Badan Siber dan Sandi Negara

PROFIL RISIKO

SEKTOR PERBANKAN

Tahun 2020

Direktorat Identifkasi Kerenanan dan Penilaian Risiko
Infrastruktur Informasi Kritikal Nasional,
Deputi Bidang Identifikasi dan Deteksi

Kata Pengantar

INDONESIA merupakan negara dengan jumlah pengguna internet terbesar di Asia Tenggara, dimana saat ini penetrasi pengguna internet sebesar 64% dari jumlah populasi penduduk. Peningkatan penggunaan internet di Indonesia tidak terlepas karena adanya kebutuhan yang tinggi terhadap transformasi digital di masyarakat mulai dari seperti mencari informasi di internet, melakukan transaksi keuangan dan jual beli secara *online*, serta melakukan bekerja dan pembelajaran secara *online*.

Transformasi digital di sektor keuangan perkembangannya sangat masif khususnya di masa pandemi ini, dimana transaksi digital sangat bermanfaat dalam membantu masyarakat dalam memenuhi kebutuhan sehari-hari yang dilakukan secara *online*.

Sektor keuangan yang didalamnya termasuk sektor perbankan merupakan salah satu sektor strategis yang wajib dilindungi keamanan informasinya, hal ini salah satunya disebabkan oleh karena sektor perbankan merupakan sektor yang paling sering terkena serangan siber. Adapun aktornya lebih banyak dilakukan oleh pelaku kriminal siber yang motifnya adalah terkait ekonomi, dampak yang diakibatkan insiden siber di sektor perbankan juga mengakibatkan kerugian baik bagi industri perbankan maupun nasabah.

Insiden siber sektor perbankan lebih sering menyasar kepada aplikasi yang digunakan oleh nasabah, yakni dalam hal ini adalah penggunaan aplikasi *internet banking* dan *mobile banking*. Berbagai macam metode yang dilakukan oleh *hacker* untuk mengeksploitasi kerentanan pada proses bisnis aplikasi *internet banking* dan *mobile banking.*

Dengan berkembangnya ancaman siber di sektor perbankan, BSSN telah menyelesaikan profil risiko siber di sektor perbankan tahun 2020 dengan lingkup *internet banking* dan *mobile banking*. Harapannya adalah dengan disusunnya profil risiko siber tersebut dapat dijadikan fokus acuan bagi industri perbankan untuk dapat melakukan mitigasi terhadap potensi ancaman dan kerentanan siber.

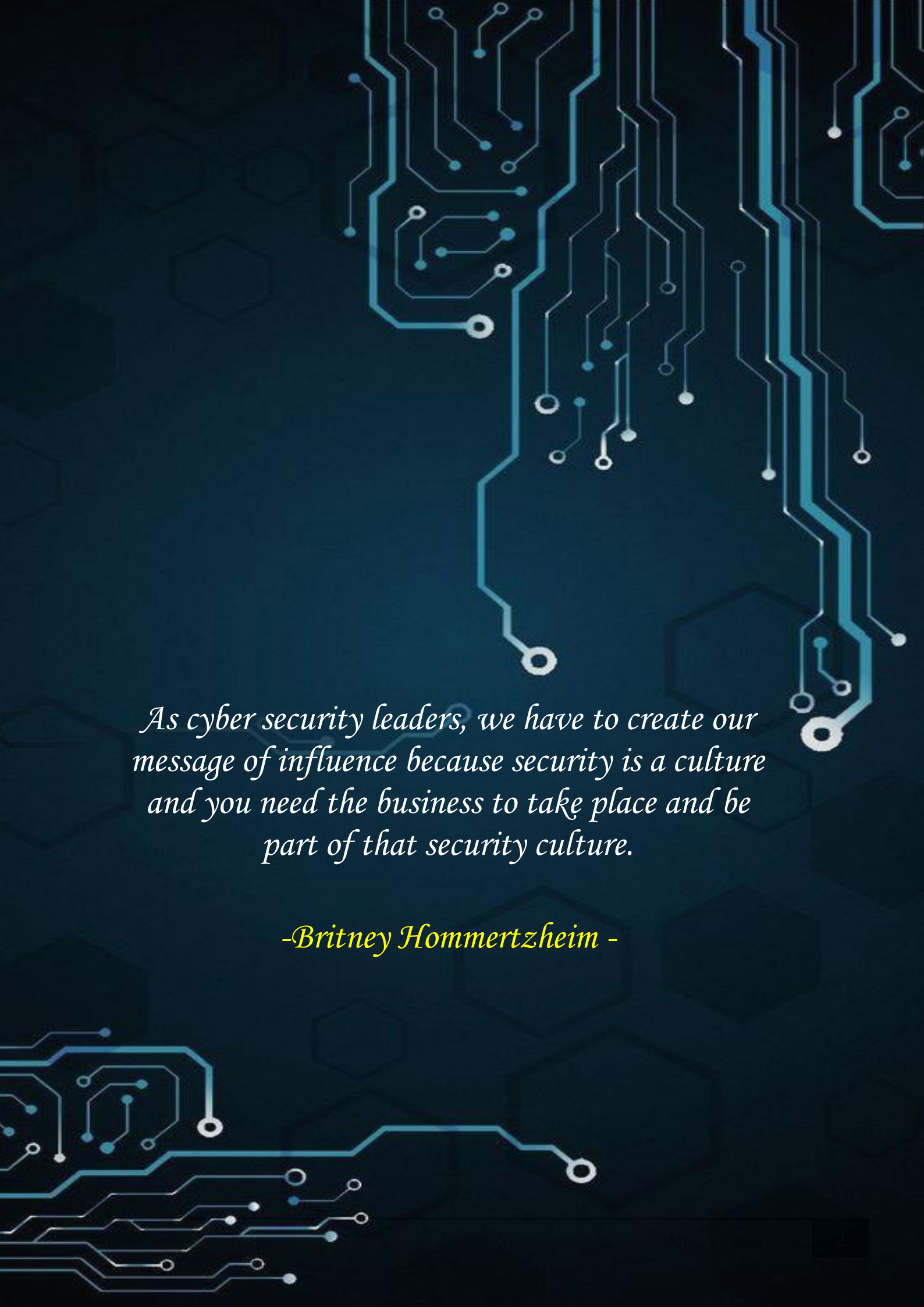
Depok, Februari 2021

Direktur IKPR IIKN,

Ditandatangani secara elektronik oleh:
DIREKTUR IKPRIIKN,
DEPUTI BIDANG IDENTIFIKASI DAN DETEKSI

INTAN RAHAYU, S.Si., M.T.
Pembina Tk. I (IV/b)

Intan Rahayu, S.Si., M.T.


As cyber security leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture.
-Britney Hommertzheim -

Tim Penyusun

PENANGGUNG JAWAB

Intan Rahayu, S.Si., M.T.	Direktur IKPRIIKN

KETUA

Sigit Kurniawan, S.ST., M.AP.	Sandiman Ahli Madya pada Direktorat IKPRIIKN selaku Koordinator Kelompok IKPRIIKN III

ANGGOTA

R. Ahmad Imanullah Z., S.ST.	Analis Identifikasi Kerentanan Siber
Yopie Maulana S., S.S.T.TP	Analis Identifikasi Kerentanan Siber
Sylvia Kharisma P., S.Tr.MP.	Pengolah Data Keamanan Siber dan Sandi
Afifah, S.Tr.TP	Pengolah Data Keamanan Siber dan Sandi
Febrianto Dicky S., S. Tr. TP.	Sandiman Pertama

Daftar ISi

LANDSCAPE

ANCAMAN SIBER DI SEKTOR PERBANKAN TAHUN 2020

A. PERKEMBANGAN TRANSFORMASI DIGITAL DI INDONESIA

INDONESIA mengalami perkembangan teknologi yang sangat cepat dengan didukung dengan pembangunan infrastruktur teknologi informasi dan komunikasi (TIK) yang pesat, terlebih dengan adanya tuntutan transformasi digital dalam memenuhi kebutuhan masyarakat sehari-hari di tengah masa pandemi covid-19 ini, seperti bekerja, belajar dan transaksi jual beli secara *online*. Harapan yang akan dituju adalah tercipta ekosistem digital yang kuat untuk kesejahteraan masyarakat sehingga dapat meningkatkan pertumbuhan ekonomi Indonesia yang saat ini sedang menurun.

Transformasi digital yang terjadi merupakan dampak dari upaya tatanan kehidupan yang baru atau era *new normal* bagi masyarakat untuk beradaptasi dalam menyesuaikan diri di tengah kondisi pandemi covid-19 ini. Transformasi digital ini pun diprediksi kedepannya tetap akan tetap berlangsung walau kondisi pandemi covid-19 telah usai. Transformasi digital saat ini juga telah mengubah pola transaksi masyarakat baik secara individu maupun secara korporasi. Berbagai bentuk transformasi digital yakni seperti dengan adanya peningkatan kebutuhan penggunaan *e-commerce, e-grocery, e-education, e-communication, e-entertainment, e-transportation, e-financial, e-payment, e-healthcare*, dan *working from home.*

Peningkatan transformasi digital salah satunya ditandai dengan adanya kenaikan jumlah nominal transaksi uang elektronik sepanjang tahun 2020. Berdasarkan data dari Bank Indonesia, bahwa jumlah nominal transaksi uang elektronik pada tahun 2020 mengalami kenaikan 46% dari tahun sebelumnya (*year on year* rentan waktu Januari-Oktober) yakni total transaksi sebesar Rp 163,4 Triliun dibanding tahun sebelumnya Rp 112,1 Triliun. Sedangkan nominal transaksi *mobile banking* terjadi kenaikan transaksi sebesar 35% di tahun 2020 dari tahun sebelumnya (*year on year* rentan waktu Januari-September) yakni dari total transaksi sebesar Rp 3.349 Triliun dibanding tahun sebelumnya Rp 2.493 Triliun.

