BADAN SIBER & SANDI NEGARA

buku putih keamanan siber

PROFIL RISIKO SIBER

FINTECH PEER-TO-PEER LENDING

(Layanan Pendanaan Bersama Berbasis Teknologi Informasi)

2022

bssn.go.id

10 Risiko Siber *Fintech P2P Lending*

1. ***Kebocoran informasi sensitif karena kurangnya pengawasan terhadap layanan yang diberikan oleh pihak ketiga.***
2. ***Kebocoran informasi sensitif karena saluran komunikasi yang tidak dilindungi.***
3. ***Serangan phishing karena kurangnya kesadaran keamanan informasi.***
4. ***Gangguan ketersediaan & integritas (availability & integrity) karena pengelolaan konfigurasi yang buruk.***
5. ***Gangguan ketersediaan & integritas (availability & integrity) karena kesalahan arsitektur keamanan.***
6. ***Hilangnya aspek ketersediaan (availability) pada sistem karena serangan Distributed Denial of Service (DDoS).***
7. ***Kebocoran data karena celah kerentanan keamanan pada aplikasi.***
8. ***Kebocoran data karena kredensial yang lemah.***
9. ***Serangan Advanced Persistent Threat (APT) yang memanfaatkan kesalahan atau lemahnya kesadaran keamanan informasi personil.***
10. ***Serangan Advanced Persistent Threat (APT) yang memanfaatkan Brute Force Attack.***

Tim Penyusun

Penanggung Jawab

Edit Prima
Direktur Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata (KSS KPP),
Deputi Bidang Keamanan Siber dan Sandi Perekonomian,
Badan Siber dan Sandi Negara

Ketua Tim

Baderi

Anggota

Nayuki
Afifah
Agus Indramawan
Alvin Devara Lesmana
Andhika Prastyo
Ariadi Basuki
Ariq Bani Hardi
Ardita Widyasari
Dwi Retno Ambarwati
Febrianto Dicky Saputra
Mawidyanto A. M
Mohamad Endhy Aziz
Nunik Yulianingsih
Rezki Wicaksono
Reynaldi Agnar Maulana
Rio Yunia Pratama
Riski Pradipta
Sandromedo C. Nugroho
Yogi Nur Hakim
Yurike Nuramelia
Zelstein Mauli Pasaribu

Direktorat Keamanan Siber dan Sandi Keuangan,
Perdagangan dan Pariwisata,
Deputi Bidang Keamanan Siber dan Sandi Perekonomian,
Badan Siber dan Sandi Negara

Jalan Raya Muchtar 70
Depok, Jawa Barat – 16516

☏ +62 21 77973360
humas[at]bssn.go.id

Pendahuluan

Latar Belakang

Perkembangan digitalisasi di Indonesia turut mempengaruhi industri jasa keuangan. Saat ini semakin banyak layanan keuangan digital yang menyesuaikan dengan kebutuhan masyarakat. Kehadiran *financial technology* (*fintech*) terbukti memberikan kemudahan layanan finansial di tengah masih banyaknya masyarakat Indonesia yang masuk ke dalam kategori *unbanked*. Salah satu layanan keuangan digital yang berkembang dengan signifikan adalah Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI), atau dikenal juga sebagai Fintech P2P Lending. Fintech P2P Lending mempertemukan pemberi dana (*lender*) dengan penerima dana (*borrower*) melalui platform digital (*online*).

Berdasarkan data statistik Asosiasi *Fintech* Pendanaan Bersama Indonesia (AFPI), hingga September 2022 tercatat agregat penyaluran pendanaan mencapai Rp 455 Triliun yang disalurkan oleh 960.396 pemberi pinjaman (*lender*) kepada 90,21 juta penerima pinjaman (*borrower*). Hal ini adalah bukti nyata kontribusi industri Fintech P2P Lending dalam memeratakan inklusi keuangan di Indonesia. Digitalisasi industri keuangan, termasuk layanan yang diberikan oleh Fintech P2P Lending, merupakan hal yang terus didorong oleh pemerintah untuk pertumbuhan ekonomi serta inklusi keuangan. Namun, hal yang juga wajib menjadi penekanan adalah adanya keseimbangan antara inovasi dan kemudahan yang dibawa oleh industri, dengan sisi keamanan dan perlindungan terhadap konsumen.

Badan Siber dan Sandi Negara (BSSN), sesuai dengan mandat tugas yang diberikan berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 sebagai perubahan atas Peraturan Presiden 133 Tahun 2017, bersama dengan instansi-instansi regulator terkait serta asosiasi industri, terus berupaya mengawal dan memastikan sisi keamanan siber dan perlindungan konsumen menjadi prioritas utama melalui berbagai inisiatif kebijakan dan kolaborasi, agar ekosistem keuangan digital yang dibangun dapat terus tumbuh dan memberikan manfaat yang luas kepada masyarakat.

Tujuan & Manfaat Penyusunan Dokumen

Tujuan penyusunan buku putih ini adalah mengidentifikasi risiko-risiko siber prioritas pada platform P2P Lending atau Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI), serta memberikan langkah rekomendasi untuk memitigasi risiko-risiko tersebut.

Adapun manfaat dari dibuatnya dokumen ini antara lain:

- Sebagai referensi bagi industri Fintech P2P Lending dalam mengidentifikasi risiko-risiko siber yang perlu menjadi prioritas di organisasi;
- Memberikan rekomendasi kepada industri Fintech P2P Lending dalam memitigasi risiko-risiko siber prioritas yang telah teridentifikasi;
- Sebagai referensi bagi pihak-pihak terkait (regulator, akademisi, praktisi, dsb) dalam mengembangkan ekosistem layanan keuangan digital serta perlindungan terhadap konsumen.

Keamanan Siber pada Fintech P2P Lending

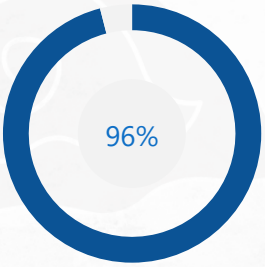
Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) atau dikenal sebagai Fintech P2P Lending adalah penyelenggaraan layanan jasa keuangan yang mempertemukan pemberi dana (*lender*) dengan penerima dana (*borrower*) dalam melakukan pendanaan konvensional atau berdasarkan prinsip syariah melalui sistem elektronik dengan menggunakan internet. Hingga 22 April 2022, jumlah penyelenggara Fintech P2P Lending yang berizin di Otoritas Jasa Keuangan (OJK) berjumlah 102 organisasi.

