TLP:CLEAR

TEGUH SECARA TEREKA

MENGALIHKAN KESEIMBANGAN RISIKO KESELAMATAN SIBER:

PRINSIP-PRINSIP DAN
PENDEKATAN BAGI PERISIAN
TEGUH SECARA TEREKA

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Isi Kandungan

PENGENALAN: TERDEDAH SECARA TEREKA

Teknologi sudah diintergasikan ke dalam hampir semua sudut kehidupan seharian, apabila sistem-sistem yang menghadap-Internet semakin menghubungkan kita kepada sistem-sistem kritikal yang membawa kesan secara langsung ke atas kemakmuran ekonomi, sara hidup, malah soal kesihatan kita sekali, yang merangkumi pengurusan identiti peribadi sehingga ke penjagaan perubatan. Satu contoh kelemahan kesulitan sebegini ialah pencerobohan siber yang 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 yang serius[1].

Oleh yang demikian, 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 terus 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. Kami juga menggesa pengeluar perisian untuk membina produk-produk mereka dalam cara yang memudahkan pengotomasian konfigurasi, pemantauan dan pengemaskinian rutin. Pengeluar digalakkan untuk mengambil milik tanggungjawab untuk memperbaiki hasil keputusan 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 ini hanya akan dapat dipatahkan dengan menggabungkan amalan-amalan teguh secara tereka sahaja. **Nota:** Ungkapan “teguh secara tereka” merangkumi kedua-dua teguh secara tereka dan teguh secara lalai sekali.

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

[1] Pihak organisasi pengarang mengakui bahawa frasa “keselamatan” mempunyai pelbagai maksud bergantung kepada konteks ia digunakan. Bagi tujuan panduan ini, “keselamatan” akan merujuk kepada pemartabatan tahap kepiawaian keselamatan teknologi untuk melindungi pelanggan daripada kegiatan siber yang berniat jahat.

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. Lama sebelum ia dibangunkan, produk-produk yang teguh secara tereka telah dikonseptualisasikan dengan keselamatan pelanggan sebagai sebuah matlamat teras perniagaan ini, bukan sekadar sebuah unsur teknikal sahaja. Produk-produk teguh-secara-tereka bermula dengan matlamat tersebut sebelum pembangunannya dimulakan. Produk-produk sedia ada pula boleh berubah kepada satu keadaan teguh secara tereka melalui tahan pengolahan berganda. 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 berikut[2] 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)
- Pusat Keselamatan Siber Kebangsaan Norway (Norway's 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)
- Agensi Internet & Keselamatan Korea (Korea Internet & Security Agency) (KISA)
- Direktorat Siber Kebangsaan Israel (Israel's National Cyber Directorate) (INCD)
- Pusat Kebangsaan Kesiapsiagaan Kejadian dan Strategi bagi Keselamatan Siber Jepun (Japan's National Center of Incident Readiness and Strategy for Cybersecurity) (NISC) dan Pusat Penyelarasan Pasukan Respons Kecemasan Komputer Jepun (Japan Computer Emergency Response Team Coordination Center) (JPCERT/CC)
- Jaringan OAS/CICTE Pasukan Respons Kejadian Siber Kerajaan (OAS/CICTE Network of Government Cyber Incident Response Teams) (CSIRT) Rantau Amerika
- Agensi Keselamatan Siber Singapura (Cyber Security Agency of Singapore) (CSA)
- Agensi Siber dan Maklumat Keselamatan Kebangsaan Republik Czech (Czech Republic's National Cyber and Information Security Agency) (NÚKIB)

Pihak agensi pengarang mengiktiraf sumbangan sebahagian besar rakan-rakan sektor swasta dalam memajukan teguh secara tereka dan teguh secara lalai. Produk ini berhasrat untuk memajukan sebuah perbualan antarabangsa mengenai 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. Dalam 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, Kos Teknologi Tidak Selamat dan Apa Yang Kita Boleh Buat Mengenainya (The Cost of Unsafe Technology and What We Can Do About It).

[2] Selanjutnya dirujuk sebagai "organisasi pengarang" ("authoring organizations").

APA YANG BAHARU

Penerbitan awal laporan ini telah merancakkan perbincangan hebat dalam kalangan pihak industri perisian. Berita yang dilaporkan setiap hari mengenai organisasi dan individu yang dikompromi menggariskan lagi keperluan untuk mengadakan perbincangan lanjut mengenai cara bagaimana untuk menangani masalah-masalah yang kronik dan sistematik di dalam produk-produk perisian.

Selepas ia dikeluarkan pada April 2023, pihak organisasi pengarang (selanjutnya dirujuk sebagai "kami") telah menerima maklum balas yang bernas daripada ratusan individu, syarikat, dan persatuan perusahaan. Permintaan yang paling lazim dinyatakan dalam maklum balas tersebut ialah untuk menyampaikan butiran yang lebih terperinci terhadap tiga prinsip utama yang dinyatakan kerana ia berkaitan dengan kedua-dua pihak pengeluar perisian serta para pelanggan mereka. Dalam dokumen ini, kami akan mengembangkan laporan asal tersebut dan akan menyentuh tema-tema lain misalnya jumlah pengeluar dan pelanggan, kematangan pelangaan, dan skop prinsip-prinsip berkenaan.

Perisian wujud di mana-mana sahaja dan tiada satu-satunya laporan yang akan mampu meliputi keseluruhan sistem perisian, pembangunan produk perisian, atur gerak dan penyelenggaraan pelanggan, dan integrasi dengan sistem-sistem lain, secara sepenuhnya. Bagi mana-mana panduan di bawah ini yang tidak memetakan sesuatu keadaan persekitaran dengan jelas, kami akan mengalu-alukan pandangan pihak komuniti tentang bagaimana amalan-amalan yang diterangkan dalam kertas ini telah membawa kepada penambahbaikan keselamatan tertentu.

Laporan ini adalah berkaitan juga kepada pengeluaran sistem perisian dan model-model kecerdasan buatan (AI). Walaupun ia mungkin berbeza daripada rupabentuk perisian tradisional, amalan-amalan keselamatan asas masih terpakai bagai model dan sistem AI. Sesetengah amalan teguh secara tereka mungkin memerlukan modifikasi untuk mengambil kira pertimbangan yang berkaitan khusus dengan AI, namun begitu ketiga-tiga prinsip-prinsip yang merangkumi soal teguh secara tereka masih terpakai ke atas semua sistem AI.

Kami mengiktiraf bahawa usaha untuk mentransformasikan kitaran hidup pembangunan perisian (SDLC) agar ia dapat diselaraskan dengan prinsip-prinsip teguh secara tereka ini bukanlah satu tugas yang mudah dan akan memakan masa. Tambahan pula, pengeluar perisian kecil-kecilan mungkin akan berasa tercabar untuk melaksanakan sebahagian besar daripada cadangan ini. Kami percaya bahawa industri perisian perlu memastikan agar alat-alat dan prosedur-prosedur yang menjadikan produk-produk mereka lebih selamat akan disediakan secara lebih meluas. Dengan adanya semakin ramai individu dan organisasi yang menumpukan perhatian mereka ke arah penambahbaikan keselamatan perisian, kami percaya bahawa terdapat ruang bagi penginovasian yang akan merapatkan jurang antara pengeluar yang lebih besar dan yang lebih kecil bagi manfaat semua pelanggan mereka.

Pengemaskinian kepada laporan teguh secara tereka yang asal ini ialah sebahagian daripada komitmen kami untuk membina perkongisan bersama ramai daripada komuniti pemegang taruh yang saling terhubung yang menjadi landasan bagi ekosistem teknologi kami. Ianya adalah hasil daripada maklum balas yang diterima daripada sebahagian besar ekosistem tersebut, dan kami akan terus mendengar dan belajar daripada perspektif-perspektif tersebut. Walaupun terdapat pelbagai cabaran di hadapan, kami berasa sangat optimistik bila kita semakin belajar mengenai para individu dan organisasi yang telah mendokong sebuah falsafah teguh secara tereka, seringkali dengan berjaya.

BAGAIMANA UNTUK GUNA DOKUMEN INI

Kami menggesa agar para pengeluar perisian untuk mematuhi prinsip-prinsip yang termaktub dalam dokumen ini. Pengeluar perisian boleh menunjukkan komitmen mereka dengan mendokumentasikan tindakan yang diambil mereka secara umum, selaras dengan langkah-langkah yang disenaraikan di bawah ini. Kami menggalakkan pengeluar perisian untuk mencari taktik-taktik yang menepati semangat prinsip ini dan mencipta artifak yang akan membina sebuah kes yang akan menyakinkan baik pelanggan semasa mahupun yang akan datang yang masih berasa waswas, bahawa mereka sedang mengabadikan falsafah teguh secara tereka.

Selain tindakan yang patut diambil oleh para pengeluar perisian, para pelanggan juga boleh mempermanfaatkan dokumen ini. Syarikat yang membeli perisian mesti menanyakan soalan mendalam kepada vendor-vendor mereka, dengan berinspirasikan contoh-contoh pematuhan prinsip yang tersenarai dalam dokumen ini. Dengan cara demikian, para pelanggan boleh membantu dalam mengalihkan pasaran ke arah produk-produk yang lebih teguh secara tereka. Satu contoh soalan yang pelanggan boleh bertanya kepada vendor mereka diberi di dalam Panduan bagi Pemerolehan Teknologi K-12 (Guidance for K-12 Technology Acquisitions) CISA.

Kami menggalakkan pelanggan perusahaan untuk memasukkan amalan-amalan ini ke dalam proses-proses pemerolehan, penilaian usaha wajar vendor, keputusan penerimaan risiko perusahaan, dan langkah-langkah lain yang diambil ketika menilai para vendor. Para pelanggan juga patut mendesak vendor mereka untuk mendokumentasikan secara umum langkah-langkah teguh secara tereka yang diambil oleh setiap vendor. Secara keseluruhannya, ini akan mewujudkan sebuah isyarat permintaan yang kuat bagi keselamatan, yang akan menggalakkan dan membenarkan pengeluar perisian untuk mengambil langkah ke arah keselamatan yang lebih meluas. Dalam erti kata lain, dalam kita mengejar untuk mewujudkan sebuah falsafah teguh secara tereka yang menyakinkan dalam kalangan pengeluar perisian, kami juga perlu mewujudkan sebuah budaya “teguh secara permintaan” dengan pelanggan mereka.

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 seterusnya 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 tukar ganti dan pelaburan yang sukar, termasuk yang "terselindung" daripada pelanggan (contohnya pemigrasian daripada bahasa pengaturcaraan yang menyingkirkan keterdedahan yang meleluasa). Mereka patut mengutamakan ciri-ciri, mekanisme dan pelaksanaan peralatan yang akan melindungi pelanggan, daripada ciri-ciri produk yang dianggap menawan tetapi memperluaskan permukaan yang terdedah kepada 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 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 keputusan 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 postur keselamatan para pelanggan secara meluas dan mengurangkan kemungkinan dikompromi. Prinsip-prinsip teguh secara tereka bukan sahaja akan memperkukuhkan postur 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 Saranan 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 lalai 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. Teguh secara lalai ialah satu bentuk teguh secara tereka.

- 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 postur keselamatan siber yang kuat lagi hebat. Para pengeluar boleh membantu pelanggan mereka dengan mengoptimumkan konfigurasi produk teguh – meneguhkan "laluan lalai" (default path) - 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.

SARANAN-SARANAN BAGI PENGELUAR PERISIAN

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 keputusan keselamatan para pelanggan mereka melalui prinsip-prinsip Teguh secara Tereka dan Teguh secara Lalai.

PRINSIP KESELAMATAN PRODUK PERISIAN

Para 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

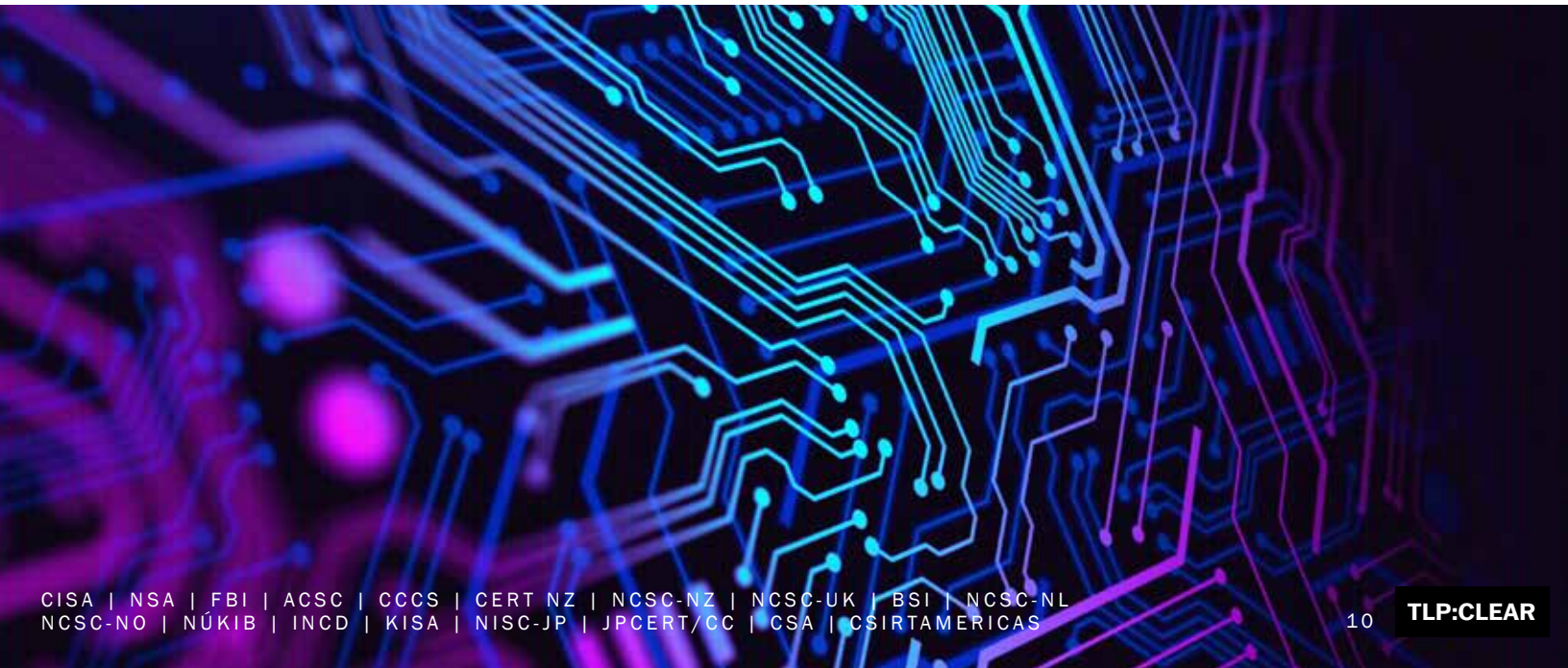
Mengambil milik tanggungjawab ke atas soal hasil keputusan keselamatan pelanggan dan mengolah produk-produk dengan sewajarnya. Beban tanggungan keselamatan tidak sepatutnya terletak di atas bahu para pelanggan sahaja.