B. ANCAMAN SIBER DI SEKTOR PERBANKAN

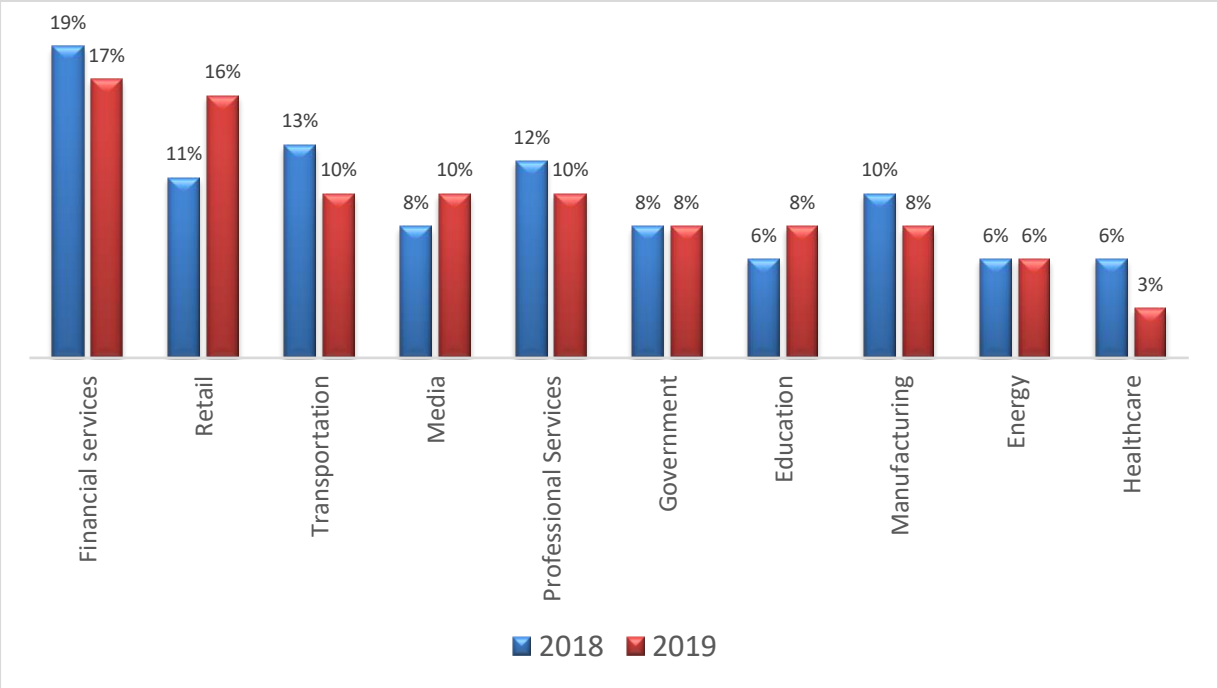
TRANSFORMASI digital yang terjadi untuk memudahkan kebutuhan sehari-hari masyarakat ternyata tidak hanya mendatangkan keuntungan namun juga ada ancaman yang dapat merugikan masyarakat baik dari sisi individu maupun korporasi. Ancaman yang dimaksud adalah adanya serangan siber yang berpotensi untuk mencuri uang nasabah atau korporasi, menggagalkan sistem transaksi keuangan, mencuri data pribadi, melakukan penipuan, dll.

Pada masa pandemi ini ancaman serangan siber semakin meningkat, data dari Pusat Operasi Keamanan Siber Nasional BSSN bahwa sepanjang tahun 2020 terjadi 495 juta serangan siber atau naik 5 kali lipat dibanding tahun sebelumnya yang sebesar 228 juta serangan siber. Hal ini selaras dengan apa yang disampaikan dalam Word Economic Forum mengenai Global Risk Report 2021, bahwa risiko serangan siber cukup tinggi dibawah risiko bencana alam dan kerusakan lingkungan serta infeksi penyakit seperti yang terlihat pada Gambar 1.1. berikut :

Gambar 1.1 Global Risk Landscape

Dari data tersebut diatas maka dapat diambil kesimpulan bahwasanya serangan siber menjadi salah satu risiko yang harus dipertimbangkan dengan melakukan identifikasi kerentananan dan penilaian risiko siber secara komprehensif dan detail baik dari jenis ancaman, kerentanan dan dampak yang dapat ditimbulkan dari serangan siber bila hal itu terjadi.

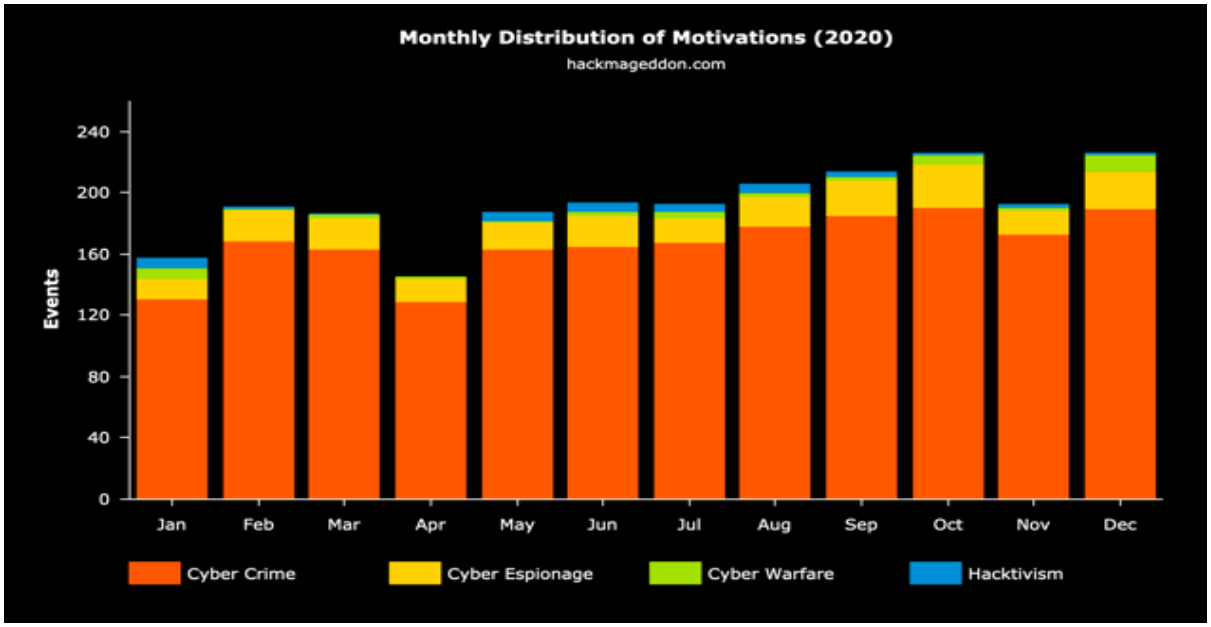
Dari berbagai serangan siber yang terjadi, terdapat sektor-sektor yang sering mengalami insiden siber seperti yang didapat datanya dari IBM X-Force untuk tahun 2018 dan 2019 sebagaimana Gambar 1.1 berikut ini:



Gambar 1.2. Industri Yang Paling Sering Terkena Insiden Siber

Selama 2 tahun berturut-turut, secara global sektor keuangan merupakan sektor yang paling sering terkena insiden siber. Hal ini dapat dimungkinkan terjadi karena sektor keuangan khususnya sektor perbankan sudah banyak bertranformasi ke digitalisasi sehingga membuka peluang terhadap serangan siber. Adapun serangan siber yang mentargetkan di sektor perbankan memiliki tujuan terhadap motif ekonomi dengan pelakunya adalah kriminal siber. Berbagai kasus di Indonesia juga kerap terjadi pembobolan Bank dengan menggunakan serangan siber dengan memanfaatkan *social engineering*, OTP *Fraud,* SIM *Swap*, kelemahan pada sistem perbankan dan juga *phishing*.

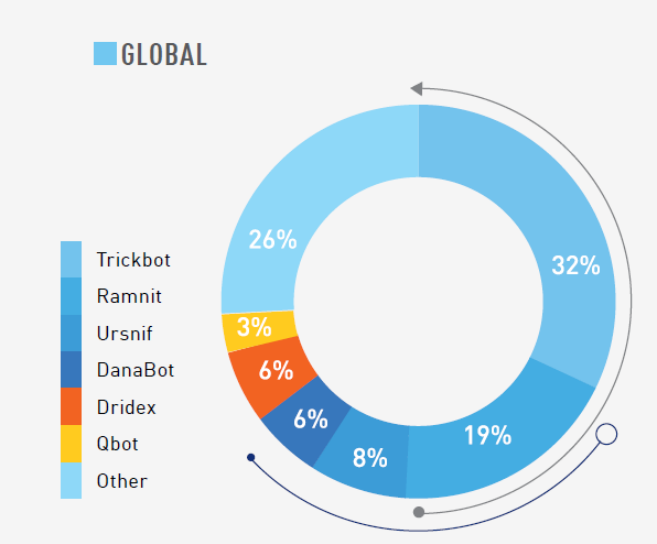
Hal ini juga dikuatkan dengan data dari hackmageddon.com dimana *cyber crime* atau kejahatan siber merupakan serangan siber dengan motivasi tertinggi sepanjang tahun 2020 dibanding serangan siber dengan motif *cyber espionage, cyber warfare* dan *hacktivism* seperti yang terlihat pada Gambar 1.2 berikut:



Gambar 1.3. Distribusi Motivasi Pada Serangan Siber

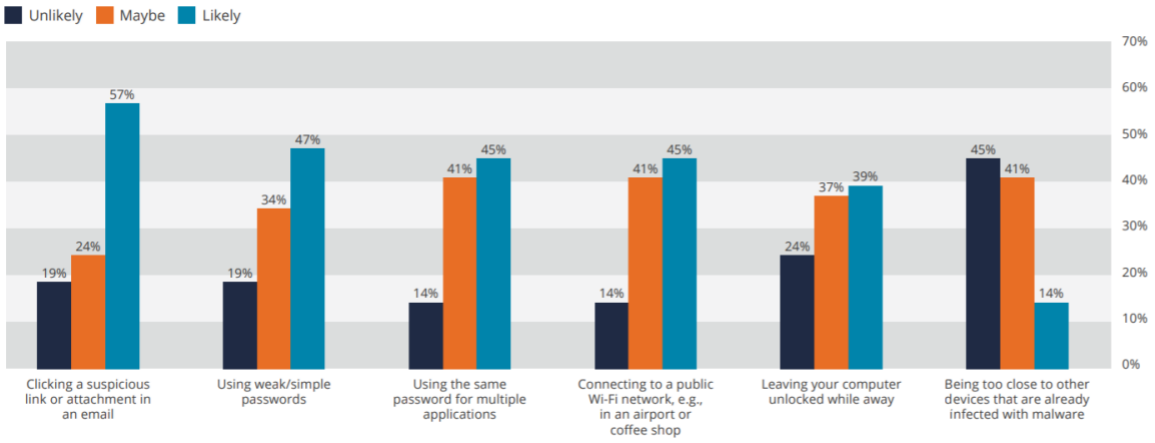
Berdasarkan data yang dihimpun dari berbagai sumber, bahwa sepanjang tahun 2020 insiden siber yang paling sering terjadi dikarenakan oleh serangan siber berupa *malware, phishing*, pencurian data, DDOS, *skimming, jackpotting*, dan adanya bug atau kelemahan pada sistem informasi di perbankan.

Salah satu faktor insiden siber yang sering muncul adalah *malware, virus,* atau *trojan*. *Check Point Research* mencatat t*op banking trojan* yang paling banyak ditemukan di tahun 2020, antara lain trickbot, ramnit, ursnif, danabot, dridex, dan qbot seperti pada Gambar 1.3.



Gambar 1.4. Top Banking Trojan

Serangan siber berupa *phishing*, *malware*, virus, *trojan* dan serangan lainnya yang menyebabkan terjadinya insiden, juga dapat dipicu karena kurangnya *security awareness*. Berdasarkan hasil *survey* MediaPro tahun 2020 diketahui bahwa 19% personil memiliki persepsi bahwa mengklik tautan/*link email* yang mencurigakan tidak mungkin menyebabkan suatu *device* terinfeksi *malware* dan 14% personil memiliki persepsi bahwa menggunakan koneksi internet publik tidak mungkin menyebabkan suatu *device* terinfeksi *malware*. Hasil survei ini sebagaimana tercantum pada Gambar 1.4.