Penyelenggaraan Fintech P2P Lending saat ini telah diatur dalam Peraturan Otoritas Jasa Keuangan (OJK) Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, termasuk dalam hal sistem pengamanan yang diterapkan dalam organisasi dan sistem elektronik yang dioperasikan. Peraturan tersebut juga mengatur rekam jejak audit, akses dan penggunaan data pribadi, serta jangka waktu data dan penghapusan data.

Untuk mengenali lebih jauh risiko-risiko, berikut dengan penerapan keamanan siber dalam industri Fintech P2P Lending, BSSN bekerjasama dengan Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) untuk melakukan survey yang memotret gambaran penerapan keamanan siber, sekaligus memetakan risiko-risiko siber yang dinilai merupakan prioritas pada industri Fintech P2P Lending.[1]

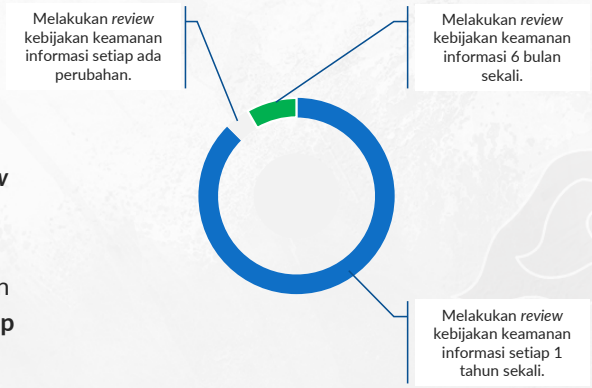
Potret kondisi penerapan keamanan siber industri Fintech P2P Lending disajikan dalam infografis pada gambar berikut, dan profil risiko siber yang menjadi prioritas dalam industri Fintech P2P Lending dijabarkan dalam bab selanjutnya (Profil Risiko & Rekomendasi).

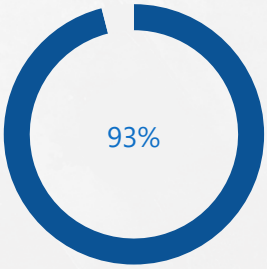
[1] Survey dilakukan dalam rangkaian Kegiatan Workshop Profiling Risiko oleh Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata, BSSN pada September 2022 yang dihadiri oleh perwakilan dari 28 perusahaan Fintech P2P Lending anggota AFPI.



Berdasarkan survey yang dihadiri oleh perwakilan dari industri Fintech P2P Lending, 96% dari organisasi sudah **memiliki kebijakan yang mengatur keamanan informasi** di organisasi.

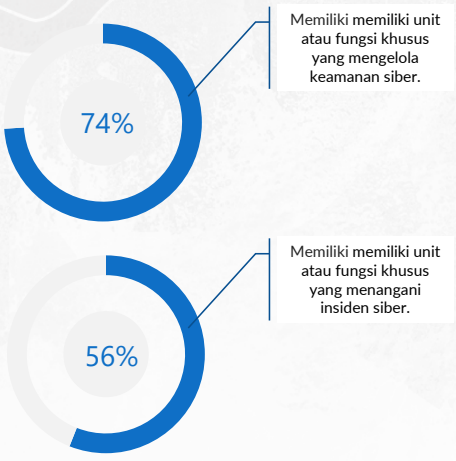
Organisasi yang sudah memiliki kebijakan keamanan informasi sebagaimana poin 1 di atas, 84% diantaranya **melakukan *review* kebijakan setiap 1 tahun sekali**. 4% diantaranya melakukan ***review* kebijakan setiap 6 bulan sekali**, dan 8% sisanya melakukan ***review* setiap kali terdapat perubahan**.





Sebanyak 93% organisasi dari peserta survey sudah **menerapkan standar dan memiliki sertifikasi ISO 27001** tentang Sistem Manajemen Keamanan Informasi.

74% organisasi sudah telah memiliki **unit atau fungsi khusus yang mengelola keamanan siber**, dan sebanyak 56% organisasi sudah memiliki **unit atau fungsi khusus yang menangani insiden siber**.



Potret penerapan keamanan siber pada industri Fintech P2P Lending.

Profil Risiko & Rekomendasi

Bagian ini menjabarkan 10 risiko siber yang perlu menjadi prioritas dalam industri Fintech P2P Lending, berikut dengan rekomendasi mitigasi yang dapat dilakukan organisasi untuk mengurangi risiko-risiko tersebut.[2]

1 *Kebocoran informasi sensitif karena kurangnya pengawasan terhadap layanan yang diberikan oleh pihak ketiga.*

Deskripsi

Risiko ini dapat terjadi ketika akses yang diberikan kepada pihak ketiga (mitra perusahaan, penyedia jasa, dsb) terhadap informasi sensitif yang dimiliki organisasi tidak dilakukan pengamanan dan pengawasan dengan baik. Informasi sensitif yang bocor umumnya tidak dalam volume yang besar, namun tidak dimitigasi dengan baik tetap dapat berakibat fatal. Minimnya peninjauan dan penerapan kontrol yang ketat terhadap informasi yang dibagikan dan/atau diberikan kepada pihak ketiga dapat berakibat pada bocornya informasi sensitif tersebut.

Dampak

Dampak dari risiko ini meliputi, namun tidak terbatas pada:

- Bocornya informasi sensitif kepada pihak-pihak yang tidak berkepentingan, seperti data terkait konsumen/nasabah.
- Rusaknya reputasi organisasi karena kegagalan dalam melindungi data sensitif.

[2] Profil Risiko dan Rekomendasi yang dijabarkan adalah hasil pengolahan dan tindak lanjut survey dalam rangkaian Kegiatan Workshop Profiling Risiko oleh Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata, BSSN. Penjabaran setiap profil risiko tidak berdasarkan urutan atau prioritasi tertentu.