2

Mencakupi 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 demikian. 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 kritikal kepada keselamatan produk, eksekutif-eksekutif kanan merupakan para pembuat keputusan utama bagi melaksanakan perubahan di dalam sesebuah organisasi. Para eksekutif perlu mengutamakan keselamatan sebagai sebuah elemen kritikal pembangunan produk di keseluruhan organisasi tersebut, dan dalam perkongsian bersama para pelanggan mereka.



Untuk menghidupkan 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.

Lakukan pengendalian di sekitar kepentingan keselamatan perisian komputer bagi menjayakan 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. Akhir sekali, kepemimpinan kanan harus mempertanggungjawabkan pasukan-pasukan berkenaan untuk menyampaikan produk-produk teguh sebagai sebuah elemen utama kecemerlangan dan kualiti produk.

Sebagai sebahagian daripada pengemaskinian Oktober 2023 kepada panduan ini, ketiga-tiga prinsip ini dikembangkan lagi menerusi keterangan, demonstrasi, dan kesan bukti berikut.

PRINSIP 1: Mengambil Milik Hasil Keputusan Keselamatan Pelanggan

KETERANGAN

Amalan terbaik moden menetapkan bahawa pengeluar perisian melabur dalam usaha keselamatan produk yang termasuk **pengerasan pengaplikasian, ciri-ciri pengaplikasian,** dan pengaplikasian **pengesetan lalai.**

Pengeluar perisian perlu melaksanakan **pengerasan aplikasi** dengan menggunakan proses dan teknologi yang meningkatkan kos bagi sesebuah pelaku yang berniat jahat untuk mengkompromikan aplikasi. Pengaplikasian protokol dan prosedur pengerasan yang menolong produk untuk menahan serangan daripada pelaku pintar yang berniat jahat. Terma-terma seperti pengerasan, keselamatan produk, dan daya tahan kesemuanya berkait rapat dengan kualiti produk. Idenya ialah bahawa keselamatan mesti "dibenamkan" dan bukan sekadar "dipateri". [1] Dengan membenamkan keselamatan, pengeluar perisian bukan sahaja boleh meningkatkan keselamatan pelanggan mereka tetapi juga meningkatkan kualiti produk mereka. Contoh taktik-taktik ini termasuklah dalam memastikan input pengguna ditentusah dan dibersihkan, dan tidak dimasukkan secara langsung ke dalam kod (iaitu, sebaliknya dengan menggunakan soalan berparameter), menggunakan bahagian pengaturcaraan beringatan selamat (memory safe programming language), pengurusan kitaran hidup pembangunan perisian komputer (SDLC), dan menggunakan pengurusan kunci kryptografik yang disokong perkakasan.

Aplikasi perlu menyokong **ciri-ciri pengaplikasian** yang berkaitan keselamatan siber. Kadangkalanya dipanggil "keupayaan", ciri-ciri ini melanjutkan pengfungisan sesebuah produk atau perkhidmatan dalam cara yang menolong mengekalkan atau meningkatkan postur keselamatan seseorang pelanggan.

Contoh ciri-ciri berkaitan keselamatan termasuk menyokong keselamatan lapisan pengangkutan (transport layer security) (TLS) bagi semua sambungan jaringan, sokongan daftar diri tunggal (single sign on) (SSO), keselamatan pengesahsahihan pelbagai faktor (multi-factor authentication) (MFA), pengelogan odit kejadian keselamatan, kawalan akses berdasarkan peranan (role-based access control) (RBAC), dan kawalan akses berdasarkan-pengunsuran (attribute-based access control) (ABAC).

Sebahagian ciri-ciri produk ini boleh dikonfigurasikan yang membenarkan pelanggan untuk mengintegrasikan produk tersebut dengan lebih mudah ke dalam persekitaran dan aliran kerja sedia ada. Konfigurasi ini bererti aplikasi mesti memastikan **pengesetan lalai** ditetapkan sehingga para pelanggan mengkonfigurasikannya sendiri. Pengesetan lalai berkenaan perlu ditetapkan secara teguh "di luar kotak" supaya para pelanggan tidak akan perlu memanjangkan sumber-sumber secara berlebihan untuk menjadikan timbunan produk teknologi mereka lebih selamat.

Setiap elemen ini – pengerasan aplikasi, ciri-ciri keselamatan aplikasi, dan pengesetan lalai aplikasi – memainkan sebuah perana di dalam keselamatan aplikasi tersebut, dan hasil postur keselamatan pihak pelanggan. Pengeluar perisian patut memikirkan mengenai setiap satu daripada elemen ini dan bagaimana ianya terkait antara satu sama lain. Para pengeluar patut memikirkan lebih daripada soal pelaburan mereka sahaja untuk memasukkan elemen-elemen ini ke dalam produk mereka. Para pengeluar patut mengambil langkah seterusnya dan mempertimbangkan cara bagaimana elemen-elemen tersebut mengubahkan postur keselamatan dunia sebenar pelanggan mereka, biar apa pun baik-buruk kesannya.

Para pengeluar patut mengambil milik hasil keputusan keselamatan pelanggan mereka, daripada sekadar mengukur diri mereka sendiri hanya berdasarkan usaha dan pelaburan mereka. Tanggungjawab ini sepatutnya diletakkan di bahagian hulu, iaitu pada pihak pengeluar, di mana ia mempunyai kemungkinan terbesar untuk mengurangkan peluang pengkompromian.

Malangnya, ini bukannya apa yang sedang berlaku pada ketika ini. Terlalu ramai pengeluar meletakkan beban keselamatan ke atas bahu pelanggan, daripada melabur di dalam **pengerasan aplikasi yang komprehensif.** Contohnya, apabila pengeluar menampalkan satu keterdedahan, kami sering melihat pendedahan keterdedahan yang sama kerana mereka telah menangani petanda gejalanya dan bukan punca kekurangan tersebut itu sendiri. Produk tersebut mungkin akan melaksanakan mitigasi berbeza dalam pelbagai bahagian dasar kod bagi kelas keterdedahan yang sama. Sebagai satu contoh, selepas pengeluar membaiki satu keterdedahan pembersihan input, penyelidik atau penyerang telah menemui laluan kod yang tidak menerima manfaat daripada pembersihan input yang diperbaiki. Pengeluar menerapkan satu pembaikan setiap kali dan bukannya menyatukan asas kod untuk menyingkirkan kelas keterdedahan tersebut di serata aplikasi tersebut.

Ciri-ciri aplikasi boleh mewujudkan manfaat mahupun risiko bagi pelanggan. Ciri-ciri yang membenarkan titik-titik integrasi kepada lebih banyak sistem dan versi boleh meningkatkan lagi nilai sesuatu produk dengan lebih hebat. Tetapi namun begitu, menyokong ciri-ciri tanpa pelan persaraan, seperti sebuah protokol penjaringan, boleh menjadikan pelanggan terdedah jika mereka tidak memilik pemahaman mengenai implikasi penggunaan berterusan ciri tersebut. Contohnya, sesetengah produk masih menggunakan protokol penjaringan yang berasal daripada zaman 1990an atau 2000an yang kini diketahui sememangnya tidak selamat. Terdapat pelbagai faktor yang boleh melambatkan cara bagaimana pelanggan boleh mempercepatkan penaiktarafan dan pengaturgerakan langkah-langkah keselamatan moden. Mereka mungkin menggunakan produk yang diintegrasikan dengan jaringan lain organisasi tersebut, tetapi tidak mempunyai langkah-langkah keselamatan moden, yang menghalang pasukan IT daripada pemodenan. Biarpun begitu, pengeluar perisian boleh mengambil kira rekacorak ini ke dalam proses perancangan mereka untuk menggalakkan pelanggan untuk kekal dengan pengemaskinian semasa.

Pengesetan lalai aplikasi ialah satu bidang tambahan yang mempunyai potensi risiko kepada para pelanggan. Pengeluar sering memilih pengesetan lalai tertentu, yang menjadikannya lebih mudah bagi pelanggan untuk menggunakan ciri-ciri aplikasi yang mereka mahu. Malangnya, amalan ini memperluaskan permukaan serangan bagi pelanggan yang mungkin tidak akan memerlukan ciri-ciri dan protokol tertentu yang telah dihidupkan secara lalai. Tambahan pula, sebahagian besar kawalan keselamatan ditogolkan secara lalai atau memerlukan pelanggan untuk mengambil masa untuk mengkonfigurasikan pengesetan mereka untuk meningkatkan keselamatan. Pemodelan ancaman nyata ialah satu taktik yang mungkin membantu dalam memaklumkan keputusan tentang ciri-ciri mana yang patut dihidupkan secara lalai atau pengesetan mana yang diperlukan untuk diteguhkan secara lalai. Satu taktik lagi pula ialah untuk menyiasat cara-cara bagaimana untuk menjadikan ciri-ciri lebih mudah ditemui oleh pihak pentadbir.

Sesetengah pengeluar menghantar produk berkelalaian yang boleh mewujudkan risiko kepada sesetengah atau malah kesemua pelanggan mereka. Daripada mengesetkan kelalaian yang lebih selamat, mereka sering memilih untuk mengeluarkan sebuah **panduan pengerasan** yang mesti dilaksanakan oleh pihak pelanggan atas tanggungan perbelanjaan mereka sendiri. Panduan pengerasan sering dirundung beberapa masalah biasa. Sesetengah panduan pengerasan sukar dicari dan tidak disokong dengan baik. Yang lain pula rumit untuk dilaksanakan, dan kadangkala memerlukan pembangunan perisian untuk menulis sebuah modul lanjutan. Biarpun begitu, yang lain menganggap bahawa pembacanya memiliki pengalaman keselamatan siber yang meluas untuk memahami cara-cara bagaimana pelbagai pengesetan mengubah permukaan serangan. Para pengamal yang tidak memiliki pemahaman penuh mengenai cara-cara bagaimana penyerang bekerja mungkin akan gagal untuk melaksanakan arahan panduan pengerasan dengan wajar, khususnya jika arahan tersebut tidak menerangkan "trade off" dengan jelas. Selanjutnya, tidak semua panduan pengerasan ditulis oleh jurutera yang mengenali taktik-taktik dan ekonomi-ekonomi penyerang secara rapat, dan ini menyebabkan mereka untuk mewujudkan panduan pengerasan yang tidak berkesan walaupun ia diterapkan dengan sewajarnya. Berjuta-juta pelanggan sedang mengambil alih tanggungjawab untuk memperkukuhkan pelbagai contoh perisian atau sistem, seringkali di dalam persekitaran sumber berkekangan. Bergantung kepada panduan pengerasan sahaja tidak serupa sama sekali.

Pengesetan sesebuah aplikasi patut dinilai secara berterusan untuk mengetahui sama ada pengesetan itu telah dibuat secara lalai atau disetkan oleh pelanggan, berlatarkan pemahaman semasa pengeluarnya mengenai landskap ancaman yang ada. Aplikasi patut dibuat dengan petunjuk jelas mengenai potensi risiko yang mungkin terjadi akiba pengesetan itu dan patut menjadikan petunjuk itu mudah diketahui. Seperti juga kereta moden yang mempunyai petunjuk amaran mengenai tali pinggang keledar dan menyatakan petunjuk itu dengan membunyikan sebuah amaram jika anda cuba untuk memandu tanpa memasang tali pinggang keledar anda, perisian juga patut menyatakan petunjuk mengenai keadaan keselamatan sesebuah sistem. Jika sebuah aplikasi dikonfigurasi supaya ia tidak memerlukan MFA bagi akaun-akaun pentadbir, ia patut menyedarkan para pentadbir secara berkala bahawa mereka dan seluruh organisasi mereka berada di dalam keadaan merbahaya jika mereka tidak menkonfigurasikan MFA. Tambahan pula, jika sesebuah aplikasi dikonfigurasi untuk menyokong protokol-protokol lebih tua yang kini diketahui sedang menerapkan kriptografi lemah, ia patut menjelaskan secara berkala kepada pihak pentadbir bahawa organisasi tersebut sedang berada di dalam keadaan merbahaya dan menyediakan sumber-sumber untuk menyelesaikan keadaan ini. Kami menggesa pengeluar untuk melaksanakan teguran rutin yang dibina ke dalam produk itu dan bukannya bergantung kepada para pentadbir untuk meluangkan masa, kepakaran, dan kesedaran untuk menafsirkan panduan pengerasan. Peluang jelas wujud untuk penginovasian bagi mengimbangi pertimbangan keselamatan dan kebergunaan.