Gambar 1.5. Hasil Survei Persepsi Personil Mengeni Potensi Terjadinya Infeksi *Malware* pada Suatu *Device*

PROFIL RISIKO

DI SEKTOR PERBANKAN

TAHUN 2020

BERDASARKAN hasil survei Direktorat IKPRIIN, diperoleh Profil Risiko Sektor Perbankan selama Tahun 2020 yang dikategorikan dalam 4 (empat) level yaitu *very high, high, medium*, dan *low*. Level risiko ini dikategorisasikan berdasarkan skala dampak dan skala kemungkinan dari setiap risiko yang terindentifikasi. Kriteria penetapan level risiko tersebut digambarkan pada table 2.1. sebagai berikut:

Tabel 2.1. Skala Dampak dan Kemungkinan

		Skala Dampak			
		Tidak Signifikan	*Cukup Signifikan*	*Signifikan*	*Sangat Signifikan*
Skala Kemungkinan	*Kecil*	Rendah	Rendah	Rendah	Sedang
	Sedang	Rendah	Rendah	Sedang	Tinggi
	Besar	Rendah	Sedang	Tinggi	Tinggi
	Sangat Besar	Rendah	Sedang	Tinggi	Sangat Tinggi

Kriteria skala dampak terdiri dari “tidak signifikan”, “cukup signifikan”, “signifikan”, dan “sangat signifikan”. Kriteria dampak pada penilaian ini mencakup 4 (empat) aspek yaitu dampak finansial, dampak operasional, dampak hukum, dan dampak reputasi. Masing-masing skala pada setiap aspek dampak didefinisikan pada tabel 2.2. sebagai berikut:

Tabel 2.2. Kriteria Dampak

Skala Dampak	Definisi			
	Reputasi	**Operasional**	**Finansial**	**Hukum**
Tidak Signifikan	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan pemangku kepentingan (stakeholder) atau nasabah	Penundaan proses bisnis antara 0 sampai dengan 30 menit	Kerugian dan/atau adanya pengeluaran biaya sampai dengan maksimal sebanding dengan 0 – 5% revenue bank	Terdapat permasalahan hukum (misal: pelanggaran) namun belum menjadi tuntutan hukum
Cukup Signifikan	Terdapat pemberitaan negatif yang dapat mempengengaruhi kepercayaan sebagian kecil dari stakeholder atau nasabah	Penundaan proses bisnis antara 30 menit sampai dengan maksimal 1 jam.	pengeluaran biaya sampai dengan maksimal sebanding dengan 6 – 10% revenue bank	Tuntutan hukum dengan dampak relatif kecil
Signifikan	Terdapat pemberitaan negatif yang dapat mengakibatkan penurunan kepercayaan sebagian besar dari stakeholder atau nasabah	Penundaan proses bisnis antara 1 jam sampai dengan maksimal 3 jam	pengeluaran biaya sampai dengan maksimal sebanding dengan 11 – 20% revenue bank	Tuntutan hukum yang berdampak pada kinerja/performa organisasi
Sangat Signifikan	Terdapat pemberitaan negatif yang dapat menghilangkan kepercayaan dari stakeholder atau nasabah	Penundaan proses bisnis lebih dari 3 jam	pengeluaran biaya sampai dengan maksimal lebih dari 20% revenue bank	Tuntutan hukum yang mengancam eksistensi dan manajemen puncak organisasi

Sedangkan kriteria skala kemungkinan terjadi terdiri dari skala "kecil", "sedang", "besar", dan "sangat besar". Masing-masing skala kemungkinan didefinisikan pada tabel 2.3. sebagai berikut:

Tabel 2.3. Kriteria Kemungkinan

Skala	Definisi
Kecil	Kejadian tidak lebih dari 2 kali per tahun
Sedang	Kejadian lebih dari 2 kali/tahun, namun tidak lebih dari 5 kali/tahun
Besar	Kejadian lebih dari 5 kali/tahun, namun tidak lebih dari 10 kali/tahun
Sangat Besar	Kejadian lebih dari 10 kali/tahun

Adapun di dalam dokumen profil risiko siber ini ditampilkan untuk level *very high, high* dan *medium* karena merupakan risiko yang harus dapat dilakukan mitigasinya. Risiko-risiko yang ditemukan memberikan dampak pada aspek finansial, aspek reputasi, aspek operasional dan/atau aspek hukum. Risiko yang teridentifikasi dapat dijelaskan pada tabel 2.4. sebagai berikut:

Tabel 2.4. Risiko yang Teridentifikasi

Level Risiko	Risiko yang Teridentifikasi
Very High	*social engineering, processing failure, hardware failure, internal fraud*, serangan *hacker*
High	*bug* pada aplikasi, serangan virus, *fraud* eksternal, *data leak* karena adanya *malware/trojan*, *SQL injection*, terhambatnya operasional TI karena kurang Sumber Daya Manusia TI, kelemahan konfigurasi terhadap serangan *malware*, serangan *phishing*
Medium	*skimming*, kegagalan sistem TI, kelemahan sistem saat mendesain dan menetapkan prosedur, adanya dependensi pihak ketiga sehingga *problem management* belum maksimal diselesaikan, gangguan jaringan pada ATM, penyalahgunaan akses sistem, penyalahgunaan hak akses *core*

	banking, penyalahgunaan hak akses pada perangkat jaringan

Risiko dengan level *very high* yang teridentifikasi antara lain *social engineering, processing failure, hardware failure, internal fraud,* dan serangan *hacker*. Risiko-risiko ini dapat memberikan dampak yang sangat signifikan terhadap organisasi apabila terjadi, terutama terkait dampak operasional dan finansial. Faktor yang menyebabkan adanya potensi risiko ini dapat berasal dari pihak internal maupun eksternal organisasi. Risiko *social enginering* yang paling sering ditemukan disebabkan oleh kurangnya *security awareness* dari nasabah. Sedangkan risiko *processing failure, hardware failure*, dan *internal fraud* dapat disebabkan karena kurangnya pengujian, kurangnya kontrol dan monitoring, atau faktor lainnya. Sedangkan untuk serangan *hacker* dapat dipengaruhi karena adanya kerentanan sistem ataupun kurangnya *security awareness* dari nasabah.

Beberapa risiko dengan level *high* yang teridentifikasi juga dapat disebabkan oleh faktor eksternal maupun internal. Faktor eksternal seperti serangan *malware*, *virus*, dan *phishing* dapat terjadi karena disebabkan oleh kurangnya *security awareness* nasabah, ataupun karena kelemahan sistem seperti tidak adanya *antimalware*/*antivirus*. Sedangkan faktor internal masih ditemukannya *bug*, sistem tidak *update*, kurangnya pengujian keamanan atau faktor lainnya. Beberapa risiko lainnya yang teridentifikasi pada level *high* diantaranya adalah *fraud eksternal*, *data leak*, *SQL injection*, terhambatnya operasional, dan kelemahan konfigurasi.

Risiko-risiko pada level *medium* yaitu risiko kegagalan sistem dan kelemahan sistem saat mendesain dan menetapkan prosedur, risiko *skimming*, dan risiko gangguan jaringan pada ATM. Risiko-risiko ini dapat disebabkan karena kurangnya monitoring sistem, kurangnya pengujian sistem dan sebagainya. Kemudian ada pula risiko

penyalahgunaan akses sistem, penyalahgunaan hak akses *core banking*, dan penyalahgunaan hak akses perangkat jaringan yang dapat disebabkan beberapa faktor. Misalnya tidak menggunakannya *secure channel* saat transmisi, audit aspek keamanan tidak dilaksanakan secara berkala, manajemen *password* yang buruk, penggunaan jaringan internet publik yang tidak aman, ataupun faktor lainnya.

Selain risiko dengan level *very high, high*, dan *medium* juga ditemukan risiko-risiko dengan level *low*. Namun frekuensi terjadinya risiko-risiko pada level *low* ini sangat kecil dan dampak yang ditimbulkan juga tidak signifikan baik dari dampak finansial, operasional, reputasi, maupun hukum.

Berkaitan dengan risiko siber diatas, Direktorat IKPRIIKN juga melakukan identifikasi terkait profil ancaman dan kerentanan layanan *mobile banking* dan *internet banking* di Indonesia tahun 2020. Hal ini mengingat kedua layanan ini yang paling banyak digunakan pada layanan digital banking di sektor perbankan Indonesia dalam melakukan transaksi keuangan.

Mobile banking adalah salah satu layanan digital banking yang disediakan oleh bank untuk melakukan berbagai transaksi perbankan melalui berbagai fitur yang ada pada *smartphone*. *Mobile banking* memungkinkan pelanggan mengakses rekening bank mereka melalui perangkat *smartphone* untuk memeriksa saldo maupun melakukan transaksi keuangan lainnya. Sedangkan untuk *internet banking* adalah layanan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi, dimana nasabah dapat menggunakan perangkat komputer *desktop, laptop, tablet*, atau *smartphone* yang terhubung ke jaringan *internet* sebagai penghubung antara perangkat nasabah dengan sistem bank. Keberadaan *mobile banking* maupun *internet banking* memberikan kemudahan serta kenyamanan nasabah dalam melakukan transaksi secara cepat. Namun tentunya keamanan sistem menjadi aspek utama

yang harus diperhatikan untuk menekan terjadinya potensi risiko siber. Dan untuk meminimalisir suatu risiko siber pada *mobile banking* dan *internet banking*, maka hal pertama yang harus dilakukan adalah identifikasi ancaman maupun kerentanan siber dari masing-masing sistem.