Rekomendasi

Organisasi sebaiknya menerapkan langkah-langkah berikut untuk mengurangi risiko kebocoran informasi sensitif yang disebabkan karena minimnya kontrol terhadap layanan yang diberikan oleh pihak ketiga.

- Menyusun dan menetapkan kebijakan yang mengatur kerjasama dengan pihak ketiga dan secara rutin melakukan reviu atas kerjasama yang sudah dilakukan dengan pihak-pihak ketiga di luar organisasi, termasuk dalam hal akses ke data penting atau sensitif milik organisasi;
- Meningkatkan pengawasan terhadap pihak ketiga yang diberikan akses ke ke data penting atau sensitif milik organisasi;
- Memastikan pihak ketiga menerapkan ketentuan-ketentuan dalam melindungi data dan akses ke data sensitif yang sudah diberikan oleh organisasi, misalnya dengan memenuhi persyaratan sertifikasi keamanan informasi yang masih berlaku;
- Menambahkan mekanisme keamanan dalam pertukaran informasi antara organisasi dengan pihak ketiga yang diberikan akses ke informasi sensitif, seperti:
    1) Kontrol perlindungan informasi dari upaya penyadapan, akses tidak sah, penyalinan, modifikasi, dan penghapusan informasi secara tidak sah, termasuk kontrol akses yang sepadan dengan klasifikasi informasi yang dilindungi, misalnya dengan menggunakan teknik kriptografi.
    2) Kontrol untuk pelacakan dan mekanisme anti sangkal terhadap informasi yang sudah diakses.
    3) Identifikasi terhadap pihak-pihak yang berperan sabagai pemilik informasi, pemroses informasi, pemilik risiko, dan pengguna informasi, sesuai dengan peraturan yang berlaku.
    4) Penanganan dan penanggung jawab pada saat terjadi insiden keamanan informasi.
    5) Penerapan klasifikasi atas setiap jenis data atau informasi, misalnya menggunakan sistem pelabelan.
    6) Kebijakan atau pedoman dalam menggunakan aset-aset TI dalam proses pertukaran informasi secara aman.
    7) Kebijakan penyimpanan dan masa retensi data sensitif untuk diterapkan di organisasi maupun oleh pihak ketiga yang diberikan akses.

2 *Kebocoran informasi sensitif karena saluran komunikasi yang tidak dilindungi.*

Deskripsi

Risiko kebocoran data yang sering mengemuka disebabkan karena saluran komunikasi yang tidak dilindungi atau diterapkannya teknik pengamanan yang memadai, seperti kesalahan atau tidak diterapkannya saluran komunikasi terenkripsi berbasis SSL/TLS, tidak diterapkannya teknik kriptografi yang sesuai standar keamanan, dsb. Dengan semakin banyaknya interkoneksi antar berbagai aplikasi, peretas dapat melakukan pencurian informasi sensitif dengan memantau lalu lintas paket data yang dikirim-terimakan dalam keadaan tidak terenkripsi (*cleartext*).

Dampak

Dampak dari risiko ini memiliki karakteristik yang sama dengan risiko terkait kebocoran informasi sensitif sebagaimana dijabarkan sebelumnya, yang meliputi namun tidak terbatas pada bocornya informasi sensitif kepada pihak-pihak yang tidak berkepentingan, kerusakan reputasi perusahaan, dan beberapa dampak turunan lain. Dalam lingkup dampak yang lebih kecil, kebocoran informasi teknis, seperti struktur direktori, *library,* atau *framework* yang digunakan pada aplikasi tetap berisiko untuk dimanfaatkan peretas dalam serangan-serangan siber lanjutan.

Rekomendasi

Organisasi sebaiknya menerapkan langkah-langkah berikut untuk meminimalisasi risiko kebocoran data karena saluran komunikasi yang tidak dilindungi.

- Menetapkan dan menerapkan klasifikasi atas setiap jenis data atau informasi dalam organisasi, dan memastikan bahwa tim pengembang aplikasi mengetahui dan memahami klasifikasi atas setiap jenis data atau informasi tersebut.
- Menyusun pedoman pengembangan aplikasi yang aman sebagai rujukan dan standar dalam pengembangan berbagai aplikasi di organisasi.
- Menetapkan persyaratan keamanan (termasuk penerapan *secure programming*, penerapan teknik kriptografi yang sesuai dengan standar industri, dsb) dalam proses pengembangan aplikasi.

- Melakukan penilaian kerentanan atau *penetration test* secara terencana, terdokumentasi dan dimasukkan dalam siklus pengembangan aplikasi.
- Menyediakan sarana dan prasarana pendukung implementasi keamanan dalam pengembangan aplikasi (misal, SSL *certificates*, *local source code repository*, dsb).
- Menerapkan standar untuk pesan atau gambar yang ditampilkan saat terjadi permasalahan pada aplikasi.

3 *Serangan phishing karena kurangnya kesadaran keamanan informasi.*

Deskripsi

Phishing adalah salah satu bentuk kejahatan siber melalui serangan rekayasa sosial (*social engineering*) dengan memperdaya korban atau target serangan. Peretas menggunakan metode-metode tertentu agar korban memberikan informasi kredensial yang dimiliki seperti kata sandi, *token*, dsb. Selain itu, *phishing* juga dapat dilakukan sebagai metode untuk membuat korban menjalankan suatu *malicious software* (*malware*), sehingga peretas memperoleh akses ke dalam sistem tanpa disadari oleh korban.

Phishing dapat menyasar siapapun dalam organisasi, sehingga perlu adanya kewaspadaan dari seluruh pihak terhadap jenis serangan ini. Serangan *phishing* berkontribusi besar pada banyak kejadian insiden siber, seperti kebocoran data nasabah, kebocoran akun pengelola TI (administrator), kebocoran data konfidensial organisasi, dsb. Kebocoran data ini dapat berakibat fatal bagi organisasi yang menjadi korban. *Phishing* dengan rekayasa sosial lebih sering digunakan oleh peretas karena mudahnya mengeksploitasi kelemahan manusia, yaitu ketidaktahuan dan rendahnya kesadaran keamanan informasi.