Setiap satu daripada elemen-elemen di atas mewujudkan sebuah keadaan yang tidak boleh diterima di mana pelanggan perlu menyelidik, membiaya, membeli, mendapatkan kakitangan, mengaturgerak, dan memantau **produk keselamatan** tambahan untuk mengurangkan peluang pengkompromian. Organisasi saiz kecil dan sederhana (small and medium sized organisations) (SMOs) umumnya tidak berupaya untuk memudahcarakan pilihan-pilihan ini. Mereka menghadapi kekurangan dalam kepakaran, pembiayaan, dan masa yang membebankan bandwith dan fungsi, yang memaksa keselamatan ke keutamaan yang lebih rendah, dan, dalam agregatnya, memburukkan lagi risiko bersama. Sebaliknya, pelaburan keselamatan oleh sekitar beberapa pengeluar akan seterusnya berskala. Satu frasa biasa yang meringkaskan masalah ini ialah bahawa industri perisian memerlukan produk lebih kukuh, bukan lebih banyak produk keselamatan. Pengeluar perisian patut menerajui transformasi itu.

> ***Industri perisian memerlukan produk lebih teguh, bukan lebih banyak produk keselamatan. Pengeluar perisian patut menerajui transformasi itu.***

Hari ini, kita kadangkala membaca komen daripada pengeluar yang menjelaskan bahawa seseorang pelanggan telah dikompromi kerana mereka tidak menghidupkan sesuatu ciri keselamatan yang khusus, atau menurut panduan pengerasan tertentu. Sebaliknya, selepas sebuah kompromi berlaku, pengeluar patut menjelaskan sama ada sesuatu ciri keselamatan khusus atau panduan pengerasan khusus berupaya untuk menghalang kompromi tersebut dahulu dan mempertimbangkan untuk menjadikannya satu kelalaian tanpa sebarang caj. Dalam kes-kes tersebut di mana produk tersebut tidak dikeraskan dengan sepenuhnya dalam fasa-fasa perekaan dan pelaksaan, pengeluar patut menjelaskan bahawa mereka sedang berusaha untuk menyingkirkan kelas keterdedahan tersebut daripada talian produk mereka.

Pengeluar perisian mempunyai sebuah tanggungjawab untuk menentukan bahawa produk-produk mereka direka dan dibangunkan dengan keselamatan sebagai satu keutamaan tinggi. Ke arah itu, mereka patut **mengukur keputusan usaha-usaha mereka di lapangan secara objektif**. Kami menyeru pengeluar untuk tidak sahaja memfokus kepada usaha dalaman mereka, tetapi untuk mengukur dan melapor secara objektif dan berkala hasil dan keberkesanan usaha keselamatan dan konfigurasi sesuatu produk, dan untuk membina sebuah lingkaran maklumbalas yang mewujudkan perubahan dalam SDLC yang membawa kepada penambahbaikan yang boleh diukur dalam keselamatan pelanggan dan produk yang lebih teguh. Pelaporan patut mengandungi data yang dianonimkan yang boleh diguna oleh komuniti akademik dan penyelidikan keselamatan untuk menjejak trend-trend peringkat-tinggi dan mengukur perkembangan di seluruh eko-sistem ini.

MENDEMONSTRASIKAN PRINSIP INI

Pengeluar perisian dan perkhidmatan dalam talian patut mencari jalan untuk mendemonstrasikan kejayaan dalam melaksanakan prinsip ini. Mereka patut berusaha untuk menyampaikan kesan bukti dalam bentuk artifak untuk diperiksa oleh pihak luar. Tiada satu pun artifak secara sendirinya akan membuktikan bahawa sesebuah pengeluar sedang menerapkan satu program teguh secara tereka yang kuat, tetapi dengan menyampaikan pelbagai artifak, mereka akan membina sebuah kes mengenai komitmen pengeluar untuk membangunkan produk-produk teguh. Pendekatan ini adalah dalam semangat “tunjuk, bukan sahaja beritahu”.

Untuk mendemonstrasikan prinsip ini, pengeluar perisian patut mempertimbangkan langkah-langkah seperti yang terkandung di dalam senarai berikut. Organisasi pengarang mengakui bahawa hanya segelintir pengeluar perisian sahaja yang boleh melaksanakan amalan-amalan ini dengan segera dan menghasilkan artifak-artifak berkaitan pada permulaan perjalanan teguh secara tereka mereka. Selanjutnya, pengeluar perisian perlu mengutamakan senarai ini bergantung kepada cara bagaimana pelanggan mengaturgerakkan produk tersebut ke lapangan untuk mencapai manfaat keselamatan terbesar.

AMALAN-AMALAN TEGUH SECARA LALAI

1. **Singkirkan kata laluan lalai.** Kata laluan lalai terus terkait sebagai penyebab bagi sebahagian besar serangan yang berlaku setiap tahun. Membuat satu komitmen untuk menyingkirkan masalah kronik ini akan menafikan akses mudah kepada penyerang. Begitu juga, pengeluar patut mempertimbangkan amalan-amalan kata laluan apa yang patut dilaksanakan, misalnya had panjang minima kata laluan dan tidak membenarkan kata laluan yang diketahui sudah diceroboh.

2. **Lakukan ujian lapangan.** Dengan evolusi teknologi yang berterusan dan semakin menjadi kompleks, ia menjadi semakin penting juga bagi pengeluar perisian untuk melakukan ujian pengguna berpusatkan-keselamatan untuk memahami postur keselamatan produk-produk mereka dalam lapangan. Sama seperti bagaimana kajian pengguna memaklumkan keperluan pembangunan perisian, pengeluar perisian juga patut melakukan kajian pengguna yang berpusatkan-keselamatan untuk memahami di mana pengalaman pengguna keselamatan (security user experience) (UX) masih tidak mencukupi. Dengan memerhatikan cara bagaimana pelanggan mengaturgerak dan menggunakan produk-produk mereka dalam persekitaran dunia sebenar, pengeluar perisian boleh meraih pandangan mendalam berharga mengenai kebergunaan dan keberkesanan ciri-ciri keselamatan dan kawalan mereka. Pandangan mendalam ini boleh membantu dalam mengenalpasti kawasan-kawasan yang memerlukan penambahbaikan dan untuk memperhalusi produk-produk mereka untuk memenuhi keperluan keselamatan pelanggan mereka dengan lebih baik. Contohnya, ujian lapangan mungkin mencadangkan perubahan kepada aliran UX, kelalaian, pengamaran, dan pemantauan. Ujian lapangan juga mungkin menunjukkan di mana penambahbaikan lalu di dalam rekabentuk produk tersebut telah mengurangkan velositi penampalan keselamatan, mengurangkan kesilapan konfigurasi, dan meminimumkan permukaan serangan.

Pengeluar patut mempertimbangkan perkara-perkara berikut:

- Adakah pelanggan melaksanakan panduan pengerasan dengan tepat?
- Adakah ciri-ciri keselamatan sedia ada produk itu berfungsi seperti yang dijangka dalam lapangan?
- Adakah ciri-ciri ini benar-benar menahan serangan dunia-sebenar?
- Ciri-ciri manakah yang boleh mengurangkan kemungkinan pengkompromian dengan lebih baik?

Nota: Untuk memperolehi pandangan lebih mendalam ke dalam elemen-elemen ini, pengeluar perisian mungkin ingin berkongsi dengan para pelanggan untuk melakukan latihan pasukan mereka untuk melihat cara bagaimana produk tersebut menghalang serangan. Ujian lapangan ini mungkin akan mengambil tempat di tapak fizikal pelanggan, secara maya, atau melalui telemetri daripada aplikasi tersebut dalam cara yang memelihara privasi.

3. **Mengurangkan saiz panduan pengerasan.** Pengeluar boleh memperbaiki postur keselamatan pelanggan dengan menyelaras atau malah menyingkirkan panduan pengerasan produk dan memfokuskan kepada langkah-langkah keselamatan yang paling kritikal yang pelanggan patut utamakan bila mengaturgerakkan produk-produk mereka. Daripada membanjiri pelanggan dengan sebuah senarai berjela mengenai langkah-langkah keselamatan, pengeluar patut mengenalpasti risiko keselamatan tertinggi yang melemahkan produk-produk mereka dan menyampaikan panduan yang jelas dan terperinci mengenai cara bagaimana untuk memitigasikan risiko-risiko ini. Tambahan pula, pengeluar patut menyediakan peralatan dan pengautomasian kepada pelanggan yang meringkaskan proses pelaksanaan kawalan keselamatan, seperti skrip-skrip yang boleh diaturkerahkan dengan mudah di dalam persekitaran mereka. Sebagai tambahan lagi, peralatan ini patut berupaya menentusahkan dan menunjukkan dengan jelas perubahan-perubahan yang dibuat daripada garis dasar asal. Dengan menyelaraskan panduan pengerasan dan menyampaikan peralatan dan pengautomasian yang mudah-untuk-diguna kepada pelanggan, pengeluar boleh mengurangkan beban ke atas pelanggan mereka dan membantu memastikan bahawa produk-produk mereka diaturgerakkan dalam sebuah rupa yang teguh. Satu taktik ialah untuk mempertimbangkan pelaksanaan prinsip Pareto untuk mengurangkan jumlah langkah bagi kes penggunaan lazim (80%), dan kemudian menyediakan panduan dan peralatan berkonteks bagi senario yang kurang lazim (20%). Dengan cara ini, pengeluar perisian boleh menjadikan perkara yang mudah menjadi mudah, dan memungkinkan perkara yang sukar. Ujian lapangan

akan menjadi sebuah alat yang sangat berkuasa untuk mengukur berapa lama akan diambil oleh para pelanggan untuk menemui, memahami, dan melaksanakan panduan pengerasan. Pengeluar patut mempertimbangkan bagaimana produk itu boleh menegur pentadbir untuk mengambil tindakan di dalam produk itu sendiri daripada hanya bergantung kepada mereka untuk menerapkan tugas-tugas daripada sebuah panduan pengerasan.

4. **Dengan berusaha secara aktif untuk tidak menggalakkan pengunaan ciri-ciri legasi yang tidak selamat.**
Mengutamakan keselamatan melalui laluan penaiktarafan jelas daripada penyesuaian ke belakang. Menerbitkan hantaran blog yang menunjukkan penerimapakaian ciri-ciri dan protokol yang lebih selamat, dan merendahkan ciri-ciri yang tidak selamat melalui pengumuman mengenainya, kemungkinannya daripada dalam produk itu sendiri. Sejumlah besar pelanggan telah menunjukkan bahawa mereka tidak akan mengekalkan sistem mereka mengikut tuntutan semasa dengan jaringan, identity, dan ciri-ciri keselamatan kritikal yang lain. Dalam sesetengah kes, pelanggan sangat khuatir kalau kefungsian sedia ada akan rosak dengan sebuah penaiktarafan. Dengan menjadikan penaiktarafan selancar mungkin, besar kemungkinan pelanggan akan menaiktaraf dan mendapatkan pembaikan keselamatan dengan lebih kerap dan pantas. Pengeluar perisian patut menegur pelanggan secara lebih agresif ke arah laluan penaiktarafan yang mengurangkan risiko pelanggan.

5. **Laksanakan amaran yang menangkap perhatian.**
Sama seperti bunyi amaran tali pinggang keledar di dalam kereta yang akan membunyikan amaran berterusan bila tali pinggar keledar tidak dipasang, pengeluar patut melaksanakan amaran yang menepati masa dan berulang-ulang bila pengguna atau pentadbir benar-benar berada di dalam keadaan yang tidak selamat, yang memberi amaran kepada para pentadbiran berkenaan bahawa mereka sedang menggunakan protokol yang tertiris di dalam persekitaran mereka dan mencadangkan laluan yang dinaiktaraf. Laksanakan amaran yang menepati masa dan berulang-ulang bila pengguna dan pentadbir, atau konfigurasi aplikasi tersebut, berada di dalam keadaan yang tidak selamat. Pastikan mod tidak selamat tersebut jelas kepada para pentadbir secara berkala. Satu ciri tambahan mungkin memerlukan seorang pentadbir tinggi untuk mengakui kekurangan MFA dalam akaun mereka setiap kali mereka mendaftar masuk, atau malah akan mematikan sesetengah ciri utama sehingga mereka menghidupkan MFA tersebut. Terdapat ruang bagi inovasi untuk mencapai matlamat-matlamat ini tanpa mewujudkan kebosanan amaran.

6. **Wujudkan templat konfigurasi teguh.**
Templat-templat ini boleh mengesetkan sesetengah konfigurasi terlebih dahulu untuk menyimpan pengesetan berdasarkan kemahuan risiko sesebuah organisasi. Walaupun ia mungkin terlampu mudah untuk mengadakan templat keselamatan rendah/sederhana/tinggi, contoh itu menunjukkan berapa banyak pengesetan yang boleh dikemaskini untuk menangani risiko bagi organisasi itu. Templat boleh disokong dengan panduan pengerasan terhadap risiko yang telah dikenalpasti oleh pengeluar.

AMALAN PEMBANGUNAN PRODUK TEGUH

1. **Pengakuran dokumen untuk meneguhkan sebuah kerangka kerja SDLC.** Kerangka kerja SDLC teguh menyampaikan objektif dan contoh melangkau orang, proses, dan teknologi. Pertimbangkan penerbitan sebuah keterangan terperinci tentang kawalan kerangkakerja SDLC teguh mana yang telah dilaksanakan dan menerangkan sebarang kawalan berlainan yang telah diguna. Di dalam AS, pertimbangkan penggunaan Kerangka Kerja Pembangunan Perisian Teguh NIST (NIST Secure Software Development Framework) (SSDF). Walaupun ia bukan sebuah senarai semak, SSDF "menerangkan satu set amalan dasar dan kukuh bagi pembangunan perisian teguh".