MOBILE BANKING

POTENSI risiko pada *mobile banking* dipengaruhi oleh faktor ancaman maupun faktor kerentanan siber. Ancaman-ancaman yang mungkin terjadi pada tahun 2020 pada sistem *mobile banking* diantaranya adalah penyalahgunaan hak akses, serangan *phishing* pada nasabah, pencurian data, kesalahan pengelolaan aplikasi, serangan *malware*, dan *hijack simcard*. Setiap ancaman pada *mobile banking* tersebut dapat menjadi suatu risiko apabila ditemukan satu/lebih kerentanan yang dapat memicu terjadinya ancaman. Daftar ancaman dan kerentanan siber terkini pada *mobile banking* dapat dilihat pada tabel 2.5. sebagai berikut:

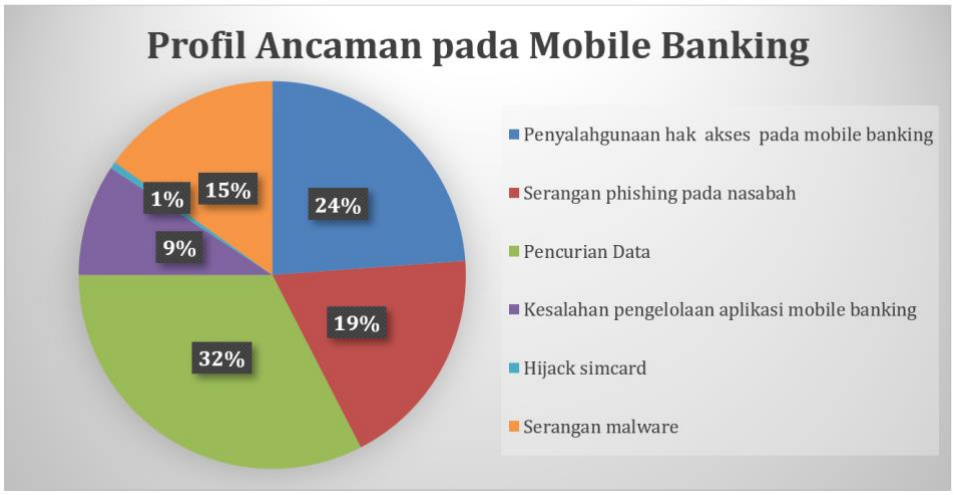
Tabel 2.5. Daftar Ancaman dan Kerentanan *Mobile Banking*

Ancaman (Threat)		Kerentanan (Vulnerability)
Penyalahgunaan hak akses pada *mobile banking*	1	Transaksi tidak menggunakan *two factor authentication*
	2	Transaksi tidak menggunakan *secure channel* saat transmisi
	3	Aplikasi yang dibuat tidak sesuai dengan desain perancangan perangkat lunak atau tidak menerapkan metode DevSecOps
	4	Audit aspek keamanan tidak dilaksankaan secara berkala
	5	*Username* dan *password* tersimpan secara otomatis *(remembering user and password)*
	6	Masih ditemukan *bug* pada perangkat lunak
	7	Manajemen *password* yang buruk
	8	Penggunaan jaringan internet publik yang tidak aman
	9	Tidak ada pembatasan pada mekanisme *login*
	10	*Recycle simcard*
	11	Aplikasi mudah di duplikasi

Ancaman (Threat)		Kerentanan (Vulnerability)
Serangan *phishing* pada nasabah	12	Aplikasi dapat disusupi *backdoor*
	13	Kurangnya *security awareness*
	14	Kurang sosialisasi akan kesadaran keamanan informasi dalam penggunaan *mobile banking*
Pencurian data	15	Aplikasi rentan dilakukan *reverse engineering*
	16	Data tidak dienkripsi menggunakan *secure channel* saat transmisi
	17	*Hard coded secret key* pada penggunaan algoritma kriptografi yang tersimpan di aplikasi
	18	Masih ditemukan *bug* pada perangkat lunak
	19	Data sensitif tertulis pada sistem *log/password* disimpan didalam *smartphone* nasabah
	20	Men-*download* aplikasi *mobile banking* dari sumber yang tidak resmi
	21	Penggunaan *device* dan/atau aplikasi lain yang memiliki celah keamanan
	22	Manajemen *password* yang buruk
Kesalahan pengelolaan aplikasi *mobile banking*	23	Dokumentasi aplikasi yang tidak lengkap
	24	Tidak ada mekanisme pengawasan pengelolaan sistem *mobile banking*
	25	Tidak ada *back up system*
	26	Kurangnya kompetensi sumber daya manusia pengelolaan sistem *mobile banking*
	27	Kurangnya kesadaran akan keamanan informasi bagi pengelola sistem *mobile banking*
Serangan *malware*	28	Tidak ada anti *malware* atau *antivirus* pada *device* pengguna
	29	Kurangnya *security awareness*
	30	Sistem tidak *update*
Hijack simcard	31	Adanya pencurian data

Berdasarkan hasil survei Direktorat IKPRIIKN, profil risiko siber pada *mobile banking* selama tahun 2020 sebagai berikut :

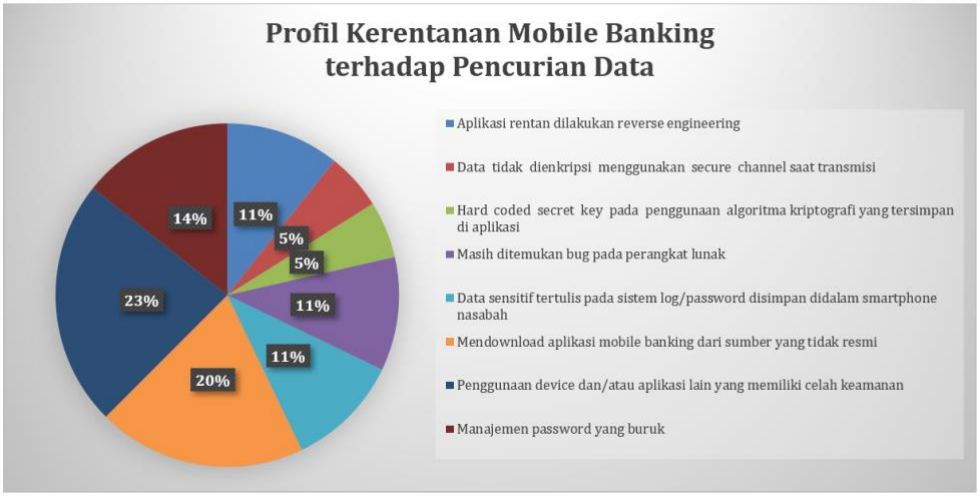
a. Ancaman Terbesar pada *Mobile Banking*



Ancaman siber pada *mobile banking* bisa berasal dari pihak eksternal maupun pihak internal. Dari hasil survei diketahui terdapat 6 (enam) ancaman siber yang paling banyak ditemukan pada *mobile banking* di Indonesia selama tahun 2020. Berdasarkan grafik diatas diketahui bahwa profil ancaman pada *mobile banking* di Indonesia selama tahun 2020 antara lain pencurian data sebesar 32%, kemudian penyalahgunanan hak akses sebesar 24%, serangan *phishing* sebesar 19%, serangan *malware* sebesar 15%, kesalahan pengelolaan aplikasi sebesar 9%, dan yang paling terkecil adalah *hijack simcard* sebesar 1%.

Pencurian data merupakan ancaman terbesar yang ditemukan pada *mobile banking* selama tahun 2020. Hal ini menggambarkan bahwa tidak hanya finansial yang menjadi sasaran utama *hacker* melainkan data nasabah juga menjadi target utama. Namun apabila terjadi pencurian data maka ancaman siber lainnya bisa saja terjadi dari dampak pencurian data yang ditimbulkan, misalnya terjadinya penyalahgunaan hak akses pada *mobile banking,* penipuan, dan lain-lain.

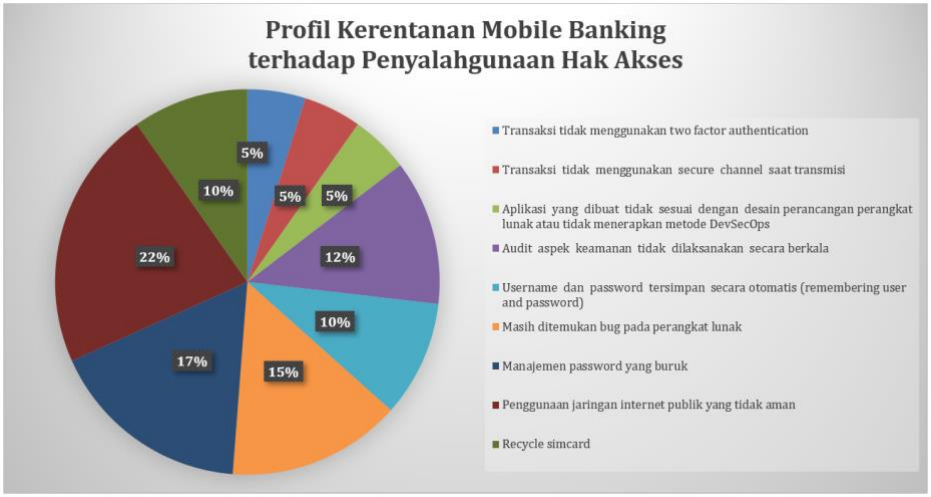
b. Kerentanan Terbesar pada *Mobile Banking* terhadap Pencurian Data



Pencurian data merupakan ancaman siber terbesar pada *mobile banking* selama tahun 2020. Dari hasil survei diketahui terdapat 8 (delapan) kerentanan terbesar yang relevan terhadap ancaman pencurian data pada *mobile banking* antara lain disebabkan oleh penggunaan *device* dan/atau aplikasi lain yang memiliki celah keamanan dengan persentase sebesar 23%, men-*download* aplikasi *mobile banking* dari sumber yang tidak resmi sebesar 20%, manajemen *password* yang buruk sebesar 14%, data sensitif/password tersimpan pada *smartphone* nasabah, masih ditemukan *bug* pada perangkat lunak, dan aplikasi rentan dilakukan *reverse engineering* masing-masing sebesar 11%, data tidak dienkripsi menggunakan *secure channel* saat transmisi serta *hard coded secret key* pada penggunaan algoritma kriptografi tersimpan di aplikasi masing-masing sebesar 5%.

Selain peran dari industri perbankan, nasabah mempunyai peran besar untuk meminimalisir kerentanan-kerentanan tersebut. Penggunaan *device* yang tidak aman oleh nasabah bisa dimanfaatkan oleh *hacker* dalam melakukan pencurian data. Kemudian dengan manajemen *password* yang buruk misalnya nasabah tidak melakukan pergantian *password* secara berkala, penggunaan *password* yang lemah, juga menjadi peluang bagi para *hacker* untuk melakukan pencurian data dengan mudah. Serta ketidaktahuan nasabah atau kurangnya *security awareness* nasabah sehingga men-*download* aplikasi dari sumber yang tidak resmi juga memiliki risiko yang tinggi akan terjadinya pencurian data nasabah.

c. Kerentanan Terbesar pada *Mobile Banking* terhadap Penyalahgunaan Hak Akses



Penyalahgunaan hak akses merupakan ancaman siber terbesar kedua setelah pencurian data yang ditemukan pada *mobile banking* selama tahun 2020. Dari hasil survei diketahui terdapat 9 (sembilan) kerentanan yang relevan terhadap ancaman penyalahgunaan hak akses pada *mobile banking* yang disebabkan oleh penggunaan jaringan internet publik yang tidak aman dengan persentase sebesar 22%, manajemen *password* yang buruk sebesar 17%, masih ditemukan *bug* pada perangkat lunak sebesar 14%, audit tidak dilaksanakan secara berkala sebesar 12%, *username* dan *password* tersimpan secara otomatis (*remembering user and password*) serta *recycle simcard* masing-masing sebesar 10%, aplikasi yang dibuat tidak menerapkan DevSecOps dan transaksi tidak menggunakan *secure channel* saat transmisi, serta transaksi tidak menggunakan *two factor authentication* masing-masing sebesar 5%.