Dampak

Dampak langsung dari serangan *phishing* sangat bergantung pada individu yang menjadi korban. Sedangkan dampak tidak langsung berpengaruh dan dapat berakibat fatal pada organisasi, meliputi kebocoran data pribadi, kebocoran kredensial penting, infeksi *malware*, kebocoran data kekayaan intelektual organisasi, gangguan operasional, sampai dengan dampak yang lebih signifikan seperti kerusakan reputasi, dampak hukum, dan sanksi/penalti.

Rekomendasi

Organisasi sebaiknya menerapkan langkah-langkah berikut untuk meminimalisasi risiko serangan *phishing* karena kurangnya kesadaran keamanan.

- Menyelenggarakan program pendidikan dan pelatihan kesadaran keamanan informasi. Program kesadaran keamanan informasi dapat dilakukan melalui pelatihan yang diselaraskan dengan kebijakan dan prosedur keamanan informasi yang ditetapkan organisasi. Kegiatan tersebut dilakukan secara berkala, atau diberikan pada pegawai baru dan pegawai yang dipindahkan ke posisi baru yang menuntut kebutuhan pengamanan informasi yang berbeda dari posisi sebelumnya.

Dalam pelaksanaannya, program kesadaran keamanan informasi perlu mempertimbangkan informasi organisasi yang harus dilindungi dan kendali keamanan informasi yang sudah diterapkan saat ini untuk melindungi informasi sensitif. Selanjutnya, pemahaman pegawai terhadap keamanan informasi harus dinilai pada setiap akhir kegiatan pelatihan untuk menguji pemahaman, pengetahuan dan efektivitas dari program peningkatan kesadaran keamanan informasi.

- Menyelenggarakan program simulasi kesadaran keamanan informasi, misalnya melalui simulasi *phishing* kepada seluruh karyawan atau dilakukan secara bertahap untuk unit kerja tertentu. Kegiatan ini dapat diprogramkan oleh organisasi sesuai kebutuhan (misal, 2-4 kali dalam setahun). Hasil dari simulasi *phishing* dapat dijadikan bahan evaluasi kesadaran keamanan informasi karyawan atau pegawai dalam organisasi.
- Membangun budaya kesadaran keamanan informasi, yang mencakup beberapa aspek penting, yaitu:
    1) Komitmen manajemen atas pentingnya keamanan informasi di seluruh organisasi;
    2) Kewajiban atau kebutuhan atas kepatuhan (*compliance*) terhadap suatu perjanjian kontrak, standar, peraturan tertentu;
    3) Tanggung jawab pribadi atas tindakan pegawai dalam mengamankan atau melindungi informasi milik organisasi atau milik pihak lain yang berkepentingan;
    4) Kebijakan dan prosedur keamanan informasi yang berlaku di organisasi, serta mekanisme kontrol atau kendali yang telah diterapkan.

4 *Gangguan ketersediaan & integritas (availability & integrity) karena pengelolaan konfigurasi yang buruk.*

Deskripsi

Salah satu proses pengelolaan teknologi informasi adalah pengelolaan konfigurasi (*configuration management*) yang bertujuan menghasilkan konsistensi dari konfigurasi dan atribut berbagai perangkat dan sistem TI yang dikelola organisasi, serta tersedianya informasi untuk catatan dan penelusuran terhadap setiap perubahan konfigurasi. Sayangnya, sering kali pengelolaan konfigurasi tidak dilakukan dengan baik yang disebabkan karena berbagai faktor seperti keterbatasan personil pengelola TI, belum adanya kebijakan pengelolaan TI yang jelas di organisasi, dsb. Pengelolaan konfigurasi yang buruk dapat dimanfaatkan oleh peretas yang berimplikasi pada gangguan pada aspek ketersediaan (*availability*) dan integritas (*integrity*) pada sistem dan data yang dikelola organisasi.

Dampak

Risiko gangguan ketersediaan & integritas (*availability & integrity*) karena pengelolaan konfigurasi yang buruk dapat berdampak pada eksploitasi kerentanan *bad configuration management* dan berimplikasi pada *system downtime* yang tidak terprediksi dan akhirnya merugikan organisasi baik secara secara finansial atau non-finansial. Dampak lainnya adalah minimnya akuntabilitas dan *audit trail* perubahan konfigurasi yang dapat merugikan organisasi.

Rekomendasi

Organisasi harus menyusun dan menetapkan kebijakan pengelolaan konfigurasi untuk diterapkan pada aset-aset TI organisasi, khususnya pada sistem atau aplikasi penting, untuk meminimalisasi risiko gangguan ketersediaan & integritas karena pengelolaan konfigurasi yang buruk. Kebijakan pengelolaan konfigurasi bertujuan memastikan adanya proses dan siklus dari perubahan konfigurasi, informasi perihal perubahan yang dilakukan, dan tersedianya dokumentasi untuk digunakan oleh pihak-pihak yang berkepentingan (*system administrator,* pengembang perangkat lunak, dsb) dengan tepat dan akurat.

Dalam menerapkan pengelolaan konfigurasi, hal-hal berikut harus menjadi pertimbangan.

- Memastikan poin-poin berikut tercakup dalam kebijakan pengelolaan konfigurasi, yakni:

1) Identifikasi atas sistem, komponen, dan perkembangan perubahan konfigurasi untuk memberikan informasi perubahan di setiap bagian komponen sistem agar tersedia mekanisme identifikasi, dokumentasi, serta pelacakan pada setiap titik waktu.
2) Evaluasi terhadap seluruh permintaan/pengajuan perubahan konfigurasi, dan persetujuan atas permintaan tersebut, dengan tujuan mengendalikan modifikasi desain sistem, *hardware*, *firmware*, *software*, dan dokumentasi.
3) Pencatatan dan pelaporan pada setiap *item* konfigurasi (misalnya, *hardware, software, firmware*, dsb) pada seluruh proses, mulai dari fase awal selama desain sampai dengan fase produksi, sehingga jika muncul suatu permasalahan pada sistem, verifikasi konfigurasi konfigurasi dasar dan perubahan yang sudah disetujui dapat dengan cepat ditentukan.
4) Verifikasi terhadap dokumentasi konfigurasi sistem dan subsistem sesuai dengan karakteristik sistem secara fungsional, sebelum disetujui atau diterima.