2. **Dokumentasikan Matlamat Prestasi Keselamatan Siber (Cybersecurity Performance Goals) (CPG) atau pengakuran yang setara.** Apabila sebuah organisasi memperakui bahawa mereka mengakuri piawaian NIST SSDF, mereka sedang memperakui bahawa SDLC mereka mengambil maklum amalan-amalan terbaik yang sudah difahami dengan baik. Namun begitu, ini tidak mencukupi untuk mereka mempunyai sebuah SDLC yang kuat sahaja. Mereka juga perlu melindungi persekitaran perusahaan dan pembangunan mereka sendiri daripada pelaku berniat jahat yang ingin mencari jalan untuk memanipulasikan sifat-sifat keselamatan produk tersebut sementara ia masih sedang dibangunkan. Ini bukannya satu kelas serangan secara teori sahaja, tetapi satu yang telah dilakukan dengan kesan buruk terhadap para pelanggan, dan seterusnya kepada keselamatan nasional. Para organisasi patut menimbangkan penerbitan butiran pengakuran organisasi tersebut kepada CISa CPGs, Kerangka Kerja Keselamatan Siber NIST (CSF), atau kerangka kerja program keselamatan siber yang lain.

3. **Pengurusan Keterdedahan.** Sesetengah pengeluar mempunyai sebuah program pengurusan keterdedahan yang memfokus kepada penampalan keterdedahan yang ditemui secara dalaman atau luaran, dan itu sahaja. Program yang lebih matang memasukkan analisis dipacu data meluas bagi keterdedahan dan punca sebab mereka, dengan mengambil langkah untuk menyingkirkan keseluruhan kelas keterdedahan secara sistematik[3]. Mereka melaksanakan program formal di sekitar pengesetan perancangan kualiti, kawalan kualiti, penambahbaikan kualiti, dan pengukuran kualiti. Mereka menganggap pengurusan kecacatan sebagai satu hal perniagaan, dan bukan sekadar satu perkara keselamatan sahaja. Program-program ini tidak begitu berbeza dari beberapa segi dengan program kualiti dan keselamatan dalam industri-industri lain.

4. **Gunakan perisian sumber terbuka secara bertanggungjawab.** Apabila perisian sumber terbuka diguna, sila bertindak secara bertanggungjawab dengan menyaring pakej-pakej sumber terbuka, memupuk sumbangan kod kembali kepada dependensi, dan membantu menampung pembangunan dan penyelenggaraan komponen-komponen yang kritikal. Untuk rujukan, Kementerian Ekonomi, Perdagangan, dan Industri (METI) Jepun telah menerbitkan "Pengumpulan Penggunaan Contoh-Contoh Kes Berkaitan Kaedah-Kaedah Pengurusan bagi Penerapan OSS and Memastikan Keselamatannya" ("Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security").

5. **Sediakan kelalaian (default) selamat bagi para pembangun.** Menjadikan laluan lalai semasa pembangunan perisian laluan yang teguh dengan menyediakan blok-blok pembinaan yang selamat bagi para pembangun. Contohnya, memandangkan suntikan keterdedahan SQL yang menyebabkan kemudaratan dunia-sebenar yang meleluasa, pastikan bahawa pembangun menggunakan sebuah perpustakaan yang diselenggarakan dengan baik untuk menghalang kelas keterdedahan itu. Juga dikenali sebagai "jalan berturap" atau "laluan yang dinyalakan dengan baik", amalan ini memastikan kepantasan mahupun keselamatan, dan mengurangkan kesilapan manusia.

6. **Pupukkan sebuah tenaga kerja pembangun perisian yang memahami keselamatan.** Pastikan bahawa pembangun perisian anda memahami keselamatan dengan melatih mereka mengenai amalan terbaik pengkodan teguh. Selanjutnya, bantulah usaha untuk mentransformasikan tenaga kerja meluas dengan mengemaskinikan amalan-amalan pengambilan pekerja untuk menilai pengetahuan keselamatan dan bekerja dengan universiti, kolej masyarakat, kem latihan bina diri lasak, dan pendidik lain untuk menganyamkan keselamatan ke dalam sains komputer dan kurikulum pembangunan perisian.

[3] NIST SSDF, PO 1.2, Contoh 2: "Definisikan dasar yang menetapkan keperluan keselamatan bagi perisian organisasi, dan tentusahkan pematuhan di titik-titik utama dalam SDLC (contohnya, kelas-kelas kekurangan perisian yang ditentusahkan oleh pintu pagar, serta respons kepada keterdedahan yang ditemui dalam perisian yang dikeluarkan)".

7. **Ujikan pengurusan kejadian insiden keselamatan (security incident event management) (SIEM) dan pengintegrasian pengorkestraan, pengautomasian, dan respons (security orchestration, automation, and response) (SOAR).** Selain melakukan ujian lapangan, bekerja secara bersama dengan penyedia SIEM dan SOAR popular beserta pelanggan terpilih untuk memahami bagaimana pasukan respons insiden menggunakan log untuk menyiasat insiden keselamatan yang disyaki atau yang benar-benar terjadi. Tidak begitu ramai pembangun perisian yang pernah mengalami merespons kepada sebuah insiden dan mungkin akan mewujudkan entri log yang tidak akan membantu para perespon sebanyak mana yang mereka jangkakan. Dengan bekerja dengan teknologi SIEM dan SOAR serta para profesional respons insiden sebenar, pasukan pembangunan boleh mewujudkan log-log yang menceritakan kisah yang tepat dan lengkap, justeru menjimatkan masa dan mengurangkan ketidakpastian semasa sesebuah insiden.

8. **Penyelarian dengan Arkitektur Kepercayaan Sifar (Zero Trust Architecture) (ZTA).** Menyelarikan panduan pengaturgerakan produk dengan, misalnya, model-model NIST ZTA dan Model Kematangan Kepercayaan Sifar CISA. Menggalakkan pelanggan untuk memasukkan prinsip-prinsip ini dalam persekitaran mereka.

AMALAN-AMALAN PERNIAGAAN PRO-KESELAMATAN

1. **Menyediakan pengelogan tanpa caj tambahan.** Perkhidmatan awan patut berkomitmen ke arah menjanakan dan menyimpan log-log berkaitan keselamatan tanpa caj tambahan. Produk-produk dalam-premis patut juga menjanakan log-log berkaitan keselamatan tanpa caj tambahan. Seterusnya, produk tersebut patut melogkan kejadian keselamatan secara lalai memandangkan ramai pelanggan mungkin tidak akan memahami nilainya sehingga selepas kejadian itu sudah pun berlaku. Taktik-taktik ini mungkin memerlukan penilaian kembali yang menyeluruh tentang apakah kejadian-kejadian keselamatan yang patut dilogkan bagi menyampaikan kesedaran keadaan keselamatan siber, cara bagaimana seseorang pelanggan boleh mengkonfigurasikan pengelogan, untuk tempoh masa berapa lama log itu patut disimpan, cara bagaimana integriti dan penyimpanan log dilindungi, dan cara bagaimana ia boleh dianalisis. Dalam sesetengah kes, penilaian kembali ini mungkin mencadangkan akan keperluan untuk pengfaktoran kembali arkitektur pengurusan log aplikasi tersebut untuk menolong agar ia boleh dipertindakkan dan pada kos yang mampu ditampung oleh pihak pengeluar. Bekerja dengan pakar respons kejadian (incident response) (IR) boleh meningkatkan peluang bagi log tersebut untuk menjadi berguna kepada para penyiasat di dalam bidang berkenaan. Sila lihat bahagian mengenai SIEMs.

2. **Menyingkirkan cukai tersembunyi.** Menerbitkan sebuah komitmen untuk sama sekali tidak mengenakan bayaran bagi ciri-ciri atau pengintegrasian keselamatan atau privasi. Contohnya, di dalam skop pengurusan identiti dan akses (identity and access management) (IAM) yang lebih meluas, terdapat perkhidmatan yang dikenali sebagai perkhidmatan pendaftaran masuk tunggal (single sign-on) (SSO). Sesetengah pengeluar mengenakan bayaran lebih untuk menghubungkan sistem mereka kepada sebuah perkhidmatan SSO (kadangkalanya dirujuk sebagai sebuah penyedia identiti). “Cukai SSO” ini bererti bahawa pengurusan identiti dan akses yang baik terletak di luar capai sebahagian besar SMOs, justeru menghalang mereka daripada mencapai sebuah postur keselamatan yang kuat. Sesetengah perkhidmatan mengenakan bayaran lebih untuk membolehkan MFA bagi pengguna. **Keselamatan tidak sepatutnya dikenakan harga sebagai sebuah barangan mewah tetapi dipertimbangkan sebagai satu hak pelanggan.** Sesetengah pengeluar telah berhujah bahawa ciri-ciri ini tidak diminta oleh ramai pelanggan, dan ia akan memakan belanja yang berlebihan untuk diselenggarakan. Hujah-hujah ini mengabaikan hakikat bahawa tidak ramai pelanggan akan memanggil untuk mengadu atau bertawar-menawar, bukan semua pelanggan yang benar-benar memahami apakah manfaat sebenar ciri-ciri ini, dan semua ciri akan memerlukan perbelanjaan untuk diselenggarakan. Namun begitu kita tidak melihat ramai pelanggan yang mengenakan bayaran tambahan untuk penyediaan atau integriti data. Kos-kos untuk menyokong ciri-ciri utama ini telah dibina ke dalam harga yang dibayar oleh semua pelanggan, sama juga seperti kos-kos yang merangkumi tali pinggang keledar, kolum stereng yang boleh dilipat, dan beg udara yang menyelamatkan nyawa dalam kemalangan.

3. **Mencakupi tahap kepiawaian terbuka.** Laksanakan tahap kepiawaian terbuka, khususnya di sekitar jaringan dan protokol identiti umum. Mengelakkan pemilikan protokol bila tahap kepiawaian terbuka disediakan.

4. **Menyediakan peralatan penaiktarafan.** Ramai pelanggan masih teragak-agak untuk menerima pakai versi terbaru produk, termasuk mengaturgerakkan ciri-ciri yang lebih baharu dan selamat seperti hubungan jaringan yang teguh. Pengeluar perisian boleh meningkatkan penerimapakaian penaiktarafan baharu oleh pelanggan dengan menyediakan peralatan untuk menolong mengurangkan ketidaktentuan dan risiko. Menawarkan lesen percuma kepada pelanggan untuk menguji penaiktarafan dan penampalan dalam sebuah persekitaran ujian sebagai satu cara untuk memotivasikan pelanggan.

PRINSIP 2: Mencakupi Ketelusan dan Kebertanggungjawaban Radikal

KETERANGAN

Pengeluar perisian patut berbangga dengan penyampaian produk yang selamat dan teguh, selain membezakan diri mereka sendiri daripada komuniti pengeluar yang lain berdasarkan kebolehan mereka untuk berbuat demikian.

Mari kita tangani satu kebimbangan biasa mengenai ketelusan. Bila para pengamal berbincang mengenai ketelusan radikal, terdapat kecenderungan bagi perbualan tersebut untuk terjerumus ke dalam kebimbangan bahawa mereka sedang menyampaikan sebuah "peta jalan untuk para penyerang". Tetapi, sejumlah besar kesan bukti menunjukkan bahawa para penyerang sudah pun melakukan kerja mereka dengan cukup baik tanpa memerlukan peta jalan sebegini, dan kebimbangan sebegini patut ditolak ke belakang untuk ketelusan yang memanfaatkan pelanggan langsung, pelanggan tidak langsung, rantaian bekalan, dan keseluruhan industri perisian.

Ketelusan membantu industri untuk mewujudkan kelaziman – dalam erti kata lain, iaitu memperlihatkan apa itu yang dimaksudkan dengan "baik". Ia membantu kelaziman tersebut untuk berubah dengan peredaran masa sebagai respons kepada keperluan pelanggan, perubahan di dalam taktik atau ekonomi pelaku ancaman, atau evolusi teknologi. Ketelusan membantu pengeluar yang agak kekurangan sumber untuk belakar daripada mereka yang mempunyai sumber-sumber yang lebih matang dan berkeupayaan. Perbualan mengenai perkongsian maklumat patut melangkau petunjuk ancaman masa-sebenar, untuk merangkumi elemen-elemen di bawah.

Ketelusan memaksa keputusan di sekitar soal keselamatan untuk dibuat pada peringkat awal proses pembangunan, dan menjadi kegiatan berterusan bagi para pemimpin perniagaan selain para jurutera dan profesional keselamatan. Ketelusan membina kebertanggungjawaban ke dalam produk itu.

Satu nota mengenai pilihan kata sifat "radikal" di hadapan "ketelusan". Hari ini, ia tidak menjadi kebiasaan bagi pengeluar perisian untuk menerbitkan maklumat terperinci mengenai cara bagaimana mereka membangun dan menyelenggarakan perisian dan cara bagaimana mereka mematangkan program mereka dengan menggunakan data mengikut peredaran masa. Dalam industri perisian, tidak ramai pengeluar yang menawarkan lawatan berpandu mengenai cara bagaimana mereka merekabentuk perisian mereka. Pengeluar perisian tidak mempunyai peluang yang banyak untuk melihat bagaimana organisasi rakan sejawatan menstrukturkan program SDLC mereka, dan cara bagaimana program tersebut berupaya untuk bertahan dalam persekitaran pelanggan mereka daripada penyerang sebenar. Pihak industri secara sepenuhnya akan meraih manfaat daripada perkongsian maklumat yang lebih atas topik seperti strategi untuk mengukur kos kecacatan keselamatan dan untuk menyingkirkan kelas-kelas keterdedahan. Sebagai hasil daripada amalan-amalan lazim ini, setiap pengeluar perisian mesti mempelajari cara bagaimana untuk menangani keselamatan produk secara bersendirian. Mungkin dengan cara tanpa mengenakan cukai mewah ke atas ciri-ciri keselamatan, soal keselamatan dan keteguhan dengan demikian akan menjadi pusat kos dan bukannya pusat keuntungan, dan syarikat boleh memperolehi manfaat dengan meringankan bebanan melalui usaha sama dan ketelusan.