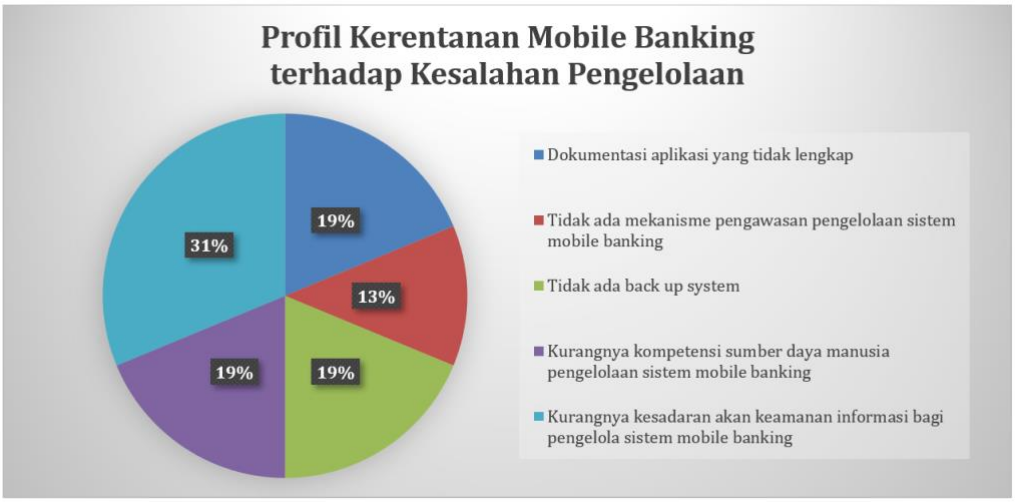
Nasabah dan pihak internal perbankan sama-sama mempunyai peranan besar untuk meminimalisir kerentanan-kerentanan tersebut. Kurangnya security awareness nasabah sehingga menggunakan jaringan internet publik yang tidak aman, menggunakan *password* yang buruk menjadi celah *hacker* untuk melakukan penyalahgunaan hak akses. Begitu pula dengan kerentanan-kerentanan yang ditemukan di aplikasi seperti adanya bug, perancangan aplikasi yang tidak menerapkan DevSecOps, dan tidak diterapkannya *two factor authentication* juga menjadi peluang *hacker* dalam menyalahgunakan hak akses.

d. Kerentanan Terbesar pada *Mobile Banking* terhadap Serangan *Phishing* Nasabah

Serangan *phishing* nasabah merupakan ancaman siber terbesar ketiga setelah pencurian data dan penyalahgunaan hak akses, yang ditemukan pada *mobile banking* selama tahun 2020. Dari hasil survei diketahui terdapat 4 (empat) kerentanan yang relevan terhadap ancaman serangan *phishing* nasabah pada *mobile banking* yaitu kurangnya sosialisasi kesadaran keamanan informasi dengan persentase sebesar 41%, kurangnya *security awareness* sebesar 38%, aplikasi dapat disusupi *backdoor* sebesar 13%, dan aplikasi mudah diduplikasi sebesar 9%. Untuk meminimalisir risiko yang disebabkan kerentanan-kerentanan tersebut dibutuhkan peranan dari pihak internal untuk memastikan keamanan aplikasi agar tidak mudah disusupi oleh *backdoor* dan tidak mudah diduplikasi, serta dibutuhkan peranan nasabah untuk meningkatan *security awareness*. Kurangnya *security awareness* nasabah yang menyebabkan terjadinya *phishing* juga dapat memiliki dampak di ancaman lainnya, diantaranya pencurian data, penyalahgunaan hak akses, dan sebagainya.

e. Kerentanan Terbesar pada *Mobile Banking* terhadap Kesalahan Pengelolaan

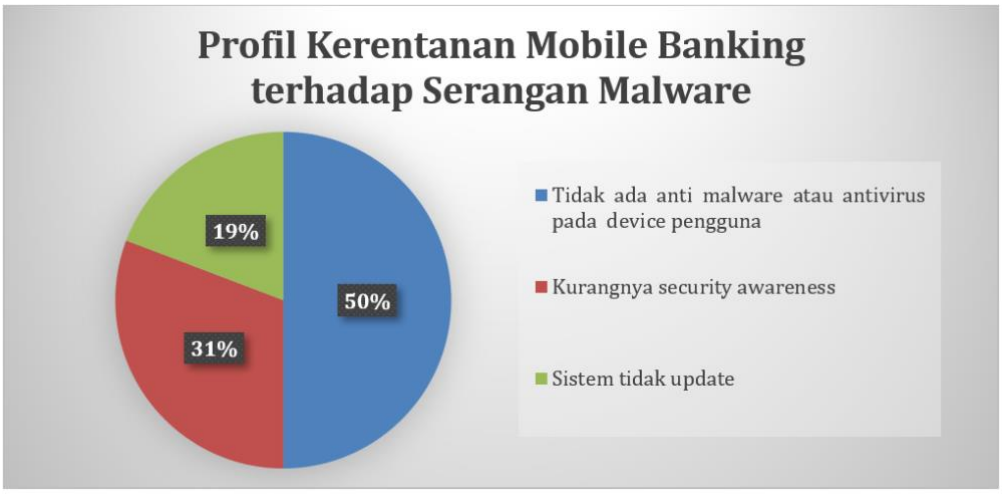
Dari hasil survei diketahui terdapat 5 (lima) kerentanan yang relevan terhadap ancaman kesalahan pengelolaan pada *mobile banking*. Kurangnya kesadaran keamanan informasi memang menjadi isu kerentanan yang paling sering ditemukan termasuk terhadap ancaman kesalahan pengelolaan *mobile banking*.



Dari survei 2020 kurangnya kesadaran keamanan informasi bagi pengelola sistem *mobile banking* memiliki persentase paling besar yaitu 31%. Kemudian diikuti dengan kerentanan akan kurangnya kompetensi sumber daya manusia pengelola sistem, tidak ada *back up* sistem, dan dokumentasi yang tidak lengkap dengan persentasi masing-masing sebesar 19%. Serta tidak ada mekanisme pengawasan pengelolaan sistem *mobile banking* sebesar 13%. Pihak internal perbankan memiliki peranan besar untuk meminimalisir kerentanan-kerentanan tersebut terhadap ancaman kesalahan pengelolaan *mobile banking*. Pihak perbankan perlu melakukan langkah antisipasi dengan melakukan dokumentasi aplikasi secara lengkap, menerapkan mekanisme pengawasan pengelolaan sistem, menyediakan *back up* sistem, meningkatkan kompetensi dan kesadaran keamanan informasi bagi pengelola sistem *mobile banking*.

.

f. Kerentanan Terbesar pada *Mobile Banking* terhadap Serangan *Malware*



Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman serangan *malware* pada *mobile banking*. Tidak ada anti *malware* atau *antivirus* pada *device* pengguna menjadi isu kerentanan paling tinggi dengan persentase sebesar 50%. Hal ini tentunya karena pihak perbankan tidak dapat mengontrol secara penuh *device* yang digunakan oleh pengguna sehingga dibutuhkan kesadaran dari nasabah itu sendiri. Selanjutnya kurangnya *security awareness* juga menjadi isu pada ancaman serangan *malware* dengan persentase sebesar 31%. *Hacker* biasanya memanfaatkan kelemahan, ketidaktahuan, dan ketidaksadaran nasabah terkait keamanan informasi untuk melakukan serangan *malware*. Kerentanan yang terakhir adalah sistem tidak *update* dengan persentase sebesar 19%. Kerentanan ini juga memiliki potensi dan peluang untuk *hacker* melakukan serangan *malware*.

INTERNET BANKING

Potensi risiko pada *internet banking* dipengaruhi oleh faktor ancaman maupun faktor kerentanan siber. Ancaman-ancaman yang mungkin terjadi pada sistem *internet banking* diantaranya adalah serangan *hacker*, penyalahgunaan hak akses, serangan *malware*, kesalahan penggunaan *internet banking*, kegagalan perangkat lunak, terbukanya informasi sensitif, serangan Ddos, dan serangan *phishing* pada nasabah. Setiap ancaman pada *internet banking* tersebut dapat menjadi suatu risiko apabila ditemukan satu/lebih kerentanan yang dapat memicu terjadinya ancaman. Daftar ancaman dan kerentanan siber terkini pada *internet banking* dapat dilihat pada tabel 2.6. sebagai berikut:

Tabel 2.6. Daftar Ancaman dan Kerentanan *Internet Banking*

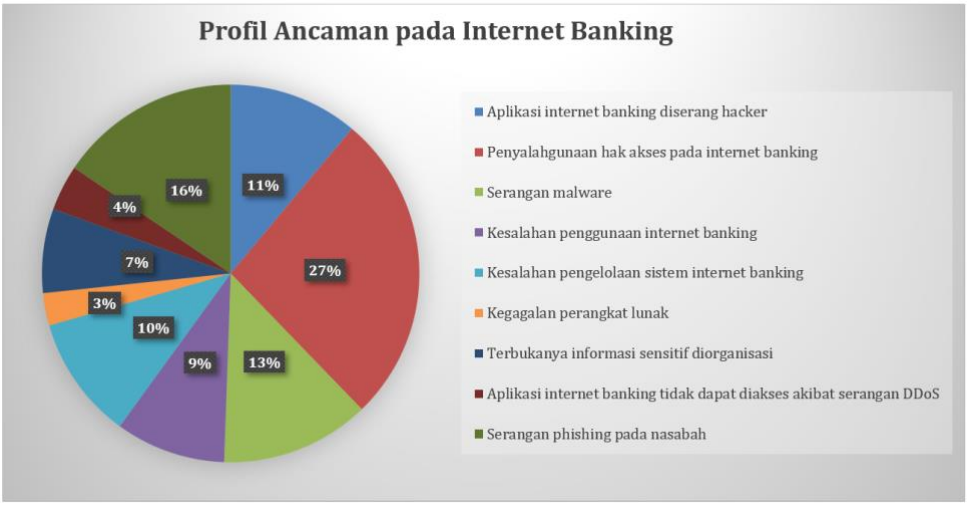
Ancaman (Threat)		Kerentanan (Vulnerability)
Aplikasi *internet banking* diserang *hacker*	1	Tidak ada atau tidak cukup waktu pengujian pada perangkat lunak
	2	Masih ditemukan *bug* pada perangkat lunak
	3	Perangkat lunak tidak dilakukan pembaruan
	4	Kurangnya mekanisme identifikasi dan otentikasi seperti otentikasi pengguna
	5	Manajemen *password* yang buruk
	6	Tidak ada penambahan perimeter keamanan pada layer dibawahnya
	7	Tidak ada atau tidak cukup waktu pengujian pada perangkat lunak
Penyalahgunaan hak akses pada *internet banking*	8	Transaksi tidak menggunakan *secure channel* saat transmisi
	9	Tidak menggunakan *two factor authentication*