- Menerapkan pengelolaan konfigurasi pengelolaan konfigurasi terpusat atau menggunakan perangkat terotomatisasi (*automated tools*) untuk efisiensi dan akurasi dalam pengelolaan konfigurasi, serta meningkatkan visibilitas terhadap status/kondisi sistem (*system health*) dan *security configuration* pada aset-aset TI yang dikelola.

5 *Gangguan ketersediaan & integritas (availability & integrity) karena kesalahan arsitektur keamanan.*

Deskripsi

Arsitektur keamanan menjabarkan desain strategi keamanan siber dari suatu organisasi yang mengarahkan komponen-komponen proses, personil dan teknologi dalam melindungi organisasi dari ancaman-ancama eksternal dan internal. Kegagalan dalam membangun arsitektur keamanan yang tepat bagi organisasi akan menyebabkan kegagalan dalam memitigasi ancaman-anacam siber yang berkembang, serta dimanfaatkan oleh peretas yang berimplikasi pada gangguan pada aspek ketersediaan (*availability*) dan integritas (*integrity*) pada sistem dan data yang dikelola organisasi.

Dampak

Dampak langsung dari risiko ini bergantung pada motivasi aktor kejahatan siber yang melakukan serangan, namun secara umum dapat merugikan organisasi baik secara secara finansial atau non-finansial. Beberapa contoh dampak fatal pada organisasi, meliputi kebocoran data pribadi, kebocoran data kekayaan intelektual organisasi, gangguan operasional, dsb.

Rekomendasi

Organisasi sebaiknya menerapkan proses pengembangan yang aman (*secure software development lifecycle*) dengan menetapkan ketentuan atau persyaratan formal dalam membangun arsitektur, sistem dan layanan berbasis TI. Untuk mencapai hal tersebut, aspek-aspek berikut harus menjadi pertimbangan.

- Membangun dan memastikan bahwa desain serta arsitektur keamanan sesuai dengan tujuan dan risiko bisnis.
- Memisahkan tugas dan fungsi dalam pengembangan, pengujian dan implementasi/operasi sistem.
- Menetapkan panduan keamanan dalam alur hidup pengembangan perangkat lunak:
  1) keamanan dalam metodologi pengembangan perangkat lunak.
  2) pedoman *secure coding* untuk setiap bahasa pemrograman yang digunakan.
- Memastikan keamanan dalam kendali versi (*version control*) aplikasi dan sistem.

- Menetapkan persyaratan keamanan dalam tahap penyusunan spesifikasi dan desain.
- Menentukan fase (*checkpoint*) untuk pemeriksaan keamanan dalam proyek pengembangan perangkat lunak.
- Memastikan dilakukannya pengujian sistem dan keamanan (misal, *regression testing*, *code scan*, *penetration test*, dsb) pada proses pengembangan perangkat lunak.
- Memastikan bahwa jika pengembangan aplikasi menggunakan tenaga *outsource*, organisasi harus memperoleh jaminan bahwa pihak ketiga yang melakukan pengembangan aplikasi mematuhi aturan organisasi untuk pengembangan yang aman.

6 *Hilangnya aspek ketersediaan (availability) pada sistem karena serangan Distributed Denial of Service (DDoS).*

Deskripsi

Serangan siber berupa Distributed Denial of Service (DDoS) dilakukan dengan membanjiri atau membuat penuh lalu lintas jaringan internet pada sistem yang menjadi target/korban. Umumnya serangan siber ini melibatkan ratusan atau bahkan ribuan perangkat komputasi yang memiliki kerentanan teknis tertentu, atau dalam kendali seorang peretas, lalu mengarahkan serangannya ke satu sistem yang menjadi target sampai dengan sistem tersebut menjadi tidak bisa diakses.

Pelaku menggunakan berbagai metode atau *tool* untuk membanjiri targetnya dengan *bad request*, menyalahgunakan protokol jaringan, atau mengeksploitasi kerentanan pada server publik sedemikian rupa sehingga sistem korban tidak dapat menanggapi permintaan. Serangan DDoS adalah serangan siber yang sangat sulit dihindari karena menargetkan aplikasi atau server yang terhubung ke internet, sehingga semua jenis dan skala industri memiliki paparan risiko yang sama.

Dampak

Dampak dari serangan DDoS bervariasi tergantung dari tipe dan durasi waktu dari serangan (mulai dari hitungan menit, jam hingga beberapa hari) dan jenis layanan yang terdampak. Dampak dari risiko ini meliputi namun tidak terbatas pada:

- Kerugian finansial, yang diakibatkan dari hilangnya pemasukan atau transaksi karena layanan tidak dapat diakses, kerusakan fisik/non-fisik pada aset yang terdampak serangan, dsb.
- Beralihnya pelanggan ke kompetitor bisnis atau layanan digital yang lain, karena umumnya masyarakat saat ini menginginkan layanan digital yang cepat dan responsif. Hal ini juga dapat berdampak pada hilangnya kepercayaan pelanggan terhadap organisasi.
- Tuntutan hukum atau sanksi tertentu, misalnya karena kegagalan dalam mencapai Service Level Agreement (SLA) yang sudah ditetapkan.

Rekomendasi

Organisasi sebaiknya menerapkan langkah-langkah berikut untuk mengurangi risiko hilangnya aspek ketersediaan (*availability*) sistem karena serangan DDoS.

- Menerapkan mekanisme perlindungan terhadap serangan DDoS, misalnya melalui mekanisme proteksi secara *on premises, outsourced solution*, atau *hybrid* DDoS *protection*.
- Menyusun dan menetapkan strategi untuk mendeteksi, mencegah, dan mengurangi serangan DDoS.
- Mengidentifikasi celah keamanan yang berpotensi dimanfaatkan untuk serangan DDoS dan menilai potensi ancaman terkait serangan jenis ini.
- Mempersiapkan tim respon yang mampu mengidentifikasi dan mengurangi dampak dari serangan DDoS, serta mengevaluasi strategi atau mekanisme pertahanan siber pada organisasi (misal, dengan melakukan *cyber drill*).
- Memperbarui perangkat lunak atau teknologi untuk pertahanan siber, serta memastikan bahwa perangkat-perangkat tersebut bekerja serta dikonfigurasi dengan optimal.
- Menerapkan mekanisme perlindungan/kontrol teknis dan administratif dalam mencegah serangan DDoS.
- Memindai secara berkala *port* jaringan dan layanan digital yang terhubung ke internet.
- Menerapkan pembaruan/*patch* keamanan secara berkala.
- Memblokir paket-paket jaringan yang tergolong ke dalam *bad request* dan memanfaatkan *real-time intelligence feeds* untuk mendapatkan informasi situasi siber aktual.