Kami mahu berfokus kepada taktik-taktik yang akan memacu evolusi industri perisian secara material. Kami tidak boleh lagi mampu membuat penambahbaikan sekadar mengambil kesempatan and secara sedikit demi sedikit sahaja. Jika kita ingin bertindak secara bersama untuk mengatasi ancaman yang bakal menjelma daripada pihak musuh yang pintar dan boleh menyesuaikan diri mereka, kami mesti mencakupi tahap ketelusan yang akan berasa kurang selesa pada hari ini, tetapi yang akan memacu industri ke hadapan. Terdapat pengeluar pada ketika ini yang mengabadikan sesetengah daripada prinsip teguh secara tereka ini. Bak kata William Gibson, "masa hadapan sudah pun tiba, cuma ia tidak diedarkan dengan sama rata". **Ketelusan radikal akan membantu mengedar maklumat tersebut dan memanfaatkan para pejuang lebih daripada musuh kami.**

Ketelusan boleh melakukan lebih untuk menolong organisasi rakan sejawat mereka untuk mematangkan SDLC mereka. Bakal pelanggan dan pelabur boleh mempelajari lebih mengenai pelaburan dan tukar ganti yang telah dibuat oleh para pengeluar, dan postur keselamatan yang telah dicipta bagi pelanggan oleh pelaburan tersebut. Pengeluar yang mencakupi ketelusan radikal akan memberi pelanggan maklumat untuk menolong mereka dalam membuat keputusan pemerolehan bukan sahaja berpandukan soal harga dan ciri-ciri, tetapi mengenai soal keselamatan juga.

Biarpun organisasi bekerja keras untuk meneguhkan rantaian bekalan dan SDLC mereka, syarikat-syarikat tetap mendapati bahawa proses-proses terbina mereka telah dikompromi dalam masa kebelakangan ini. Menerima ketelusan radikan patut membawa kepada pemberitahuan umum mengenai serangan tersebut selain penambahbaikan yang telah dibuat oleh syarikat tersebut untuk menghalang dan mengesan serangan pada masa hadapan. Bentuk perkongsian maklumat ini boleh menolong organisasi lain untuk belajar tanpa menjadi mangsa kepada nasib malang yang sama.

MENDEMONSTRASIKAN PRINSIP INI

Untuk mendemonstrasikan prinsip ini, pengeluar perisian patut mengambil langkah-langkah termasuk perkara berikut:

AMALAN TEGUH SECARA LALAI

1. **Terbitkan agregat statisik dan trend keselamatan berkaitan.** Topik contoh termasuklah penerimapakaian MFA oleh pelanggan dan pentadbir dan penggunaan protokol legasi yang tidak selamat.
2. **Terbitkan statistik penampalan.** Butirkan peratusan pelanggan yang menggunakan versi terkini produk tersebut, dan apa yang anda sedang lakukan untuk lebih memudahkan dan lebih menyakinkan pengemaskinian dibuat.
3. **Terbitkan data mengenai hak-hak keistimewaan yang tidak digunakan.** Menerbitkan maklumat agregat mengenai kebenaran melampau di serta asas pelanggan anda selain peneguran and perubahan lain yang anda sedang lakukan terhadap produk itu untuk mengurangkan permukaan serangan pelanggan tersebut. Keistimewaan yang tidak digunakan ini mungkin akan menjadi calon yang bagi bagi pengamaran kepada pentadbir, seperti bunyi amaran penggera tali pinggang keledar.

AMALAN PEMBANGUNAN PRODUK TEGUH

1. **Mewujudkan kawalan keselamatan dalaman.** Ramai syarikat telah melihat manfaat dalam memindahkan data mereka kepada penyedia awan. Kini penyedia awan itu pula menjadi sasaran penyerang. Penyedia Perisian sebagai satu Perkhidmatan (Software as a Service) (SaaS) patut menerbitkan statistik kawalan dalaman mereka. Contohnya, penyedia SaaS patut menerbitkan statistik pengaturgerakan dalaman mereka mengenai MFA kalis pancingan, seperti pengesahsahihan Identiti Pantas Dalam Talian (Fast Identity Online) (FIDO). Sebaiknya, mereka patut berupaya berkata bahawa tiada satu pun anggota kakitangan mereka boleh mengakses data pelanggan atau data lain yang sensitif tanpa melakukan pengesahan melalui MFA kalis pancingan.

2. **Menerbitkan model ancaman peringkat-tinggi.** Produk teguh secara tereka bermula dengan model ancaman tertulis yang menerangkan apa yang sedang cuba dilindungi oleh penciptanya dan daripada siapa. Model ancaman berkesan didokong oleh cara bagaimana pencerobohan ini berlaku dalam keadaan liar, dan sepatutnya meliputi kedua-dua persekitaran perusahaan dan pembangungan, selain cara bagaimana pengeluar perisian berhasrat untuk menggunakannya dalam persekitaran pelanggan.

3. **Menerbitkan perakuan-sendirian SDLC teguh yang terperinci.** Pengeluar yang mematuhi NIST SSDF, atau kerangka kerja serupa yang lain sedang berusaha secara aktif ke arah sebuah kitaran hidup pembangunan perisian yang matang. Menerbitkan sebuah perakuan-sendirian tentang kawalan mana yang telah diperlakukan oleh pengeluar, dan bagi produk yang mana, akan mendemonstrasikan satu komitmen kepada pematuhan amalan terbaik ini dan menyediakan satu tahap keyakinan yang lebih tinggi kepada pelanggan mereka. Skim-skim pensijilan lain termasuklah misalnya Metodologi Rantaian Bekalan Siber Israel (Israel Cyber Supply Chain Methodology).

4. **Mencakupi ketelusan keterdedahan.** Terbitkan satu komitmen yang akan memastikan bahawa keterdedahan produk yang dikenalpasti akan diterbitkan sebagai entri-entri CVE yang tepat dan lengkap. Hal ini khususnya benar bagi ruang enumerasi kelemahan Lazim yang mengenalpasti punca sebenar keterdedahan tersebut. Lebih tepat dan lengkap pangkalan CVE umum itu, maka lebih banyaklah peluang bagi industri untuk menjejaki bagaimana produk itu menjadi lebih teguh, dan kelas keterdedahan mana yang paling meleluasa. Namun begitu, berwaspadalah terhadap kemahuan untuk mengira CVE sebagai satu metrik negatif, memandangakan bilangan ini juga merupakan satu petanda sebuah masyarakat analisis dan pengujian kod yang sihat. Apabila pengeluar melaksanakan sebuah falsafah teguh secara tereka, terdapat kemungkinan bahawa pada mulanya bilangan CVE mentah mereka akan melonjat disebabkan penemuan yang lebih komprehensif dan pemulihan keterdedahan kod sedia ada. Pengeluar patut menerbitkan analisis keterdedahan lalu, termasuk sebarang corak dan langkah yang telah diambil untuk menangani keseluruhan kelas keterdedahan itu. Contohnya, jika sebilangan peratusan besar CVE sesebuah syarikat terkait kepada penskripan silang tapak (cross-site scripting) (XSS), pendokumentasian analisis punca penyebab, respons (seperti peralihan kepada kerangkakerja templat web yang menghalang XSS), dan hasil keputusannya akan memberi isyarat kepada pelanggan bahawa mereka tidak akan dijadikan mangsa oleh sebuah kelas keterdedahan yang mana pemitigasiannya sudah pun difahami berdekad-dekad lamanya.

5. **Menerbitkan Bil Material Perisian (SBOMs).** Pengeluar patut mempunyai pemerintahan terhadap rantaian bekalan mereka. Organisasi patut membina dan menyelenggarakan SBOM [2] bagi setiap produk, meminta data daripada para pembekal mereka, dan menyediakan SBOM untuk pelanggan dan pengguna hiliran. Ini akan membantu dalam mendemonstrasikan kewajaran mereka dalam memahami komponen-komponen yang mereka gunakan dalam penciptaan produk mereka, keupayaan mereka untuk merespons kepada risiko yang baru dikenalpasti, dan boleh membantu pelanggan mereka untuk memahami bagaimana untuk berespons jika salah satu daripada modul dalam rantaian bekalan mempunyai sebuah keterdedahan yang baru ditemui. Sebagai rujukan, Kementerian Ekonomi, Perdagangan, dan Industri (METI) Jepun telah

menerbitjan "Panduan kepada Pengenalan Bil Perisian untuk Material (SBOM) untuk Pengurusan Perisian" ("Guide of Introduction of Software Bill of Materials (SBOM) for Software Management"). Ketelusan patut dilanjutkan kepada firmware dalam peranti terbenam serta model dan data yang diguna dalam pembelajaran AI/mesin (ML). Selain membantu dalam keputusan pemerolehan dan pengupayaan operasi, SBOM memainkan peranan penting dalam infrastruktur untuk mengesan dan merespons kepada serangan rantaian bekalan yang berniat jahat.

6. **Terbitkan sebuah dasar pendedahan keterdedahan.** Terbitkan sebuah dasar pendedahan keterdedahan yang (1) memberi kuasa untuk ujian terhadap semua produk yang ditawarkan oleh pengeluar dan syarat-syarat bagi ujian tersebut, (2) menyediakan tempat teduh yang selamat dari segi undang-undang bagi tindakan yang dilakukan secara konsisten dengan dasar tersebut, dan (3) membenarkan pendedahan umum terhadap keterdedahan selepas satu garis masa yang ditetapkan. Pengeluar patut melakukan analisis punca-penyebab ke atas keterdedahan yang ditemui dan, sejauh mana yang mungkin, mengambil tindakan untuk menyingkirkan keseluruhan kelas keterdedahan. Sila lihat Templat Dasar Pendedahan Keterdedahan CISA untuk bahasa rujukan.

AMALAN-AMALAN PERNIAGAAN PRO-KESELAMATAN

1. **Umumkan seorang penaja eksekutif kanan teguh secara tereka.** Dalam banyak organisasi, keselamatan (seperti kualiti) ditugaskan kepada pasukan teknikal yang mempunyai kebolehan terhad untuk membuat perubahan struktur untuk menambahbaikkan keselamatan produk-produk ini secara dramatik. Mengumumkan seorang eksekutif perniagaan peringkat tinggi untuk menyelia program teguh secara tereka akan mentransformasikan keselamatan produk kepada sesuatu yang akan diambil berat pada peringkat tinggi perniagaan.

2. **Terbitkan sebuah peta jalan teguh secara tereka.** Pengeluar patut mendokumentasikan perubahan yang dibuat kepada SDLC mereka untuk menambahbaik keselamatan pelanggan, termasuk butir-butir mengenai laporan ujian-lapangan, tindakan yang diambil untuk menyingkirkan keseluruhan kelas keterdedahan, dan perkara-perkara lain yang disenaraikan dalam prinsip-prinsip lain. Seperti di dalam kes usaha penambahbaikan kualiti, program penambahbaikan keselamatan mempunyai fasa-fasa perancangan, kawalan dan penambahbaikan yang nyata. Dalam semangat untuk memperlihatkan daripada sekadar memberitahu, penerbitan peta jalan serta butir-butir di sebalik fasa-fasa ini akan membina keyakinan bahawa produk-produk berkenaan adalah teguh secara tereka. Setelah mencapai kemajuan bermakna, pengeluar boleh membutirkannya dalam laporan ketelusan. Berbuat demikian bukan sahaja mendemonstrasikan sebuah komitmen kepada prinsip-prinsip teguh secara tereka, tetapi juga oleh menginspirasikan pihak lain untuk mendokong program-program serupa dengan menunjukkan sebuah bukti kewujudannya.

3. **Terbitkan sebuah peta jalan memori-selamat.** Pengeluar boleh mengambil langkah-langkah untuk menyingkirkan salah satu daripada kelas keterdedahan yang terbesar dengan memigrasikan produk-produk sedia ada dan membina produk-produk baharu dengan menggunakan bahasa-bahasa memori-selamat. Walaupun hal ini mungkin tiak akan dilakukan dalam semua kes, pengeluar boleh menimbangkan pembangunan pembalut aplikasi dalam bahasa memori-selamat daripada menulis kembali keseluruhan aplikasi itu. Ini boleh juga termasuklah cara bagaimana pengeluar mengemaskinikan pengambilan pekerja, latihan, penilaian kod, dan proses-proses dalaman lain, selain cara-cara mereka sedang membantu komuniti sumber terbuka untuk melakukan perkara yang sama.

4. **Terbitkan keputusan.** Sambil mengemaskinikan SDLC mereka untuk mengabadikan sebuah falsafah teguh secara tereka, organisasi akan menemui kejayaan pantas, lebih banyak kejayan sumber intensif, dan beberapa langkah pengunduran yang tidak dijangkakan. Dengan menyampaikan kejayaan dan rintangan dalaman, keseluruhan industri boleh belajar daripada hasil keputusan ini.