Ancaman (Threat)		Kerentanan (Vulnerability)
	10	*Username* dan *password* tersimpan secara otomatis (*remembering user and password*)
	11	Aplikasi yang dibuat tidak sesuai dengan desain perancangan perangkat lunak atau tidak menerapkan metode DevSecOps
	12	Kesalahan dalam pemberian hak akses pengelola IT
	13	Audit aspek keamanan tidak dilaksanakan secara berkala
	14	Masih ditemukan *bug* pada perangkat lunak
	15	Manajemen *password* yang buruk
	16	Tidak ada dan/atau tidak dilaksanakan kebijakan akses kontrol pengelola IT pada proses otentikasi
	17	Penggunaan jaringan *internet* publik yang tidak aman
	18	Kurangnya mekanisme pemantauan hak akses
Serangan *malware*	19	Tidak ada anti *malware* atau *antivirus*
	20	Kurangnya *security awareness*
	21	Sistem tidak *update*
Kesalahan penggunaan *internet banking*	22	Antar muka yang sulit dipahami
	23	Kurangnya kesadaran akan keamanan informasi bagi nasabah
	24	Alamat URL tidak menggunakan sertifikat yang valid
	25	Dokumentasi sistem yang tidak lengkap
	26	Kesalahan pengaturan konfigurasi jaringan
	27	Tidak ada mekanisme pengawasan pengelolaan sistem *internet banking*

Ancaman (Threat)		Kerentanan (Vulnerability)
	28	Tidak ada *back up system*
	29	Kurangnya kompetensi sumber daya manusia pengelolaan sistem *internet banking*
	30	Manajemen risiko yang tidak dilaksanakan dengan baik
	31	Kurangnya kesadaran akan keamanan informasi bagi pegawai internal
Kegagalan perangkat lunak	32	Spesifikasi perangkat lunak tidak sesuai dengan kebutuhan awal
	33	Kurangnya kontrol perubahan yang efektif
Terbukanya informasi sensitif diorganisasi	34	Jalur komunikasi yang tidak dilindungi
	35	Prosedur rekrutmen dan penempatan pegawai tidak melingkupi aspek keamanan informasi
	36	Minimnya kontrol terhadap layanan yang dberikan oleh pihak ketiga
Aplikasi *internet banking* tidak dapat diakses akibat serangan DdoS	37	Tidak ada IT *capacity planning*
	38	Tidak ada anti DdoS
	39	Tidak ada *redundant system*
Serangan *phishing* pada nasabah	40	Kurangnya *security awareness*
	41	Alamat URL rentan *typosquatting*
	42	Kurang sosialisasi akan kesadaran keamanan informasi dalam penggunaan *internet banking*

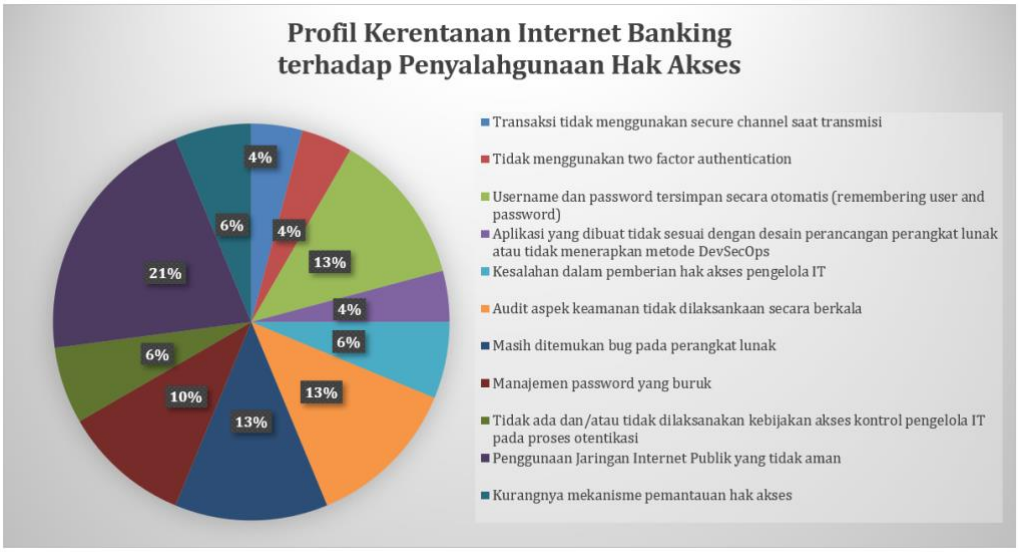
Berdasarkan hasil survei Direktorat IKPRIIKN, Profil risiko siber pada *internet banking* selama tahun 2020 sebagai berikut :

a. Ancaman Terbesar pada *Internet Banking*



Ancaman siber pada *internet banking* dapat berasal dari pihak eksternal dan pihak internal perbankan. Oleh karena itu dalam rangka meminimalisir ancaman yang mungkin terjadi pada *internet banking* perlu dilakukan langkah mitigasi dari kedua pihak secara optimal, tidak hanya dari sisi perbankan melainkan juga dari sisi nasabah/pengguna *internet banking*. Dari hasil survei diketahui terdapat 9 (sembilan) ancaman siber yang paling banyak ditemukan pada *internet banking* di Indonesia selama tahun 2020. Berdasarkan grafik diatas diketahui bahwa profil ancaman pada *internet banking* antara lain penyalahgunaan hak akses dengan persentase terbesar yaitu 27%, serangan *phishing* pada nasabah sebesar 16%, serangan *malware* sebesar 13%, serangan *hacker* sebesar 11%, kesalahan pengelolaan sistem *internet banking* sebesar 10%, kesalahan penggunaan *internet banking* sebesar 9%, terbukanya informasi sensitif organisasi sebesar 7%, serangan DDos sebesar 4%, dan kegagalan perangkat lunak sebesar 3%. Penyalahgunaan hak akses merupakan ancaman terbesar yang ditemukan pada *internet banking* sekaligus menjadi ancaman terbesar kedua pada *mobile banking* selama 2020. Oleh karena itu ancaman ini dapat menjadi perhatian sektor perbankan di tahun 2021 untuk meminimalisir kerentanan-kerentanan yang dapat menyebabkan penyalahgunaan hak akses.

b. Kerentanan Terbesar pada *Internet Banking* terhadap Penyalahgunaan Hak Akses



Penyalahgunaan hak akses merupakan ancaman siber terbesar pada *internet banking* selama tahun 2020. Dari hasil survei diketahui terdapat 11 (sebelas) kerentanan yang relevan terhadap ancaman penyalahgunaan *internet banking*. Kerentanan-kerentanan tersebut antara lain penggunaan jaringan publik yang tidak aman dengan persentase sebesar 21%, masih ditemukan *bug* pada perangkat lunak, audit aspek keamanan tidak dilaksanakan secara berkala, serta *username* dan *password* tersimpan secara otomatis dengan persentase masing-masing sebesar 13%, manajemen *password* yang buruk sebesar 10%, kurangnya mekanisme pemantauan hak akses, tidak ada dan/ atau tidak dilaksanakannya kebijakan akses kontrol pengelola TI, dan kesalahan pemberian hak akses pengelola TI masing-masing sebesar 6%. Kemudian tranksaksi tidak menggunakan *secure channel* saat transmisi, tidak menggunakan *two factor authentication*, dan aplikasi yang dibuat tidak menerapkan metode DevSecOps masing-masing sebesar 4%.

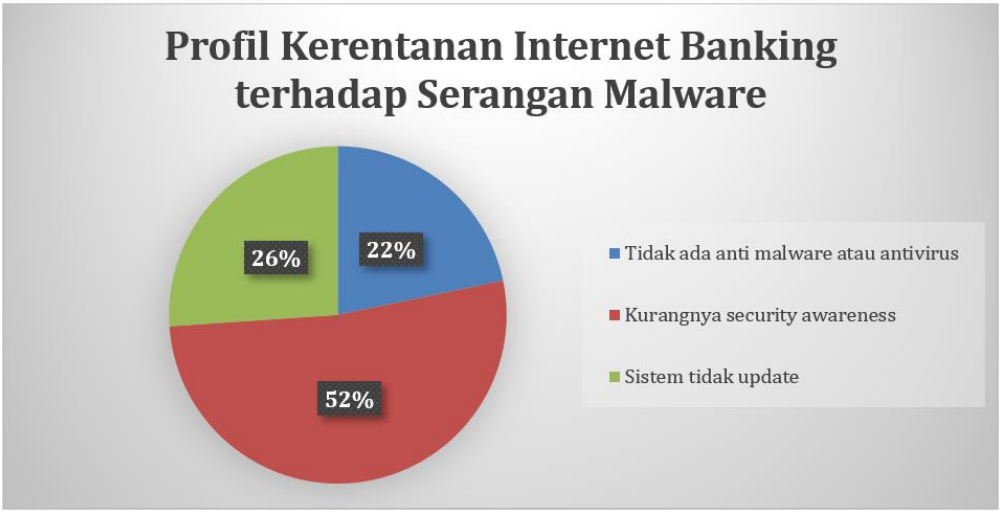
Penggunaan jaringan publik yang tidak aman menjadi kerentanan terbesar terhadap ancaman penyalahgunaan hak akses, kerentanan ini sering kali diabaikan oleh nasabah. Sehingga dapat memicu dan memberikan peluang *hacker* dalam melakukan penyalahgunaan hak akses serta bisa berdampak ke ancaman lainnya misalnya ancaman pencurian data atau bahkan terjadinya kerugian finansial.

c. Kerentanan Terbesar pada *Internet Banking* terhadap Serangan *Phishing*

Serangan *phishing* adalah serangan terbesar kedua setelah penyalahgunaan hak akses pada *internet banking* selama tahun 2020. Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman *phishing* antara lain kurangnya sosialisasi kesadaran keamanan informasi dan kurangnya *security awareness* dengan persentase masing-masing sebesar 39%, serta alamat URL yang rentan *typosquatting* dengan persentase sebesar 21%. Kurangnya *security awareness* dan kurangnya sosialisasi kesadaran keamanan informasi memang menjadi isu kerentanan yang paling sering ditemukan terhadap ancaman serangan *phishing* di *internet banking* maupun *mobile banking.* Selain itu kerentanan ini sangat sulit dikendalikan oleh internal perbankan, sehingga peran nasabah cukup besar dalam meminimalisir risiko terhadap serangan *phishing*.

d. Kerentanan Terbesar pada *Internet Banking* terhadap Serangan *Malware*

Serangan *malware* adalah serangan terbesar ketiga yang ditemukan pada *internet banking* selama tahun 2020. Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman *malware*.

