan. Mengintegrasikan komponen-komponen “panduan pengetatan” sebagai konfigurasi lalai produk itu. Pihak agensi pengarang mengambil maklum bahawa panduan pengetatan yang dipendekkan dihasilkan daripada perkongsian berterusan dengan pelanggan sedia ada dan termasuk usaha-usaha oleh sebahagian besar pasukan-pasukan produk, termasuk pengalaman pengguna (User Experience) (UX).

- Menimbangkan akibat kesan pengalaman pengguna dalam pengesetan keselamatan: Setiap pengesetan baharu meningkatkan beban kognitif pada pengguna akhir dan harus ditaksirkan bersama dengan manfaat perniagaan yang diperolehinya. Sebaiknya, sesebuah pengesetan tidak harus wujud; sebaliknya, pengesetan paling teguh harus diintegrasikan ke dalam produk itu secara lalai. Bila pengkonfigurasian diperlukan, pilihan lalai harus diteguhkan secara umum terhadap ancaman-ancaman biasa.

Pihak agensi pengarang mengambil maklum bahawa perubahan-perubahan ini mungkin mempunyai kesan-kesan pengendalian ke atas cara bagaimana perisian komputer ini dipergunakan. Oleh yang demikian, input pelanggan ialah kritikal dalam mengimbangi pertimbangan pengendalian dan keselamatan. Pihak agensi pengarang percaya bahawa pembangunan peta jalan hala tuju bertulis dan sokongan eksekutif yang mengutamakan ide-ide ini ke dalam produk-produk paling kritikal sesebuah organisasi ialah langkah pertama kepada peralihan ke arah amalan-amalan pembangunan perisian komputer yang teguh. Walapun input pelanggan adalah penting, pihak agensi penarang telah memerhatikan bahawa kes-kes penting di mana pelanggan enggan atau tidak berupaya untuk mendokong tahap kepiawaian yang dipertingkatkan, seringkalinya protokol-protokol rangkaian. Ia penting bagi pengeluar untuk mewujudkan insentif bermakna bagi pelanggan untuk kekal bergerak bersama aliran semasa dan tidak membenarkan mereka untuk kekal terdedah selama-lamanya.

PANDUAN PENGETATAN VS PELONGGARAN

Panduan pengetatan mungkin akan menyusul daripada ketiadaan kawalan-kawalan keselamatan produk yang sedang disematkan ke dalam senibina sesebuah produk daripada permulaan pembangunannya. Akibatnya, panduan pengetatan juga boleh menjadi sebuah peta hala tuju bagi pihak seteru untuk meneliti dan mengeksploitasikan ciri-ciri yang tidak selamat. Ia menjadi kebiasaan bagi sebahagian besar organisasi untuk tidak sedar tentang panduan pengetatan, justeru ia mendedahkan pengesetan konfigurasi alat peranti di dalam sebuah kedudukan tidak selamat. Sebuah model terbalik yang dikenali sebagai panduan pelonggaran harus menggantikan panduan pengetatan sebegini serta menerangkan perubahan-perubahan yang harus dibuat oleh para pengguna sambil menyenaraikan sekali risiko-risiko keselamatan yang terhasil.

Daripada membangunkan panduan pengetatan yang menyenaraikan kaedah-kaedah pengukuhan produk-produk, pihak agensi pengarang mengesyorkan pengeluar perisian komputer untuk mengalih kepada sebuah pendekatan Selamat-secara-Lalai dengan menyediakan panduan pelonggaran. Panduan ini boleh menjelaskan risiko hasil keputusan ke atas sesuatu perniagaan dalam bahasa yang ringkas dan mudah difahami, dan boleh meningkatkan kesedaran organisasi tentang risiko pencerobohan siber berniat jahat. Penggantian keselamatan harus ditentukan oleh para eksekutif kanan pelanggan, dengan mengimbangi keselamatan dengan keperluan perniagaan yang lain.

SYOR KEPADA PARA PELANGGAN

Pihak agensi pengarang mengesyorkan organisasi untuk mempertanggungjawabkan pengeluar yang membekalkan teknologi kepada hasil-hasil keselamatan produk-produk mereka. Sebagai sebahagian daripada perkara ini, pihak agensi pengarang mengesyorkan agar eksekutif organisasi-organisasi mengutamakan kepentingan pembelian produk-produk Teguh-secara-Tereka dan Teguh-secara-Lalai. Hal ini boleh dimanifestasikan melalui pengewujudan dasar-dasar yang memerlukan jabatan-jabatan IT untuk menaksir keselamatan pengeluar perisian komputer sebelum ia dibeli, selain memperkasakan jabatan-jabatan IT untuk bertindak dengan menolak kembali jika perlu. Jabatan-jabatan IT harus diperkasakan untuk membangunkan kriteria pembelian yang menegaskan kepentingan amalan-amalan Teguh-secara-Tereka dan Teguh-secara-Lalai (kedua-duanya digariskan di dalam dokumen ini dan dokumen-dokumen lain yang dibangunkan oleh organisasi berkenaan). Lebih daripada itu, jabatan-jabatan IT harus disokong oleh pihak pengurusan eksekutif bila menguatkuasakan kriteria ini dalam keputusan-keputusan pembelian. Keputusan-keputusan organisasi untuk menerima risiko berkaitan dengan produk-produk teknologi tertentu harus didokumentasikan secara rasmi, diluluskan oleh seorang eksekutif perniagaan kanan, dan diserahkan secara kerap kepada pihak Lembaga Pengarah.