PRINSIP 3: Memimpin dari Atas

KETERANGAN

Walaupun keseluruhan falsafah ini dipanggil “teguh secara tereka”, insentif-insentif untuk keselamatan pelanggan bermula jauh lebih awal sebelum fasa mereka produk tersebut. Ianya bermula dengan matlamat perniagaan dan objektif-objektif yang nyata dan tersirat serta hasil-hasil keputusan yang diingini. Hanya bila pemimpin kanan menjadikan keselamatan sebuah keutamaan perniagaan, mewujudkan insentif dalaman, dan memupuk sebuah budaya rata-upaya untuk menjadikan teguh secara tereka satu keperluan, barulah hasil yang terbaik akan dicapai oleh mereka.

Walaupun kepakaran hal subjek teknikal adalah kritikal kepada keselamatan produk, ia bukan satu perkara yang boleh diserahkan kepada kakitangan teknikal sahaja. Ia merupakan satu keutamaan perniagaan yang mesti bermula dari atas.

Sesetengah orang pernah bertanya jika seseorang pengeluar perisian menerima dua prinsip pertama dan mengeluarkan artifak bermakna, adalah prinsip ketiga diperlukan? Bagaimana sebuah syarikat mewujudkan visi, misi, nilai dan budayanya akan membawa kesan ke atas produk tersebut, dan elemen-elemen ini memiliki sebuah komponen yang berat di atas. Kami melihat perkara ini di dalam industri lain yang telah melakukan penambahbaikan dramatik dalam keselamatan dan kualiti. Pakar kualiti yang terkemuka, J.M. Juran pernah menulis:

> ***Pencapaian kepemimpinan berkualiti memerlukan pihak pengurus atasan untuk menerajui pengurusan kualiti secara langsung. Dalam syarikat-syarikat yang sudah mencapai kepemimpinan berkualiti, pihak pengurus atasan telah menerajui inisiatif tersebut secara langsung. Saya tidak tahu akan sebarang pengecualian dalam perkara ini. [3]***

Kami percaya bahawa keselamatan ialah satu sub-kategori kualiti produk Bila keselamatan dan kualiti menjadi imperatif perniagaan dan bukan sahaja fungsi teknikal yang diserahkan khusus kepada kakitangan teknikal sahaja, organisasi akan berupaya untuk merespons kepada keperluan keselamatan pelanggan mereka dengan lebih cekap dan pantas. Malah, melabur dalam sumber-sumber yang diperlukan untuk memastikan keselamatan perisian merupakan satu keutamaan teras perniagaan dari awal lagi akan mengurangkan kos jangkamasa panjang dalam menangani kecacatan perisian, dan seterusnya, mengurangkan risiko keselamatan nasional.

Dalam cara yang sama seperti bagaimana pasukan kepemimpinan telah melaksanakan program-program tanggungjawab sosial korporat (corporate social responsibility) (CSR), terdapat kesedaran yang semakin berkembang bahawa lembaga korporat, termasuk bagi pengeluar perisian, patut mengambil sebuah peranan yang lebih aktif dalam menerajui program-program keselamatan siber. Frasa tanggungjawab siber korporat (corporate cyber responsibility) (CCR) kadangkala diguna untuk menerangkan ide yang sedang muncul ini.

MENDEMONSTRASIKAN PRINSIP INI

Untuk mendemonstrasikan prinsip ini, pengeluar perisian patut mengambil langkah-langkah termasuk yang berikut:

1. **Masukkan butir-butir sebuah program teguh secara tereka ke dalam laporan kewangan korporat.** Jika pengeluar tersebut ialah sebuah syarikat urusniaga awam, tambahkan satu bahagian dalam setiap laporan tahunan yang berfokus kepada usaha-usaha teguh secara tereka. Ia adalah kebiasaan bagi laporan kewangan tahunan automobil untuk mengandungi bahagian-bahagian mengenai keselamatan pemandu dan penumpang, termasuk maklumat mengenai jawatankuasa-jawatankuasa kualiti dan keselamatan yang dipusatkan dan diedar. Perincikan program teguh secara tereka dalam sebuah laporan kewangan yang mendemonstrasikan bahawa organisasi itu sedang mengaitkan keselamatan pelanggan dengan hasil keputusan kewangan korporat dan bukan sekadar menerima pakaian sebuah frasa di dalam bahan-bahan pemasaran kerana ia merupakan trend semasa sahaja.

2. **Sampaikan laporan berkala kepada lembaga pengarah anda.** Laporan ketua pegawai keselamatan maklumat (chief information security officer)(CISO) biasanya mengandungi maklumat tentang program-program keselamatan semasa dan terancang, ancaman, insiden yang disyaki dan disahkan, serta pengemaskinian lain yang berpusat kepada postur keselamatan dan kesihatan syarikat tersebut. Selain menerima maklumat mengenai postur perusahaan itu, pihak lembaha berkenaan patut meminta maklumat mengenai keselamatan produk dan kesannya yang ada ke atas keselamatan pelanggan. Pihak lembaga tidak sepatutnya melihat hanya kepada CISO, tetapi terutamanya kepada anggota-anggota lain pengurusan syarikat itu untuk memacu pengurangan risiko pelanggan.

3. **Perkasakan eksekutif teguh secara tereka.** Terdapat satu perbezaan signifikan antara sebuah organisasi di mana pasukan teknikal mempunyai “perkongsian kepentingan eksekutif” (“executive buy-in”), dan organisasi di mana pemimpin perniagaan mengurus secara peribadi proses penambahbaikan keselamatan pelanggan dengan menggunakan proses-proses perniagaan standard. Takrif “perkongsian kepentingan eksekutif” mencadangkan bahawa seseorang telah menjual ide sebuah program keselamatan pelanggan dan ianya bukan sekadar sebuah matlamat perniagaan peringkat tinggi. Eksekutif ini mesti diperkasa untuk mempengaruhi pelaburan produk untuk mencapai hasil keputusan keselamatan pelanggan.

4. **Wujudkan insentif-insentif dalaman yang bermakna.** Sambil menyedari keperluan untuk mengelakkan daripada pengewujudan insentif songsang, selarikan sistem hadiah untuk menambahbaikkan keselamatan pelanggan agar ia sepadan dengan tingkahlaku dan hasil keputusan lain yang dihargai. Dari eksekutif teguh secara tereka kepada pengurusan produk, pembangunan eksekutif, sokongan, jualan, perundangan, dan organisasi lain, anyamkan insentif keselamatan pelanggan ke dalam pengambilan pekerja, promosi, gaji, bonus, opsyen saham, serta proses-proses lazim lain di dalam menjalankan perniagaan itu. Contohnya, bila mewujudkan kriteria untuk mempromosikan pembangun perisian, masukkan pertimbangan untuk menambahbaikkan keselamatan produk beserta kriteria lain seperti masa hidup, prestasi, dan penambahbaikan ciri-ciri.

5. **Wujudkan sebuah majlis teguh secara tereka.** Dalam sesetengah industri, ia merupakan kelaziman bagi organisasi untuk mewujudkan sebuah majlis kualiti pusat, dan untuk memendamkan wakil-wakil kualiti dalam bahagian-bahagian utama atau unit-unit perniagaan. Dengan memasukkan kedua-dua anggota terpusat dan teredar, kumpulan-kumpulan ini bekerja untuk menambahbaikkan kualiti berbanding dengan matlamat-matlamat peringkat tinggi sambil menerima telemetri daripada tempat yang jauh di dalam organisasi tersebut. Begitu juga, sebuah majlis teguh secara tereka akan menambahbaikkan keselamatan berbanding matlamat teguh secara tereka di seluruh organisasi itu.

6. **Wujudkan dan kembangkan majlis-majlis pelanggan.** Ramai pengeluar perisian mempunyai majlis pelanggan yang terdiri daripada pelanggan daripada pelbagai rantau, industri, dan saiz. Majlis-majlis ini boleh menyediakan sejumlah besar maklumat mengenai kejayaan dan cabaran pelanggan dalam mengaturgerakkan produk-produk syarikat itu. Strukturkan agenda majlis ini dengan topik-topik khusus yang menangani soal keselamatan pelanggan, biarpun ia tidak berada di dalam mata minda semasa bagi para pesertanya. Pertimbangkan ke mana majlis pelanggan ini patut menyampaikan laporan mereka dan bagaimana untuk menyapa peserta mereka untuk mendapatkan pandangan mereka terhadap keselamatan produk semasa ia diaturgerakkan. Contohnya, adakah majlis itu memiliki perasaan berat sebelah terhadap tujuan pemasaran dan jualan, atau pengurusan produk? Eksekutif teguh secara tereka itu patut membantu dalam menerajui interaksi pelanggan ini dan patut menghubungkan mereka dengan elemen-elemen lain di dalam kertas ini, misalnya kajian lapangan.

TAKTIK-TAKTIK TEGUH SECARA TEREKA

Kerangka Kerja Pembangunan Perisian Teguh (Secure Software Development Framework) (SSDF), juga dikenali sebagai SP 800-218 Institut Kebangsaan Tahap Kepiawaian dan Teknologi (National Institute of Standards and Technology) (NIST), ialah satu set teras amalan-amalan pembangunan perisian teguh peringkat-tinggi yang boleh diintegrasikan ke dalam setiap tahap kitaran hidup pembangunan perisian (software development lifecycle) (SDLC). Penurutan amalan-amalan ini boleh membantu pembangun perisian untuk menjadi lebih berkesan dalam mencari dan membuangkan keterdedahan dalam perisian yang dikeluarkan, memitigasikan potensi impak pengeksploitasian keterdedahan, dan menangani punca penyebab keterdedahan untuk menghalang pengulangannya di masa hadapan.

Organisasi pengarang menggalakkan penggunaan taktik-taktik teguh secara tereka, termasuk prinsip-prinsip yang merujuk kepada amalan-amalan SSDF. Pengeluar perisian patut membangunkan sebuah peta jalan bertulis untuk mendokong amalan-amalan pembangunan perisian teguh secara tereka yang lebih banyak di serata portfolio mereka. Berikut ialah sebuah senarai gambaran yang tidak muktamad bagi amalan terbaik peta jalan:

- **Bahasa Pengaturcaraan Memori Selamat (SSDF PW.6.1).** Utamakan penggunaan bahasa memori selamat sejauh mana yang boleh. Organisasi pengarang mengakui bahawa mitigasi memori khusus mungkin akan menolong dalam taktik jangkamasa pendeka bagi pangkalan kod legasi. Contoh-contohnya termasuklah penambahbaikan bahasa C/C++, mitigasi perkakasan, menangani perawakan ruang rekaletak (space layout randomization) (ASLR), integriti kawalan-aliran (control flow integrity) (CFI), dan "fuzzing". Biarpun begitu, terdapat konsensus yang semakin berkembang bahawa penerimapakaian bahasa-bahasa pengaturcaraan memori selamat boleh menyingkirkan kelas kecacatan ini, dan pengeluar perisian patut menerokai cara-cara untuk mendokongnya. Beberapa contoh bahasa-bahasa memori selamat moden termasuk C#, Rust, Ruby, Java, Go dan Swift. Sila baca risalah maklumat Memori Selamat RSA untuk maklumat lanjut.
- **Asas Perkakasan Teguh.** Masukkan ciri-ciri kerangka bina yang membolehkan perlindungan memori halus, seperti apa yang dijelaskan oleh Arahan RISC Keupayaan Perkakasan Yang Dipertingkatkan (Capability Hardware Enhanced RISC Instructions) (CHERI) yang boleh melanjutkan Arkitektur Set-Arahan perkakasan konvensional (Instruction-Set Architectures) (ISAs), selain ciri-ciri lain seperti Modul-Modul Pelantar Yang Diyakini (Trusted Platform Modules) dan Modul-Modul Keselamatan Perkakasan (Hardware Security Modules). Untuk maklumat lanjut, sila layari laman web CHERI Universiti Cambridge.
- **Komponen-Komponen Perisian Teguh (SSDF PW 4.1).** Peroleh dan selenggarakan komponen-komponen perisian yang diteguhkan dengan baik (misalnya perpustakaan perisian, modul-modul, perkakasan pertengahan, kerangka kerja) daripada pembangun komersial, sumber terbuka yang ditentusahkan, dan pembangun-pembangun pihak ketiga lain untuk memastikan keselamatan yang kuat dalam produk-produk perisian pengguna.
- **Kerangka kerja templat sesawang (SSDF PW.5.1).** Gunakan kerangka kerja templat sesawang yang menerapkan pelepasan automatik input pengguna untuk mengelakkan serangan sesawang seperti penskripsian silang-tapak.
- **Pertanyaan berparameter (SSDF PW 5.1).** Gunakan pertanyaan berparameter daripada memasukkan input pengguna ke dalam pertanyaan, untuk mengelakkan serangan suntikan SQL.
- **Ujian keselamatan aplikasi yang statik dan dinamik (Static and dynamic application security testing) (SAST/DAST)** (SSDF PW.7.2, PW.8.2). Gunakan peralatan ini untuk menganalisis kod sumber produk dan tingkahlaku aplikasi untuk mengesan amalan-amalan yang kerap menimbulkan kesilapan. Peralatan ini meliputi isu-isu yang merangkumi pengurusan memori yang tidak sesuai kepada pembinaan pertanyaan pangkalan data yang kerap menimbulkan kesilapan (misalnya, input pengguna tidak terlepas yang membawa kepada suntikan SQL). Peralatan SAST dan DAST boleh dimasukkan ke dalam proses-proses pembangunan dan dijalankan dengan automatik sebagai sebahagian daripada pembangunan perisian. SAST dan DAST patut saling sepadan dengan jenis-jenis ujian yang lain, misalnya ujian unit dan ujian integrasi, untuk memastikan produk-produk mematuhi keperluan keselamatan yang dijangka. Bila isu-isu dikenalpasti, pengeluar patut melakukan analisis punca penyebab untuk menangani keterdedahan sistematik.