7 *Kebocoran data karena celah kerentanan keamanan pada aplikasi.*

Deskripsi

Peretas selalu mencari cara untuk mendapatkan akses ke data penting atau sensitif milik organisasi, salah satunya dengan memanfaatkan celah-celah kerentanan yang ada pada aplikasi atau perangkat lunak. Modus tersebut dilakukan dengan memodifikasi konfigurasi atau melakukan eksploitasi pada bagian-bagian di aplikasi yang memiliki kerentanan (*vulnerable*). Selanjutnya, pelaku mendapatkan akses ke dalam sistem dan berupaya mendapatkan data penting milik organisasi.

Dampak

Karena celah kerentanan ini memungkinkan peretas mengambil alih sistem/aplikasi secara penuh dan berakibat bocornya data penting organisasi dalam jumlah besar, maka dampak dari risiko ini dapat berupa:

- Bocornya informasi sensitif kepada pihak-pihak yang tidak berkepentingan, seperti data terkait konsumen/nasabah, data konfidensial bisnis, hak kekayaan intelektual milik organisasi, dsb.
- Tuntutan hukum, dimana kewajiban pelindungan terhadap data pribadi milik masyarakat sudah diatur dalam regulasi sesuai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP) serta beberapa ketentuan regulasi lainnya.
- Rusaknya reputasi organisasi karena kegagalan dalam melindungi data sensitif.

Rekomendasi

Organisasi sebaiknya melakukan pengelolaan kerentanan keamanan (*vulnerability management*) untuk mengurangi risiko kebocoran data karena celah kerentanan keamanan pada aplikasi. Pengelolaan kerentanan pada aplikasi mencakup 3 bagian yakni: i) identifikasi kerentanan teknis; 2) evaluasi kerentanan teknis; dan 3) tindakan untuk mengatasi kerentanan teknis.

Dalam mengidentifikasi kerentanan teknis, organisasi perlu mempertimbangkan hal-hal sebagai berikut.

- Mendefinisikan dan menetapkan peran dan tanggung jawab yang terkait dengan proses pengelolaan kerentanan teknis, termasuk pemantauan

kerentanan, penilaian risiko kerentanan, pembaruan, pelacakan aset, dan tanggung jawab koordinasi saat diperlukan.

- Melakukan penilaian kerentanan atau *penetration test* secara terencana, terdokumentasi, dan dilakukan secara periodik oleh personil yang kompeten dan ditugaskan secara spesifik untuk melakukan identifikasi kerentanan.
- Menggunakan perangkat pemindaian kerentanan (*vulnerability scanner*) yang sesuai dengan teknologi yang digunakan dan untuk memverifikasi apakah pembaruan sistem (*patching*) untuk memperbaiki kerentanan tersebut berhasil.
- Melacak penggunaan *libraries* dan *source code* pihak ketiga yang berpotensi menyebabkan kerentanan di aplikasi dan sistem TI.

Dalam melakukan evaluasi kerentanan teknis yang teridentifikasi, hal-hal berikut harus menjadi pertimbangan.

- Menganalisis dan memverifikasi laporan untuk menentukan respon dan kegiatan perbaikan tertentu yang harus diperlukan.
- Setelah kerentanan teknis teridentifikasi, identifikasi risiko-risiko yang terkait dan tindakan mitigasi harus dilakukan. Tindakan tersebut dapat berupa memperbarui sistem yang rentan atau menerapkan kontrol keamanan tambahan.

Selanjutnya, dalam mengambil tindakan untuk mengatasi kerentanan teknis yeng ditemukan, organisasi harus memastikan seluruh *patch* dan perubahan harus diuji sebelum diterapkan pada sistem produksi dan didokumentasikan. Beberapa praktek berikut dapat menjadi panduan dalam mengatasi kerentanan-kerentanan teknis pada aplikasi dan sistem TI organisasi.

- Mengambil tindakan yang tepat dan secara tepat waktu dalam menanggapi hasil identifikasi kerentanan teknis, serta menentukan *timeline* untuk tindakan aksi terhadap pemberitahuan kerentanan teknis yang teridentifikasi.
- Menguji dan mengevaluasi pembaruan sebelum dipasang pada aplikasi atau sistem produksi untuk memastikan mekanisme pembaruan dilakukan dengan efektif dan tidak mengakibatkan efek samping yang tidak dapat ditoleransi.
- Menangani sistem dengan tingkat risiko yang lebih tinggi terlebih dahulu.
- Jika terdapat celah kerentanan yang teridentifikasi namun pembaruan/*patch* belum tersedia atau pembaruan tidak dapat dipasang, pertimbangkan kontrol lain, seperti:
    1) Menerapkan solusi yang disarankan oleh vendor perangkat lunak resmi atau sumber lain yang relevan.

2) Mematikan layanan, fitur, atau kapabilitas yang terkait dengan kerentanan.
3) Menambahkan kontrol akses pada *network boundary* (misal, perangkat keamanan jaringan seperti firewall).
4) Meningkatkan pemantauan untuk mendeteksi serangan-serangan yang berpotensi memanfaatkan celah keamanan yang teridentifikasi.

8 *Kebocoran data karena kredensial yang lemah.*

Deskripsi

Kredensial, berupa informasi identitas beserta kata sandi (misal, *username* dan *password*), merupakan informasi yang diperlukan pada mekanisme autentikasi untuk membatasi akses ke sumber daya tertentu atau data sensitif. Dalam kenyataannya, seringkali dijumpai pengguna dan pengelola TI masih memilih dan menggunakan *password* yang lemah, sehingga mudah ditebak oleh peretas, dieksploitasi dengan teknik-teknik serangan tertentu (misal, *brute force attack*, *dictionary attack, rainbow attack,* dsb), atau *social engineering*. Kelemahan tersebut juga disebabkan karena tidak diterapkannya kebijakan yang mengikat tentang penggunaan kredensial yang kuat, termasuk memastikan bahwa sistem dapat mengenali dan mencegah pengguna/pengelola TI menggunakan kredensial yang lemah.