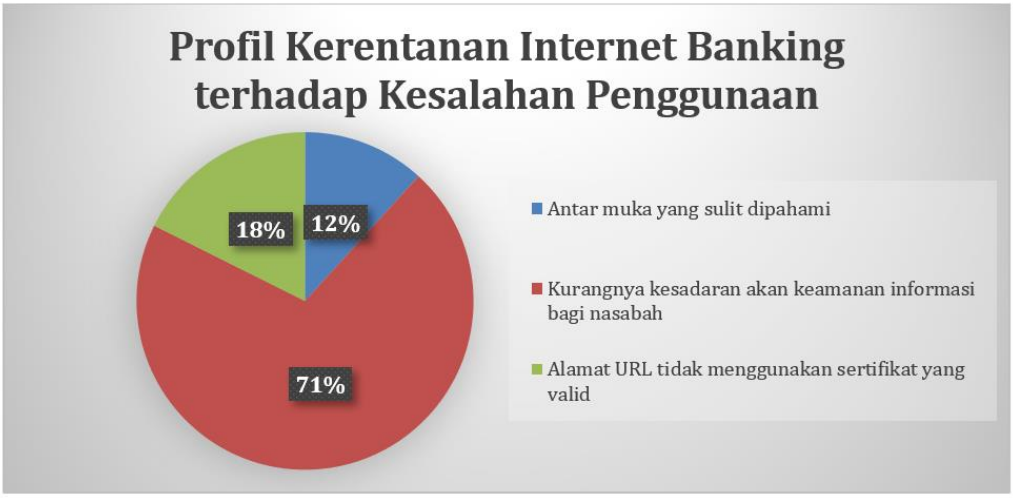


Kurangnya *security awareness* nasabah menjadi kerentanan terbesar terhadap ancaman serangan *malware* yaitu sebesar 52%. *Security awareness* ini memang menjadi isu yang sering kali ditemukan diberbagai jenis ancaman baik di *internet banking* maupun di *mobile banking*. Kerentanan terbesar kedua yaitu sistem tidak *update* dengan persentase sebesar 26% dan kerentanan terbesar ketiga sebesar 22% yaitu tidak ada anti *malware* atau *antivirus*. Nasabah dan pihak internal perbankan memiliki peranan yang sama besarnya untuk meminimalisir risiko terhadap serangan *malware* pada *internet banking*. Serangan malware juga dapat memberikan dampak terhadap ancaman lainnya misalnya penyalahgunaan hak akses, pencurian data, dan ancaman lainnya.

e. Kerentanan Terbesar pada *Internet Banking* terhadap Serangan Hacker

Dari hasil survei diketahui terdapat 7 (tujuh) kerentanan yang relevan terhadap ancaman serangan *hacker* pada *internet banking* antara lain masih ditemukan *bug* pada perangkat lunak dengan persentase sebesar 25%, manajemen *password* yang buruk sebesar 20%, tidak ada atau tidak cukup waktu pengujian pada perangkat lunak sebesar 15%. Kemudian kurangnya kontrol perubahan yang efektif, tidak ada perimeter keamanan pada layer dibawahnya, kurangnya mekanisme identifikasi dan otentikasi, serta perangkat lunak tidak dilakukan pembaharuan dengan persentase masing-masing sebesar 10%. Ketujuh kerentanan ini membutuhkan peranan internal perbankan maupun dari pihak nasabah untuk meminimalisir terjadinya risiko terhadap serangan *hacker* pada *internet banking*. *Hacker* dapat memanfaatkan celah-celah keamanan ini seperti pemanfaatan bug pada aplikasi, kelemahan mekanisme identifikasi dan otentikasi, *password* yang mudah ditebak, dan celah lainnya. Oleh karena itu pihak perbankan perlu melakukan beberapa langkah mitigasi misalnya pengujian aplikasi secara berkala, memperbaiki bug pada aplikasi, menerapkan manajemen *password* secara sistem yang aman, menerapkan kontrol perubahan yang efektif, dan langkah mitigasi lainnya yang revelan.

f. Kerentanan Terbesar pada *Internet Banking* terhadap Kesalahan Penggunaan



Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman kesalahan penggunaan pada *internet banking*. Kerentanan terbesar pertama sebesar 71% yaitu kurangnya kesadaran akan keamanan informasi bagi nasabah. Nasabah memiliki peranan yang cukup penting untuk meminimalisir risiko terhadap

kesalahan penggunaan *internet banking*, hal ini karena pihak internal perbankan tidak dapat sepenuhnya mengontrol kesadaran keamanan informasi dari nasabah secara menyeluruh. Kerentanan terbesar kedua yaitu alamat URL tidak menggunakan sertifikat yang valid dengan persentase sebesar 18%, dan kerentanan terbesar ketiga adalah antar muka yang sulit dipahami dengan persentase sebesar 12%. Untuk meminimalisir ketiga kerentanan ini dibutuhkan peranan nasabah dalam meningkatkan kesadaran keamanan, dan peranan internal perbankan untuk memperbaiki antar muka agar mudah dipahami dan menerapkan sertifikat yang valid pada alamat URL.

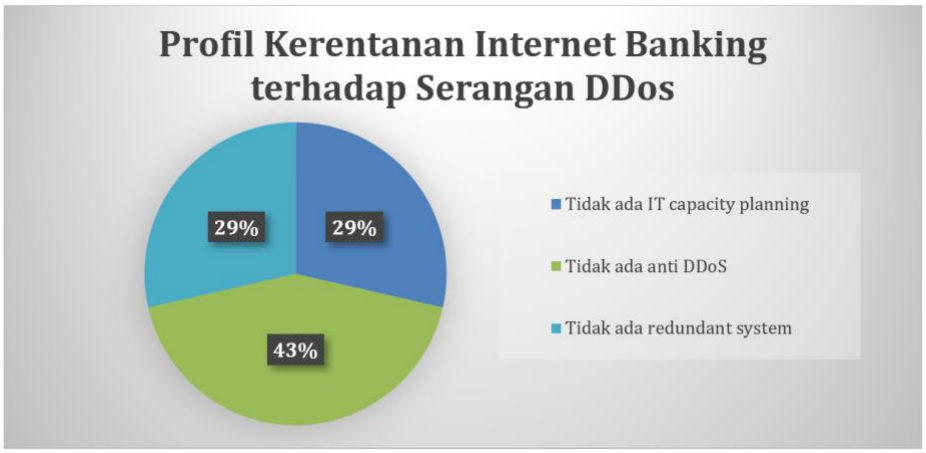
g. Kerentanan Terbesar pada *Internet Banking* terhadap Kegagalan *Software*

Dari hasil survei diketahui terdapat 2 (dua) kerentanan yang relevan terhadap ancaman kegagalan *software* pada *internet banking* yaitu kurangnya kontrol perubahan yang efektif dengan persentase sebesar 60% dan spesifikasi perangkat lunak tidak sesuai dengan kebutuhan awal sebesar 40%. Pihak internal perbankan harus memastikan bahwa spesifikasi perangkat lunak telah sesuai dengan kebutuhan awal dan melakukan kontrol perubahan secara efektif dan berkelanjutan. Sehingga potensi terjadinya kegagalan *software* dapat diminimalisir.

h. Kerentanan Terbesar pada *Internet Banking* terhadap Kesalahan Pengelolaan

Dari hasil survei diketahui terdapat 7 (tujuh) kerentanan yang relevan terhadap ancaman kesalahan pengelolaan pada *internet banking,* dimana ancaman ini disebabkan oleh adanya kerentanan dari pihak internal perbankan. Kerentanan terbesar pertama sebesar 21% yaitu manajemen risiko tidak dilaksanakan dengan baik. Kerentanan terbesar kedua sebesar 16% terdiri dari tiga kerentanan yakni kurangnya kompetensi sumber daya manusia pengelola sistem, kesalahan pengaturan konfigurasi, dan dokumentasi sistem yang tidak lengkap. Selanjutnya kerentanan terbesar ketiga sebesar 11% terdiri dari tiga kerentanan yaitu kurangnya kesadaran keamanan informasi bagi pegawai internal, tidak ada *back up system*, dan tidak ada mekanisme pengawasan pengelolaan sistem *internet banking*. Secara keseluruhan kerentanan yang ditemukan, pihak internal perbankan yang memiliki peranan cukup penting untuk meminimalisir risiko terhadap kesalahan pengelolaan pada sistem *internet banking*. Hal-hal yang memicu terjadinya kesalahan pengelolaan dapat berasal dari mekanisme/prosedur yang kurang efektif, lemahnya sistem pengelolaan, kurangnya kompetensi maupun kurangnya kesadaran dari pengola sistem *internet banking*.

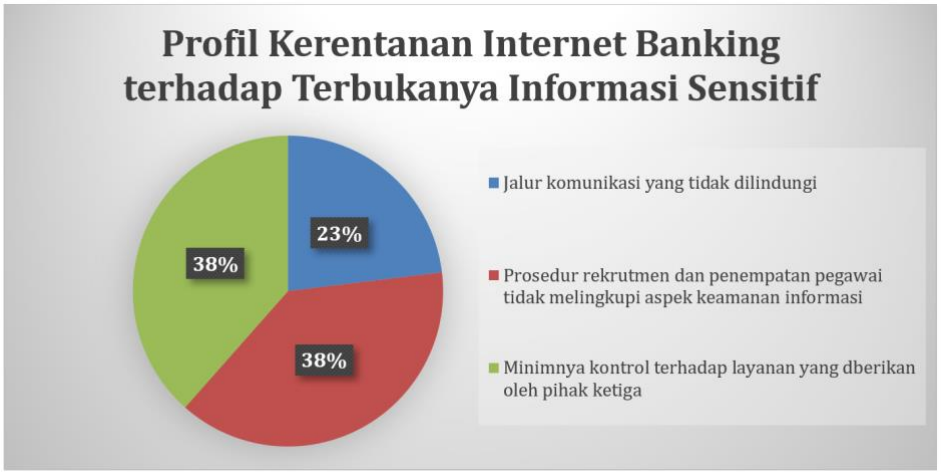
i. Kerentanan Terbesar pada *Internet Banking* terhadap Serangan DDoS



Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman serangan *Distributed Denial of Service* (DDOs) pada *internet banking* yang mengakibatkan sistem tidak bisa diakses, dimana ancaman ini juga disebabkan oleh adanya kerentanan dari pihak internal perbankan.

Ketiga kerentanan tersebut antara lain tidak adanya anti DDos dengan persentase sebesar 43%, serta tidak adanya *redundant system* dan tidak adanya IT *capacity planning* dengan persentase masing-masing sebesar 29%. Untuk meminimalisir kerentanan-kerentanan tersebut membutuhkan peranan dari pihak internal perbankan untuk menerapkan anti DDos sesuai dengan kebutuhan, menyiapkan *redundant system*, dan melakukan IT *capacity planning* sehingga potensi terjadinya serangan DDos dapat diantisipasi.

j. Kerentanan Terbesar pada *Internet Banking* terhadap Terbukanya Informasi Sensitif



Dari hasil survei diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman terbukanya informasi sensitif pada *internet banking* selama tahun 2020, dimana ancaman ini juga disebabkan oleh adanya kerentanan dari pihak internal perbankan. Ketiga kerentanan tersebut antara lain minimnya kontrol terhadap layanan yang diberikan oleh pihak ketiga dan prosedur rekrutmen dan penempatan pegawai tidak melingkupi aspek keamanan informasi dengan persentase masing-masing sebesar 38%, dan jalur komunikasi yang tidak dilindungi dengan persentase sebesar 23%. Prosedur rekrutmen dan penempatan pegawai yang tidak mencakup aspek keamanan informasi dapat berdampak dengan kurangnya kesadaran keamanan informasi (*security awareness*) yang dimiliki oleh pegawai, sehingga dapat menjadi potensi terbukanya informasi sensitif oleh pegawai tersebut secara tidak sadar ataupun dimanfaatkan oleh pihak lain. Selain itu dengan minimnya kontrol yang terhadap layanan yang diberikan oleh pihak ketiga juga menjadi peluang terungkapnya informasi sensitif, apabila beberapa akses yang diberikan kepada pihak ketiga berkaitan dengan informasi sensitif. Selain itu, penggunaan jalur komunikasi yang tidak dilindungi juga dapat dimanfaatkan oleh *hacker* untuk mendapatkan informasi sensitif melalui jalur komunikasi tersebut. Oleh karena itu, pihak perbankan memiliki peranan penting dalam meminimalisir kerentanan-kerentanan tersebut.