- **Penilaian Kembali Kod** (SSDF PW.7.1, PW.7.2). Berusaha untuk memastikan kod yang diserahkan ke dalam produk menjalani teknik-teknik kawalan kualiti seperti pewasitan oleh pembangun lain atau "pembenihan kesilapan".
- **Software Bill of Materials (SBOM)** (SSDF PS.3.2, PW.4.1). Memasukkan pengewujudan SBOM[4] untuk menyampaikan keterlihatan ke dalam set perisian yang dimasukkan ke dalam produk-produk.
- **Program pendedahan keterdedahan** (SSDF RV.1.3). Wujudkan program pendedahan keterdedahan yang membenarkan penyelidik keselamatan untuk melaporkan keterdedahan dan menerima tempat teduh yang selamat dari segi undang-undang dalam berbuat demikian. Sebagai sebahagian daripada hal ini, pembekal patut mewujudkan proses-proses untuk mengenalpasti punca penyebab keterdedahan yang ditemui. Proses-proses ini patut termasuk menentukan sama ada penerimapakaian mana-mana amalan teguh secara tereka dalam dokumen ini (atau amalan serupa yang lain) mungkin berupaya menghalang pengenalan keterdedahan tersebut.
- **Kesempurnaan CVE.** Pastikan bahawa CVE yang diterbitkan mengandungi punca penyebab atau pembilangan kelemahan lazim (common weakness enumeration) (CWE) untuk membolehkan analsis di serata industri terhadap kelemahan rekabentuk keselamatan perisian. Walaupun usaha untuk memastikan bahawa setiap CVE ialah tepat dan lengkap boleh mengambil masa yang lebih, ia membenarkan entiti-entiti yang berasingan untuk menemui trend-trend industri yang memanfaatkan semua pengeluar dan pelanggan. Untuk maklumat lanjut mengenai pengurusan keterdedahan, sila lihat panduan Pengkategorian Keterdedahan Khusus kepada Pemegang Taruh (Stakeholder-Specific Vulnerability Categorization) (SSVC) CISA.
- **Pertahanan-yang-Mendalam.** Rekakan infrastruktur agar pengkompromian sesuatu kawalan keselamatan tunggal tidak akan mengakibatkan pengkompromian keseluruhan sistem. Contohnya, memastikan bahawa keistimewaan pengguna diperuntukkan secara khusus, dan senarai kawalan akses diperjalankan, boleh mengurangkan kesan sebuah akaun yang dikompromi. Juga, teknik-teknik "sandboxing" perisian boleh mengkuarantinakan sesebuah keterdedahan untuk mengehadkan pengkompromian keseluruhan aplikasi itu.
- **Memenuhi Matlamat Prestasi Keselamatan Siber (Cybersecurity Performance Goals) (CPGs).** Rekakan produk yang memenuhi amalan-amalan keselamatan yang asas. Matlamat Prestasi Keselamatan Siber CISA menggariskan langkah-langkah keselamatan siber garis dasar, asas yang patut dilaksanakan oleh organisasi. Tambahan pula, untuk mendapatkan cara yang lebih untuk memperkukuhkan postur organisasi anda, sila lihat Kerangka Kerja Penilaian Siber UK yang berkongsi persamaan dengan CPG CISA. Jika sesebuah pengeluar gagal memenuhi CPG – misalnya dengan tidak memerlukan MFA kalis pancingan bagi semua pekerja – maka mereka tidak boleh dilihat sebagai menyampaikan produk-produk teguh secara tereka.

Organisasi pengarang mengakui bahawa perubahan-perubahan ini merupakan anjakan signifikan di dalam postur sesebuah organisasi. Oleh yang demikian, pengenalannya patut diutamakan berdasarkan pemodelan ancaman yang terukur, kekritikalan, kerumitan, dan impak perniagaan. Amalan-amalan ini boleh diperkenalkan bagi perisian baharu dan diperluaskan secara berperingkat untuk meliputi kes-kes dan produk-produk penggunaan tambahan. Dalam sesetengah kes, kekritikalan dan postur produk tertentu mungkin mewajarkan sebuah jadual yang dipercepatkan untuk menerimapakai amalan-amalan ini. Dalam kes lain, amalan-amalan ini boleh diperkenalkan ke dalam sebuah pangkalan kod legasi dan dipulihkan kembali dengan perjalanan masa.

[4] Sesetengah daripada organisasi pengarang sedang menerokai pendekatan berlainan untuk mendapatkan jaminan keselamatan sekitar rantaian bekalan perisian itu.

TAKTIK TEGUH SECARA LALAI

Selain menerimapakai amalan-amalan pembangunan teguh secara tereka, organisasi pengarang menyarankan agar pengeluar perisian mengutamakan konfigurasi teguh secara lalai di dalam produk-produk mereka. Ia patut berusaha untuk mengemaskinikan produk-produk itu agar ia mengakuri amalan-amalan ini sewaktu ia disegar semulakan. Contohnya:

- **Menyingkirkan kata kunci lalai.** Produk-produk tidak sepatutnya datang dengan kata kunci lalai yang dikongsi secara sejagat. Untuk menyingkirkan kata kunci lalai, organisasi pengarang menyarankan agar produk memerluka pentadbirnya untuk mengesetkan sebuah kata kunci yang kuat sewaktu proses pemasangan atau konfigurasi atau untuk mengirimkan produk tersebut dengan sebuah kata kunci yang kuat dan unik bagi setiap peranti.

- **Mandatkan pengesahsahihan pelbagai faktor (MFA) bagi pengguna yang diberi hak istimewa.** Kami memerhatikan bahawa banyak pengaturgerakan perusahaan ialah diuruskan oleh pentadbir yang tidak melindungi akaun-akaun mereka dengan MFA. Memandangkan bahawa para pentadbir ialah sasaran nilai tinggi, produk-produk patut menjadikan MFA sebuah pilihan untuk ditolak dan bukannya pilihan untuk diterima. Selanjutnya, sistem berkenaan patut menegur pihak pentadbir secara berkala untuk mendaftar di dalam MFA sehingga mereka berjaya menghidupkannya di dalam akaun mereka. NCSC Netherlands mempunyai panduan yang selari dengan CISA, sila lihat Risalah Fakta Pengesahsahihan Matang untuk maklumat lanjut.

- **Daftar Diri Tunggal (Single sign-on) (SSO).** Aplikasi IT patut melaksanakan sokongan daftar diri tunggal melalui tahap kepiawaian terbuka moden. Contohnya termasuk Penegasan Keselamatan Bahasa Penanda (Security Assertion Markup Language) (SAML) atau Hubungan IDTerbuka (OpenID Connect (OIDC). Keupayaan ini patut disediakan secara lalai tanpa kos tambahan.

- **Pengelogan Teguh.** Menyediakan log odit kualiti-tinggi kepada pelanggan tanpa kos tambahan atau konfigurasi tambahan. Log odit adalah mustahak bagi mengesan dan mendadakkan insiden keselamatan yang berpotensi berlaku. Ia juga mustahak semasa sesebuah penyiasatan insiden keselamatan yang disyaki atau disahkan berlaku. Pertimbangkan amalan terbaik seperti menyediakan integrasi mudah dengan sistem maklumat keselamatan dan pengurusan kejadian dengan akses pengantaramuka pengaturcaraan aplikasi (API) yang menggunakan waktu universal yang diselaraskan (UTC), pemformatan zon waktu standard, dan teknik-teknik pendokumentasian yang teguh.

- **Profil Pengizinan Perisian.** Para pembekal perisian patut menyampaikan saranan mengenai peranan-peranan profil pengizinan dan kes penggunaan yang dikhususkan mereka. Pengeluar patut memasukkan sebuah amaran jelas yang memaklumkan pelanggan mengenai peningkatan risiko jika mereka melencong daripada pengizinan profil yang disarankan. Contohnya, doktor perubatan boleh melihat rekod-rekod semua pesakit, tetapi seorang penjadual perubatan mempunyai akses terhad kepada maklumat tertentu yang diperlukan untuk penjadualan temujanji.

- **Keselamatan memandang ke hadapan dan bukannya keserasian yang menoleh ke belakang.** Ciri-ciri legasi keserasian yang menoleh ke belakang terlampau sering dimasukkan, dan sering dihidupkan, dalam produk walaupun ia menyebabkan risiko kepada keselamatan produk. Utamakan keselamatan daripada keserasian yang menoleh ke belakang, memperkasakan pasukan keselamatan untuk membuangkan ciri-ciri yang tidak teguh biarpun ia bererti bahawa ia akan menyebabkan pematahan perubahan.

- **Jejak dan kurangkan saiz "panduan pengerasan".** Kurangkan saiz "panduan pengerasan" yang terkandung di dalam produk dan berusaha untuk memastikan agar saiznya menyusut dengan peredaran masa bila versi-versi baharu perisian itu dikeluarkan. Integrasikan komponen-komponen "panduan pengerasan" sebagai konfigurasi lalai produk itu. Organisasi pengarang

mengiktiraf bahawa panduan pengerasan yang dipendekkan adalah hasil daripada perkongsian berlanjutan bersama pelanggan sedia ada dan termasuk usaha-usaha oleh ramai pasukan produk, termasuk pengalaman pengguna (user experience) (UX).

- **Pertimbangkan akibat pengalaman pengguna bagi pengesetan keselamatan.** Setiap pengesetan baharu meningkatkan beban kognitif ke atas pengguna akhir dan patut dinilai selaras dengan manfaat perniagaan yang boleh diperolehi daripadanya. Sebaiknya, sebuah pengesetan tidak sepatutnya wujud: sebaliknya, pengesetan paling teguh patut diintegrasikan ke dalam produk tersebut secara lalai. Bila konfigurasi diperlukan, pilihan lalai patut menjadi teguh secara lebih meluas terhadap ancaman-ancaman biasa.

Organisasi pengarang mengakui bahawa perubahan ini mungkin mempunyai kesan pengoperasian terhadap cara bagaimana perisian itu digunakan. Oleh yang demikian, input pelanggan adalah kritikal dalam mengimbangi pertimbangan pengoperasian dan keselamatan. Kami percaya bahawa pembangunan peta jalan bertulis dan sokongan eksekutif yang mengutamakan ide-ide ini ke dalam produk-produk paling kritikal bagi sesebuah organisasi merupakan langkah pertama kepada peralihan ke arah amalan-amalan pembangunan perisian yang teguh. Walaupun input pelanggan itu penting, kami telah memerhatikan kes-kes penting di mana pelanggan enggan atau tidak berupaya untuk menerimapakai tahap-tahap kepiawaian yang telah ditambahbaik, seringkalinya protokol-protokol jaringan. Ianya penting bagi pengeluar untuk mewujudkan insentif-insentif bermakna bagi pelanggan untuk kekal bergerak dengan kemajuan semasa dan tidak membenarkan mereka untuk kekal terdedah tanpa berkesudahan.

PANDUAN PENGERASAN VS PELONGGARAN

Panduan pengerasan mungkin terjadi akibat kekurangan kawalan keselamatan produk yang sedang dibenamkan ke dalam senibina sesebuah produk dari permulaan pembangunannya. Justeru, panduan pengerasan juga boleh menjadi sebuah peta jalan bagi pihak lawan untuk mengenalpasti dan mengeksploitasikan ciri-ciri yang tidak teguh. Ia merupakan sesuatu yang biasa bagi ramai organisasi untuk tidak menyedari tentang panduan pengerasan, dan oleh yang demikian mereka akan membiarkan pengesetan konfigurasi peranti mereka dalam postur yang tidak teguh. Sebuah model terbalik yang dikenali sebagai panduan pelonggaran patut menggantikan panduan pengesaran sebegini dan menjelaskan perubahan mana yang para pengguna patut lakukan sambil menyenaraikan risiko-risiko keselamatan yang terhasil sekali. Panduan-panduan ini patut ditulis oleh pengamal keselamatan yang boleh menjelaskan tukar ganti tersebut dalam bahasa yang jelas dan nyata untuk meningkatkan peluang agar ia akan dapat diterapkan dengan sebetulnya.

Daripada membangunkan panduan pengerasan yang menyenaraikan kaedah-kaedah untuk meneguhkan produk-produk, organisasi pengarang menyarankan agar pengeluar perisian beralih kepada sebuah pendekatan teguh secara lalai dan menyampaikan “panduan pelonggaran”. Panduan-panduan ini menerangkan risiko keputusan yang diambil kepada perniagaan dalam bahasa yang mudah dan senang difahami, dan boleh meningkatkan kesedaran organisasi mengenai risiko pencerobohan siber yang berniat jahat. Tukar ganti keselamatan patut ditentukan oleh eksekutif kanan pelanggan, dengan mengimbangi keselamatan dengan keperluan perniagaan yang lain.

SARANAN-SARANAN KEPADA PELANGGAN

Organisasi pengarang menyarankan organisasi untuk mempertanggungjawabkan pengeluar pembekalan perisian bagi hasil keputusan keselamatan produk-produk mereka. Sebagai sebahagian daripada ini, organisasi pengarang menyarankan agar para eksekutif mengutamakan kepentingan pemerolehan produk-produk teguh secara tereka dan teguh secara lalai. Hal ini boleh dimanifestasikan melalui pengewujudan dasar-dasar yang memerlukan jabatan-jabatan IT untuk menilai keselamatan perisian sebelum ia diperolehi, selain memperkasakan jabatan-jabatan IT untuk menolak balik jika perlu. Jabatan-jabatan IT patut diperkasa untuk membangunkan kriteria pemerolehan yang menegaskan kepentingan amalan teguh secara tereka dan teguh secara lalai (baik yang digariskan dalam dokumen ini mahupun yang lain yang telah dibangunkan oleh organisasi berkenaan). Selain daripada itu, jabatan-jabatan IT patut disokong oleh pengurusan eksekutif tatkala menguatkuasakan kriteria ini dalam keputusan pemerolehan. Keputusan organisasi untuk menerima risiko yang berkaitan produk-produk teknologi tertentu patut didokumentasikan secara rasmi, diluluskan oleh seorang eksekutif perniagaan kanan, dan kerap dibentangkan kepada pihak lembaga pengarah.