Beberapa ciri penggunaan kredensial yang lemah diantaranya:

- Menggunakan *password* yang terkait dengan informasi pribadi (misal, nama, nomor dan tanggal penting yang berkaitan dengan informasi pribadi).
- Menggunakan *password* yang sangat umum dan banyak digunakan oleh orang lain (misal, "123456", "*password*", "qwerty", "*sunshine*", dsb).
- Menggunakan *password* sesuai pola keyboard (misal, "123456789", "qwerty", "asdfghjkl", dsb).
- Menggunakan *password* dengan karakter yang pendek, frase sederhana, atau dan minim kombinasi (huruf besar-kecil, angka, simbol).

Dampak

Peretas dapat mengeksploitasi kredensial yang lemah dengan berbagai teknik serangan seperti *brute force attack*, *dictionary attack*, *social engineering*, dsb. Hal tersebut dapat berdampak pada bocornya akses sistem dan informasi sensitif kepada pihak-pihak yang tidak berkepentingan, seperti data terkait konsumen/nasabah, data konfidensial bisnis, hak kekayaan intelektual milik organisasi, dsb. Risiko ini juga dapat menyebabkan dampak yang lebih fatal pada organisasi, meliputi kebocoran data pribadi, kebocoran kredensial penting, infeksi *malware*, kebocoran data kekayaan intelektual organisasi, gangguan operasional, sampai dengan dampak yang lebih signifikan seperti kerusakan reputasi, dampak hukum, dan sanksi/penalti.

Rekomendasi

Organisasi sebaiknya melakukan pengelolaan informasi autentikasi melalui manajemen dan penanganan informasi autentikasi yang aman. Dalam mengelola informasi autentikasi, organisasi harus memastikan bahwa:

- *Password*, *personal identification number* (PIN), atau metode sejenisnya dibuat secara otomatis sebagai informasi autentikasi rahasia sementara (*temporary*) tidak dapat ditebak dan unik untuk setiap personil, dan personil tersebut diwajibkan untuk mengubahnya setelah penggunaan pertama.
- Terdapat prosedur untuk memverifikasi identitas personil sebelum pemberian informasi autentikasi yang baru, pengganti atau sementara.
- Informasi autentikasi, termasuk informasi autentikasi sementara, dikirimkan kepada pengguna dengan cara yang aman (misal, melalui kanal terautentikasi dan terlindungi) dan menghindari penggunaan pesan elektronik yang tidak menggunakan enkripsi dan terlindungi.
- Informasi autentikasi bawaan (*default*) atau disediakan oleh penyedia barang/jasa (vendor) harus langsung diubah setelah pemasangan/instalasi sistem atau perangkat lunak.
- Terdapat mekanisme pencatatan kejadian penting terkait pengelolaan informasi autentikasi yang dirahasiakan, serta dengan menggunakan metode pencatatan yang telah disetujui (misal, menggunakan aplikasi *password vault*).

Setiap personil yang memiliki akses atau menggunakan informasi autentikasi harus memastikan bahwa:

- Menjaga kerahasiaan informasi autentikasi rahasia (*password*, PIN, dsb), tidak membagi informasi autentikasi rahasia dengan siapapun, dan hanya membagi informasi autentikasi rahasia yang digunakan dalam konteks identitas yang terhubung dengan banyak pengguna (*multiple users*).
- Informasi autentikasi yang bocor harus segera diubah setelah adanya pemberitahuan kebocoran atau indikasi kebocoran.
- Jika informasi autentikasi yang digunakan berupa *password*, pilih *password* yang kuat berdasarkan rekomendasi praktik terbaik, contohnya:
    1) *password* tidak didasarkan pada hal yang dapat ditebak atau informasi pribadi individu (misal, nama, nomor telepon, tanggal lahir, dsb);
    2) *password* tidak didasarkan pada kata atau kombinasi kata dalam kamus;
    3) gunakan *password* yang mudah diingat dan diusahakan untuk mengandung alfanumerik dan karakter spesial;

4) *password* memiliki panjang minimal yang telah ditentukan.

- *Password* yang sama tidak digunakan dalam layanan dan sistem yang berbeda.
- Kewajiban untuk mematuhi ketentuan-ketentuan ini dimasukkan ke dalam syarat dan ketentuan kepegawaian di organisasi.

Jika informasi autentikasi yang digunakan berupa *password*, sistem manajemen *password* harus:

- Mengizinkan personil untuk memilih dan mengubah *password* mereka sendiri, serta memiliki prosedur konfirmasi untuk mengatasi kesalahan masukan.
- Merekomendasikan penggunaan *password* yang kuat menurut rekomendasi praktik terbaik.
- Mewajibkan personil untuk mengubah *password* mereka setelah penggunaan pertama kali.
- Mendorong penggantian *password* sesuai kebutuhan, contohnya setelah terjadi insiden keamanan siber.
- Mencegah penggunaan *password* yang umum digunakan serta penggunaan ulang *password* sebelumnya.
- Tidak menampilkan *password* di layar saat dimasukkan.
- Menyimpan dan mengirim *password* dalam bentuk terlindungi.

9 *Serangan Advanced Persistent Threat (APT) yang memanfaatkan kesalahan atau lemahnya kesadaran keamanan informasi personil.*

Deskripsi

Advanced Persistent Threat (APT) merupakan jenis serangan siber tingkat lanjut dengan kompleksitas tinggi serta menggunakan banyak komponen yang berbeda dibandingkan jenis ancaman-ancaman lain. Serangan APT berbeda dengan *malware* biasa karena dirancang untuk dapat bersembunyi di jaringan komputer korban dalam waktu yang lama.