PERLINDUNGAN KEAMANAN SIBER SEKTOR PERBANKAN TAHUN 2020

DALAM perkembangan layanan *digital banking*, pihak bank harus memperhatikan aspek perlindungan nasabah, khususnya keamanan yang berhubungan dengan privasi nasabah. Secara umum, keamanan layanan *online banking* atau *digital banking* ada empat, yaitu keamanan koneksi nasabah, keamanan data transaksi, keamanan koneksi *server*, dan keamanan jaringan sistem informasi dari *server*. Disamping itu, aspek penyampaian informasi produk perbankan sebaiknya disampaikan secara proporsional, artinya bank tidak hanya menginformasikan keunggulan atau kekhasan produknya saja, tapi juga sistem keamanan penggunaan produk yang ditawarkan.

Berbagai upaya preventif telah diterapkan oleh kalangan perbankan di Indonesia yang menyelenggarakan layanan *digital banking.* Hal tersebut juga didukung dari pihak regulator yang telah mengeluarkan beberapa aturan main dan panduan dalam penyelenggaraan layanan *digital banking*. Sebagai contoh, Bank Indonesia sebagai bank *central* yang memiliki kewenangan dalam mengatur dan mengawasi bank, serta Otoritas Jasa Keuangan (OJK) yang memiliki fungsi pengawasan terhadap sektor jasa keuangan, telah mengeluarkan serangkaian peraturan dan surat edaran yang harus dipatuhi oleh dunia perbankan antara lain mengenai penerapan manajemen risiko dalam penyelenggaraan kegiatan *internet banking* dan penerapan prinsip *Know Your Customer* (KYC). Beberapa peraturan yang dikeluarkan terkait dengan pengelolaan atau manajemen risiko penyelenggaraan kegiatan *internet banking* antara lain:

1. Peraturan Otoritas Jasa Keuangan No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum;
2. Peraturan Otoritas Jasa Keuangan No. 12/POJK.03.2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum; dan

3. Peraturan Otoritas Jasa Keuangan No. 13/POJK.03/2020 tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 38/Pojk.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Terkait dengan perlindungan konsumen, pihak Bank Indonesia juga telah menetapkan tujuh prinsip perlindungan konsumen yang harus diperhatikan oleh perbankan, seperti yang tertuang pada Peraturan Bank Indonesia No. 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia. Prinsip-prinsip tersebut meliputi:

- Kesetaraan dan perlakuan yang adil;
- Keterbukaan dan transparansi;
- Edukasi dan literasi;
- Perilaku bisnis yang bertanggung jawab;
- Perlindungan aset konsumen terhadap penyalahgunaan;
- Perlindungan data dan/atau informasi konsumen;
- Penanganan dan penyelesaian pengaduan yang efektif.

Penggunaan layanan *digital banking* (*internet banking dan mobile banking*) selain memberikan kemudahan akomodasi kegiatan perbankan, juga dapat menjangkau masyarakat di *remote area* atau *unbankable*. Namun, digitalisasi layanan keuangan juga menimbulkan isu permasalahan yang krusial, diantaranya adalah keamanan data nasabah. Berdasarkan data profil risiko dan ancaman serta kerentanan pada sektor perbankan yang telah dijelaskan pada bab sebelumnya, dapat dilihat bahwa pengamanan terhadap layanan digital banking tidak hanya bergantung pada sisi penyedia layanan saja, namun juga perlu didukung oleh pengamanan dari sisi pengguna. Pengamanan yang diperlukan tersebut mencakup keseluruhan aspek, meliputi aspek teknologi, *people* dan proses.

Berikut beberapa pendekatan aspek keamanan yang menjadi perhatian di dalam mengamankan layanan *digital banking*, baik dari sisi pengguna maupun penyedia layanan digital banking.

1. Aspek Keamanan Sisi Penyedia Layanan (Perbankan)
    a. Menerapkan kebijakan keamanan siber pada semua aspek

       Penerapan keamanan siber menjadi hal yang penting sehingga tercipta lingkungan dan budaya keamanan siber di organisasi, hal ini agar potensi terjadinya insiden akibat lemahnya salah satu keamanan rantai *supply chain* dapat dimitigasi dengan baik.
    b. Melaksanakan Manajemen Risiko Siber

       Ancaman dan kerentanan siber harus teridentifikasi dengan baik secara detail agar dapat diketahui potensi risiko siber apa yang terjadi di organisasi sehingga dapat dilakukan mitigasi risiko yang tepat sasaran untuk meminimalisir terjadinya insiden siber. *Risk culture* juga harus terbangun dan menjadi kebiasaan bagi setiap pegawai di organisasi, stakeholder maupun shareholder.
    c. Menerapkan *Two Factor Authentication*

       Penggunaan *two factor authentication* atau *multiple factor authentication* dibutuhkan untuk memastikan bahwa transaksi keuangan yang berjalan dilakukan oleh nasabah/pengguna yang sah. Pemindaian sidik jari dapat dijadikan sebagai metode verifikasi tambahan pada aplikasi perbankan. Aplikasi juga mengharuskan ponsel dilindungi oleh kata sandi (*password*), jika ingin menggunakan pemindaian sidik jari.
    d. SSL Secured *Website*

       Situs *website* atau aplikasi perbankan yang menjadi tempat terjadinya transaksi keuangan harus memiliki jalur komunikasi yang aman sehingga informasi yang diteruskan antara *server* bank dan *browser* nasabah tetap terjaga keamanannya.

e. *Automatic Timeout Sessions*

Pihak perbankan harus menutup *session* transaksi nasabah yang tidak aktif dalam beberapa menit untuk menghindari adanya *spying* dan *human error.*

f. *Fraud Monitoring*

Bank harus memiliki pemantauan secara terus-menerus terhadap aktivitas-aktivitas yang mencurigakan dan anomali.

g. Penerapan *Devsecops* Pada Aplikasi Perbankan

Faktor keamanan harus menjadi fokus mulai dari lingkungan *development* hingga lingkungan *production*. Pengujian dan monitoring terhadap keamanan sistem aplikasi harus dilakukan secara terus menerus agar dapat memastikan aplikasi dalam keadaan yang aman. Penggunaan *secure coding* juga dapat meminimalisir adanya celah keamanan pada aplikasi.

h. Sosialisasi Keamanan Penggunaan Aplikasi

Pihak bank perlu secara aktif, terus-menerus dan berkelanjutan memberikan literasi dan sosialisasi keamanan penggunaan aplikasi *digital banking* dan keamanan siber kepada nasabah, mengingat beragamnya latar belakang pengguna layanan *digital banking* di Indonesia.

2. Aspek Keamanan Sisi Pengguna Layanan (Nasabah/Customer)

a. Waspada Terhadap *Phishing*

Pengguna atau nasabah harus waspada terhadap emai*l phishing* dan teks *phishing*. Metode *phishing* ini kerap dilakukan dengan mengirimkan *link* tertentu yang dikirim mengatasnamakan pihak bank yang sah. *Link* tersebut sebenarnya berisi *malware*, yang apabila pengguna meng-*klik link* tersebut, maka pengguna akan diarahkan untuk

login atau memberikan identifikasi informasi pribadi lainnya.

b. Pelaporan Anomali dan Insiden

Pengguna secara aktif harus mengidentifikasi dan melaporkan segala aktifitas yang mencurigakan serta insiden yang terjadi untuk menghindari kerugian finansial yang berkelanjutan.

c. Mengunduh Aplikasi Resmi dari Bank

Pengguna harus mengunduh aplikasi yang resmi dikeluarkan oleh pihak bank dengan cara memeriksa ulasan, membaca ringkasan dengan seksama, dan memeriksa kembali siapa dan dari mana aplikasi tersebut berasal, sebelum aplikasi tersebut dipasang pada perangkat pengguna.

d. Waspada Penggunaan Fasilitas dan Jaringan Publik

Pengguna saat melakukan transaksi *digital banking* agar tidak menggunakan perangkat komputer yang bukan miliknya begitu juga menggunakan jaringan internet berupa *wifi* publik. Hal ini agar menghindari adanya penyadapan atau perekaman terhadap akun kredensial pengguna yang menggunakan media jaringan *wifi* publik dan perangkat komputer.

e. Mengkustomisasi Transaksi *Online Banking*

Aplikasi mengizinkan pengguna untuk dapat mengubah kontrol terhadap akun perbankan pengguna, seperti penggunaan *password* yang kuat serta penggantian *password* secara berkala, pembatasan transaksi *online banking*, dan sebagainya sehingga dapat mencegah terjadinya kerugian finansial terhadap transaksi yang mencurigakan dan anomali.

f. Menerapkan Keamanan Pada Perangkat Pengguna

Penggunaan antivirus pada perangkat pengguna dapat mencegah terjadinya ancaman tingkat lanjut seperti

ransomware dan *malvertising*. Selain itu, *update* terhadap penggunaan sistem operasi terbaru pada perangkat pengguna juga turut meningkatkan aspek keamanan pada perangkat pengguna.

g. Bijak Dalam Bersosial Media

Penggunaan sosial media agar tidak menginformasikan data pribadi ataupun informasi sensitif yang berkaitan dengan data yang digunakan dalam transaksi perbankan di ruang publik atau sosial media. Data pribadi dan informasi sensitif masyarakat sering digunakan oleh pelaku kejahatan sebagai sumber data dalam melakukan *fraud* dan pencurian saldo nasabah.

Referensi

[1] Data Serangan Siber 2020, Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara;

[2] Statistik Nominal Transaksi Uang Elektronik (2019-2020), Bank Indoneia;

[3] Statistik Transaksi Delivery Channel (2019-2020), Bank Indonesia;

[4] Peraturan Otoritas Jasa Keuangan No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

[5] Peraturan Otoritas Jasa Keuangan No. 12/POJK.03.2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum;

[6] Peraturan Otoritas Jasa Keuangan No. 13/POJK.03/2020 tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 38/Pojk.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum;

[7] Peraturan Bank Indonesia No. 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia;

[8] Cyber Security Report 2020, Check Point Research;

[9] State of Privacy and Security Awareness Report 2020, Media Pro;

[10] The Global Risks Report 2021 16th Edition, World Economic Forum;

[11] X-Force Threat Intelligence Index 2020, IBM.