Perkhidmatan IT perusahaan utama yang menyokong postur keselamatan organisasi itu, misalnya jaringan perusahaan, identiti perusahaan dan pengurusan akses, serta operasi keselamatan dan keupayaan respons, patut dilihat sebagai fungsi perniagaan kritikan yang didana untuk diselarikan dengan kepentingan mereka kepada kejayaan misi organisasi itu. Organisasi patut membangunkan sebuah pelan untuk menaiktarafkan keupayaan-keupayaan ini untuk meraih manfaat pengeluar yang mencakupi amalan-amalan teguh secara tereka dan teguh secara lalai.

Sejauh mana yang mungkin, organisasi patut berusaha untuk menempa hubungan strategik bersama pembekal-pembekal IT utama mereka. Hubungan sebegini termasuklah keyakinan pada pelbagai tahap organisasi itu dan menyediakan wahana untuk menyelesaikan isu-isu dan mengenalpasti keutamaan-keutamaan yang dikongsi. Keselamatan patut menjadi sebuah elemen kritikal bagi hubungan sebegini dan organisasi patut berusaha untuk memperkukuhkan kepentingan amalan-amalan teguh secara tereka dan teguh secara lalai dalam kedua-dua dimensi formal (misalnya kontrak-kontrak atau perjanjian-perjanjian vendor) dan tidak formal hubungan itu. Organisasi patut menjangkakan ketelusan daripada pembekal teknologi mereka mengenai postur kawalan dalaman selain peta jalan mereka ke arah penerimapakaian amalan-amalan teguh secara tereka dan teguh secara lalai.

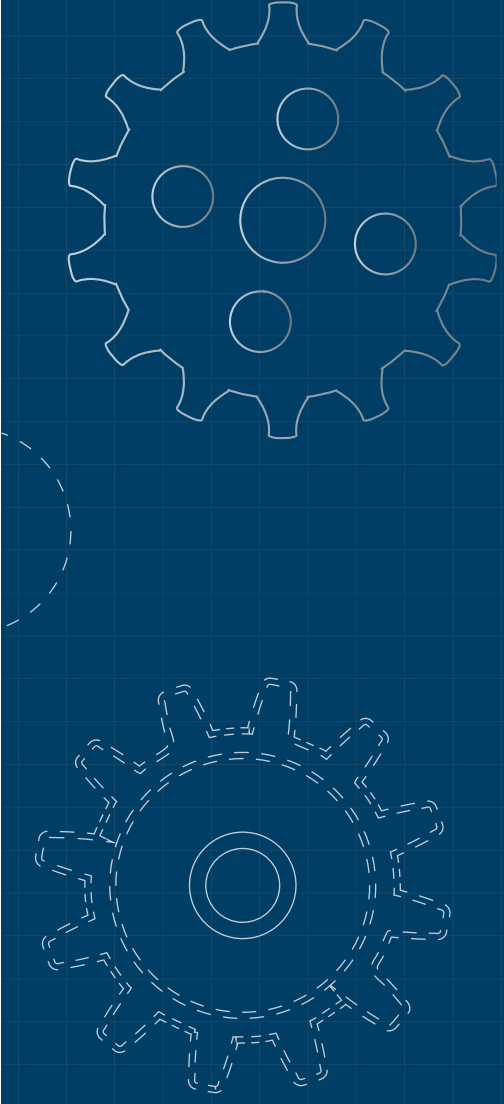
Selain menjadikan teguh secara lalai sebagai satu keutamaan di dalam sesebuah organisasi, pemimpin IT patut berusahasama dengan rakan sejawat industri mereka untuk memahami produk dan perkhidmatan mana yang akan mengabadikan dengan cara terbaik prinsip-prinsip perekaan ini. Pemimpin ini patut menyelaraskan permintaan mereka untuk membantu pengeluar dalam mengutamakan inisiatif-inisiatif keselamatan mereka yang akan datang. Dengan bekerjasama, pelanggan boleh memberi input bermakna kepada pengeluar dan mewujudkan insentif kepada mereka untuk mengutamakan keselamatan.

Sewaktu mempermanfaatkan sistem awan, organisasi patut memastikan mereka memahami model kebertanggungjawaban terkongsi bersama pembekal teknologi mereka. Maksudnya, organisasi sepatutnya mempunyai pandangan yang jelas mengenai tanggungjawab keselamatan pembekal dan bukan sekadar tanggungjawab pelanggan sahaja.

Organisasi patut mengutamakan penyedia awan yang telus mengenai postur keselamatan mereka, kawalan dalaman, dan keupayaan untuk memenuhi kewajipan mereka di bawah model kebertanggungjawaban terkongsi ini.

PENAFIAN

Maklumat yang terkandung di dalam laporan ini disediakan “seadanya” untuk tujuan pemberian maklumat sahaja. CISA dan organisasi pengarang tidak mengendors sebarang produk atau perkhidmatan komersial, termasuk mana-mana subjek analisis. Sebarang rujukan kepada entiti komersial atau produk komersial, proses-proses, atau perkhidmatan dengan lambang perkhidmatan, jenama, pengeluar, atau sebaliknya secara khusus tidak bererti atau mencadangkan pengendorsan, rekomendasi, atau pilih kasih oleh CISA dan organisasi pengarang. Dokumen ini merupakan sebuah inisiatif bersama oleh CISA yang tidak secara automatiknya berfungsi sebagai sebuah dokumen pengawalseliaan.



Sumber-Sumber

CISA

- Panduan SBOM CISA (CISA's SBOM Guidance)
- Matlamat Prestasi Keselamatan Siber Silang-Sektor CISA (CISA's Cross-Sector Cybersecurity Performance Goals)
- Garis Panduan Saling Pengoperasian Teknologi (Guidelines on Technology Interoperability)
- Pertahanan Terhadap Serangan Rantaian Bekalan Perisian CISA dan NIST (CISA and NIST's Defending Against Software Supply Chain Attacks)
- Kos Teknologi Tidak Selamat dan Apa Yang Kita Boleh Buat Mengenainya (The Cost of Unsafe Technology and What We Can Do About It) | CISA
- Hentikan Pemindahan Tanggungjawab terhadap Keselamatan Siber (Stop Passing the Buck on Cybersecurity): Mengapa Syarikat Mesti Membina Masukkan Keselamatan Ke Dalam Produk-Produk Tech (Why Companies Must Build Safety Into Tech Products) (foreignaffairs.com)
- Panduan Pengkategorian Keterdedahan Khusus Pemegang Taruh CISA (SSVC) (CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance)
- Risalah Fakta Kalis Pancingan MFA CISA (CISA's Phishing Resistant MFA Fact Sheets)
- Panduan Siber bagi Perniagaan Kecil-Kecilan | CISA (Cyber Guidance for Small Businesses) | CISA

NSA

- Risalah Maklumat Keselamatan Siber NSA mengenai Keselamatan Memori (NSA's Cybersecurity Information Sheet on Memory Safety)
- Meneguhkan Rantaian Bekalan Perisian ESF NSA (NSA's ESF Securing the Software Supply Chain): Amalan Terbaik bagi Pembekal (Best Practices for Suppliers)

FBI

- Memahami dan Merespons kepada Serangan Rantaian SolarWinds: (Understanding and Responding to the SolarWinds Supply Chain Attack): Perspektif Persekutuan (The Federal Perspective)
- Ancaman Siber – Respons dan Pelaporan (The Cyber Threat - Response and Reporting)
- Strategi Siber FBI (FBI's Cyber Strategy)

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

- Garis Panduan Identiti Digital NIST (NIST's Digital Identity Guidelines)
- Kerangka Kerja Keselamatan Siber NIST (NIST's Cyber Security Framework)
- Kerangka Kerja Pembangunan Perisian Teguh NIST (NIST's Secure Software Development Framework) (SSDF)

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

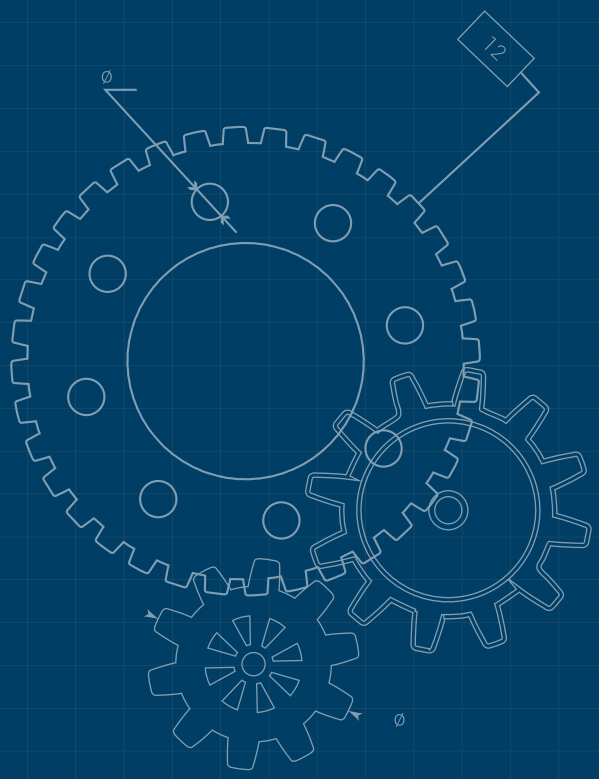
- Panduan Kod Amalan IoT bagi Pengeluar ACSC (ACSC's IoT Code of Practice Guidance for Manufacturers)

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

- Kerangka Kerja Penilaian Siber UK (The UK's Cyber Assessment Framework)
- Panduan Pembangunan dan Pengaturgerakan Teguh NCSC UK (The UK NCSC's Secure Development and Deployment guidance)
- Panduan Pengurusan Keterdedahan NCSC UK (The UK NCSC's Vulnerability Management guidance)
- Kit Peralatan Pendedahan Keterdedahan NCSC UK (The UK NCSC's Vulnerability Disclosure Toolkit)
- CHERI Universiti Cambridge (University of Cambridge's CHERI)
- Itu sahaja dan terima kasih untuk segala butirannya (So long and thanks for all the bits) NCSC.GOV.UK

Pusat Keselamatan Siber Kanada (Canadian Centre for Cyber Security) (CCCS)

- Panduan CCCS mengenai Melindungi Terhadap Serangan Rantaian Bekalan Perisian (CCCS's Guidance on Protecting Against Software Supply Chain Attacks)
- Rantaian bekalan siber (Cyber supply chain): Satu pendekatan kepada penilaian risiko (An approach to assessing risks)
- Panduan Pusat Keselamatan Siber Kanada bagi Perkakasan Tebusan CONTI (Canadian Centre for Cyber Security's CONTI ransomware guidance)



Pejabat Persekutuan Jerman bagi Keselamatan Maklumat (Germany's Federal Office for Information Security) (BSI)

- Kompendium BSI Grundschutz (The BSI Grundschutz compendium) (module CON.8)
- IEC 62443 Tahap Kepiawaian Antarabangsa (The international standard IEC 62443), Bahagian 4-1
- Laporan Keadaan Keselamatan-IT di Jerman (State of IT-security in Germany report), 2022
- Amalan keselamatan aplikasi sesawang BSI (BSI practices of web application security)

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

- Risalah Fakta pengesahsahihan Matang NCSC-NL (NCSC-NL's Mature Authentication Factsheet)

Pusat Kebangsaan Kesiapsiagaan Insiden dan Strategi untuk Keselamatan Siber Jepun (Japan's National Center of Incident Readiness and Strategy for Cybersecurity) (NISC)

- Strategi Keselamatan Siber Kebangsaan Jepun (Japan's National Cybersecurity Strategy)

Kementerian Ekonomi, Perdagangan dan Industri Jepun (Japan's Ministry of Economy, Trade and Industry) (METI)

- Panduan Pengenalan Bil Perisian Material (Software Bill of Materials) (SBOM) bagi Pengurusan Perisian (Guide of Introduction of Software Bill of Materials (SBOM) for Software Management)
- Pengumpulan Contoh Kes Penggunaan Berkaitan Kaedah-Kaedah Pengurusan bagi Penggunapakaian OSS dan Memastikan Keselamatannya (Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security)

Agensi Keselamatan Siber Singapura (Cyber Security Agency of Singapore)

- Nasihat Teknikal mengenai Pembangunan API Teguh (Technical Advisory on Secure API Development)
- Dasar Pendedahan Keterdedahan CSA SingCERT (CSA SingCERT Vulnerability Disclosure Policy)
- Senarai Semak Respons Insiden CSA SingCERT (CSA SingCERT Incident Response Checklist)
- Buku Permainan Respons Insiden CSA SingCERT (CSA SingCERT Incident Response Playbooks)
- Kerangka Kerja Keselamatan secara Tereka CSA (Security by Design Framework)
- Senarai Semak Kerangka Kerja Keselamatan secara Tereka (CSA Security by Design Framework Checklist)
- Panduan CSA kepada Pemodelan Ancaman Siber (CSA Guide to Cyber Threat Modelling)
- Skim Pelabelan Keselamatan Siber CSA (CSA Cybersecurity Labelling Scheme)

Lain-Lain

- Bagaimana Sistem Kompleks Gagal (How Complex Systems Fail)
- Keterampilan Baharu dalam kegagalan sistem kompleks (The New Look in complex system failure)

RUJUKAN

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran mengenai Kualiti secara Tereka (Juran on Quality by Design) oleh J.M. Juran, 1992.