Perkhidmatan-perkhidmatan IT syarikat utama yang menyokong kedudukan keselamatan organisasi tersebut, misalnya rangkaian syarikat, identiti dan pengurusan akses syarikat, dan pengendalian keselamatan dan keupayaan respons, harus dilihat sebagai fungsi kritikal perniagaan yang dibiayai agar ia diselaraskan dengan kepentingannya kepada kejayaan misi organisasi berkaitan. Organisasi-organisasi harus membangunkan sebuah pelan untuk meningkatkan keupayaan-keupayaan ini untuk memanfaatkan pengeluar yang memeluk amalan-amalan Teguh-secara-Tereka dan Teguh-secara-Lalai.

Sejauh mana yang boleh, organisasi-organisasi harus berusaha untuk menempa hubungan perkongsian strategik dengan pembekal-pembekal IT utama mereka. Jalinan hubungan sebegeni merangkumi keyakinan di pelbagai peringkat organisasi tersebut dan menyediakan wahana bagi menyelesaikan isu-isu dan mengenalpasti keutamaan-keutamaan yang dikongsi. Keselamatan harus menjadi sebuah unsur kritikal dalam jalinan hubungan sebegini dan organisasi-organisasi harus berusaha untuk memperkuatkan kepentingan amalan-amalan Teguh-secara-Tereka dan Teguh-secara-Lali dalam kedua-dua dimensi rasmi (contohnya, perjanjian kontrak atau vendor) dan tidak rasmi hubungan berkenaan. Organisasi-organisasi harus mengharapkan ketelusan daripada pembekal teknologi mereka berkenaan kedudukan kawalan dalaman mereka selain peta jalan hala tuju mereka ke arah pendokongan amalan-amalan Teguh-secara-Tereka dan Teguh-secara-Lalai. Selain menjadikan Teguh-secara-Lalai satu keutamaan di dalam sesebuah organisasi, pemimpin IT harus berusahasama dengan rakan sejawat industri mereka untuk memahami produk-produk dan perkhidmatan-perkhidmatan mana yang merangkumi prinsip-prinsip rekabentuk ini dengan terbaik. Para pemimpin ini harus menyelaraskan permintaan mereka untuk membantu para pengeluar mengutamakan inisiatif-inisiatif keselamatan mereka yang bakal diadakan. Dengan bekerjasama, para pelanggan boleh membantu menyediakan input bermakna kepada para pengeluar dan mencipta insentif bagi mereka untuk mengutamakan keselamatan.

Apabila memanfaatkan sistem-sistem awan, organisasi-organisasi harus memastikan mereka memahami model tanggungjawab yang dikongsi bersama dengan pembekal teknologi mereka. Ini bermakna, organisasi-organisasi harus mempunyai pandangan jelas tentang tanggungjawab keselamatan pihak

pembekal dan bukan sekadar tanggungjawab pelanggan sahaja. Organisasi-organisasi harus mengutamakan penyedia awan yang telus tentang sikap keselamatan, kawalan dalaman, dan keupayaan untuk memenuhi kewajipan mereka di bawah model tanggungjawab dikongsi.

PENAFIAN

Maklumat dalam laporan ini disampaikan 'seadanya' bagi tujuan penyampaian maklumat sahaja. CISA, dan pihak agensi pengarang tidak mengendors sebarang produk atau perkhidmatan komersial, termasuk sebarang subjek analisis. Sebarang rujukan kepada entiti komersial atau produk komersial yang khusus, proses-proses, atau perkhidmatan dengan tanda perkhidmatan, jenama, pengeluar, atau sebaliknya, tidak mewakili atau membayangkan pengendorsan, cadangan, atau menyeberat sebelah oleh CISA dan pihak agensi pengarang. Dokumen ini merupakan sebuah inisiatif bersama oleh CISA dan tidak berfungsi secara automatik sebagai sebuah dokumen kawal selia.

SUMBER-SUMBER RUJUKAN

CISA

- CISA's SBOM Guidance
- CISA's Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST's Defending Against Software Supply Chain Attacks
- The Cost of Unsafe Technology and What We Can Do About It | CISA
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | CISA NSA
- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

Institut Kepiawaian dan Teknologi Kebangsaan (National Institute for Standards and Technology) (NIST)

- NIST's Digital Identity Guidelines

- NIST's Cyber Security Framework
- NIST's Secure Software Development Framework (SSDF)

Pusat Keselamatan Siber Australia (Australian Cyber Security Centre) (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

Pusat Keselamatan Siber Kebangsaan United Kingdom (UK's National Cyber Security Centre) (UK)

- The UK's Cyber Assessment Framework
- The UK NCSC's Secure Development and Deployment guidance
- The UK NCSC's Vulnerability Management guidance
- The UK NCSC's Vulnerability Disclosure Toolkit
- University of Cambridge's CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

Pusat bagi Keselamatan Siber Kanada (Canada's Centre for Cyber Security) (CCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks
- Cyber supply chain: An approach to assessing risks
- Canadian Centre for Cyber Security's CONTI ransomware guidance

Pejabat Persekutuan Negara Jerman bagi Keselamatan Maklumat (German Federal Office for Information Security) (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- State of IT-security in Germany report, 2022
- BSI practices of web application security

Pusat Keselamatan Siber Kebangsaan Netherlands (The Netherland's National Cyber Security Centre)

- NCSC-NL's Mature Authentication Factsheet

Lain-Lain

- How Complex Systems Fail
- The New Look in complex system failure