Dengan tingkat kompleksitas serangan yang tinggi, serangan APT dilakukan secara terstruktur dan seringkali memanfaatkan kerentanan dari sisi manusia dengan berupa ketidaktahuan, kesalahan atau lemahnya kesadaran keamanan informasi dari personil. Oleh karena itu, serangan APT menuntut tingkat kewaspadaan, pencegahan dan pengendalian yang lebih dibandingkan ancaman-ancaman lainnya.

Dampak

Dampak dari risiko ini bergantung pada individu yang menjadi korban. Sedangkan dampak tidak langsung dapat berakibat sangat fatal pada organisasi, meliputi kebocoran data pribadi, kebocoran kredensial penting, infeksi *malware*, kebocoran data kekayaan intelektual organisasi, gangguan operasional, sampai dengan dampak yang lebih signifikan seperti kerusakan reputasi, dampak hukum, dan sanksi/penalti.

Rekomendasi

Rekomendasi yang dapat dilakukan untuk meminimalisasi risiko dari serangan Advanced Presistent Threat (APT) karena kesalahan manusia atau kurangnya wawasan personil dapat mengacu rekomendasi sesuai poin 5 (serangan *phishing* karena kurangnya kesadaran keamanan). Selain itu, khusus untuk pengelola TI organisasi, perlu dibekali secara khusus peningkatan kesadaran dan kompetensi untuk mengenali dan mendeteksi ancaman-ancaman dari APT.

Agar organisasi memiliki kewaspadaan terhadap ancaman-ancaman siber yang berkembang khususnya terkait APT, organisasi sebaiknya juga mempertimbangkan untuk mengelola aktivitas terkait intelijen siber, yang meliputi namun tidak terbatas pada:

- Mengidentifikasi, memeriksa dan memilih sumber informasi internal dan eksternal yang diperlukan dan relevan sebagai masukan (*input*) bagi

pengelolaan intelijen siber. Sumber data internal misalnya perangkat perimeter jaringan, perangkat *endpoint*, dsb, sedangkan sumber eksternal misalnya *intelligence feeds*, data dari penyedia *cyber threat intelligence*, dsb.

- Melakukan pengumpulan informasi dari sumber yang dipilih, baik dari sumber internal dan eksternal.
- Memproses informasi yang telah dikumpulkan dan mempersiapkannya untuk proses analisis (misalnya dengan menerjemahkan, mengubah data ke dalam format tertentu, menguatkan/menambahkan informasi, dsb).
- Menganalisis informasi intelijen siber untuk memahami keterkaitan informasi tersebut dengan organisasi dan tindakan apa yang mungkin diperlukan.
- Mengkomunikasikan dan membagikan informasi intelijen siber kepada unit bisnis atau pihak lain yang relevan, serta dalam format sesuai/dapat dipahami.

10 *Serangan Advanced Persistent Threat (APT) yang memanfaatkan Brute Force Attack.*

Deskripsi

Serangan Advanced Presistent Threat (APT) yang memanfaatkan *brute force attack* merupakan jenis kejahatan siber mutakhir, dengan kompleksitas yang tinggi, dilakukan secara berkelanjutan, dan memanfaatkan metode *trial and error* untuk menemukan informasi *credential* (akun *login*, kunci enkripsi, menemukan web tersembunyi, dll). Peretas melakukan intrusi ke jaringan korbannya tanpa terdeteksi untuk mencuri informasi sensitif dalam rentang waktu yang lama.

Sasaran dari APT yang memanfaatkan *brute force attack* umumnya merupakan organisasi yang memiliki nilai aset tinggi, dengan tujuan utamanya mengarah pada pencurian informasi penting/sensitif atau akses ke sistem untuk transaksi dengan nilai yang tinggi.

Dampak

Dampak dari risiko ini dapat berakibat sangat fatal pada organisasi, meliputi kebocoran data pribadi, kebocoran kredensial penting, infeksi *malware*, kebocoran data kekayaan intelektual organisasi, gangguan operasional, sampai dengan dampak yang lebih signifikan seperti kerusakan reputasi, dampak hukum, dan sanksi/penalti.

Rekomendasi

Organisasi sebaiknya melakukan langkah-langkah sesuai rekomendasi pada poin 9 untuk meminimalisasi risiko dari serangan Advanced Presistent Threat (APT) yang memanfaatkan *brute force attack.* Untuk dapat mendeteksi ancaman-ancaman siber yang berkembang khususnya terkait APT, organisasi sebaiknya juga mempertimbangkan untuk mengelola aktivitas terkait intelijen siber, yang meliputi namun tidak terbatas pada:

- Membangun dan menyiapkan sistem keamanan dengan pendekatan pertahanan siber modern. Fokus keamanan bukan hanya mencegah/tindakan preventif, namun juga menitik beratkan pada kapabilitas untuk bisa mendeteksi dan melakukan tindakan responsif saat terdeteksinya ancaman-ancaman siber yang bersifat serius termasuk serangan APT.
- Membangun kapabilitas pemantauan keamanan secara berkelanjutan, misalnya melalui fasilitas Security Operations Center (SOC) yang dibangun secara mandiri atau bermitra dengan pihak ketiga (*managed security service provider*/MSSP).

buku putih keamanan siber

METODOLOGI

Dalam penyusunan Buku Putih ini, BSSN membuat katalog risiko siber yang relevan pada industri *Fintech Peer-to-Peer Lending*. Selanjutnya, bersama dengan Asosiasi *Fintech* Pendanaan Bersama Indonesia (AFPI) dan perwakilan dari industri *Fintech Peer-to-Peer Lending,* BSSN melakukan kategorisasi dan menyusun prioritas terhadap 10 risiko siber, berikut dengan rekomendasi mitigasi yang dapat dilakukan organisasi pada industri *Fintech Peer-to-Peer Lending* untuk mengurangi risiko-risiko tersebut.

Ditandatangani secara elektronik oleh:
DIREKTUR
KEAMANAN SIBER DAN SANDI
KEUANGAN, PERDAGANGAN, DAN PARIWISATA

Dr. Edit Prima, M.Kom

Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata,
Deputi Bidang Keamanan Siber dan Sandi Perekonomian,
Badan Siber dan Sandi Negara

Jalan Raya Muchtar 70
Depok, Jawa Barat – 16516

☏ +62 21 77973360
humas[at]bssn.go.id